IFIP AICT 406

Ronald C. Dodge Jr.
Lynn Futcher
(Eds.)

Information Assurance and Security Education and Training

8th IFIP WG 11.8 World Conference
on Information Security Education
WISE 8, Auckland, New Zealand, July 2013, Proceedings
WISE 7, Lucerne Switzerland, June 2011 and
WISE 6, Bento Gonçalves, RS, Brazil, July 2009
Revised Selected Papers

Springer

IFIP Advances in Information and Communication Technology 406

IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP's aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

> IFIP's mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- Open conferences;
- Working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is also rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is about information processing may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly, National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.

Ronald C. Dodge Jr. Lynn Futcher (Eds.)

Information Assurance and Security Education and Training

8th IFIP WG 11.8 World Conference
on Information Security Education
WISE 8, Auckland, New Zealand, July 8-10, 2013, Proceedings
WISE 7, Lucerne Switzerland, June 9-10, 2011 and
WISE 6, Bento Gonçalves, RS, Brazil, July 27-31, 2009
Revised Selected Papers

Springer

Volume Editors

Ronald C. Dodge Jr.
The United States Military Academy
606 Thayer Rd., West Point, NY 10996, USA
E-mail: ronald.dodge@usma.edu

Lynn Futcher
Nelson Mandela Metropolitan University
P.O. Box 77000, Port Elizabeth, 6031, South Africa
E-mail: lynn.futcher@nmmu.ac.za

ISSN 1868-4238 e-ISSN 1868-422X
ISBN 978-3-642-39376-1 e-ISBN 978-3-642-39377-8
DOI 10.1007/978-3-642-39377-8
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013941483

CR Subject Classification (1998): K.6.5, D.4.6, K.3, E.3, C.2, H.3, I.6

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The World Conference on Information Security Education (WISE) serves to provide a forum for discussing information assurance and security education and awareness and the research supporting both underlying security principles and teaching. This year's conference was held in Auckland, New Zealand, during July 8–10, 2013. This year marked the 8^{th} bi-annual WISE – 16 years old! In this span, we have seen the name of the field shift from information security to information assurance to cyber security. This field is somewhat unique in the computer science body of knowledge because of its cross-cutting nature. Information assurance and security touches every topic in computer science. In programming, our code needs to follow rules and structure that safeguard against unintended paths; our operating systems need to protect resources and data; and our networks need to move data in a manner that preserves integrity, confidentiality, and availability. Our discipline even reaches outside of computer science in developing secure cryptographic functions and security that is "usable."

While this broad application seems daunting, one of the greatest challenges is the competing nature that security plays in our discipline. Security is rarely achieved without some impact on performance, usability, or cost. Our challenge is to ensure that we inculcate the principles of security into the most basic and entry level courses, ensuring that just as we strive to make programs more efficient – we also strive to make them secure. The trailblazers in our community have provided a strong foundation upon which to continue to build the discipline.

These proceedings are in small part a look back over the history of WISE. In one of the new papers for WISE 8, we look back over the 16-year history and discuss the accomplishments of each WISE. We also include papers from WISE 6 and WISE 7 to bring them under the Springer/IFIP listing and make them available to a wider audience. WISE 6 was held in conjunction with the World Conference on Computers in Education (WCCE), July 27–31, 2009, in Bento Gonçalves, RS, Brazil. WISE 7 was held in conjunction with IFIP SEC, June 9–10, 2011, in Lucerne, Switzerland. WISE has always held the paper submission and review process to the strictest of standards. All papers are submitted and reviewed in a double-blind manner and reviewer conflict is identified in an automated process (institution and co-authorship based) as well as self-identified conflict. The reviewer pool is an international body, with representatives from four continents. Each paper receives a minimum of three reviews. While the conference focus is on education and pedagogy, the papers selected represent a cross section of applicable research as well as case studies in security education.

For all those who have contributed many a late night organizing, reviewing, and evangelizing – we thank you for the strong base you have provided for our field.

May 2013

Ron Dodge
Lynn Futcher

Organization

Conference Chairs

WISE 8: Ronald Dodge, United States Military Academy, USA
WISE 7: Colin Armstrong, Curtin University, Australia
WISE 6: Ronald Dodge, United States Military Academy, USA

Program Chairs

WISE 8: Lynn Futcher, Nelson Mandela Metropolitan University, South Africa
WISE 7: Lynn Futcher, Nelson Mandela Metropolitan University, South Africa
WISE 6: Lynn Futcher, Nelson Mandela Metropolitan University, South Africa

Program Committee

Colin Armstrong	Curtin University, Australia
Helen Armstrong	Curtin University, Australia
Matt Bishop	University of California at Davis, USA
William Caelli	IISEC Pty Ltd
Nathan Clarke	University of Plymouth, UK
Manuel Corregedor	University of Johannesburg, South Africa
Lynette Drevin	North-West University, South Africa
Ronald Dodge	United States Military Academy, USA
Steven Furnell	Plymouth University, UK
Lynn Futcher	Nelson Mandela Metropolitan University, South Africa
Mariana Gerber	Nelson Mandela Metropolitan University, South Africa
Brian Hay	University of Alaska Fairbanks, USA
Hans Hedbom	Karlstad University, Sweden
Suresh Kalathur	Boston University, USA
Stewart Kowalski	Stockholm University, Sweden
Stefan Lindskog	University of Adelaide, Australia
Javier Lopez	University of Malaga, Spain
Natalia Miloslavskaya	Moscow Engineering Physics Institute, Russia
Kara Nance	University of Alaska Fairbanks, USA
Vincent Nestler	California State University, San Bernardino, USA
Yanzhen Qu	Colorado Technical University, USA
Tim Rosenberg	iSIGHT Partners

Corey Schou	Idaho State University, USA
Jill Slay	University of South Australia
Blair Taylor	Towson University, USA
Marianthi Theoharidou	Athens University of Economics and Business, Greece
Kerry-Lynn Thomson	Nelson Mandela Metropolitan University, South Africa
Johan van Niekerk	Nelson Mandela Metropolitan University, South Africa
Basie von Solms	University of Johannesburg, South Africa
Stephen Wolthusen	Royal Holloway University of London, UK
Louise Yngström	Stockholm University, Sweden

Table of Contents

WISE 8

WISE 7

WISE 6

Back to Basics: Information Security Education for the Youth via Gameplay

Rayne Reid and Johan Van Niekerk

Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
s208045820@live.nmmu.ac.za, Johan.VanNiekerk@nmmu.ac.za

Abstract. Cyber technology and information resources are both fundamental components of everybody's daily life. This means that both society's adults and youths are exposed to both the benefits and dangers that accompany these resources. Cyber security education is becoming a necessary precaution for individuals to learn how to protect themselves against the dangers of the technologies and resources. This is particularly important for the current and future youth who are the most technology literate generations. This paper presents a novel educational approach that can be used to introduce information security concepts to the youth from a very young age.

Keywords: Information security education, Case study, Educational Gameplay, Brain-compatible Education.

1 Introduction

The 21st century has witnessed numerous technological innovations and developments. Several of these developments have involved information technology (IT) infrastructure. These information technologies and their companion "cyberspace" have gradually become commonplace in many aspects of modern life. As a result users are becoming increasingly dependent on these technologies and cyberspace.

Unfortunately although cyber space provides many advantages to a user, it is also introduces many dangers to the user. The exposure of people, old and young, to the online and interactive world has resulted in them becoming potential targets for a vast array of information security threats. Examples of potential threats may include online attacks, exposure of personal information and many possible scenarios in terms of which other people pose a threat to the user by their using technological channels to reach an intended victims [1]. It is, thus, essential that individuals learn to protect themselves against these dangers. This is particularly important for the current and future youth who have grown-up in this technology-saturated environment.

The current youth are often more technology literate that the older generations. Generation Y (born 1977-1990) and the online teens (born 1991 – now, including generation Z) account for over 30% of the internet user population [2]. Similarly Generation Z (born 1995 – 2012, over 23 million people) are often already using the internet and other technologies. Generation Z has grown up in contact with highly sophisticated media and computer environment and will be more Internet savvy and

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 1–10, 2013.

expert than even Generation Y [3]. This trend has persisted since the start of the development of most modern technologies. It has thus resulted in the question of "How can the youth be educated about cyber security?"

Traditionally children have looked to their parents to teach them how to cope with danger. However in the case of technology- related lessons, parents are often less technology literate or educated than the youth. As a result they are seldomly equipped to teach kids cyber safety. A more creative and semi-/fully- formalized information security education approach is therefore needed.

This paper examines a novel approach, which introduces a brain-compatible information security game. It will focus on the introduction of information security awareness games, which were accompanied by information security awareness talks into a primary school class as a case study environment. The games themselves will be created to comply with the brain-compatible pedagogy.

2 Background

2.1 Information Security Education

Information security is a multifaceted problem and a comprehensive solution to this problem will normally encompass physical, procedural and logical forms of protection against threats [4]. Information security education provides the knowledge and skills needed to implement information security practices.

Traditionally formal information security education programs have mainly targeted organisational audiences. However recent national legislation and cyber awareness campaigns (such as the campaigns run in the UK and USA) target the general public[5, 6].This implies the inclusion of the youth as well. Cyber security education that is appropriate for organizational environments would be less effective for educating the youth; therefore a more 'fun' approach is required.

2.2 Children and Educational Play

Traditionally formal education approaches have been adopted for information security education; however this may not be an effective approach for a *very young* target audience. A more fun approach is may be more suitable for such an audience. However should a fun approach be adopted, it should still implementable in a formal education environment. This would take advantage of the fun aspect as well as the formal education environments tendency to augment and build upon fundamentals taught using the fun approach. An educational game may therefore be an effective solution.

The young of many species learn skills though gameplay e.g. lion cubs learn to hunt and fight through mock battles and hunts with litter mates and later 'practice prey'. Similarly young humans learn skills through 'make believe' and educational games which enable fun learning.

Admittedly this learning is not completely sufficient for current life; however it is the basic building blocks, which provide the foundation knowledge which may be augmented by formal education. It is therefore the focus of this research for introducing knowledge to the youth.

'Fun' Education is an effective mechanism for people, especially of children, as it has the added benefit of holding their attention, being fun, engaging their interest, and preventing the children from disassociating from what is being learnt and done [7]. It does however require structure to be effective as an education toll. This can be accomplished through the introduction of pedagogy to the game, so as to help promote learning. One, tried and tested, pedagogy is brain-compatible education.

2.3 Brain-Compatible Education (BCE)

Brain-compatible education may be defined as learning based on the educational principles, methods and techniques which endeavour to teach subject-matter in a manner and format which is naturally complementary to the physical and psychological processing functions of the brain [8, 9].

This means it is an approach that manipulates education presentations and environments to appeal to natural learning processed. To achieve this brain-compatible educators design and orchestrate life-like, enriching, and appropriate experiences for learners [10]. This means that instructional strategies are employed to allow all students may process information more effectively so as to ensure maximum understanding, retention and recall [11].

Brain-compatible principles and techniques have been effectively used in real-world classrooms and some online environments in the presentation of formal lessons. Its implementation is guided by a number of principles some of which are presented in Table 1.

Table 1. Brain-compatible principle applied in the design of the artefact [7]

1	A learning experience should be as multifaceted as possible, catering for as many learning styles as possible and providing as many opportunities for each learner to develop as possible
2	Positive emotions should be used to aid recognition and recall
3	Relate all new material back to old material and thereby build new knowledge on old knowledge
4	The search for meaning is innate and occurs through patterning
5	Every brain simultaneously perceives and creates parts and wholes during the learning process
6	It is necessary to review material repetitively to solidify recall and recognition.
7	Both the focused and peripheral attention of a learner should be involved in the learning process
8	Allow learners to progress through the course at their own pace.

These simple and neurologically sound principles are the general theoretical foundation of brain-compatible education [10]. When applied to educational material the brain-compatible principles guide educators in the definition and selection of appropriate educational programmes and methodologies and presentation techniques. Some of these principles will be applied and explained in the creation of the research artefact. The relevant principles are presented in Table 1. The next section will examine the case study portion of this research.

3 Case Study

3.1 Methodology

This research will follow various procedures of the case study protocols described by Yin [12] and Creswell [13]. The structure of the paper will be to firstly provide the context of the case study and its experiment; secondly to describe the research artefact, thirdly to describe the research instrument and fourthly to describe the implementation of the case study experiment. Finally the results and analysis of the research will be presented with accompanying conclusions which have been reached.

3.2 Description of the Context

Cyber security is a topic that is seldomly addressed in current South African school environments. Until recently this has been an acceptable practice. However because cyber technologies and information facilities have integrated into the daily lives of many people, including children of all ages, it has become necessary to educate children about cyber awareness and security. The subject matter should therefore be gradually introduced to the young target audience.

The context in which this case study occurs is at a primary school level (ages 7-13), using educational gameplay as the first subject matter primer. A fun information security game (research artefact) therefore had to be developed. The design of the artefact had to be carefully considered, this is discussed in the next sub-section.

3.3 The Artefact (Creation of BCE Information Security Board Game)

The artefact is targeted at a primary school audience. Therefore considerations in the design of the game included: age appropriateness content and delivery, inductivity or familiarity of use, ease of understanding, level of learnability and the potential for compliance with brain-compatible education principles. Existing children's games, which targeted this age group, were considered as the basis for the artefacts design.

'Snakes and Ladders', a popular board game played by children in many cultures, was chosen as the foundation game on which the information security educational game would be based. Numerous reasons accounted for this decision. Firstly the game, having existed since the 2nd century in India, is a popular game whose gameplay and rules is probably known to the target audience [14]. Secondly its

original purpose of teaching children the difference between 'good and evil' is similar to teaching children good and bad information security behaviours [14]. Thirdly, it currently targets children from age 7+. Fourthly pedagogical principles and appropriate information security educational content could be easily incorporated into the design. The design, content, and game play rules will be discussed in the below sub-sections.

3.3.1 Design

This section will present the reasons why 'Snakes and Ladders' was selected as a good redevelopment candidate for this research. These reasons will also be linked to implementation considerations from a brain-compatible educational perspective. The focus of this section is therefore the presentation design.

Firstly the game had to cater for multiple learners learning rates. Brain-compatible education advocates self-paced progression (Principle 8) therefore this had to be catered for in the game environment. This was achieved by presenting the content in a game format which required the players to take turns, and to move according to a dice throw. This therefore allowed the learners to play and learn at their own pace, but ensured that the dice regulated the general pace of the entire the game. In brief it prevented overly long pauses, such as those experienced in games such as chess.

Secondly the design, or redesign of the game had to maintain the interactivity and "fun feel" of the game. This was necessary to ensure a mental and physical involvement in the game, a social and communicative experience, and a fun, peer-supported learning experience. This was considered essential as it implements Principle 1 by appealing multiple learning styles, especially those favoured by kinaesthetic and auditory (social) learners.

Thirdly the game had to be entertaining enough to hold the player's focused and peripheral attention. This was necessary so as to comply with Principle 7. The abovementioned interactivity and social nature of the game would help achieve this. Interactivity combined with the "fun factor" of the game, the learner would become emotionally stimulated, and this would cause further interest and encourage focus.

The "fun factor" of the game also appeals to the learner's positive emotions. Principle 2 advocates that a learner is more likely to learn and retain content if they are experiencing positive emotions. Negative emotions may result in distraction, disinterest and the prevention of knowledge retention. Many aspects of gameplay appeal to this principle. Firstly a game, by its nature is fun, with its design encouraging changes in the emotional state e.g. happiness for ascending a ladder. Secondly the interaction between learners enables fun communication and competitiveness. Finally winning as incentive, increases the fun factor and appeals to Principle 2, it also encourages progression throughout the game (Principle 8). This emotional appeal is also further encouraged through the use of colour on the board.

Colour was used to influence the emotional state of the learners and also their focus – Principle 2. The background of the board's lesson material was coloured various shades of yellow and green (see figure 1). Yellow; the first colour to be distinguished by the brain; elicits positive moods and attracts the learners' attention [15]. This change to the material also relates to principle 7 and the enhancement of the

learners' attentiveness. Green encourages productivity and long-term energy and is, thus, an appropriate colour for a classroom activity [15]. The colours used also implemented principle one, by engaging visual learners. This type of learner is particularly drawn to colours, graphics and written concepts. These learners would therefore be the most likely to focus and benefit from the built-in education mechanisms of the "Snakes and Ladders" game.

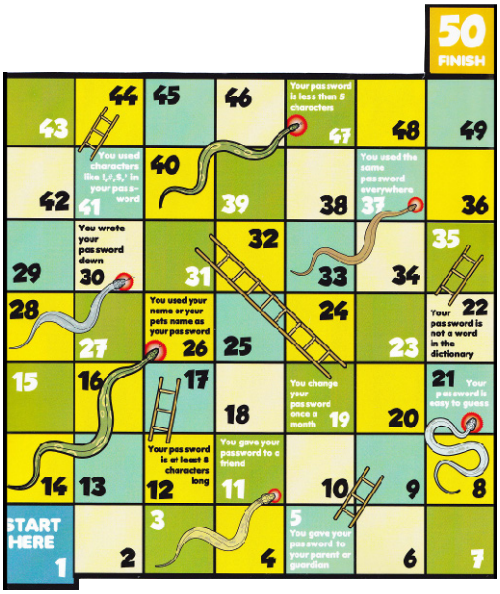


Fig. 1. The Research Artefact - Snakes and Ladders Password Board

The final design considerations relate to the educational reinforcement mechanisms. As an educational tool the game has to provide consequences and rewards for lessons learned during the game. This was easily introduced into "Snakes and ladders" as its original purpose was to teach the difference between good and evil, and such mechanisms were therefore already inherent.

Information Security lessons/messages was placed above snakes and below ladders on the board (see figure 1). Positive lessons were reinforced by enabling ascension of the board via ladders. Conversely negative lessons were reinforced by forcing the player to descend down the board via snakes. This design associated negative consequence with negative message and positive consequence with positive message, and thereby enabled behaviour patterning (principle 4). This patterning also enabled principle 5 by creating knowledge components around a central topic which the player learned as a whole concept.

The snakes and ladders where placed randomly throughout the board, alongside information security lessons. These designs, and other similar designs, were used to present a number of different topics. The content presented in this case study will be addressed by the next section.

3.3.2 Content

Multiple games were created for many different topics. Examples of topics included social networking, password security, and virus security. Each of the boards had a similar design, but different content. The board presented, which relates to the results reported by this paper, taught password security content.

The content included within the game was topic related, in this case pertaining to secure password management. Various rules specifying the do's and don'ts of password security were placed above snakes and below ladders (see figure 1).

The do's and don'ts included lessons such as: the creation of a strong password, the frequency of change required to ensure a secure password, whom the password may possibly be shared with etc. They were written in a format that the player had/had not complied with a 'rule' of secure password management. The 'learner-centric' perspective serves to conform to Principle 3 of brain compatible education of contextualising lessons from a learner's viewpoint.

The do's were placed below the ladders e.g. "Your password is at least 8 characters long". The don'ts were placed above snakes e.g. "You gave your password to a friend". A complete list of the lessons presented in this particular password board is presented in Table 2.

Table 2. Password lessons of do's and don'ts

Do's	Don'ts
You gave you password to your parent or guardian	You gave your password to a friend
Your password is at least 8 characters long	Your password is less than 5 characters
You change your password at least once a month	You wrote your password down
Your password is not a word in the dictionary	You used your name or your pets name as a password
You used characters like !,#,$ in your password	You used the same password everywhere
	Your password is easy to guess

These lessons were then learnt in accordance with the rule of the 'Snakes and Ladders' gameplay. These rules will be presented in the next section.

3.3.3 The Rules of Play

The 'Snakes and Ladders' games can be played by 2-6 players. Each player has a token which the place and move on the board. Play begins with everyone's token being placed at the start of the game. The first player then rolls the dice and moves the token along the sequential squares according to the number thrown.

If the square a player lands on contains an information security educational message, they read it out loud and perform the accompanying action. The verbal

sharing of the message helps the learners to cognitively consider the lesson (principle 1). If the message was a do not lesson, they are swallowed by the snake and move their token to the square which contains the snakes tail. If the lesson was a do they ascend the ladder and place their token in the square at the top of the ladder.

Players take sequential turns to roll the dice and move their tokens. The first player to reach the 50th square (Finish) is the winner.

The effectiveness of this research artefact as an information security educational tool will be determined through a survey. The survey (research instrument) used to do this will be presented in the next section.

3.4 Research Instrument

Part one of the research instrument consisted of a survey designed to acquire quantitative data about whether the learners had gained knowledge about secure password management after playing the game. The questions on the survey dealt with the subject area on which the game focussed. They were close-ended, multiple choice questions which related to a few select lessons that were included on the board. These tested student knowledge gain.

Part two of the research instrument consisted of a few interview questions targeted at teachers who allowed their classes to play the game. The interview questions tried to determine the teacher's perceptions of the effectiveness of the game as a teaching tool and it's the perceived effect on the learner's knowledge and behaviour

Both parts of this research instrument were implemented alongside the research artefact in the context of the case study. This is presented by the next section.

3.5 Implementation (experiment)

The research artefact was freely distributed to many primary schools within South Africa. Some of the schools targeted in the distribution were also given an introductory information security awareness talk and lesson using the research artefact. However for the purposes of this case study, two schools were selected as a target group and their data was gathered.

At School-A a grade 5 class of eleven students between the ages of eleven and twelve participated. At School-B a grade 3 classes of fifteen students between the ages of nine and ten participated. Both class teachers ran the survey in their classes, and then were themselves interviewed by the researcher. The research was conducted in this manner to comply with ethical research policies.

In relation to ethical research, children are classified as a vulnerable target group. Therefore due to ethical considerations both internal at Nelson Mandela Metropolitan University (NMMU) and externally at the target schools, the researcher did not interact directly with the students.

Surveys were provided to the target school's teachers. The teachers first had the children answer the surveys before playing the game. After the answer session, the children were then asked to play the game. After the game had been played they

answered the survey questions a second time. The children were not allowed to share or discuss their answers. The researchers later interviewed the teachers.

This implementation was used as this research is the first stage of a larger research goal. The results presented are relevant to each case, however due to a lack of double blind testing they are not formal enough for statistical significance. A statistically significant approach will be conducted in the next stage of this research.

3.6 Results and Analysis

Within the survey, three questions, which related to the lessons presented in the game, were asked. These questions were asked before and after the game activity to determine whether there had been a change in the learner's knowledge and response. The results showed a definite positive trend which confirmed that the learners had gained knowledge relevant to secure password management (see Table 3).

Table 3. Aggregated Learner Survey Results

Question Number	Before playing the Game		After playing the Game	
	Correctly Answered (%)	Incorrectly Answered (%)	Correctly Answered (%)	Incorrectly Answered (%)
1	53.33	46.67	92.31	7.69
2	34.62	65.38	73.07	26.93
3	66.67	33.3	88.46	11.54

The interview questions aimed to determine: whether the teachers perceived the game as an effective teaching tool; and whether they perceived the learners to be more aware of the matters which the game taught after the game had been played.

Both of the teachers felt that the learners had definitely learned valuable lessons, relating to the topic, via the game. They also observed that the learners had undergone small behaviour changes which indicated a higher awareness of the issues. Both of the teachers concluded that they perceived the 'Secure Password – Snakes and Ladders' game to be an effective education tool.

4 Conclusions

Information security education is necessary for today's youth. Gameplay is an effective knowledge delivery system for youth, and can be used as a delivery mechanism for information security educational lessons. Such education does not have to be in an online environment. This case study has shown how a traditional board game approach could be effectively used in classrooms for such education. The case study has shown that the playing of this game lead to information security knowledge gain and to a certain amount of retention amongst the case study's students. It is therefore the conclusion of this author that gameplay in this format could be a viable option for the education of the future generation. Further research should be done to further improve the process.

5 Future Work

The research shown in this paper forms the preliminary starting stage of a larger information security education research plan. The next stage will prove effectiveness via controlled studies in order to prove statistical significance.

Acknowledgement. Professor R.Von Solms is acknowledged for his game content contribution.

References

1. Atkinson, S., Furnell, S., Phippen, A.: Securing the next generation: enhancing e-safety awareness among young people. Computer Fraud & Security, 13–19 (2009)
2. Jones, S., Fox, S.: Generations Online in 2009 Generational Differences in Online Activities Generations explained, Washington, D.C. (2009)
3. Schroer, W.J.: Generations X,Y, Z and the Others, http://www.socialmarketing.org/newsletter/features/generation3.htm
4. Furnell, S.M., Gennatou, M., Dowland, P.S.: Promoting security awareness and training within small organisations. In: 1st Australian Information Security Management Workshop. University of Deakin, Australia (2000)
5. The UK Cyber Security Strategy (2011)
6. White House: The National Strategy to Secure Cyberspace (2003)
7. Reid, R., Van Niekerk, J., Von Solms, R.: Guidelines for the creation of brain-compatible cyber security educational material in Moodle 2.0. In: Information Security South Africa (ISSA), Johannesburg, pp. 1–8 (2011)
8. Jensen, E.P.: Teaching with the Brain in Mind. New Directions for Adult and Continuing Education, 49–60 (2008)
9. Caine, R.N., Caine, G., McClintic, C.L., Klimek, K.J.: 12 brain/mind learning principles in action: The fieldbook for making connections, teaching, and the human brain. Corwin Press, Thousand Oaks (2005)
10. Caine, R.N., Caine, G.: Making Connections: Teaching and the Human Brain. Association for Supervision and Curriculum Development, Alexandria (1991)
11. Banikowski, A.K.: Strategies to Enhance Memory Based on Brain-Research. Focus on Exceptional Children 32 (1999)
12. Yin, R.K.: Case Study Research: Design and Methods. Sage Publications, Inc., Thousand Oaks (2009)
13. Creswell, J.W.: Qualitative inquiry and research design. Sage Publications (2007)
14. Avedon, E.: Snakes & Ladders or Chutes and Ladders, http://www.gamesmuseum.uwaterloo.ca/VirtualExhibits/Whitehill/snakes/index.html
15. Taylor, A.: How the Brain Learns Best. Journal of Adventist Education, 42–45 (2007)

Virtual Penetration Testing: A Joint Education Exercise across Geographic Borders

Helen Armstrong[1], Matt Bishop[2], and Colin Armstrong[1]

[1] Information Systems, Curtin University, Australia
{helen.armstrong,C.Armstrong}@cbs.curtin.edu.au
[2] Computer Science, University California, Davis
mabishop@ucdavis.edu

Abstract. This paper describes an exercise that combines the business case for penetration testing with the application of the testing and subsequent management reporting. The exercise was designed for students enrolled in information systems and computer science courses to present a more holistic understanding of network and system security within an organization. This paper explains the objectives and structure of the exercise and its planned execution by two groups of students, the first group being information systems students in Australia and the second group comprising students enrolled in a computer security course in the United States.

Keywords: Penetration testing, vulnerability testing, security education.

1 Introduction

Today's organization typically relies on a multitude of new and aging information technology and heterogeneous systems all stuck together with ethereal adhesive. Integration complexity rises as new systems and applications are added, together with the risks. A secure technology environment is an unspoken requirement for decision makers in today's globally competitive marketplace, and ensuring these systems are secure is an ongoing battle for an IT Department. Conducting assessable assignments in a simulated realistic business environment facilitates achieving better learning outcomes, and past research has shown that practical application of knowledge cements understanding, and builds skill levels, of the learner. Learning through experience and hands-on techniques are well tested and produce superior skills-based learning outcomes in IT security (Kercher & Rowe 2012, Papanikolaou et al. 2011).

Skill and knowledge in securing networks and systems are essential foundations for security practitioners. Most security curricula discuss these at length. Skills in network attack and defense come from this foundation. Those two particular skills enable the practitioner to test the security of an organization's networks and systems through the use of penetration testing, giving feedback to an organization on the security of its enterprise information technology as seen by attackers. However, security skills and knowledge are limited to the discipline within which the education is

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 11–19, 2013.

delivered. Security studies in computer science and computer engineering commonly include areas and a focus on the equipment, technology, infrastructure, protocols, cryptography and systems applications whilst those in information systems and information technology have a more business focus including security policy, disaster recovery, network security management and information security (ACM 2008, 2010). In many cases there is a chasm between security management and the technical gurus: computer scientists have a deep understanding of the inner workings of the network and operating system but little or no skill in presenting a business case to management. On the other hand the information systems people focus on solving business problems and creating opportunities using technology and thus understand the effect of risks and security breaches on the organization's ability to achieve its goals and bottom line. However courses in information systems are seldom designed to understand the capabilities or limitations of the inner workings of the technology.

This paper describes a joint exercise between two groups of students that traverses the chasm described above. A group of information systems students in a business school in Australia interact with a group of students in a computer science program in the US to build a business case for, and design and execute, penetration testing of an organization's network security. The paper presents a discussion of related work, the framework used and a description of the project which is still a work in progress.

2 Related Work

Over the past decade much has been written on practical exercises in educational environments involving hacking and penetration testing. These publications fall into several main groups. Cyber defense forms a distinct group presenting red and blue team exercises (for example see Conklin 2006, Kercher & Rowe 2012, Lathrop Conti and Ragsdale 2003, Mattson 2007), a second group discusses designing network security exercises and experiments (examples: Logan and Clarkson 2005, Papanikolaous et al. 2011, Peisert & Bishop 2007, Tjaden & Tjaden 2006, Vigna 2003), and a third group focuses on network security laboratory design (examples: Aboutabl 2006, Anantapadmanabhan et al. 2003). By now we should have the design and delivery of practical network protection education under control! However, the need for cross disciplinary knowledge and experience is finding its way into a list of needed skills for security professionals, and potential employers are increasingly seeking employees with broader skills than technical skills, such as problem solving, team facilitation, and good spoken and written communications. To the authors' knowledge, no prior publication covers an exercise similar to that described in this paper – one that links business and computer science students in the same exercise across international boundaries with significant time differences. This exercise reflects situations that are increasingly more common for IT professionals who work in teams from distributed locations, often experienced in large global organizations.

The need for penetration testing is well published, but the question is whether we are preaching to the choir. Swanson (2000) explains such testing not only ensures an organization has adequate protection in place, but confirms also that they are working

as designed and that the employees are using them effectively. Chickowski (2013) reports that one of the challenges faced by security professionals is performing vulnerability testing on the applications that businesses can least afford to have compromised. Organizations can't defend against vulnerabilities of which they are not aware. Outsiders continually seek vulnerabilities by scanning and mapping organizational assets, and organizations should know where their vulnerabilities lie to defend those assets. Kennedy et al. (2011) posit that penetration testing is one of the most effective ways to identify systemic weaknesses and deficiencies in systems. The penetration tester can identify ways an attacker can compromise a system by attempting to circumvent security measures. However, penetration testing is not the only answer – managers must realise that it does not try to identify all vulnerabilities. It simply illustrates how a system can be compromised. Penetration testing and vulnerability analyses can be excellent means to highlight the need for security, particularly where managers see sensitive data compromised and security policies not being adhered to.

3 The Penetration Testing Framework

The exercise uses the Penetration Testing Execution Standard as the foundation for the approach and the activities carried out (PTES, 2012). The PTES provides a standardized approach, a baseline to assist in client expectation management as well as risk management. This standard is currently in the beta stage of development and is being used widely across the globe. It is supported by a set of technical guidelines to provide direction when undertaking a penetration test. The PTES development team encourages its users to "think outside of the box" when following the guidelines, as all situations do not fit a common mold.

The main phases of the PTES are as follows:

1. Pre-engagement Interactions: This first phase encompasses agreement with the client on the objectives of the exercise, the scope of the penetration test, and an agreement on the terms of engagement. Clients must understand what is involved in a penetration test, and they have to specify the limits of penetration and exploitation activities, particularly where systems are operating live during the testing. Requirements for lines of communication and reporting must make clear who is to receive and act upon the information in the final report.

2. Intelligence Gathering: This phase involves gathering information about the organization from public sources such as databases, social media, web sources, media coverage, public company reports, and other external and internal footprinting activities. Some common activities in this phase are gathering information on what applications are running, which ports are open/blocked, what devices are connected, patch levels on system applications, storage infrastructure, VMs and any known vulnerabilities of web applications. This information identifies the list of potential targets. Some information regarding the security measures in place within the organization may be gleaned from these sources by identifying network and host-based protection mechanisms and security measures applied applications, VMs and storage. The 'attacker'

needs to learn about a target, including how it behaves, how it operates, and from that determine how it can be attacked (Kennedy et al. 2011).

3. Threat Modeling: This phase is sometimes termed 'enumeration' and entails a more detailed investigation of threats by gathering more information about users, network connections and available services and then modeling the most effective approach to attacking through the vulnerabilities identified in the intelligence gathering phase. This phase analyses business assets (such as intellectual property, trade secrets, etc.) and business processes as well as identifying threat agents and their capabilities. Using this information the tester will identify those potential vulnerabilities that pose the greatest threat in the client's environment as well as opportunities to maximize the success of the attack. By thinking like the attacker, the tester models an attack by analyzing the weaknesses discovered.

4. Vulnerability Analysis: This phase involves mapping the target environment, scanning ports, and running vulnerability scans on the target organization's system to confirm the existence of the vulnerabilities to be used in the exploitation phase. The analyst may use both active and passive means to identify vulnerabilities. Existing tools such as nmap (Lyon 2008) and metasploit (Kennedy et al. 2011) will confirm some vulnerabilities; others may require developing special tests solely for this environment or organization. This phase may not necessarily identify a single vulnerability as the avenue for attack, as a combination of several vulnerabilities often gives the tester much greater success.

5. Exploitation: This phase commences once the vulnerabilities have been mapped in detail. The tester will seek to gain privileged access to the target system by exploiting the vulnerabilities discovered in the previous phase. Methods to bypass countermeasures using both manual and automated methods are employed and detection mechanisms circumvented. When the tester is sure that an exploit will result in success as defined by the ground rules of the test, the tester may execute an exploit. Note that in many cases, stealth and speed are important to a successful attack remaining undetected; this must be considered in light of the goals of the test.

6. Post Exploitation: Once the organization's system has been successfully compromised the tester then moves into detailed exploitation of the target's infrastructure, pillaging and capturing valuable information and resources such as source code, intellectual property, and funds from high profile systems. This phase focuses on attacks that have the greatest business impact and uses whatever sources it can access—including the often-overlooked backups. Commonly the tester inserts backdoors for future entry, and other Trojan horses as permitted by the terms of reference for the testing. After documenting and gathering evidence of all exploitations and their results, the tester cleans up, removing test data, activity logs, malware and rootkits, and returns the system to a clean environment. Hackers spend a significant amount of time in this phase to conceal the fact of compromise and the tester must do likewise in order to identify weaknesses in reporting and attention across the enterprise.

7. Reporting: This final phase reports the testing activities carried out, the results and the means for remediation. This report forms the foundation for decisions on allocating resources to security to protect the organization's systems against future attacks. The report should include executive level content explaining the risks,

including business impacts and the bottom line, quantifying the risks. As executive staff or board members with little IT knowledge will call for different language and detail than the CIO and IT professionals so the technical details are not included in the executive-level sections. Technical content will then follow, detailing the penetration metrics and technical findings, together with the test cases and examples used. Details of the vulnerability analysis, exploitation and post-exploitation should be included. The contents of the report should be discussed with the client before issuing the report as a deliverable, so that potential protective measures can be discussed and investigated with the aim to fill the gaps. Recommendations and an action plan, also previously discussed with the client, are included before the written report is presented. An executive summary is useful to highlight not only the most important areas for attention, but also confirm the value of the penetration testing.

4 Overview of the Joint Exercise

The education exercise comprises a group of students enrolled in an information security management undergraduate course within the School of Information Systems in Western Australia (InfoSys group) and a group of students enrolled in a computer science course in University of California, Davis (ComSci group). The two groups of students will work together to design and complete a penetration test on a client's information technology, each group completing activities within their discipline area and contributing to the learning outcomes of their degrees as well as interacting across discipline boundaries.

The objectives of the exercise are to:

- Develop skills in presenting a business case for penetration testing to management,
- Develop skills in designing and executing penetration testing in a safe and ethical environment, and
- Develop skills in presenting penetration testing results to management.

The physical deliverables for the education exercise include:

- Business Case Report to the Organization's Executive Management detailing the need for and objectives of a penetration test, cost/benefit analysis and an overall project plan for the penetration test activity, including the methodology to be followed, the objectives of each phase, activities included in each phase, resources, time frame and constraints (InfoSys group). The scope and boundaries must also be detailed including the rules of engagement.
- Detailed Penetration Testing design, specifying the tasks to be undertaken and the tools to be used in each activity (ComSci group).
- Penetration Test results, including activities carried out, results including vulnerabilities detected, and strengths and weaknesses of the system tested (ComSci group).
- Final report to management detailing the activities carried out, strengths and weaknesses, impacts associated with weaknesses and vulnerabilities detected, and recommended security measures to minimize the organization's exposure and losses (InfoSys group).

5 Business Case Scenario

Both sets of students are advised that they will work together to plan, carry out and report on a penetration test for the organization General Airline and Grading Assignments, LLC (GAGA). This company is based in the Remote Access Virtual Environment (RAVE), and consists of several client workstations running different flavors of Windows and Linux. A central server provides the support for the company's sales, services, and records. The recent attacks on Spamhaus, and on the New York Times, have made GAGA aware that connecting to the Internet for their business may pose some risk. This risk might be amplified; they feel, by having their web server and assignment grading service accessible to the world. So they have asked whether a penetration test can help them be sure their systems are secure, and if so what is the business case for such a test. Both groups of students (located in Australia and California) are employed by Penetration Testing and Assessments (PTA) with the information systems students providing the business related expertise and the computer science students providing the technical expertise. The information systems students will produce the business case report at the beginning of the project and the final report to management at the end of the exercise (deliverables 1 and 4). The computer science students will carry out the testing, logging all activities and report their results to the information systems students (deliverables 2 and 3).

Table 1. Division of Project Duties

Deliverable	Task	InfoSys	ComSci
Business case	Objectives, cost/benefit analysis, methodology, overall project plan	✓	×
Terms of engagement	Scope and boundaries, terms of engagement	✓	×
Penetration testing design	Document high level testing requirements	✓	×
Penetration testing design	Detailed design of testing process and tools	×	✓
Penetration testing	Conduct testing process	×	✓
Penetration testing	Maintain testing records	×	✓
Penetration test results	Prepare technical test report	×	✓
Final report	Prepare final management test report	✓	×

The exercise will follow activity stages related to the deliverables as illustrated in Table 1. The InfoSys students will raise the business case for penetration testing and provide the scope and terms of agreement for the exercise. These students will write a document explaining to management the objectives of the activity, the associated benefits and costs, the testing process to be carried out based upon the PTES

methodology and an overall project plan detailing timelines and resource allocation. Agreement must also be reached with the client regarding the rules of engagement once penetration has been achieved, including boundaries for the exploitation activities, and this will depend upon the objectives of the test and whether the system is live at the time of penetration and exploitation.

The ComSci group will carry out activities relating to the identification and exploitation of vulnerabilities. Their first task will be to gather information about the target, using tools like nmap to determine which ports are open, and look at network traffic to see what systems it talks to. This information will enable the students to hypothesize flaws which will need to be documented for use in developing the detailed testing plan. Testing the hypotheses comes after the ComSci group has discussed these with the InfoSys group to identify which ones pose the greatest threat to the client's environment and which have the most likelihood of success. Once priorities related to the objectives and an ordered list are established, the detailed testing stage can begin. The ComSci group will then carry out the Vulnerability Analysis and Exploitation phases. They will try to confirm whether the vulnerability is present without exploiting it; which is a challenging task, because they have to think of a way to demonstrate its existence. They also must develop exploits for the vulnerabilities they find. The ComSci group will record all activities and their results. Descriptions need to be sufficiently detailed to reproduce the results and will include: date and time, event name, event synopsis (*very* brief) e.g. Brute Force, etc., event description, intended result, actual result (vulnerability identified or no vulnerability), tools and scripts used, and attachments or associated documentation.

In the post exploitation stage the ComSci group must interact closely with the InfoSys group to ensure they adhere to the rules of engagement and achievement of the objectives. This stage would commonly involve copying files, inserting new files, deleting existing ones, or inserting Trojan horses (usually back doors) to allow an attacker to enter the system with minimal fuss. When carrying this out the goal is avoid detection. Cleaning up before they exit is a crucial stage for post exploitation. The students will not know whether, or how, the teaching staff will be monitoring the systems and the students' activities. Again the students must record all their activities and results. This is also for their protection, because if GAGA claims they have damaged their systems in a way that is not allowed, the session recording will show them they did not.

The reporting phase involves developing a technical report describing the vulnerabilities the ComSci group found and assessing the security posture of the systems, evaluating the technical problems GAGA has, and providing technical recommendations to address the vulnerabilities you have discovered. This report needs to be supported by references to what they have found in their testing. This technical report forms part of the final report to be presented to GAGA management.

The InfoSys group develops the final report that not only includes the technical details of the testing provided by the ComSci group, but also suggests means of minimizing the risks arising from the vulnerabilities detected at both the technical and management levels. The information systems students will thus need knowledge of information security management, including considerations of standards, methodologies and

frameworks for undertaking specialized information security operations, secondary considerations include physical security; control of access, both logical and remote; security considerations in the design, testing, implementation of computer systems including the role of standards; administrative controls and their impact on reducing risk; controls in networks; recognition and measurement of potential loss; Information Systems audit concepts and techniques; and scenarios and case studies.

The students themselves will be required to manage the communications between the InfoSys and ComSci groups. The two sets of students will collect into small groups, forming internationally linked groups of 5-6 students. These students will need to communicate regularly over the course of the exercise to ensure effective information transfer and decision making. There is a 15 hour time zone difference between the two sets of participants. Perth in Western Australia is located slightly west of 120^0 East of Greenwich in Britain and therefore at plus eight hours Coordinated Universal Time (UTC). The UC Davis campus in California is approximately 120^0 West of Greenwich and therefore at minus seven hours Coordinated Universal Time. While students in both project groups may find the resulting time difference inconvenient, this additional dimension provides a real world working environment that they may commonly encountered during their careers. Effective communications between the project participants may therefore become a determinant of project success. As Table 1 illustrates, it is imperative that the InfoSys group effectively explain the business case and terms of engagement to the ComSci group. Both groups then need to negotiate the penetration testing design phase, and the ComSci group must communicate operational aspects of the penetration testing, agree on the level of exploitation as the testing progresses, and provide the test results to the InfoSys group. Finally the InfoSys group must ensure the final report accurately reflects all tasks undertaken before submitting it to the management of GAGA, LLC.

6 Work in Progress

This project is currently underway and thus a work in progress. Many aspects are proving challenging as the exercise progresses. Not only is the time difference posing a challenge, but the timing of semester classes and due dates for submission of assignments differs between the universities involved. Understanding of the tasks required appears to be clear and the students are experienced in working in teams to achieve specific goals. What is a learning experience is the cross discipline communication and building an understanding of the science versus business needs.

There are many advantages this type of exercise delivers. Not only do the students have the opportunity to work on an exercise involving highly industry relevant skills development, but also working as a team across global and specialty expertise domains. This exercise is anticipated to develop time management skills, project management skills, problem solving skills and social, technical, and communication skills. In addition it presents opportunities to extend personal networks in an industry specific set of security practitioner roles and an associated appreciation for different stakeholder perspectives.

References

1. Kercher, K., Rowe, D.: Risks, Rewards and Raising Awareness: Training a Cyber Workforce Using Student Red Teams. In: Proceedings of SIGITE 2012, Calgary, Alberta, Canada, October 11-13 (2012)
2. Papanikolaous, A., Karakoidas, V., Vlachos, V., Venieris, A., Ilioudis, C., Zouganelis, G.: A hacker's perspective on educating future security experts. In: 2011 IEEE Panhellenic Conference on Informatics (2011)
3. ACM, CS2008 Curriculum Update (2008), http://www.acm.org/education/curricula-recommendations (accessed May 3, 2013)
4. ACM, IS2010 Curriculum Update (2010), http://www.acm.org/education/curricula-recommendations (accessed May 3, 2013)
5. Conklin, A.: Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course. In: Proceedings of the 39th Hawaii International Conference on System Sciences, Hawaii (2006)
6. Lathrop, S., Conti, G., Ragsdale, D.: Information warfare in the trenches. In: Irvine, C., Armstrong, H. (eds.) Security Education and Critical Infrastructures. Kluwer Academic Publishers (2003)
7. Mattson, J.: Cyber Defense Exercise: A Service Provider Model. In: Futcher, L., Dodge, R. (eds.) Fifth World Conference on Information Security Education. IFIP, vol. 237, pp. 51–86. Springer, Boston (2007)
8. Logan, P., Clarkson, A.: Teaching students to hack: curriculum issues in information security. In: ACM SIGCSE 2005, Louis Missouri (February 2005)
9. Peisert, S., Bishop, M.: How to Design Computer Security Experiments. In: Futcher, L., Dodge, R. (eds.) Fifth World Conference on Information Security Education. IFIP, vol. 237, pp. 141–148. Springer, Boston (2007)
10. Tjaden, B., Tjaden, B.: Training Students to Administer and Defend Computer Networks and Systems. In: Proceedings of ITiCSE 2006, Bologna, Italy, June 26-28 (2006)
11. Vigna, G.: Teaching network security through live exercises. In: Irvine, C., Armstrong, H. (eds.) Security Education and Critical Infrastructures. Kluwer Academic Publishers (2003)
12. Aboutabl, M.: The CyberDefense Laboratory: A Framework for Information Security Education. In: IEEE IAW West Point Military Academy, New York (2006)
13. Anantapadmanabhan, V., Frankl, P., Memon, N., Naumovich, G.: Design of a laboratory for information security education. In: Irvine, C., Armstrong, H. (eds.) Security Education and Critical Infrastructures. Kluwer Academic Publishers (2003)
14. Swanson, D.: Secure Strategies. Information Security Magazine (October 2000), http://www.infosecuritymag.com/articles/october00/features3.shtml (accessed April 3, 2013)
15. Chickowski, E.: Too Scared to Scan, Dark Reading, TechWeb, United Business Media (UBM), Manhasset, NY (March 27, 2013), http://www.darkreading.com/security/application-security/240151869/too-scared-to-scan.html (accessed April 3, 2013)
16. Kennedy, D., O'Gorman, J., Kearns, D., Aharoni, M.: Metasploit, The Penetration Tester's Guide. No Starch Press Inc., CA (2011)
17. PTES, Penetration Test Execution Standard (2012), http://www.pentest-standard.org/ (accessed March 30, 2013)
18. Lyon, G.: Nmap Network Scanning. Insecure.Com LLC Sunnyvale CA,USA (2008)

Developing Cyber Competition Infrastructure Using the SCRUM Framework

Heath Novak, Daniel Likarish, and Erik Moore

Regis University, Denver CO, U.S.A
{novak667,dlikaris,emoore}@regis.edu

Abstract. In March 2012, the Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC) was hosted at Regis University and attended by seven colleges from the region. CCDC was developed by the University of Texas in San Antonio to provide a structured environment for practical education tied to established information assurance learning objectives in the implementation of security techniques, strategies and processes. The Regis University infrastructure team designed the competition scenario to emulate an e-commerce web business. The pervasiveness of web application attacks resonated with the event developers at Regis University because of recent reported attacks against Valve, Inc. and their Steam video game retail and social networking service. This paper will outline at a high level the event architecture and technical infrastructure details, a discussion on Agile development methodologies (specifically SCRUM) and how they can be applied to competition infrastructure development.

Keywords: Collegiate Cyber Defense Competition, CCDC, Cybersecurity, Information Assurance Curriculum, Agile, SCRUM, SDLC, Capability Maturity Model Integration, CMMI.

1 Introduction

The Collegiate Cyber Defense Competition (CCDC) [10], developed and organized by the University of Texas, San Antonio has steadily grown to encompass all 50 States in the Union. In 2012, Regis University joined the CCDC family by hosting the Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC). A total of seven schools participated in the event and six out of the seven teams competed for the chance to be invited to the Nationals competition. Victorious student competitors from all hosted CCDC regional competitions are invited to compete for the top prize at the University of San Antonio Nationals. The last report by an official within the University of San Antonio CCDC steering committee stated that all 50 states are onboard to take part in the competition. These schools have a special motivation to be involved because they can gain recognition for their cyber defense curriculum as well as offer a unique opportunity for students to gain hands-on experience assisting in developing the infrastructure for the competition. By competing in the event, students are offered an additional learning opportunity for personal growth and are provided a venue to demonstrate their business and technical skills to potential employers.

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 20–31, 2013.

The task of developing the information systems infrastructure is not trivial and takes a great deal of coordination and technical savvy. Black is the color identifier for the team in charge of infrastructure development and maintenance for the event. The skills gained and exercised as a member of the Black Team is unique and well-suited for individuals in a general or security-focused information systems engineering role as necessary skills exercised include systems engineering, project management, systems administration, and software development. This paper reviews the project management methodologies as applied to the goals and situation of the Black Team at the Regis-hosted CCDC event and makes general recommendations based on outcomes.

2 CCDC: The Collegiate Cyber Defense Competition

The CCDC event is typically composed of five primary teams: the competitors (Blue teams), the attackers (Red team), the competition infrastructure engineers (Black team), the Blue team facilitators (White team) and the judges/rules enforcers (Gold team) [10]. The CCDC event typically consists of six Blue teams competing in the event, although the RMCCDC event hosted by Regis University had a seventh non-competing team. Each Blue teams consisted of eight individuals (two graduate and six undergraduate students) tasked with protecting a pre-configured and provided information system infrastructure functionally identical to that of the other teams.

The information system infrastructure consists of flat network architecture, various servers and workstations supporting valid business or mission-critical applications that emulate the internal functions of a real-world organization. Injecting realistic customer, business, and security events into the event enhanced the knowledge gained by the participants to achieve greater real-world value and therefore more benefit later when they enter the workforce.

The scenario touches on current events and includes valid applications that leverage standard Internet protocols and security controls. Further, the scenario includes enough content to keep the competitors busy with deliverables that demand effective communication between team members in order to emphasize the importance of interpersonal communication during periods of critical activity. One key facet of the event is the injection of stress, or "injects," such as providing deadlines for specific business reports and change requirements as written and enforced by the Gold team. These injects are service level agreements (SLAs) that are provided up-front and include specific deadlines for completion, typically within an hour. Injects can also be issued randomly, in order to simulate normal, on-demand business activities. Inject responses allow the Gold Team to assess how the competitors handle normal business activities along with the threat of attack from malicious actors.

3 Background

Regis University previously hosted and developed information systems infrastructure for CANVAS (Computer and Networking Virtualization and Simulation) cyber competition. This initial foray into this realm of cyber competition development offered

insight into how to improve the development of infrastructure for future events including consideration of the project management methodologies. The Regis project team developing cyber competitions improved its approach in developing RMCCDC from lessons learned in the development of CANVAS, such as introducing advanced scenarios based on current threats, prevailing security and networking technologies, and improved monitoring capabilities. But the team fell victim to some of the same mistakes and constraints adversely affecting the effectiveness of monitoring and testing coverage. The network topology for the public and private networks designed for the event made it difficult to monitor full Red and Blue Team activities. As a result, a flat, isolated network will be favored for future events. Testing was hampered by severe time constraints caused by late arrival of necessary equipment and Black Team scheduling difficulties. In order to improve the level of capability of the team, efficiency of work, and quality of outcome, the team decided to apply a standard methodology for a systems development life cycle (SDLC). The reason that the team decided this is because it recognized standard artifacts of project dysfunction in the previous work and realized that a more formal approach was necessary to ensure success. Cyber competitions are a type of product, one from which the host can gain value as well as the various participating teams. During our trial and tribulations in building RMCCDC, we realized that cyber competitions exemplify the goals and challenges of Enterprise Architecture; that is to integrate novel approaches in executing in the most efficient and agile way possible, the strategies for developing of the final product. It is therefore quite clear that an appropriate development lifecycle methodology be leveraged for developing cyber competitions.

Based on the above realization, in 2012, the Regis University Black Team implemented a diluted version (i.e. lacking a full set of phases) of an Agile SDLC, where there is somewhat less formality and a greater emphasis on people and their interactions. Although the Agile Methodology is generally specific to software development, the same principles can apply to system engineering projects, at least those facets that relate to people and their interactions. Additionally, agile methodologies place strong emphasis on risk management, since projects of any size are rife with risk requiring effective time management, communication and prioritization of tasks. The focus on risk was particularly important to the team because of the need to produce a resilient infrastructure with a volunteer team in a limited time. Extending analysis of these affinities, the next sections present a review of Agile methodologies, and then particularly SCRUM methodologies as applied by the Regis cyber challenge development team along with an evaluation of the change in performance outcomes attributable to the use of the SCRUM methodology.

4 Agile Software Development Methodologies

Initially, the cyber competition development team did not consider using an agile method to drive development of the competition infrastructure; this came about as we were actively working to get the deliverables completed. We realized later into the process that due to the timeframe, scheduling and manpower availability constraints,

we couldn't use a traditional software development lifecycle (SDLC) approach. Since we just started taking part in the CCDC circuit and didn't have experience in developing cyber competitions other than CANVAS we chose to embrace, in an ad-hoc way, the ideals set forth in the Agile Manifesto (http://www.agilemanifesto.org). There are many conceptual and practical parallels between software development and information systems infrastructure development, which includes just about every Internet technology engineering discipline. Therefore, we feel confident that using an agile project management methodology greatly improves the final competition deliverable as well as satisfying several academic objectives for students taking part. We assert that using the SCRUM framework, developed by Ken Schwaber and Jeff Sutherland [8], would serve the purposes of the competition host best.

5 SCRUM, an Agile Method

First and foremost, SCRUM is a process *framework*. More specifically, it is an iterative and incremental agile software development method, so again its focus is on managing software development. Yet, there are parallels with software development and information system infrastructure development such that the same core values and mechanisms of the SCRUM framework can be applied to cyber competition infrastructure. As a result, it serves to take a closer look at how we could have leveraged, and leverage more effectively in the future, the SCRUM management framework for development of RMCCDC infrastructure.

The actionable roles in SCRUM consist of SCRUM Masters, Product Owners, and a Development team [7]. A SCRUM Master is very much like a "Project Angel" since they enforce process adherence and protect the development team from disruptions that can cause missed deadlines [7]. There is typically a single Product Owner in the SCRUM framework, a person who is the primary stakeholder. In the case of cyber competitions hosted by schools, the product owner would be the Director of the Computer Information Systems Dept. or pertinent faculty members in charge of meeting obligations agreed to by the University as a new member of the CCDC family. The Development Team would be the Black Team, which is generally comprised of current Practicum students and former alumni volunteers.

In addition to the different SCRUM roles, the other important facet of SCRUM is the iterative process within the SCRUM framework, specifically a concept referred to as a "Sprint." A Sprint is the "heart" of SCRUM and is in essence a time-box of one month or less in which to get things "Done" [9]. A Sprint is completely agile in nature considering that it directly follows the manifesto by embracing "individuals and interactions over processes and tools" [1]. Sprints contain the following characteristics; 1) change control to protect Sprint goals, 2) Development Team composition remains constant, 3) quality goals do not decrease, and 4) the scope may be clarified and re-negotiated between Product Owner and Development Team as issues are discovered [8].

In SCRUM, there is also a concept referred to as a backlog, which defines specific work deliverables that result from the stories defined in the Release Planning phase [8]. Stories are based on use cases, a carryover from traditional software development requirements definitions. Since we are developing cyber competitions, the primary requirement is contingent on the chosen scenario, in this respect a form of use case, since it models something that exists in the information technology industry, such as a for-profit web application or critical infrastructure (e.g. power utility, railway station, prison, etc.).

6 How Ad-Hoc SCRUM was Applied to RMCCDC

Our initial requirements phase encapsulated the classic SDLC initial requirements phase: to identify the general requirements for the final product and provide enough detail for the system designers to begin designing the solution. The Product Owner, Regis University, along with the development team decided to raise the bar from what we built for the initial foray into cyber competitions, CANVAS. This time out, we introduced elements drawn from the Open Web Application Security Project (OWASP) Top Ten list of web application attack methods (http://www.owasp.org). Therefore, we knew we wanted to build an infrastructure modeled as closely as possible to a public, for-profit web application as well as the expected supporting systems, such as email server, domain controller, FTP server, etc. that an organization would use to satisfy daily business needs. After identifying a model inspired by a real life hacking incident, the aforementioned Steam™/Valve® hack [6], we decided to emulate this environment for our scenario. The end product was a web application simulation, one that could be attacked by a Red team and protected by a Blue team. The requirements defined by these systems, their respective configurations, and content would be the backlogs that the development team members would work on. We propose that a SCRUM Master (or multiple depending on the size of the project) be assigned to manage the development of specific components of the environment in order to keep progress on track.

We assigned a SCRUM Master to maintain progress on the web application backlog (including the Apache server, PHP code, database, FTP server, etc.), another SCRUM Master managed the network development, and a third SCRUM Master to manage the business support environments; Windows systems that implement common business support functions such as role-based access control (e.g. Active Directory), email services with Exchange 2007, employee workstations, etc.). We assigned SCRUM Masters based on their core competency and interest level within each discrete technology domain (i.e. network, web application, business support servers, etc) in order to maximize effectiveness. However, the size and complexity of the infrastructure will dictate the necessity for multiple SCRUM Masters. The assignment of SCRUM Masters is greatly dependent on the manpower, competency, and interest

level on hand since students may not desire a project manager type of role. The scenario requirements outlined for RMCCDC provided enough detail for the designers in the next phase to identify how they would implement the infrastructure in question.

Iteration 0, the phase following the initial requirements phase in the SCRUM process, includes the development of the necessary infrastructure required for the scenario in question. This stage included the acquisition, installation, and configuration of various information systems, including storage area network (SAN) equipment, networking equipment, and virtual infrastructure hosts with various relevant guest operating systems (i.e. Linux and Microsoft Windows) to serve the desired applications. This portion of the development process was not without problems, so the team solved problems as they arose, which necessarily generated a backlog of work that needed to be completed. Due to scheduling issues with our volunteer staff, we utilized email or instant messaging to communicate critical progress or blockers and spaced out our standups to twice a week rather than daily, leveraging Practicum course time for this activity. When necessary, priorities were reset and other important tasks were given favor so that at least some progress would continue. The Product Owner and Development team developed a project plan, network topology diagrams, and system characteristics to be used in the infrastructure. To minimize risk, we pursued the quickest and most cost-effective method to build a working e-commerce web site. We chose Drupal as the web site engine and UberCart as the shopping cart module since they best met our needs at the time. The public-facing web and database servers, along with an IPv6 network, created a sufficiently challenging attack surface for the Blue Teams to protect.

Since CCDC is largely an academic device, the alignment of individual student projects with the development of cyber competition infrastructure is encouraged. For instance, after offering the opportunity to take part in the development, specifically to Practicum participants, it would behoove the Practicum instructor to gather from students their specific areas of interest and/or core competency, so they could be more effectively utilized. After all, a motivated worker is a productive worker. In a sense, we would be "killing multiple birds with one stone," such that students would get graded work in an area of their specific interest while gaining the valuable skill set of building a functioning information system for a real customer - the competition participants. In other words, they gain some measure of startup experience. Various facets of systems engineering and software development are touched on, such as quality assurance, project management, information security, and systems engineering. As we discuss the Development Iterations phase, it should become clear to the reader how the scholastic endeavors of students are served through their involvement in cyber competition infrastructure development.

In the Development Iterations phase, we implemented the required systems using common-off-the-shelf (COTS) software. We installed and verified the minimum operational levels; that the guest operating system in the virtualization environment would successfully boot, that we were able to install applications and that the applications functioned as we would expect. We then introduced and enumerated vulnerabilities for individual components to be mitigated by the Blue Teams, as well as business

injects, tasks performed as part of normal business operations, during the competition. We were mindful of feature creep, we didn't want to block good ideas that come late; rather we prioritized based on value or ease of integration. This again should remind us of the facet of SCRUM that allows for continuous re-evaluation and the promotion of effective additions to the product.

The best way to test the competition environment is to put it through dry runs with mock Red and Blue teams (such as the Black team split into two groups) to verify that the environments built for each team functioned as expected. Our experience with CANVAS was such that we literally crammed what should have been four weeks of testing time into one week. We experienced similar problems with RMCCDC, but mostly because of delays in hardware acquisition that pushed critical portions of the infrastructure, in this case the network, into backlog. The late arrival of equipment and delayed implementation of network resources prevented the necessary stress and penetration testing to ensure confidence that the infrastructure would handle the load during the event. It is clear that the testing portion of the implementation phase was not nearly sufficient for a regional cyber competition, much less a national one. However, the infrastructure held up well during the competition thanks in large part to the effective work completed up-front in the design and implementation of the systems infrastructure.

The next phase of RMCCDC, called the Pre-Release phase in SCRUM, include integration of the various infrastructure components (e.g. network, servers, applications). This integration is a crucial piece of the puzzle since it will be what will be released for use during the competition and must be tested to make sure everything works as expected. In other words, final acceptance testing occurs in this phase. Additionally, all documentation will need to be finalized, such as business injects and instructions for the event i.e. access control, printing availability, communications, rules, etc.

The Production phase would be the actual competition itself. We had several problems, mostly with the network, that caused some unnecessary frustration for pretty much everyone. However, strong teamwork and effective troubleshooting saved the day, as we were able to get activities moving pretty quickly after the initial outages. Future cyber competition development must take better care in adhering to each phase of the SDLC, but with a special emphasis on testing and tracking metrics to gauge effectiveness. Agile methodologies, and by extension SCRUM, are quite different from traditional development methodologies in that they favor maximization of return on investment (ROI) rather than satisfaction of requirements [9]. As a result, there are very limited formal metrics or measurements that can be used to track progress or success. In fact, the most formal metric is based on output from SCRUM meetings, short "stand up" sessions that highlight individual efforts. The "stand up" session is meant to stimulate discussion and admission of problems that could affect progress. Stand-ups are also used to discuss progress on "Burn Downs", the term used to define the quantitatively the work remaining in a sprint. SCRUM Masters are expected to perform most of the documentation and performance monitoring since they are not responsible for specific development tasks [2].

7 Capability Maturity Model Integration

There is value in discussing how SCRUM relates to advanced models for information systems development, such as the Capability Maturity Model Integration (CMMI), a product of Carnegie Mellon Institute, is focused on managing continued process improvement in the enterprise. Cyber competition development does not need to reach the higher levels of CMMI, but it is useful to understand how CMMI can relate to this proposal. RMCCDC reached CMMI Level 1, which is basically the same as saying that the final product followed general ad hoc processes. As discussed previously, we recommend reaching a level better than Level 1, since doing so will improve the chances of a successful implementation and maximize the learning potential for students taking part on the Black Team.

Neil Potter of *The Process Group* analyzed how SCRUM and CMMI work together [7]. It turns out that SCRUM, an agile project management framework, fits very well in the first three levels of CMMI. Since our goal with using SCRUM is to improve the successful completion of cyber competition development and to get to the point where it is possible to introduce more sophisticated scenarios, it is obviously useful to be able to speak about performance in CMMI terms. Incidentally, the inclusion of SCRUM and CMMI practices enrich the experience and learning objectives for the Black Team members building the infrastructure.

8 SCRUM and CMMI Mapping

SCRUM does not cover Levels 4 or 5 in CMMI, and for good reason, because doing so would violate the fundamental tenets of agile life cycle development. SCRUM mandates flexibility and a focus on customer needs, which are often in flux throughout a project life cycle. Therefore, it is not desirable to integrate Level 4 and 5 processes because they are often heavy in measurements and documentation. We would not want project management tasks to take away from the already limited time available to build the infrastructure.

Researchers at the Technical University of Madrid have analyzed and mapped the various phases of SCRUM to levels 1, 2, and 3 of CMMI [5]. The researchers used a novel approach that visualizes quite clearly how well SCRUM covers the various goals of CMMI in the early levels. The mapping, as developed by the Madrid researchers, is a polar coordinate of the CMMI level 2 practices: Project Plan, Project Monitoring and Control, and Requirements Management. The SCRUM methodology is mapped to this polar coordinate with a scale of 0-9 for each component of a practice where the average support level that SCRUM methodology can substantively support for each CMMI level 2 practice is 7.2 for Requirements Management; 7.0 for Monitoring Project Against Plan and 6.8 for establishing estimates. This ability of SCRUM to fulfill specific CMMI practices is because both life cycle approaches are working towards the same goal – a fully functioning product that meets the

customers' needs. Neil Potter takes the mapping a bit further by showing clearly how SCRUM maps to an extent in CMMI Level 3 [7]. Thus, introducing SCRUM as the framework for developing cyber competitions also satisfies learning objectives related to the CMMI project management methodology– a net win for the hosting university.

We also recognized that proper risk management goes a long way to weeding out potential blockers or constraints so as to increase the chances of successful project completion. Therefore, risk management must be invoked throughout the development process to minimize loss probability.

9 Risk Management in Cyber Competitions

Risk Identification is generally the first step in risk management, which includes categorizing the potential risks in order to determine which components have the greatest impact on the success or failure of the project [4]. Taken in the context of a cyber competition, an example of a risk would be the choice of network hardware or a specific network design and how it would affect the overall competition experience. For instance, threats such as unavailable network hardware or a poorly designed network would have a negative effect on competition success. Therefore, the network portion of the competition would be a High Risk item, such that several different threats to the network portion of the infrastructure could cause delays in build-out, testing, and dependent tasks (e.g. application development) or cause the final competition infrastructure to have failures during the event, thereby incurring negative reaction to the competition by all participants involved. A matrix should be used to list out all risks and apply a corresponding score, determined from the loss probability, in order to identify priority.

Risk estimation is used to estimate the probability of potential loss [4]. Using the network example, loss estimation would be severe if the network is being built from scratch and less severe as the time goes by and the network build-out nears stability. Therefore, the network portion of the infrastructure should be prioritized above all other infrastructure components. If possible, the network should be built and maintained in a flat, isolated, constant state in order to minimize the problems just described for future events. Once the network is developed and kept stable, less time will be required for testing and more time can be allocated to other more advanced scenario components.

Risk Evaluation is another facet of the risk management process [4]. The goal of evaluating risk is generally understood in two different approaches; 1) to identify the best response, such as a contingency plan, or 2) to undergo risk aversive action that can lead to either reduction or acceptance [4]. Feasibility analysis also comes in handy during risk evaluation, since it helps to identify facets of the competition scenario that may be too difficult to carry out and are best left out of the event (i.e. risk avoidance). Using SCRUM can ease the risk management process by keeping competition

developers in synch with deliverable status during daily standups, allowing the ability to change course without adversely impacting the project.

How did we fare in leveraging risk management in RMCCDC? We were effective in identifying the risks and taking steps to either mitigate them or avoid them altogether. Using the same network example, we recognized that changing the network topology and Internet Protocol addressing schemes each time a competition is developed created risk, so we developed a plan to maintain an isolated network that would be maintained in a constant state, with minimal changes. The network would be leveraged for course projects when it is not used for competitions, thereby minimizing the costs associated with unused resources. This practice also allowed us to maintain knowledge of the state of the environment so we could address emerging problems sooner.

10 Conclusion

There are many benefits to the development and execution of cyber competitions at the collegiate level. They are primarily based on assessing and exercising technical skill in the realm of cybersecurity, but are also effective for students attuned to other information technology disciplines. They offer an unparalleled apparatus for education as well as team and individual skill assessment on technical activities related to system administration, network operations, and software development. How well do team members work together to solve a problem or develop a solution? How well do individual team members handle their respective tasks? These questions can be asked of Blue Teams as well as Black Teams. The development of cyber competition infrastructure is not a trivial undertaking and requires people skilled in information technologies to design, develop, implement and test the infrastructure. Competition infrastructure development is an excellent learning apparatus, in that multiple facets of information technology are touched upon. Thus, students should take a significant part in developing the competition infrastructure because the exercise offers highly valuable skill development.

Scenario details, the theme for the competition, are very important since it will primarily determine the learning objectives in the competition. It is important to mention that they are not easily used as a gauge for large-scale or global assessment of attack techniques or mitigation capabilities due to scope; the cost of equipment, space, and demands related to network isolation. Realism is paramount, but the scope should be focused on the flavor-of-the-month attacks in order to educate about, or assess relevant skill sets against, current attack methods. CANVAS 2011 focused on Smart Grid security and touched on the Stuxnet phenomenon while RMCCDC 2012 focused a bit more on web application security because they were highlights in their respective time periods.

Traditional SDLC methods do not truly fit the characteristics of developing cyber competition infrastructure at the academic level, because traditional methods are often stringent and heavy on documentation, measurements, and formal meetings. A loose group of students, part-time volunteers, and faculty would not be able to follow such a strict and formal project plan. Therefore, SCRUM is an excellent choice for adoption because it was created to ease the difficulty of managing projects that have tight time schedules, fluid requirements, and limited resources, which are all staple characteristics of cyber competition development. Additionally, SCRUM is growing in popularity in the business world due to its success in improving the effectiveness of project management, so the students and volunteers taking part in developing the competition will gain valuable experience with its use. SCRUM is compatible with the first three levels of CMMI, thereby showing that continuous process improvement can be maintained using SCRUM. Additionally, Risk Management techniques should be leveraged to minimize loss probability of cyber competition components. Using the SCRUM framework for developing cyber competition infrastructure will not only improve the successful deployment but also prepare students for following similar frameworks in their future IT careers.

References

1. The Agile Manifesto (2012), http://www.agilemanifesto.org
2. Brown, C., DeHayes, D., et al.: Methodologies for Custom Software Development. In: Managing Information Technology, 6th edn. Pearson Prentice Hall (2009) ISBN-10: 0-13-178954-6
3. Carlin, A., Manson, D., Zhu, J.: Developing the cyber defenders of tomorrow with regional collegiate cyber defense competitions (CCDC). Information Systems Education Journal 8(14) (2010) ISSN: 1545-679X, http://isedj.org/8/14/ISEDJ.814.Carlin.pdf (retrieved May 1, 2012)
4. Coyle, S., Conboy, K.: A case study of risk management in agile systems development. In: 17th European Conference on Information Systems (2009), http://www.ecis2009.it/papers/ecis2009-0642.pdf
5. Diaz, J., Garbajosa, J., Calvo-Manzano, J.A.: Mapping CMMI level 2 to scrum practices: An experience report. In: O'Connor, R.V., Baddoo, N., Cuadrago Gallego, J., Rejas Muslera, R., Smolander, K., Messnarz, R. (eds.) EuroSPI 2009. CCIS, vol. 42, pp. 93–104. Springer, Heidelberg (2009)
6. Poeter, D.: Valve's steam forums hacked, not clear if credit card number were stolen. PC Magazine, PCMag.com. (2011); http://www.pcmag.com/article2/0,2817,2396246,00.asp (retrieved March 10, 2012)
7. Potter, N.: Comparing scrum and cmmi, how they can work together. The Process Group (2010), http://www.dfw-asee.org/archive/scrum-cmmi-v1p6-45mins.pdf (retrieved)
8. Pressman, R.: Agile Development. In: Software engineering, a practitioner's approach, 6th edn., pp. 85–87. McGraw-Hill Series in Computer Science (2005) ISBN: 0-07-285318-2

9. Schwaber, K., Sutherland, J.: The scrum guide, the definitive guide to scrum: the rules of the game (2011), http://www.scrum.org/storage/scrumguides/SCRUM_Guide.pdf (retrieved May 12, 2012)
10. White, G., Williams, D.: Collegiate Cyber Defense Competitions. The ISSA Journal (October 2005), https://www.issa.org/Library/Journals/2005/October/White,%20Williams%20-%20Collegiate%20Cyber%20Defense%20Competitions.pdf (retrieved April 15, 2012)

Security Education: The Challenge beyond the Classroom

Steven M. Furnell[1,2]

[1] Centre for Security, Communications and Network Research, Plymouth University, Plymouth, United Kingdom
[2] Security Research Institute, Edith Cowan University, Perth, Western Australia
sfurnell@plymouth.ac.uk

Abstract. While it is easy to identify formal security education efforts directed towards professional programmes and academic curricula, it is arguable that the far larger population of end-users rarely benefit from such focused consideration. The paper discusses the nature of the challenge and presents survey evidence to illustrate that users are not coping with the technologies that they are expected to interact with, even when the threats concerned are relatively long-standing. Specific results are presented to show the persistence of bad practice with passwords, alongside the difference that can result if more effort were to be made to promote related guidance. Further evidence is then presented around end-user practices in relation to malware protection, suggesting that their limited understanding of the threats often leads to them protecting some devices but overlooking others. The discussion then concludes by recommending more proactive approach when targeting the end-users who may otherwise be unaware of their risks.

Keywords: Security education, End-user awareness, Passwords, Malware.

1 Introduction

As the importance of the domain has increased, there has been a corresponding growth in the range of academic programmes and professional accreditations that one can pursue in order to build and demonstrate a level of competence (e.g. see [1] for an indication of the range of available certifications). However, security issues are far more pervasive than the workplace environment, and so it is clearly not enough for efforts to focus solely upon the would-be security professionals. Indeed, the real security education challenge facing modern society goes beyond the issue of developing academic curricula and specifying appropriate bodies of knowledge from which to certify the industry practitioners, and actually represents a relevant issue for all IT users.

This paper begins by briefly evidencing the breadth and magnitude of the security awareness task that can now confront typical IT users. It then moves on to present evidence of difficulties that users can still face in dealing with long-standing security technologies when they have not been guided to use or regard them appropriately.

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 32–38, 2013.

The discussion then concludes with thought towards the more proactive stance that ought to be taken in terms of promoting and requiring security practice amongst the end-user community.

2 Too Much to Know?

It is relevant to recognise the magnitude of the challenge that now faces users in terms of understanding the various security features that are placed before them. As an example, Figure 1 presents an illustration of this, taken from the Security-related Action Center settings within Windows 8. There are a total of nine distinct aspects that users apparently need to be aware of in order to know that their operating system's security features are configured and operating correctly. Of course, most users are likely to be fine in terms of taking reassurance that things are 'On' or 'OK', but they are likely to be rather less likely to understand what it all really means. Moreover, in cases where something is showing a different status (e.g. in the Figure it can be seen that Network Access Protection is currently 'Off'), they ideally need to be able to take a view as to whether that represents a problem for them.

The real challenge is that the situation depicted in Figure 1 is by no means atypical of those that can now be regularly encountered, and the observation applies across multiple operating system platforms and end-user applications. One positive aspect is that many aspects now come pre-configured with security enabled (e.g. with OS firewalls, automatic updates, and wireless encryption all being cases where the default settings have changed from security 'off' to 'on' in the last decade or so). However, default settings will not be appropriate for all scenarios, and so if they are to make effective and informed use of the security that is available to them, users need to have a tangible baseline of knowledge and understanding, and this in turn needs to be fostered through appropriate efforts towards awareness and education. The next section proceeds to present some related evidence for these claims.

3 Evidencing the Impact of Security Education

While Figure 1 listed a range of features that can now be found on current systems, users have not even proven themselves to be competent at using the security technologies that have surrounded them for years. A classic, but nonetheless valid, example here can be provided in relation to passwords. A recent survey of 246 IT users, conducted by the author's research centre, revealed the limited extent to good password practice is actually followed. Respondents had been asked to consider the password used for their most important/valuable account, and Table 1 shows the extent to which individual aspects of practice were reflected across the respondent group. Perhaps most significantly, only 25% of respondents were able to satisfy all five points [2].

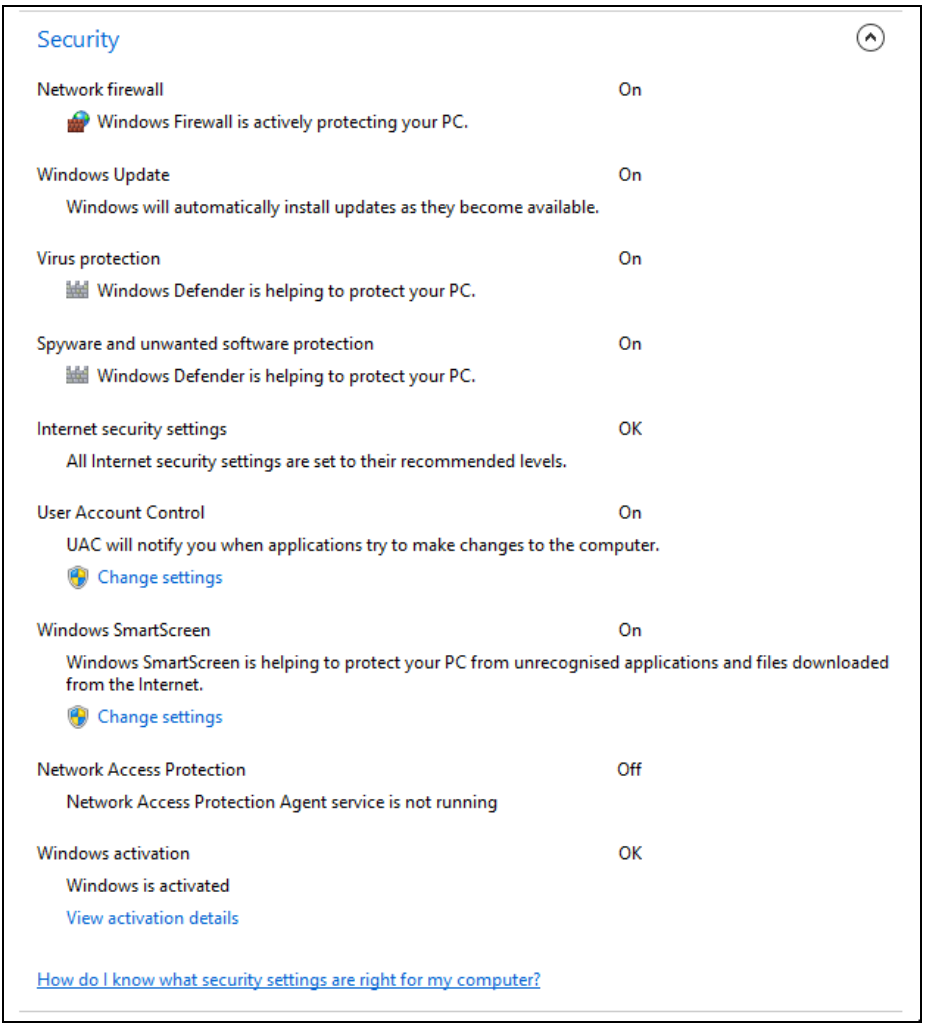


Fig. 1. Baseline security options facing end-users in Windows 8

Table 1. Responses to statements around password usage

Statement	Agreement (n=246)
It is at least 8 characters long	82%
It has alphabetic and numeric characters	84%
It includes other characters (e.g. punctuation symbols)	49%
It uses a word you would find in a dictionary	18%
It is based on personal information about me	26%

Of course, some might argue that these findings actually reflect the failing of password *technology*, which users find difficult to use properly and therefore find means to simplify in order to aid their own ease of use. However, this potentially overlooks the fact that there is often a massive weakness in the password education efforts to which such users are exposed. Not only do many organisations still do little or nothing about it (other than perhaps having a few rules, which they may *enforce* but do not *explain*), but the websites on which many users are likely to be most regularly encountering passwords also do far less than they could in order to promote and encourage good practice. For example, in an assessment of ten leading websites against their enforcement of six possible aspects of good practice (namely *enforcing* a minimum length of 8 characters and the use of multiple character types, alongside *preventing* the password choice from being the user's surname, user id the word 'password' or wider dictionary words) the overall enforcement rate was just 42% [3]. Moreover, the sites concerned were extremely inconsistent in the level of guidance that they provided to users, and while there were some cases in which comprehensive and explanatory guidance was offered, most sites seemed content with warning messages for which the underlying rationale was not explained (e.g. a Facebook message at the time would advise users that 'Your password should be more secure. Please try another.', without giving any indication of how more security might be achieved). Looking again to more recent research, we have sought to investigate whether better guidance may yield better behaviour, and the initial indications suggest that it does. Using the five points from Table 1 as a basis for good practice, 27 users were asked to created password-protected accounts as the starting point for participation in a study of website usability. Unbeknownst to the participants, there were two variants of the site – one in which password guidance was provided, and the other in which they were left to select passwords unaided (with neither case actually *enforcing* any password rules). There were notable differences in the results, with the guided group (n=13) scoring an average of 3.8/5, against just 1.9/5 from the unaided (n=14) group [2]. Analysis revealed that areas such as password length, use of other characters, and avoidance of personal information were the ones most likely to be improved by the provision of the guidance. Thus, what this can arguably be shown to illustrate is that education and awareness can have a tangible effect upon the users' behaviour with a technology that they would otherwise be inclined to use badly.

4 Knowing a Little, But Not Enough

While it would be rare these days to find users that are totally ignorant of the risks to be faced online, it would be equally fair to say that while users often have an awareness of certain threats that can affect them, the *extent* of their knowledge does not stretch very far. A very good example here relates to the threat of malware, which (like passwords) can now be regarded as a long-standing aspect of the user-facing security landscape. Indeed, antivirus protection is now a very commonplace safeguard on PCs in both home and workplace contexts. However, there is again evidence that users' real understanding of the threat has not kept pace with the technology that they

are using, and this is particularly apparent in relation to mobile devices such as smartphones and tablets, where recent years have seen a sizeable increase in the actual threat). For example, while the problem had been largely theoretical for many years (but with predictions having been made by antivirus vendors since the mid-2000s), the period around 2011/12 saw the market conditions become such malware writers began to take a more active interest. Key aspects were the emergence of a sizeable population of device owners, and the fact that sufficient of them was using an OS platform that could be targeted. As a consequence, according to figures from Kaspersky Lab, 2012 saw a massive rise in the number of malicious programs on the Android platform, rising from less than 6,000 at the start of the year to over 43,000 by the end [4]. Android was consequently playing host to over 99% of the malicious programs identified on mobile platforms (which is in part thanks to its more open app distribution process when compared to its main competitor, iOS, where apps have to pass an approval process before being placed on the platform's official App Store), and thus attracting a significantly disproportionate share of the mobile malware when compared to its share of the mobile device market.

The clear message here is an increasing threat to the associated user population, but returning again to the survey of 246 end users, it would appear to be a message that is not naturally getting through. From this group, 28 of them had an Android-based mobile device, but only 19% of these had antivirus protection for it. While it could be argued that this small sample might just be an unrepresentative group of security-resistant users, an interesting point to note was that 82% of the same sub-group had antivirus protection on their traditional PC. As such, it seems likely that lack of awareness rather than lack of regard for security may have been the main reason for so many more mobile devices going unprotected. This situation suggests that if the risks of new platforms are not overtly communicated, users currently seem to have little ability to take the lessons learned in one context (e.g. the desktop PC) and apply them to another (e.g. the mobile device).

5 Recommendations and Conclusions

The evidence above points towards a clear need for security education in the wider context, as there is enough evidence from successive and sustained cases of bad practice to show that they are not skills that users can be relied upon to naturally possess or develop as part of their wider IT development. If the situation is to improve, then the obvious answer is that something more proactive needs to be done about it. However, this is again an area in which attempts have historically been poor, even within workplace contexts. For example, findings from Ernst & Young's Global Information Security Survey 2012 revealed that while the top-rated area of risk-exposure was 'careless or unaware employees' (ranked first out of 16 threats/vulnerabilities, and rated first choice by 37% of respondents), the issue of 'Security awareness and training' was ranked as a top security priority by only 9% (placing it 17th out of twenty possible areas), thus showing a clear disconnect between the problem and what organisations are prepared to do about it [5]. Without a

tangible uplift in terms of attention and investment, it seems unlikely that the issue will heal itself automatically.

The onus is to increase threat awareness for private individuals and staff within organisations. While much of the responsibility for the latter must still rest with employers (and so can also be seen to be within their control), the issue of wider public awareness requires necessarily broader steps to be taken. Recent years have already seen some notable activities in this direction, with a European example being the introduction of a Cyber Security Month [6], which took place for the first time in October 2012. However, one of the main findings documented from this was the need to "Better define the specific audience that is targeted by the awareness initiative in order to tailor the message content to the target group's knowledge or technical aptitude" [7], which serves to illustrate the ongoing challenge that awareness-raising is likely to pose.

In many ways, the way in which users are encouraged to think about their IT devices is still based around the wrong model. While they are routinely purchased in the same manner as other consumer electronics devices, a more appropriate parallel can be made to the purchase of a car. With a car there is an upfront recognition that the driver needs to be competent in order to use it safely, and that the car itself is expected to be fitted with a range of safety and protection features, and that the vehicle needs to be appropriately maintained if it is to continue to operate correctly. While it would not be realistic to regulate IT usage to quite this degree, there are nonetheless some steps that could be taken to alter the mindset around it. As an example, here are a few related thoughts:

- There needs to be something that clearly highlights and explains the key issues for new users as they take product home. While there is often plenty of material to be found for those inclined to go looking for it (e.g. in the UK a good user-facing resource is provided by GetSafeOnline,org), many people will not be aware enough to look for this in the first place. Even the provision of a leaflet in the box with the product could go a long way to raising upfront awareness.
- Users need to be encouraged to be aware of security issues and practices from their early encounters with IT. Inclusion of security education as a 'key skill' within school and university curricula would be a relevant contribution here, thus ensuring that relevant baseline exposure is provided for all users, rather than just those that have chosen to study the topic as the basis for a career. This does not equate to turning everyone into security experts, but rather to ensure that protection issues are given an effective level of emphasis as part of any wider introduction to IT usage.
- Increase the expectation (and perhaps obligation) to use appropriate safeguards. While many devices will now be provided with software such as antivirus or wider Internet Security suites as part of the bundle, it is still perfectly possible to purchase and use PCs without this being in place. Clearly there still needs to be a place for consumer choice over products, and competition between associated vendors, but it ought to become a question of *what* product to have rather than *whether* to have one). Moreover, looking

at the wider context of online devices, there is currently far less of an established culture of bundling protection with smartphones and tablets, but they (and their users) are becoming equally in need of protection.

While the paper is unable to report the results of putting such ideas into practice, this is clearly no basis to accept the status quo. Indeed, what we *can* see from the findings of the earlier studies is the result of the current approach. In the meantime, security educators should take the opportunity to push their messages to as wide an audience as possible, in order to raise awareness and support a more effective security culture amongst the public at large.

References

[1] Goodchild, J.: The Security Certification Directory, CSO Online (October 24, 2012), http://www.csoonline.com/article/485071/the-security-certification-directory (accessed April 25, 2012)

[2] Furnell, S., Bär, N.: Essential lessons still not learned? Examining the password practices of end-users and service providers. To Appear in Proceedings of HCI International 2013, Las Vegas, Nevada, July 21-26 (2013)

[3] Furnell, S.: Assessing password guidance and enforcement on leading websites. Computer Fraud & Security, 10–18 (December 2011)

[4] Kaspersky Lab. Today's Mobile Threatscape: Android-Centric, Booming, Espionage-friendly, Virus News (February 28, 2013), http://www.kaspersky.com/about/news/virus/2013/Todays_Mobile_Threatscape_Android_Centric_Booming_Espionage_friendly

[5] Ernst & Young. Fighting to close the gap – Ernst & Young's Global Information Security Survey (2012), EYG no. AU1311, http://www.ey.com/giss2012

[6] ENISA. European Month of Network and Information Security for All - A feasibility study (December 14, 2011) ISBN-13 978-92-9204-056-7

[7] ENISA. Be Aware, Be Secure. Synthesis of the results of the first European Cyber Security Month (December 17, 2012) ISBN 978-92-9204-063-5

Background to the Development of a Curriculum for the History of "Cyber" and "Communications" Security

William Caelli[1], Vicky Liu[1], and Dennis Longley[2]

[1] Science and Engineering Faculty, Queensland University of Technology, 2 George Street, Brisbane, Qld. Australia
w.caelli@iisec.com.au, v.liu@qut.edu.au
[2] International Information Security Consultants Pty Ltd, 21 Castle Hill Drive South, Gaven, Qld. Australia
d.longley@iisec.com.au

Abstract. For any discipline to be regarded as a professional undertaking by which its members may be treated as true "professionals" in a specific area, practitioners must clearly understand that discipline's history as well as the place and significance of that history in current practice as well as its relevance to available technologies and artefacts at the time. This is common for many professional disciplines such as medicine, pharmacy, engineering, law and so on but not yet, this paper submits, in information technology. Based on twenty five elapsed years of experience in developing and delivering cybersecurity courses at undergraduate and postgraduate levels, this paper proposes a rationale and set of differing perspectives for the planning and development of curricula relevant to the delivery of appropriate courses in the history of cybersecurity or information assurance to information and communications technology (ICT) students and thus to potential information technology professionals.

Keywords: information assurance education, cybersecurity education, data network security, Internet security, history of computing, history of communications technology, information security, convergence.

1 Introduction

Why teach the history of cybersecurity and/or information assurance? The answer is that at least three distinct themes can be determined in relation to the position of cybersecurity/information assurance history in the creation, development and presentation of courses of study in the area. These are:

1. any profession that claims to be so, acknowledges and builds upon its history;
2. the profession of cyber and network security or information assurance should be no different in this way from any other profession such as medicine, law, science, military affairs and others and should build upon general education in the ICT area for both specialist and general professional activity in the discipline, and

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 39–47, 2013.

3. the challenge is to make such history relevant to students in the age of total convergence in the information technology area and to relate it to current practice, products and systems.

The environment in which an educated cybersecurity professional will practice has been envisaged by Al Gore, former Vice-President of the USA in the following way in his book *"The Future"* [1]:

"The emergence of a planet-wide electronic communications grid connecting the thoughts and feelings of billions of people and linking them to rapidly expanding volumes of data, to a fast growing web of sensors being embedded ubiquitously throughout the world, and to increasingly intelligent devices, robots, and thinking machines, the smartest of which already exceed the capabilities of humans in performing a growing list of discrete mental tasks and may soon surpass us in manifestations of intelligence we have always assumed would remain the unique province of our species; "

Given this scenario, vaguely reminiscent of the envisaged *"Noosphere"* of Vernasky and Chardin [2] and even the planetary intelligent machine of the *"Krell"* in the 1952 movie, *"The Forbidden Planet"*[3], loosely based on a Shakespearean play, the security and protection of such an information environment takes on new meaning and urgency.

In summary, for any discipline to be regarded as a "professional" undertaking, and whose members may then be accepted and treated by society at large as true "professionals" in that specific area, the discipline must ensure that its practitioners clearly understand that discipline's history as well as the place and significance of that history in current practice. This includes a clear understanding of the *"what/how/why"* of currently available technologies, including professional practice procedures and the like, as well as of ICT artefacts, including base products, integrated systems, services, etc.. This commonly forms an educational base for many professional disciplines such as medicine, pharmacy, engineering, law and so on but not yet, this paper submits, for information technology although references have been made to such histories on some curricula proposals and final versions as discussed later. This paper discusses such history against the consideration of the need for education and training of specific cybersecurity/information assurance professionals. The specific case of education and training in military level cyber-operations is not included in this discussion but is worthy of further analysis. It also has resonance with the more general requirements for cybersecurity awareness in any ICT education program.

Based on twenty five elapsed years of experience in developing and delivering cybersecurity courses at undergraduate and postgraduate levels, this paper proposes a rationale and set of differing perspectives for the development of curricula relevant to the delivery of an appropriate course in cybersecurity history to information and communications technology (ICT) students and thus potential information technology professionals. It does not propose specific curricula in a normal sense, as a set of topics, learning outcomes and the like but rather discusses the bases on which such selections could be made. It proposes particular emphasis on explanation of historical matters as these relate to information technology from differing perspectives which must be understood and catered for by the ICT professional in practice, e.g. interactions with users, managers and other ICT professionals. Particular emphasis is placed on the role of the ICT "professional" through education at the university

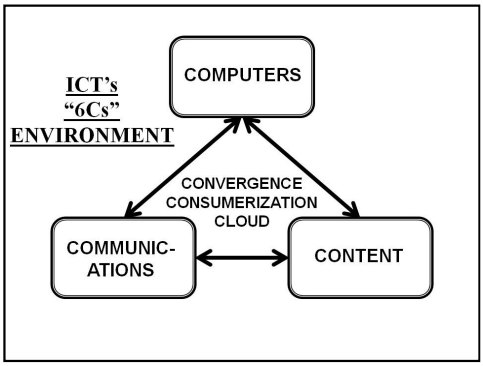


Fig. 1. 6C Environment for ICT

undergraduate level in general as well as via specialised postgraduate cybersecurity program. It proposes that the basis for this curriculum could be set out on the grounds of perception of four distinct generations of information technology professionals within the information technology and data communications network environments in which they worked along with the growing perception of the related science and technology. One aim is to be able to invigorate students in a way that enables them to be able to understand and appreciate the background to any current cybersecurity product, system or service offering from, or claim made by, the ICT industry in general and the specific cybersecurity industry more particularly. The aim is to cover such developments over the last 50 to 60 years in both technological and societal contexts, winding up in an age of total convergence of computers, communications and content (3C) and to thus provide students with an engaging insight into "how we got here" and "why" products, systems and services are what they are and/or what they should be. A particular emphasis is placed on relating this history to the requirements of protection in a globally connected information services environment based around associated data networks and the environments in which new graduates will be employed.

Simply put, the current information environment may be considered the result of convergence of computers, communications and content, commonly referred to here as 3C. Further, 3C has to be considered in the context of a further set of three factors. These include the convergence just mentioned, consumerisation of the ICT products, systems and services offered by the industry itself and finally the result of "cloud" computing service offerings on an international scale that brings a global information environment service into being, together nominated in Figure 1 as the "6C" situation.

2 Roles and Functions of the ICT and Cybersecurity Professional

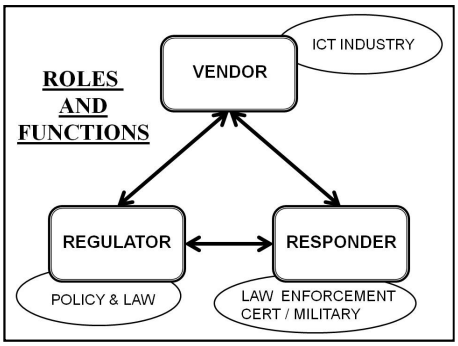


Fig. 2. Roles and Functions

Depending upon where an ICT or cybersecurity professional finds their professional practice employed, their responsibility, and thus need to understand the historical background to the discipline, may be tailored as needed. As illustrated in Figure 2, roles played and functions undertaken may vary between activities:

* within a traditional ICT vendor, under the usually accepted meaning of the term "ICT industry", as distinct from users or

consumers of its products, systems or services but including development of applications for such technologies and artefacts for sale or deployment;
* related to the role of an appropriate regulator responsible for associated policy, law and regulation in the cybersecurity realm; and
* associated with a responder to attacks on or malfunction of information systems including law enforcement and military entities, internal or external response teams, etc.

3 Structures and People

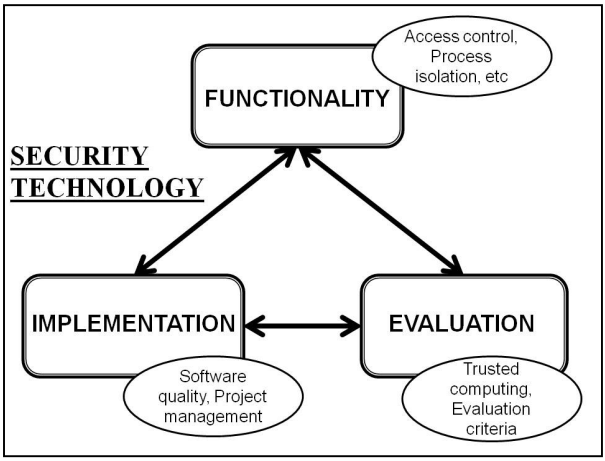


Fig. 3. Security Technology

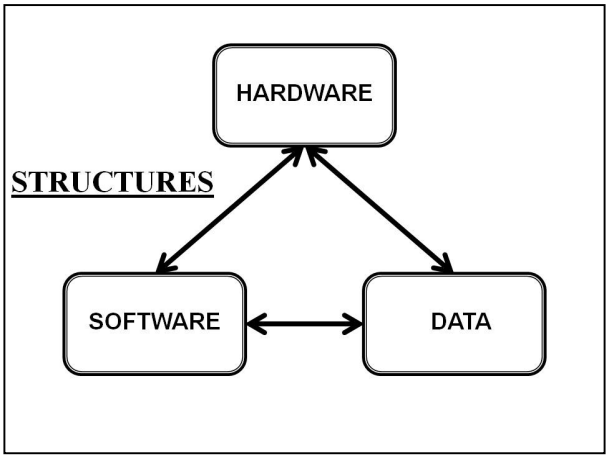


Fig. 4. Structures relevant to Cybersecurity

The existence of underlying security technologies and systems in any information system can be seen as being related to three distinct aspects, viz. hardware, software and data as in Figure 3. In turn, the historical context of the development of associated security technologies in each of these areas sets the scene for today's product, systems and services offerings. For example, the computer and data network "add-on" security industry is now a very large global activity that, it could be argued, owes its very existence to the failure of the normal ICT industry to provide adequate, proven and reliable security features within the base products it offers. Thus, it is necessary to understand the historical context to the three aspects, again, of any information security product or system. Its functionality specification, its reliable and verifiable implementation in a secure

manner itself and, finally, its independent evaluation must be determined by the ICT professional as being fit for the purpose claimed, as illustrated in Figure 4.

4 Policy, Laws and Regulations

The cybersecurity professional will be involved in either development of public policy and law/regulations relevant to information systems or responsible for the interpretation and implementation of relevant technologies, products, systems, services, policies and procedures for an owner/manager of that information system or even a combination of both of these. At the extreme end of the ”spectrum”, the ICT cybersecurity professional may be regarded as a member of the military, involved in cyber operations in response to attack or a member of law enforcement / response teams concerned with investigation of such attacks. In this sense the cybersecurity professional may take on a role of user, manager or professional in the ICT area or be responsible for liaison with people designated in those functions, as illustrated in Figure 5. The question is one of creating appropriate educational curricula to meet these varying situations and requirements. Examples assist in clarifying these concepts. The cybersecurity professional may be responsible for the creation and dissemination of user procedures for use of information system resources in a company, including, for example development and propagation of a bring-your-own-device (BYOD) policy. At the management level, the cybersecurity professional should normally be involved, but often is not, in the requirements definition and procurement activities related to information systems creation and deployment. In this case, for example, some form of labelled “mandatory access control (MAC)” functionality may be favoured over “discretionary access control (DAC)” but this must be specified at procurement time.

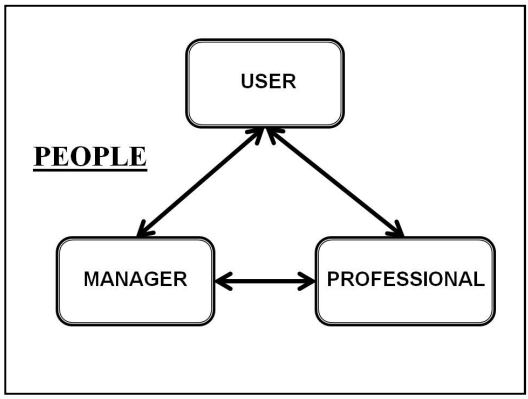


Fig. 5. People / roles and functions

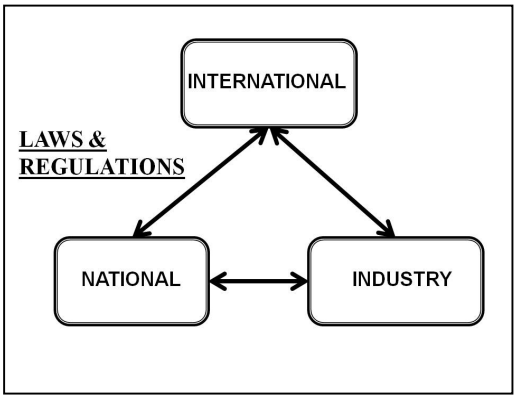


Fig. 6. Legal and Regulatory Regimes

The cybersecurity professional must in turn become familiar with the relevant legal and regulatory

regimes appropriate to the enterprise involved, including consideration of these parameters at the international, national and industry levels, as in figure 6. Examples here may range for export restrictions on advanced cryptographic systems under the *"Wassenaar Arrangement"* [4] to industry specific regulations, such as the USA's HIPAA requirements for the healthcare industry at a national level and then to PCI-DSS contractual obligations in the payment card area.

5 Real Curricula and Industry Training

At present it appears that full elucidation of the history of information assurance, information security or cybersecurity, under whichever term it may be defined, and the significance of that history in explaining the "why" of current information assurance schemes is severely limited if not totally lacking. For example, the following topics may illustrate the problem:

- *"C2 by '92"* [5] and the failure of mandatory regulations in information assurance in the USA for government/defence procurement;
- the Microsoft *"Palladium / NGSCB"* [6] project for the "hardening" of the Windows based PC in the early 2000s;
- IS 7498-2 [7] and the security architecture for the open systems interconnection (OSI) model and structures for computer connectivity on a global scale;
- the *"Rainbow Series"* of specifications for "trusted computing" from the USA's Department of Defense, particularly the preface to the 1983 *"Orange Book"* or *"TCSEC / Trusted Computer Systems Evaluation Criteria"* explaining the rationale for the publication[1];
- the MULTICS memory segmentation and capability architecture and associated "ring" protection scheme, later embedded into the Intel iAPX-286 and later microprocessors, and so on.
- market failure of "B2" / mandatory access control based, or similarly oriented, operating systems such as Digital Equipment Corporation's (DEC) SEVMS, Gemini Inc. GEMSOS, Secure XENIX, USA's National Security Agency's (NSA) SELinux and SE Android, etc.
- development of the *"Wassenaar Arrangement"* covering export of "dual-use" technologies and artefacts including cryptographic systems and advanced secure computer systems as well as reverse engineering technologies;
- lack of incorporation or acceptance of appropriate and defined security structures into the overall Internet TCP/IP and DNS structures; and so on.

[1] "The criteria were developed with three objectives in mind: (a) to provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information; (b) to provide guidance to manufacturers as to what to build into their new, widely-available trusted commercial products in order to satisfy trust requirements for sensitive applications; and (c) to provide a basis for specifying security requirements in acquisition specifications.

Some curricula already exist in the information assurance area and even, by implication, in the cybersecurity/cyber operations arena. Examples of these follow.

a. IEEE/ACM
The November 2012 *"Ironman"* version [8] of the IEEE/ACM's body of knowledge (BOK) definition in the area of "information assurance and security" has been published as document CS2013 as part of the overall computer science curriculum. It acknowledges that the situation in this area is "unique" in that relevant matter overlap with all the other areas defined in the computer science curriculum. It states as follows:
"In CS2013, the Information Assurance and Security KA is added to the Body of Knowledge in recognition of the world's reliance on information technology and its critical role in computer science education. Information assurance and security as a domain is the set of controls and processes both technical and policy intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, and confidentiality and providing for non-repudiation. The concept of assurance also carries an attestation that current and past processes and data are valid. Both assurance and security concepts are needed to ensure a complete perspective. Information assurance and security education, then, includes all efforts to prepare a workforce with the needed knowledge, skills, and abilities to protect our information systems and attest to the assurance of the past and current state of processes and data."

However, any historical perspective in this area is separated into an overall "history of computing" section in the BOK. However, the complexity related to inclusion of information assurance curricula into IT programs aimed at the development of the normal IT professional has been a topic of discussion for many years and was clearly alluded to in the earlier ACM IT curriculum guidelines of 2008 [9].

b. USA – Committee on National Security Systems
Documents labelled broadly as *"4011"* to *"4016"* set out "training" requirements for various positions in relation to information assurance functions within the USA's Federal Government, Department of Defense and allied organisations [10]. The history of information security gets mentioned but does not receive any detailed analysis of its place in the educational program.

c. International Information Systems Security Certifications Consortium (ISC^2) – $CISSP^2$
This organisation, established in 1989, has developed a certification program for information security professionals given the "*Certified Information Systems Security Professional (CISSP")* designation. It has associated with it a *"Common Body of Knowledge (CBK)"*. The process of personal accreditation under the scheme involves

[2] One of the authors, Caelli, is a Fellow of ISC^2.

study and examination coupled with designated years of experience for various levels of certification, now expanded beyond the original CISSP. The CBK is described by ISC[2] as follows:
"The (ISC)² CBK is a taxonomy - a collection of topics relevant to information security professionals around the world. The (ISC)² CBK establishes a common framework of information security terms and principles which allows information security professionals worldwide to discuss, debate, and resolve matters pertaining to the profession with a common understanding."
It sets out a number of domains relevant to the security professional but does not emphasize the historical background to the domains of interest that are set out.

d. Universities and Colleges
Many universities and colleges in the USA participate in that country's *"National Centers of Academic Excellence (CAE)"* program of its National Security Agency and Department of Homeland Security [11]. These educational institutions, however, adhere to the defined CNS and related curricula. In the separate NSA sponsored area of "cyber operations" education a separate curriculum is published with particular emphasis on the data networking arena. Many also participate in the activities of the *"Colloquium for Information Systems Security Education (CISSE)*[3]", a not for profit society based in Maryland, USA.

e. Other Organisations

i) ISACA[4]
This organisation, formerly the *Information Systems Audit and Control Association*, now just uses its acronym as its name. It also offers a range of industry certifications knows as CISA/CISM/CGEIT/CRISC depending upon an individual's role and certification requirements. In an established manner ISACA publishes its knowledge requirements list as the *"2013 Candidate's Guide to the CISM ® Exam and Certification"*. Once again, while acknowledged, the historical context to the various topics outlined is not given any detailed reasoning or background. Concentration is largely, as may be expected, on the "what" and "how" of the topics.

ii) SANS Institute, EC-Council, CREST (UK) and others.
Other industry level organisations also exist to provide information assurance education and training. Once again, however, the concentration is on the "what and how" aspects of cybersecurity with some emphasis on sub-sets of the overall information assurance area, e.g. CREST (UK) which describes itself as follows: *" The Council for Registered Ethical Security Testers. CREST exists to serve the needs of a global information security marketplace that increasingly requires the services of a regulated and professional security testing capability."*

[3] One of the authors, Caelli, is a member of the Board of CISSE.
[4] One of the authors, Caelli, is an Honorary CISM of ISACA.

6 Conclusions

A trained cybersecurity technician should be able to readily answer questions related to the "what and how" of any relevant information security matter. However, a cybersecurity professional should be readily able to answer the *"Why is it so?"* question, the catch-phase of the late Professor Julius Sumner Miller, a prominent physics educator and TV presenter [12]. While numerous industry based education and training groups exist and offer various levels of certification, many of which are accepted by both the private sector and government organisations, including defence related entities, curricula do not emphasize historical background to the topics outlined and thus the "why" of many aspects of information assurance / cybersecurity.

References

1. Gore, Al: The Future: Six Drivers of Global Change, Random House (2013)
2. Noosphere, http://en.wikipedia.org/wiki/Noosphere
3. The Forbidden Planet, http://en.wikipedia.org/wiki/Forbidden_Planet
4. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, http://www.wassenaar.org/
5. Computers at Risk: Safe Computing in the Information Age. National Academies Press (1990)
6. Levy, S.: The Big Secret: An exclusive first look at Microsoft's ambitious plan to remake the personal computer to ensure security, privacy and intellectual property rights. Will you buy it? Newsweek (July 1, 2002)
7. ISO 7498-2:1989: Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture, http://www.iso.org
8. Computer Science Curricula 2013, Ironman Draft (Version 1.0) (February 2013), http://ai.stanford.edu/users/sahami/CS2013/ironman-draft/cs2013-ironman-v1.0.pdf
9. Lunt, B., et al.: Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. ACM/IEEE (2008)
10. Committee for National Security Systems, http://www.cnss.gov
11. National Centers of Academic Excellence, http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml
12. Wikipedia entry, http://en.wikipedia.org/wiki/Julius_Sumner_Miller

Information Assurance and Security in the ACM/IEEE CS2013

Ronald C. Dodge

United States Military Academy, West Point, NY, USA
ronald.dodge@usma.edu

Abstract. The ACM/IEEE Computing Curriculum 2013 is a community effort with representation from Academia and industry to outline curricular recommendations for undergraduate Computer Science degree programs. The effort began in 1968 [1] and conducts a complete review every ten years. The previous complete review was completed in 2001. [2] The current 2013 review is being developed to incorporate rapidly changing topics as technology and the world's use of technology evolves; however must do so within the curricular constraints of a complete undergraduate curriculum. The construction of the CS2013 is due for completion in December 2013. This effort describes the architecture of CS2013 and the details of the creation of a new knowledge area for Information Assurance and Security in the CS2013 computing curriculum.

1 Introduction

The world that our undergraduates must be prepared to succeed in is changing rapidly. Topics or study areas that seemed critical when a student began his or her undergraduate program may be out of date or encompassed by another emerging topic by the time they graduate. The Association for Computing Machinery and the Institute of Electrical and Electronics Engineers Computer Society (IEEE CS) has a long standing interest in providing input into the educational programs, teaching the future professionals in the field. Since 1968 [1], a joint commission from the two bodies has created a set of curricular recommendations for institutions to use in shaping the Computer Science undergraduate curriculum. This effort has traditionally been fully reviewed every 10 years with a minor interim assessment at the five year mark. The last major review was completed in 2001 and the interim review was completed in 2008. [2][3] Each new version of the ACM/ IEEE Computing Curriculum provides an opportunity for undergraduate Computer Science programs to review and assess their curriculum against a community constructed set of objectives. The process this year included many changes from previous years, including formally creating a knowledge area for Information Assurance and Security. This new knowledge area is unique among the slate of 18 knowledge areas due to its prevalence throughout all knowledge areas. In this paper, we begin in section two by providing further discussion of the CS2013 process and structure. In section three, we discuss in depth the Information Assurance and Security knowledge area. In section four, we conclude

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 48–57, 2013.

with observations about the general state if institutions capacity to support the security goals of the CS2013 Body of Knowledge.

2 The Joint ACM/ IEEE Computer Science 2013

The ACM and IEEE-Computer Society chartered the CS2013 effort with the following directive:

> *To review the Joint ACM and IEEE-CS Computer Science volume of Computing Curricula 2001 and the accompanying interim review CS 2008, and develop a revised and enhanced version for the year 2013 that will match the latest developments in the discipline and have lasting impact.*
>
> *The CS2013 task force will seek input from a diverse audience with the goal of broadening participation in computer science. The report will seek to be international in scope and offer curricular and pedagogical guidance applicable to a wide range of institutions. The process of producing the final report will include multiple opportunities for public consultation and scrutiny*

The ACM and IEEE each appointed two co-chairs to manage the process and select the steering committee members. The group began work in the fall of 2010, beginning its work by reviewing the previous ACM/IEEE computing curriculum body of knowledge and preparing a survey to collect and validate existing topics and identify new and emerging requirements. The committee has met approximately every six months in person, supported with monthly teleconferences. The analysis resulted in the committee establishing the following goals:

1. Computer Science curricula should be designed to provide students with the flexibility to work across many disciplines.
2. Computer Science curricula should be designed to prepare graduates for a variety of professions, attracting the full range of talent to the field
3. CS2013 should provide guidance for the expected level of mastery of topics by graduates.
4. CS 2013 must provide realistic, adoptable recommendations that provide guidance and flexibility, allowing curricular designs that are innovative and track recent developments in the field.
5. The CS2013 guidelines must be relevant to a variety of institutions.
6. The size of the essential knowledge must be managed.
7. Computer Science curricula should be designed to prepare graduates to succeed in a rapidly changing field.
8. CS2013 should identify the fundamental skills and knowledge that all computer science graduates should possess while providing the greatest flexibility in selecting topics.

9. CS2013 should provide the greatest flexibility in organizing topics into courses and curricula.
10. The development and review of CS2013 must be broadly based.

The review of the prior bodies of knowledge and the feedback from a survey (described in paragraph 2.1) established the initial set of knowledge areas (KA). In this set of 18 KA's, six new areas emerged. Of particular note is the inclusion of the Information Assurance and Security Knowledge Area (IAS). Each KA was assigned a chair and at least two other committee members.

- AL-Algorithms and Complexity
- AR-Architecture and Organization
- CN-Computational Science
- DS-Discrete Structures
- GV-Graphics and Visual Computing
- HCI-Human-Computer Interaction
- IAS-Information Assurance and Security (new in 2013)
- IM-Information Management
- IS-Intelligent Systems
- NC-Networking and Communication (new in 2013)
- OS-Operating Systems
- PBD-Platform-based Development (new in 2013)
- PD-Parallel and Distributed Computing (new in 2013)
- PL-Programming Languages
- SDF-Software Development Fundamentals (new in 2013)
- SE-Software Engineering
- SF-Systems Fundamentals (new in 2013)
- SP-Social Issues and Professional Practice

As the subcommittees produced drafts of their Knowledge Areas, others in the community were asked to provide feedback, both through presentations at conferences and direct review requests. The Steering Committee also collected community input through an online review and comment process. The KA subcommittee Chairs (as members of the CS2013 Steering Committee) worked to resolve conflicts, eliminate redundancies and appropriately categorize and cross-reference topics between the various KAs. Thus, the computer science community beyond the Steering Committee played a significant role in shaping the Body of Knowledge throughout the development of CS2013. This two-year process ultimately converged on the version of the Body of Knowledge presented in the IronMan draft. [4]

2.1 Survey Input

The development work of creating the initial set of KA's to include in the overall body of knowledge relied heavily on two measures of input; prior ACM/IEEE computer science curriculum work and a survey distributed to institutions worldwide.

The purpose of the survey was to gather information on area of knowledge that had either increased or decreased in importance. The survey was sent to over 3500 institutions (1500 in the United States and 2000 internationally), addressed primarily to Computer Science (and related discipline) department chairs and directors of undergraduate studies. The response rate was unfortunately lower than desired (201 responses), however produced valuable input. The respondents represented a wide variety of institution type and size:

- research-oriented universities (55%)
- teaching-oriented universities (17.5%)
- undergraduate-only colleges (22.5%)
- community colleges (5%)

- less than 1,000 students (6.5%) 77
- 1,000 to 5,000 students (30%) 78
- 5,000 to 10,000 students (19%) 79
- more than 10,000 students (44.5%)

2.2 Overview of the CS2013 Body of Knowledge Structure

There are two fundamental concepts for the Body of Knowledge. The first and most fundamental is that the Knowledge Areas *are not* intended to correlate directly to a specific course. The intent is not to imply any restriction on how an institution may desire to address any of the content. The second concept is the tiered approach to describing the importance of given content. The Body of Knowledge is structure hierarchically as shown in Figure 1

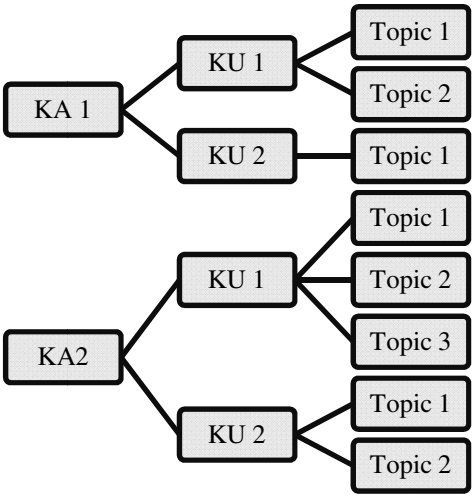


Fig. 1. Body of Knowledge Structure

Each KA (as listed in paragraph 2), is broken down into sub areas called Knowledge Units. Each Knowledge Unit is described by a collection of topics and related learning outcomes. The learning outcomes are also represented by three degrees of mastery:

- ***Familiarity***: The student understands what a concept is or what it means.
- ***Usage***: The student is able to use or apply a concept in a concrete way.
- ***Assessment***: The student is able to consider a concept from multiple viewpoints and/or justify the selection of a particular approach to solve a problem.

As described earlier, it is expected that topics will span multiple courses. The topics are identified as either core-tier 1, core-tier 2, or elective. The core-tier 1 and core-tier 2 topics are further described by the number of hours that is expected within the undergraduate computer science curriculum. Each hour is reflective of the lecture or supervised learning hours within which the topic is one of the key learning objectives. These hours along with the learning outcomes are intended to provide guidance on the depth of coverage. Understanding that not all programs would or should be alike, the following guidance is provided:

- A curriculum should include all topics in the Tier-1 core and ensure that all students cover this material.
- A curriculum should include all or almost all topics in the Tier-2 core and ensure that all students cover the vast majority of this material.
- A curriculum should include significant elective material: Covering only "Core" topics is insufficient for a complete curriculum.

A much more detailed discussion of the motivation and philosophy behind the body of knowledge may be found in [4].

3 CS2013 Information Assurance and Security Knowledge Area

The Information Assurance and Security Knowledge Area is new in the CS2013 Body of Knowledge. It was clear both in the analysis from the steering committee and the survey results, that the broad range of topics defined by information security are an essential component of any undergraduate computer science program. This new KA was proposed as part of the very first steering committee meeting. During the World Conference on Information Security Education (WISE 7) in June, 2011, organized by an internationally focused IFIP technical working group (WG 11.8), the topic was discussed and further refined to use the title "Information Assurance and Security".

Information assurance has been defined as "a set of controls (technical and policy) intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection,

detection, and reaction capabilities."[5] [6] This concept of assurance also carries a connotation of an attestation that past processes or data is valid.

Information assurance and security education, then, includes all efforts to prepare a workforce with the needed knowledge, skills, and abilities to assure our information systems and attest to the validity of the current state of processes and data. Information assurance and security education has been growing in importance and activity for the past two decades.

The McCumber model [7] [8] has been widely used over the past 10 years to broadly define the relationships between information states, security services, and security operations (called counter measures in the original model). As the security and assurance landscape has matured, the relationships should be clarified to address that the full spectrum operational aspect of security is not correctly contained by the term counter measures and that emergence of assurance of processes (current and past) is playing a critical role in the field of IAS.

3.1 The Construction of the IAS KA

The aim of the IAS KA is to define the core (core-tier1 and core-tier2) and elective knowledge threads that depict what a computer science undergraduate should possess upon graduation.

The IAS KA is unique in the collection of KA's due to its pervasive nature in all KA's. One can express this cross cutting impact by comparing security to performance. In the past, many concepts in Computer Science were performance based. Algorithms were developed to increase the performance of memory utilization or database searches. In this light, the way we do things in Computer Science must be done securely. This is not to say that Information Assurance and Security does not have concepts that belong solely to the IAS KA. As shown in table 1, concepts that are unique to IAS are listed with specific core tier 1 and tier 2 hours.

Table 1. Information Assurance and Security Knowledge Units/Hours

Knowledge Unit	Core-Tier1	Core-Tier2	Electives
IAS/Foundational Concepts in Security	1	-	N
IAS/Principles of Secure Design	1	1	N
IAS/Defensive Programming	1	1	Y
IAS/Threats and Attacks	-	1	N
IAS/Network Security	-	2	Y
IAS/Cryptography	-	1	N
IAS/Web Security	-	-	Y
IAS/Platform Security	-	-	Y
IAS/Security Policy and Governance	-	-	Y
IAS / Digital Forensics	-	-	Y
IAS/Secure Software Engineering	-	-	Y

Each knowledge unit contains a collection of topics. For the knowledge unit, "IAS/Principles of Secure Design", the topics are shown below. Each topic has an associated learning outcome with a desired level of comprehension (Familiarity, Usage, and Assessment). While we also list the topics associated with the other KU's with the IAS KA, further detail (learning outcomes) and elective topics are left for review in [4]. As detailed below in the Principles of Security Design, the topics document cross reference locations where the referenced topic is also presented in another KA. As an example, the cross reference for the very first topic, "least privilege and isolation" extends to the KA's for Operating Systems, System Fundamentals, and Programming languages. Those references are listed after the Principles of Security Design.

IAS/Principles of Secure Design [1 Core-Tier1 hours, 1 Core-Tier2 hours]
Topics:
[Core-Tier1]

- Least privilege and isolation (cross-reference OS/Security and Protection/Policy/mechanism separation and SF/Virtualization and Isolation/Rationale for protection and predictable performance and PL/Language Translation and Execution/Memory management)
- Fail-safe defaults (cross-reference SE/Software Construction/ Coding practices: techniques, idioms/patterns, mechanisms for building quality programs and SDF/Development Methods/Programming correctness)
- Open design (cross-reference SE/Software Evolution/ Software development in the context of large, pre-existing code bases)
- End-to-end security (cross reference SF/Reliability through Redundancy/ How errors in-crease the longer the distance between the communicating entities; the end-to-end principle)
- Defense in depth
- Security by design (cross reference SE/Software Design/System design principles)
- Tensions between security and other design goals

[Core-Tier 2]

- Complete mediation
- Use of vetted security components
- Economy of mechanism (reducing trusted computing base, minimize attack surface) (cross reference SE/Software Design/System design principles and SE/Software Construction/Development context: "green field" vs. existing code base)
- Usable security (cross reference HCI/Foundations/Cognitive models that inform interaction design)
- Security composability
- Prevention, detection, and deterrence (cross reference SF/Reliability through Redundancy/Distinction between bugs and faults and NC/Reliable Data Delivery/Error control and NC/Reliable Data Delivery/Flow control)

Learning outcomes
[Core-Tier1]
1. Describe the principle of least privilege and isolation and apply to system design [application]
2. Understand the principle of fail-safe and deny-by-default [familiarity]
3. Understand not to rely on the secrecy of design for security (but also that open design alone does not imply security) [familiarity]
4. Understand the goals of end-to-end data security [familiarity]
5. Understand the benefits of having multiple layers of defenses [familiarity]
6. Understand that security has to be a consideration from the point of initial design and throughout the lifecycle of a product [familiarity]
7. Understanding that security imposes costs and tradeoffs [familiarity]

[Core-Tier2]
8. Describe the concept of mediation and the principle of complete mediation [application]
9. Know to use standard components for security operations, instead of re-inventing fundamentals operations [familiarity]
10. Understand the concept of trusted computing including trusted computing base and attack surface and the principle of minimizing trusted computing base [application]
11. Understand the importance of usability in security mechanism design [familiarity]
12. Understand that security does not compose by default; security issues can arise at boundaries between multiple components [familiarity]
13. Understand the different roles of prevention mechanisms and detection/deterrence mechanisms [familiarity]

The cross reference topics that are documented in the first Principles of Security Design topic are:

OS/Security and Protection [2 Core-Tier2 hours]
Topics:
- Overview of system security
- Policy/mechanism separation
- Security methods and devices
- Protection, access control, and authentication
- Backups

SF/Virtualization and Isolation [2 Core-Tier 2 hours]
Topics:
- Rationale for protection and predictable performance
- Levels of indirection, illustrated by virtual memory for managing physical memory resources
- Methods for implementing virtual memory and virtual machines

PL/Language Translation and Execution [3 Core-Tier2 hours]
Topics (only includes 50% of listed topics)

- Run-time layout of memory: call-stack, heap, static data
  - Implementing loops, recursion, and tail calls
- Memory management
  - Manual memory management: allocating, de-allocating, and reusing heap memory
  - Automated memory management: garbage collection as an automated technique using the notion of reachability

3.2 Distributed Nature of the IAS KA Topics

The IAS KA is the most heavily cross referenced KA in the CS2013 Body of Knowledge. As can be inferred from the example provided in the preceding paragraph, the relatively small number of recommended curriculum hours is not representative of the presence of IAS topics and concepts in the CS2013 Body of Knowledge. As can be seen in Table 2, while IAS has 9 combined core hours, there are 63.5 hours distributed through the other KA's

Table 2. IAS Cross KA Hour Distribution

KA's	Core-Tier1	Core-Tier2	Elective
IAS	3	6	Y
IAS distributed in other KA's	32	31.5	Y

As an example of security topics that are addressed in KA's outside of IAS, System Development Fundamentals contains 10 Core-tier 1 hours that address important security concepts.

SDF/Development Methods [10 Core-Tier1 hours]
Topics:

- Program comprehension
- Program correctness
  - Types or errors (syntax, logic, run-time)
  - The concept of a specification
  - Defensive programming (e.g. secure coding, exception handling)
  - Code reviews
  - Testing fundamentals and test-case generation
  - Test-driven development
  - The role and the use of contracts, including pre- and post-conditions
  - Unit testing
- Simple refactoring
- Modern programming environments

  - Code search
  - Programming using library components and their APIs
- Debugging strategies
- Documentation and program style

4 Conclusions and Recommendations

The importance of security concepts and topics has emerged as a core requirement in the Computer Science discipline, much like the importance of performance concepts has been for many years. The development of the IronMan draft for the CS2013 computing curriculum has highlighted the emphasis programs are now placing on security topics. This development however has also identified some weaknesses in the capacity institutions have to adequately address the integration of the security. The emerging nature of security is reflected in the challenge of Computer Science programs and faculty with security experience to inculcate the security concepts in the breadth of courses.

References

1. ACM Curriculum Committee on Computer Science, Curriculum 68: 213 Recommendations for Academic Programs in Computer Science. Comm. ACM 11(3), 214, 151–197 (1968)
2. ACM/IEEE-CS Joint Task Force on Computing Curricula, ACM/IEEE Computing Curricula 2001 Final Report, 217 (2001), http://www.acm.org/sigcse/cc2001
3. ACM/IEEE-CS Joint Interim Review Task Force, Computer Science Curriculum 221 2008: An Interim Revision of CS 2001, Report from the Interim Review Task Force. 222 (2008), http://www.acm.org/education/curricula/ComputerScience2008.pdf
4. ACM/IEEE-CS CS2013 IronMan draft, http://ai.stanford.edu/users/sahami/CS2013/ironman-draft/cs2013-ironman-v1.0.pdf
5. National Security Agency, http://www.nsa.gov/ia/iaFAQ.cfm?MenuID=10#1
6. NIST publication 800-53., http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
7. Machonachy, W.V., Schou, C.D., Ragsdale, D., Welch, D.: A model for Information Assurance: An Integrated Approach. In: Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, June 5-6. United States Military Academy, West Point (2001)
8. McCumber, J.: Information Systems Security: A Comprehensive Model. In: Proceedings 14th National Computer Security Conference, National Institute of Standards and Technology, Baltimore (1991)

Fostering Content Relevant Information Security Awareness through Browser Extensions

Marius Potgieter, Craig Marais, and Mariana Gerber

School of Information and Communication Technology, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa 041 504 1111
{s208108589,s204005264}@live.nmmu.ac.za,
Mariana.Gerber@nmmu.ac.za
http://www.nmmu.ac.za

Abstract. A call for adopting information security awareness amongst end-users has been suggested over the years. Adoption can occur through various methods. These methods each hold their own characteristics, whether being of a positive or negative nature. The challenge to find an appropriate method on which to establish and engage in a security dialog with a user has been written on extensively over the past few years. A number of common key points have been raised in research that addresses information security awareness and how it is conveyed to users. Additional to these common key points, this paper suggests using browser integration as a medium to promote security values and provide security suggestions based on a specific users behavioural pattern.

Keywords: information security, awareness, browser extensions, content delivery, brain-compatible learning, usability.

1 Introduction

Personal security is something taken very seriously; people have some concept of what they find important to ensure their security [1]. This stems from peoples views and awareness of what could be seen as threats to their security. In the physical world these threats are aspects that people understand and can easily relate to. The consequences of not protecting against physical threats would mean a loss, which would result in a feeling or a sense of concern for people, since it could impact on their physical body or possessions. People use the web for many purposes; to interact socially, conduct business and purchase goods (amongst other activities), causing activities that would normally be conducted in the physical world to now also exists within the cyber world. Through their activities, engagement with and usage of the web, a digital persona is increasingly built [2]. This digital persona exists as information scattered over the web that relates back to the user it belongs to. This digital persona is just as vulnerable to an array of threats as the physical person [3]. Creating awareness of these threats is the core of information security awareness [4] [3].

The way people are informed about information security has been a topic of serious discussion for many years. Within the corporate environment the need

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 58–67, 2013.

for information security awareness has been recognised through international standards and policies [5] or information security culture [6]. These efforts have resulted in a noticeable level of awareness within companies [7][8]. Alarmingly the largest group vulnerable to the cyber security threats are home users [8]. Without targeting awareness programs directly at this vulnerable user group, a serious lack of information security awareness could exist [9].

Users commonly interact with the web through browsers. These web browsers provide a way for users to traverse the World Wide Web. Unfortunately the standard browsers do not make the user aware of the various dangers that the web contains. Web browsers, as they are, do not contain comprehensive means for making users aware of these threats, although most of them contain the functionality to extend their capabilities. These extendable capabilities are fittingly referred to as browser extensions (or plugins). These extensions can be designed to integrate into the browser to provide a specialised functionality. Extensions have access to what the browser is retrieving, presenting and traversing; and thus provide opportunities that will be explored.

This paper presents an approach to information security awareness that utilises the browser's own innate knowledge. This knowledge stems from what the browser is currently presenting to the user in a form of a web page or other activities performed on the web. This will be used to provide personalised and content-relevant awareness information to the user, warning against possible dangers that can be encountered. This paper, further, explores current security usability research to enhance user awareness, through browser extension, in a way that best suits the user. This approach will be validated using security usability for end-user applications that define criteria that increases overall usability [10].

This paper will employ logical reasoning and argumentation to develop an approach to deliver targeted information security awareness content by means of a model. This model will be implemented and then be critically analysed using above mentioned criteria.

This paper will provide background information on browsers and how they can be extended. It will then investigate Information Security Awareness and how it relates to browsers. A model will then be presented, applied and evaluated using leading studies in end-user usability.

2 Web Browsers

Web Browsers are used by users that want to interact with the World Wide Web. Commonly used browsers include are Chrome, Firefox, Internet Explorer, Opera, and Safari. The browser operates by retrieving information stored at various locations on the web and displaying the content to the user. The user requests what information is to be retrieved though the browsers address bar that forms part of the user interface. The interface also contains other features to assist the user in navigating the web. These include features like the back/forward button, bookmarking, refresh etc. All features, except the display that shows the requested web content, are considered part of the web browsers user interface.

After the users request is processed by the browser engine that fetches the content from the web and passes the content to the rendering engine to be processed, the rendering browser engine processes the content and displays the website for the user to see. Additional to having features, browsers also comprise components.

Components forming part of browsers are: the networking (used as platform independent method of making requests to the web), JavaScript Interpreter (that processes and executes JavaScript code that was part of the content received), UI Backend (this draws features on the screen like popup boxes or windows) and data storage (stores information on the local machine e.g. some websites use this to identify users that return to their website using cookies).

These components commonly appear in most standard web browsers that are available to users. Fig. 1 presents all the mentioned components of standard web browsers and their interrelationships, each browser will implement this structure to its own specifications.

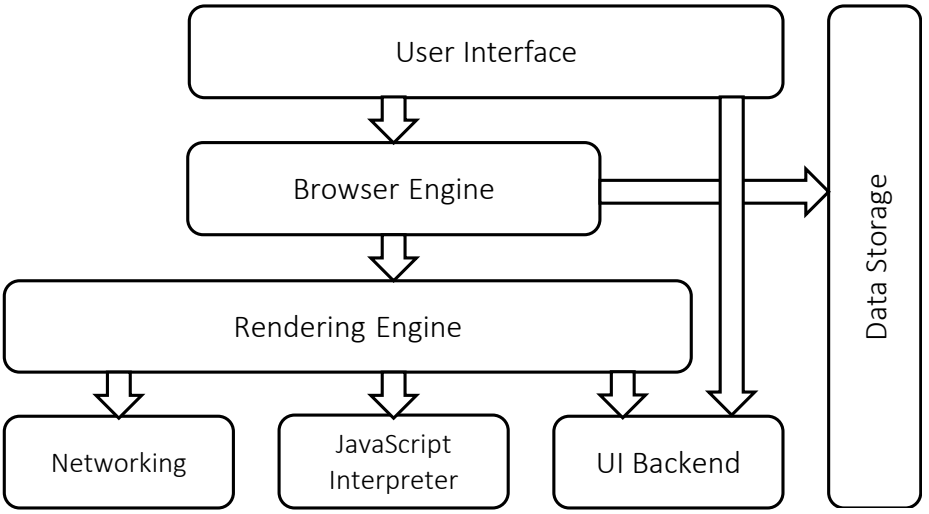


Fig. 1. Browser component relationship

3 Browser Extensions

Browser extensions are developed just like any other regular application, with the exception that it uses the browser as platform to run on. Each browser uses its own design and API (application programming interfaces) to create extensions. These extensions are, thus, created for each unique browser type e.g. Chrome Browser, Firefox Browser. Once developed, these extensions are put through a simple evaluation system by the parent company that owns the targeted browser (Each company has its own specific evaluation criteria). This evaluation is to

determine whether the extension follows the company standards of the particular browser and once approved, gets placed in the browsers extension library. These repositories of extensions (e.g. Google Chrome Store) are accessible to anyone who wants to add the extension to their browser. Some of these extensions, when installed, requests permission from the user to access personal data of the user to be used in the extension. Extensions that have been updated by their developers get updates (on the users machine) either automatically or by requesting the users approval. This ensures that the user is kept up to date with the current version of the extensions that they are using.

4 Information Security Awareness and Browsers

The aim of information security awareness is to make as many users as possible aware of the dangers that exist relating to the use of the World Wide Web. The vast majority of users interact with the World Wide Web through browsers. This makes it an ideal platform to launch a tool (in the form of a browser extension) that would provide appropriate information security awareness content to the user regarding their web activities.

Providing the user with information security awareness information or suggestions gathered from what is happening within the browser, provides relevance to the user. An Information Security Awareness Extension would utilise various methods of analysing possible information gathered from the browser that can be used to provide targeted awareness information to the user. This section will explore a few of those techniques.

4.1 Browser State Analysis

The browser state will provide information about what is happening with the browser as an application. These include examples like:

- *Security Level* e.g. what security protocol is being used by the browser; this would include the standard protocol - Hypertext Transfer Protocol (HTTP) and the more secure Hypertext Transfer Protocol Secure (HTTPS).
- *Loading State* of the webpage, either being uploading or downloading information.
- *Visited Webpage URL (uniform resource locator)* the website being visited has a specific location on the world wide web.
- *Installed or loaded Extensions / Plugins* e.g. extensions and plugins include applications that extend the capabilities of the browser as explained in previous section. These could include useful functionality like being able to play Adobe Flash material, but there could be the possibility that other extensions could be malicious.
- *Default Homepage* is commonly set by the user depending on their preferences. It remains possible for third party applications (or extensions) to modify this preference. It is common for spyware or adware to modify this preference to redirect the user to a website containing misleading information.

– *Stored Login Usernames and Passwords* are commonly kept stored within the browser in a secure database on request of the user. This is commonly stored once the user created a registration form on a website for the first time or used the login information for the first time to access the website.

4.2 Web Content Analysis

Once the webpage has loaded the content is available for analysis. The content would be in the form of HTML files, possibly with imbedded JavaScript. The content of a website could also include third-party code in the form of applications (or applets) e.g. Adobe Flash. These include examples like:

– *Webpage Content (HTML)* is generally what the user sees displayed on the browser window. The content includes simple text, images, links to other webpages etc. that is used to navigate the World Wide Web.
– *Input Fields* are used to gather information from users in the form of textbox fields, checkboxes, dropdown fields etc. These fields would require the user to input personal information such as first name, surname, date of birth, personal address etc.
– *Password Fields (Login information)* are used to authenticate a users identity. The password field gets displayed when creating a user account for the first time and for subsequent login sessions (when not stored as discussed previously).
– *Credit Card Input Fields / Other E-Commerce Payment options* will become available when purchasing or providing payment on a website. Many website use third-party services in this regard e.g. PayPal.
– *Rich Media Content (e.g. Adobe Flash, Microsoft Silverlight etc.)* are development platform applications outside the scope of the standard browser development engine (JavaScript). These are commonly embedded within the browser content as packaged applications that run on their own engine that needs to be installed inside the browser (like with Microsoft Silverlight) or on the computer (with Java JRE).

4.3 Data Storage Analysis

Data regarding the users behaviour on websites sometime get stored in the form of cookies or other storage locally on the users machine. Data storage includes:

– *Cookies and Internal Databases* contain information gathered about the user when visiting a website that stores certain information about the user and that visit to their website (also referred to as a web session). An example of this is the shopping cart created while purchasing from an online store.

As seen in these analysis techniques, the browser provides a wealth of information regarding exposure that the user has to the World Wide Web. This information can be used as event triggers to supply the user with information, targeting

specific threats by providing specific awareness information, applicable to the users current browser content or behaviour.

An example would be to provide the user with targeted awareness information about creating a secure password, once the Web Content Analysis has seen that a password field exist within the web content. The Browser State Analysis would then provide information if the password for that specific website already exists, or not. If no password has been created for that website, the browser extension will assume (through simple induction rules within the extension) that the user is about to create a password for the first time and supply the user with a tutorial on how to create a secure password. If a password already exists for the site, information regarding general password security will be displayed [11]. A model for such browser extension will be discussed.

5 Awareness Model and Design

A model for browser extension to address the lack of content relevant information security awareness associated with dangers of using the World Wide Web is depicted in Figure. 2. This model will be referred to as the Targeted Awareness Browser Extension Model. The model consists of engines that will provide the targeted awareness content to the user through the extensions user interface. An implemented example of this model will be the Information Security Awareness Extension.

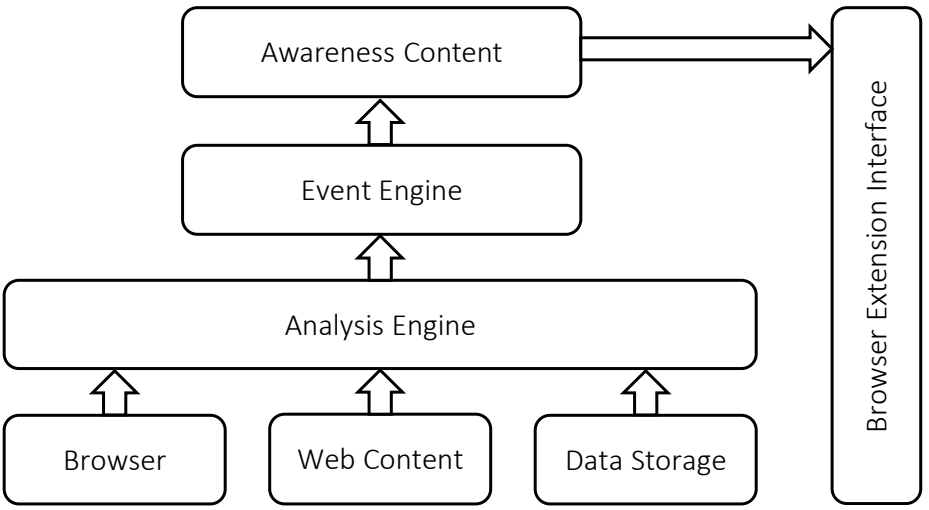


Fig. 2. Targeted Awareness Browser Extension Model

The components of this model will now be explored in further detail.

5.1 Analysis Engine

The analysis engine will provide the event engine with possible threats or targeted awareness information depending on the status or content of the browser. This information will be gathered from the users browser, web content and data storage, which comprise the lowest layer illustrated in the Awareness Model.

5.2 Event Engine

The event engine will determine whether something within the browser is generating a possible incident that can be raised as a topic of awareness to the user. The event engine will pass event information to the awareness content and allowing it to further target the user with appropriate content.

5.3 Awareness Content

The content provided by the extension will be directly related to a category or topic the event engine defined as relevant to what is currently occurring within the browser (as discovered by analysis engine). The way the content is structured will follow established brain-compatible techniques for providing information security education as defined by Reid [12] and using rich-media as discussed by Shaw [13]. This will provide a greater degree of understandability and learnability of the content and, thus, increases the diversity of the target audience that this browser extension could potentially target. Awareness content will be assigned a theme so that a user can easily identify the type of awareness information that is currently being displayed (e.g. with passwords the use of green as a topic colour would be considered an appropriate choice as an example of an assigned theme).

Further examples of targeted awareness information include:

- When the user visits a banking website (determined by the engine analysing the web address of the website being visited), appropriate content will be displayed about phishing attacks and how these can target the user.
- While posting comments on a Social Media Website (e.g. Facebook) the user will be provided information about possible privacy settings available, how to enable/disable them and the possible threats of ignoring them.
- An unknown website wants to load a third-party embedded application using Rich Media Content, the user will be provided with information about how malicious content can be distributed using such Rich Media Content.

5.4 Browser Extension Interface

The browser extension interface will consist of a vertical side panel within the browser application. This side panel will adjust the size of the browser window accordingly so that the content will create as little as possible intrusion into the users standard screen estate assigned to the browser. Using standard resolution

used by a majority of the web user population [14] while having the browser extension open (active) there will be no significant reduction in the size of content within the browser window. This will promote a less intrusive design while still providing a visible interface that can be interacted with.

6 Awareness Extension Usability

When considering end-users, the usability of a security feature within an application becomes an issue. The way in which users interact with computers is an established field of study, referred to as HCI (Human Computer Interaction). The use of recognised HCI concepts in the design of security in computers have been suggested to improve user acceptance [15] of a system or application. Further study was done by Furnell [10] by identifying challenges users experienced in understanding security features within applications. However, evaluating security awareness usability as a feature within applications, has not been the subject of extensive study. This section aims to evaluate the usability of the Information Security Awareness Extension using criteria proposed by Furnell [10]. The following is a summary of these criteria:

- *Understandable* the information provided by a security feature needs to be presented in a meaningful way to the intended user population.
- *Locatable* users need to be able to have the security feature easily at hand.
- *Visible* - visibility of system status allows the user to observe the internal state of the system. Using status indicators and warnings will provide users with information about possible safeguards that need to be enabled.
- *Convenient* the security feature should not disturb the user from their regular routine. The feature could be considered as inconvenient or intrusive and thus negating or reducing the user experience of the feature.

The Information Security Awareness Extension will be evaluated according to the above mentioned criteria to emphasize and validate security usability. To achieve this, the criteria will now be discussed in relation to the Information Security Awareness Extension.

- *Understandable* Following recommendations for creating brain-compatible material for information security education [12] the content will accommodate a wide user audience, level of understanding and learnability. Since the awareness content that is generated and displayed to the user is content specific, the security message will be applicable to the user's current task. The awareness message will thus be meaningful to the user and can either be applied practically (in the case of the above mentioned example of creating a secure password while on a website asking for the user to provide a password) or that the message is of such relevance that user will take time to consider possible security threats.
- *Locatable* Since the browser extension will be integrated within the browser environment where most users are exposed to the threats of the World Wide

Web, the awareness extension will always be active and displayed in a familiar location. The browser extension will supply information on an event-based system which will display content when it is appropriate to alert or inform the user of possible dangers.

- *Visible* The awareness content will provide users with visual indications of what is being displayed. Depending on the status of the event raised by the event engine, the content will either be an alert or guidelines and general information. Alerts will warn the user about possible threats and provide relevant content on the topic and its dangers (e.g. the browser analysis alert the event engine the user is not using a secure protocol while sending information over the web). Guidelines and general information will deliver non-critical content for the users consideration (e.g. while browsing a social media website like Facebook it will provide information on topics like cyber-bullying).
- *Convenient* as mentioned in the above section of the Browser Extension Interface we explored the reason why the extension will not intrude on the users regular routine. Other convenience factors include the fact that the browser extension will be publically (as well as freely) available on the browsers specific extension repository (e.g. with Google Chrome it Chrome Web Store). This provides a framework by which the extension can be updated. Since any changes made to the extension submitted to the repository will automatically update the users extension on his local machine. In this way the extension (and content) can be kept up-to-date without any further user intervention.

By evaluating the Information Security Awareness Extension against these criteria, it has been established that this approach follows recommendations by leading studies in information security usability with end-users.

7 Conclusion

The aim of information security awareness is to make users aware of the information security related dangers. This paper focused primarily on users information security awareness regarding the dangers associated with the usage of the World Wide Web and provided an information security awareness approach relating to these dangers. The platform on which awareness of these dangers are raised is ideally suited within browser extension. The innate knowledge provided by the browser can deliver targeted information security awareness content to the user on possible information security dangers. It also has been established that the design for such a browser extension should ideally conform to current security usability studies.

In response to this paper, further research will be done on how the implementation of such a browser extension can be achieved. Further investigation of this solution, towards promoting information security awareness by utilising browser extensions, will be reported on in subsequent papers.

References

1. Lazarus, L.: The right to security securing rights or securitising rights? Cambridge University Press (2012)
2. Williams, S.A., Fleming, S.C., Lundqvist, K.O., Parslow, P.N., et al.: Understanding your digital identity. Learning Exchange 1(1) (2010)
3. Wu, Y., Guynes, C.S., Windsor, J., et al.: Security awareness programs. Review of Business Information Systems (RBIS) 16(4), 165–168 (2012)
4. Veerasamy, N., Taute, B.: Introduction to emerging threats and vulnerabilities to create user awareness. Information Security South Africa (2009)
5. I. O. for Standardization and I. E. Commission, ISO/IEC 27002, ser. International Standard. ISO/IEC (2007)
6. Furnell, S., Thomson, K.-L.: From culture to disobedience: Recognising the varying user acceptance of it security. Computer Fraud & Security 2009(2), 5–10 (2009)
7. Talib, S., Clarke, N.L., Furnell, S.M.: An analysis of information security awareness within home and work environments. In: ARES 2010 International Conference on Availability, Reliability, and Security, pp. 196–203. IEEE (2010)
8. Wood, P.: Internet security threat report: 2011 trends. Symantec Corporation, 350 Ellis Stree, Mountain View, CA 94043 USA. Tech. Rep. 17 (April 2012)
9. Stander, A., Dunnet, A., Rizzo, J.: A survey of computer crime and security in south africa. In: Proceedings of the ISSA 2009 Conference, p. 217. ISSA (2009)
10. Furnell, S.M., Jusoh, A., Katsabas, D.: The challenges of understanding and using security: A survey of end-users. Computers & Security 25(1), 27–35 (2006)
11. Ross, B., Jackson, C., Miyake, N., Boneh, D., Mitchell, J.C.: Stronger password authentication using browser extensions. In: Proceedings of the 14th Usenix Security Symposium, vol. 1998 (2005)
12. Reid, R., Van Niekerk, J., Von Solms, R.: Guidelines for the creation of brain-compatible cyber security educational material in moodle 2.0. In: Information Security South Africa (ISSA), pp. 1–8. IEEE (2011)
13. Shaw, R.S., Chen, C.C., Harris, A.L., Huang, H.-J.: The impact of information richness on information security awareness training effectiveness. Computers & Education 52(1), 92–100 (2009)
14. w3schools, Browser display statistics (April 2013), `http://www.w3schools.com/browsers/browsers_display.asp`
15. Johnston, J., Eloff, J., Labuschagne, L.: Security and human computer interfaces. Computers & Security 22(8), 675–684 (2003)

PKI Interoperability: Still an Issue? A Solution in the X.509 Realm

Ahmad Samer Wazan[1], Romain Laborde[2], François Barrere[2], Abdelmalek Benzekri[2], and David W. Chadwick[3]

[1] Institut Mines-Telecom/Telecom SudParis, CNRS UMR 5157 SAMOVAR, 91000 EVRY, France
samer.wazan@telecom-sudparis.eu
[2] Paul Sabatier University, IRIT UMR 5505, 31400 Toulouse, France
{laborde,barrere,benzekri}@irit.fr
[3] University of Kent, Computing Laboratory, Canterbury, Kent, CT2 7NF
d.w.chadwick@kent.ac.uk

Abstract. There exist many obstacles that slow the global adoption of public key infrastructure (PKI) technology. The PKI interoperability problem, being poorly understood, is one of the most confusing. In this paper, we clarify the PKI interoperability issue by exploring both the juridical and technical domains. We demonstrate the origin of the PKI interoperability problem by determining its root causes, the latter being legal, organizational and technical differences between countries, which mean that relying parties have no one to rely on. We explain how difficult it is to harmonize them. Finally, we propose to handle the interoperability problem from the trust management point of view, by introducing the role of a trust broker which is in charge of helping relying parties make informed decisions about X.509 certificates.

Keywords: PKI, X.509, Trust, Interoperability.

1 Introduction

While the potential of PKIs is high, this technology continues to suffer from many problems that slow its global adoption. In 2003, the OASIS technical committee investigated the reasons that prevent the widespread adoption of PKI technology. The major results of this survey [1] are:

- Poor PKIs interoperability;
- Too much legal work required;
- Hard for end users to use;
- PKI poorly understood.

Although this survey was undertaken in 2003, the issues related to interoperability, complexity of legal work and the difficulty of use by end users are still accurate and still cause severe problems.

These issues are not mutually exclusive; they are highly related to each other. The interoperability problem is the most difficult one, because it is the most complex and

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 68–82, 2013.

confusing. Peter Smith has highlighted the complexity of PKI interoperability [2]: "*[PKI] interoperability is something of a will-o'-the-wisp. You think you understand what people mean by it, and then quickly realize that you don't. In my experience, it's possible when discussing interoperability to be at cross-purposes for all of the time}". If such a group of experts has difficulties to cope with this issue, how can we imagine an unskilled person can perform this task? Today, users of certificates, and in particular relying parties, are left on their own to face this problem*".

In this paper, we open Pandora's Box by trying to explain the reasons for the interoperability problem in the field of PKIs. We show that the problem cannot be solved by defining harmonized juridical, organizational and technical rules, especially because of the cultural/juridical differences between countries. Thus, PKIs today are isolated islands; each PKI seeks to comply only with the requirements of the jurisdiction where their root CA premises are located.

Although explaining the PKI interoperability issue is the main objective of this paper, our research is also aimed at resolving this problem from a trust management point of view. Our proposed solution is also briefly presented. Our trust management based approach requires defining a new role, the trust broker, which will help relying parties to evaluate the risks and to take informed decisions about using the certificates of remote users, which they have obtained.

The rest of the paper is structured as follows. Section 2 explains what exactly a public key infrastructure is. It presents the main involved entities and PKI deployment models. In section 3, we illustrate the problem of PKI interoperability and show how it is difficult to solve the problem by defining harmonized juridical and technical rules between countries. In section 4, we present our proposition that consists in handling the interoperability problem from a trust management point of view. We also briefly present our proposal to define a new trusted third party, the trust broker, and we demonstrate the feasibility of our proposal. Finally, in section 5 we present our conclusions.

2 What Is a Public Key Infrastructure?

Many definitions of a PKI exist. The American Bar Association (ABA) defines a PKI as: "*The sum total of the hardware, software, people, processes, and policies that, together, using the technology of asymmetric cryptography, facilitate the creation of a verifiable association between a public key (the public component of an asymmetric key pair) and the identity (and/or other attributes) of the holder of the corresponding private key (the private component of that pair), for uses such as authenticating the identity of a specific entity, ensuring the integrity of information, providing support for non repudiation, and establishing an encrypted communications section*".

Thus, a PKI is not only a set of computers used for generating the key pairs and the associated certificates. It is also the set of policies, processes and people responsible for a certificate's life cycle management. The certification authority (CA), which asserts the correctness of the certificate information by appending its signature on the certificate, is the main entity of this infrastructure.

A PKI is based on a trust model described by the X.509 standard (Fig. 1). The model is composed of three entities: the certification authority (CA), the certificate

holder and the relying party (RP). The CA plays the role of trusted third party by guarantying the correctness of the certificate information to the RP. Thus, the CA trusts the certificate holder and so issues it with a public key certificate. The relying party trusts the CA for the validity of the certificate's information. Consequently the relying party can indirectly trust the certificate holder for the current transaction.

According to RFC 5280, which defines an X.509 certificate profile for the Internet, an RP has the obligation to review the CA policy documents before accepting a certificate. It declares: "*A certificate user should review the certificate policy generated by the certification authority (CA) before relying on the authentication or non-repudiation services associated with the public key in a particular certificate*".

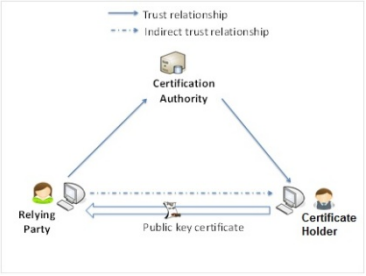


Fig. 1. X.509 trust model

To respect this obligation an RP must typically read two documents: the Certificate Policy (CP) and the Certification Practice Statement (CPS) documents. The CP document defines the application domain of a certificate and the security requirements to be realized by the CA. The CPS document defines how the CA has implemented the security requirements. It must be fairly obvious to anyone that this is a ludicrous requirement to place on most computer users.

Two different deployment models can be distinguished for PKIs: the ***closed*** and the ***open*** models. The closed model is usually applied to contexts with limited scope such as a collaboration between organizations where each organization manages its own PKI including one or more CAs. All the relationships between all the entities (RPs, CAs and certificates holders) participating in the collaboration are clarified through agreed contracts between the involved organizations.

In the open model, the relationship between a CA and certificate holders is also clarified by contracts. But, there is no such explicit contractual relationship between the CA and the relying parties (RPs). Therefore, the regulation of the relationships between a CA and the RPs is defined in legislative and regulatory frameworks rather than contracts. However, the lack of consensus between countries about the implementation of these frameworks or the way that PKIs should be regulated has given rise to the problem of interoperability between PKIs in this open model.

3 The PKI Interoperability Obstacle

Generally, two kinds of regulations can be identified: economic regulations and social regulations [3]. The objective of the economic regulations is to increase economic

efficiency by reducing barriers to competition and innovation, often by deregulation. The objective of the social regulations is to protect the public interests such as health, safety and the environment. Thus economic interests come as secondary concern to the social regulations.

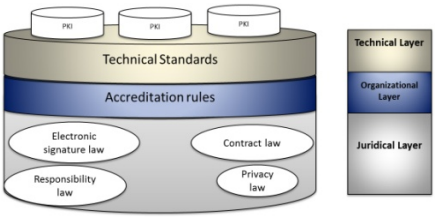


Fig. 2. Regulation layers

A PKI depends on three layers of regulations: juridical, organizational and technical (Fig. 2). PKI interoperability requires compatibility at these three layers. Currently, profound differences still exist between countries at each layer: juridical, organizational and technical. In the following sections, we try to interpret what the interoperability problem actually means by exposing the juridical, organizational and technical differences that exist between countries.

3.1 Juridical Differences

The implementation of a PKI requires the processing of different legal issues: how to recognize electronic signatures, the validity of electronic contracts, the legal responsibilities of the involved entities (CAs, certificate holders and RPs) and the privacy rules.

Generally, the legal differences that exist today come from the different legal traditions that have evolved and are now being followed in the different countries. There are mainly two different traditions: the common-law tradition that relies on legal precedent to assess legal affairs, and the civil-law tradition that relies on the existence of laws rather than decisions of courts to assess legal affairs [4]. Consequently countries have treated all the legal issues related to PKIs according to their different legal traditions.

Differences Concerning the Legal Recognition of Electronic Signatures. Three different approaches exist for validating electronic signatures: (a) the minimalist approach; (b) the technology-specific approach and (c) the two-tiered approach [6].

The minimalist approach is based on the principle of technological neutrality, which gives a minimum legal effect to all technologies. The principle of technological neutrality ensures that the legislation remains valid even when the technologies become obsolete. This approach is often applied in common law countries such as the US, UK and Australia. Under this approach, electronic signatures are equivalent to handwritten signatures if they fulfill certain functions. In case of dispute, the validity of electronic signatures is established a posteriori by a judge, or by a public authority [5].

In **the technology specific-approach**, laws favor one form of electronic signature; usually digital signatures. In this case, laws specify technical, juridical and financial requirements imposed on CAs in order to validate electronic signatures generated by their certificates. The disadvantage of this approach is that it makes uncertain the legal status of other types of electronic signature. The Utah State was the first to adopt such a law in 1995.

The two-tiered approach combines the advantages of both previous approaches. It is often followed in countries whose tradition is civil-law. It provides a balance between flexibility and certainty by setting minimum requirements for all types of electronic signatures and at the same time by defining a clear legal effect for certain forms of electronic signature that meet specific technical requirements. The European Union has adopted this approach through its directive 1999/93/EC on electronic signatures.

Differences about the Legal Validity of Electronic Contracts. There are two types of electronic contract: contract at a click "*clickwrap contract*" and contract at navigation "*browsewrap contract*". A "*clickwrap contract*" is a contract to which a consumer must agree by clicking the icon "I agree" before completing the transaction. A *browsewrap* contract, which is often accessible using links labeled "Legal" or "Terms of Use", is so named because such agreements state that a web site user is bound simply by "browsing" the web site [8]. In other words, the term *browsewrap* refers to any contract not requiring an explicit manifestation of assent.

Electronic contracts, whether they are *browsewrap* or *clickwrap*, are both considered a contract of adhesion. These contracts do not allow for negotiation; they are based on the principle "take it or leave it" where one party is restricted to accept all the terms prepared by the other powerful party. These contracts usually raise questions about the fairness to the weaker party.

Countries like the US tend to regularize electronic contracts mainly based on only the traditional laws of contracts, whilst other countries like those in Europe, add different extensions to the traditional laws of contracts [7]. By consulting case law handled until 30-06-2008 by the American courts [8], electronic contracts have been invalidated in the following cases:

- If it is not possible to prove that the consumer has obviously noted the existence of an electronic contract. (However, if a consumer has noticed the existence of a contract, it will be valid even if the consumer did not read the clauses);
- If the contract has been modified by the powerful party without notifying the weak party ;
- If the electronic contract infringes the traditional doctrines of contract laws (e.g. kids rules, unfairness rules, etc.).

Laws regulating contracts differ between the US and the EU mainly because of the EU directive on unfair contract terms (which regulates contracts offered by merchants to consumers whether online or offline); the distance selling directive (which regulates transactions between remote merchants and consumers, whether by means of television, telemarketing, Internet or other electronic communications medium) and the Electronic Commerce Directive (which promotes transparency and accountability

in online commerce) [7]. Annex 1 of the EU directive on unfair contracts contains a list of terms that may be considered abusive. It provides examples of unfair terms. In France, the directive was extended by national legislation to make the use of the French language mandatory. Although countries like Canada, Australia and the UK share a common legal culture with the US, nevertheless their approaches to consumer protection have been similar to the EU approach [9].

In the context of PKIs, a consumer can be at the same time a RP and a certificate holder. CAs try to regularize their relations with RPs and certificate holders through electronic contracts rather than written contracts due to their remote nature. These contracts contain information about different issues, such as: the responsibility and obligations of certificate holders towards the CA and RPs and vice-versa, the identification of the jurisdiction where the dispute will be held in case of problems, the arbitration procedures before filing complaints against a CA, the limitation of a CA's liability, and regulations about holding the personal information of consumers, etc.

Contracts between CAs and certificate holders are generally of type "*clickwrap*", because CAs are always asking the consent of certificate holders when their certificates are issued. Electronic contracts for RPs are of type "*browsewrap*" because these contracts are placed in the extensions of certificates; and a RP must inspect the extensions of a certificate to find the related electronic contract. Given the difficulty of access to the contract, it seems probable that courts would invalidate these contracts because RPs are not usually aware of their existence, and sometimes not even of the certificate. In the EU, if the consumer has not agreed explicitly before the conclusion of a transaction, the contract is not valid. Similarly in the US, courts may consider the contract inadequate when the CA cannot prove the RP has read the conditions of use of a certificate prior to its use. Consequently, different countries try to regulate directly the relationship between the involved parties (CAs, certificate holders and RPs) by issuing explicit laws handling the rights and the liability of each party. This point is presented in detail below.

Differences about the Liability of the Involved Entities. Liability issues play an important role in the relationship between RPs, certificates holders and CAs. Regulating liability issues can be executed in two ways: by contract or by law. Relations between the CA and the certificate holder are contractual, whereas relations between CAs and RPs are not based on contracts in the open model.

Differences between countries about liability issues can be recognized in three main areas: the extent that laws cover the involved parties, the burden of proof and the possibility to limit the liability of CAs. Concerning the extent that laws cover the involved parties, four categories can be identified [5]:

- No specific provisions on liability;
- Provisions on liability rules only for suppliers of PKIs ;
- Rules of liability for certificate holders and suppliers of PKIs;
- Liability rules for all the parties.

The differences between jurisdictions appear also on the designation of the party which has the burden of proof in case of a problem. There are two main options: Ordinary negligence where it is the responsibility of the injured party to demonstrate that

the damage was caused by the other party's fault or breach of its obligations, and presumed negligence where a party's fault is presumed whenever damage has resulted from an act attributable to it (e.g. directive 1999/93/EC).

Finally, the ability of the PKI providers to limit their responsibilities has been treated differently between countries. CAs try systematically to limit their responsibilities towards certificate holders and RPs. Although most legal systems recognize the right of CAs to limit or to exclude their responsibilities through contractual arrangements, this right has been subject to various restrictions and conditions [5].

Differences about Privacy Rules. CAs could have problems related to privacy. To generate certificates, CAs need to collect a set of personal and business information about people requesting certificates. Governments have adopted different approaches to regularize the legal rules related to privacy. The difference between the US and EU approaches to social and economic regulations also influences the rules for the protection of personal information. In the EU, the protection of private information is considered a basic human right. In the US however, the person who collects and stores private information is supposed to be the owner, unless a specific law creates a right for the data subject for a specific type of personal information [10].

3.2 Organizational Differences

The organization of a PKI varies from one country to another depending on the level of intervention of governments, which is generally considered in most countries to be a means of trust enhancement. Three main models can be identified [5]:

- *Self-regulation*: In this model, an organization can start up a PKI business without any prior accreditation. No license is required. The US is an example of this;
- *Limited government intervention*: some governments establish a voluntary accreditation system. Under this system, a PKI provider is not forced to search for a license. But licensed PKIs have more advantages than unlicensed PKI providers. The audit of PKIs is normally done by entities accredited by the concerned government. Singapore and the EU are examples of this model;
- *Complete control of governments*: Governments setup mandatory accreditation systems where PKI providers are forced to get a license before starting their business. Governments also conduct the audit process. China and Malaysia follow this model.

The level of technological and administrative maturity in a country plays an important role in determining the appropriate organizational model for PKIs. It is difficult to exclude the intervention of governments in countries whose technological and administrative maturity is not sufficiently developed. In these countries, governments must intervene to facilitate the using of a new technology. Winn et al [11] present an example that shows how the intervention of the Chinese government has contributed to the success of the market in accounting software in China. The study shows that this success was due to government intervention in the market. It shows also that the organizational model of self-regulation for accounting software has been successfully adopted when the market has reached a certain level of maturity.

3.3 Technical Differences

It has never been easy to define a common set of standards between countries. The structure of standards developing organizations (SDOs) varies across countries according to their political, economical and legal structures. SDOs in the US operate outside any form of public control and focus solely on market conditions, while the EU SDOs are under government surveillance and are guided by both the social and economic expectations of the market [14].

Winn, J. K. [14, 20] demonstrates this difficulty by contrasting the standardization processes adopted in the US and the EU.

Standardization Process in the US. Most standards are developed by private organizations such as the National Fire Protection Association, and the Institute of Electrical and Electronics Engineers (IEEE). In order for a standard produced by these organizations to be recognized as an "American National Standards" by the American National Standards Institute (ANSI), the procedures followed to develop that standard must meet the "essential requirements" established by ANSI. These are designed to ensure fairness in the procedures used for developing these standards [14].

One of the advantages to private organizations of being accredited by ANSI is that it will be easier for them to have their standards submitted to ISO, and they can then get international recognition. However, meeting all the requirements of ANSI could slow the development process, especially since it can be difficult to obtain a consensus from all the participants. For example, some participants who are developing proprietary technologies can deliberately delay the development of a public standard in order to drive the market to adopt their own proprietary technology [14].

The suppliers of IT products need a flexible development process for standards. They prefer generally to work with consortiums because they can adapt more rapidly to market evolutions than the traditional standardization organizations. Consortiums have generally a limited number of participants and simplified development procedures for standards.

In the US, many *de facto* standards exist in the context of PKIs. One of the best known is the "extended validation certificate" standard [15]. It describes a set of technical and legal criteria that CAs must meet in order to generate "extended validation" certificates, which are used to authenticate web servers. The standard is established by a group of commercial CAs and by the producers of well known web browsers such as Firefox and Internet Explorer.

Standardization Process in the EU. Governments tend to play a more important role in the elaboration of standards. EU countries usually have one National Standards Body (NSB) responsible for managing all the national standards. The EU has adopted a strategy called the "New Approach" in order to harmonize the efforts of law reform with the efforts of standards' development between the member states. In the New Approach, after the preparation of a directive that defines the "essential requirements" related to one issue, the standardization process will be initiated by one of the three recognized organizations in Europe for the development of standards: the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications

Standards Institute (ETSI). The European Commission (EC) may then send an observer to verify whether the resulting standards meet the essential requirements of the legislation of the directive.

However, it is difficult to adapt the "New Approach" strategy to the development of ICT standards; this is partly because the process of the New Approach to the development of standards is much slower than the simple process of informal standardization followed in the US for developing ICT standards [12].

The EU directive on electronic signatures is a **light version** of the New Approach; unlike the directives based on the traditional New Approach, the electronic signature directive doesn't require the development of formal standards to support compliance to the directive of electronic signatures [20]. CEN, CENELEC and ETSI have introduced new types of products, such as CEN CWAs (Workshop Agreements), ETSI TS (Technical Specifications) and GS (Group Specifications), for accompanying the rapid evolution of the ICT market, and for facing the growing influence of international consortia working outside the EU. These products provide an alternative to the formal rigid process of standardization for the development of formal European Norms (ENs).

The work of developing standards for electronic signatures has been entrusted to the "European Electronic Signature Standardization Initiative" (EESSI). EESSI is an ad hoc body set up under the aegis of "the Information and Communications Technologies Standards Board (ICTSB)", an organization that specializes in coordination between the European standards bodies CEN, CENELEC and ETSI. EESSI's work was completed in 2003 and published in the Official Journal. As a consequence, the differences in strategies for developing standards have resulted in different standards in the domain of PKIs.

3.4 Discussion

Neither the US nor the EU has found an effective way to promote the adoption of PKI technologies. In the US, the removal of legal, technical and organizational barriers in the market of PKIs has not led to the establishment of strong mechanisms for authentication and signatures. By promoting the unregulated competition among providers of identity technologies, many technical solutions have been deployed in the market, but none of these solutions has really dominated the market. Consequently, identification and authentication for Internet transactions in the US remain mainly based on UserID/Password; despite the well known security problems associated with them [12]. In February 2005, the Federal Deposit Insurance Corporation released a report indicating the severity of the problem of identity theft in the US and concluded that reinforcing online identification systems is essential to solve the problem. This is why the Obama administration is trying to reduce fraud on the Internet by developing an ecosystem for online identity management at the national level. The administration is currently working on the National Strategy for Trusted Identities in Cyberspace. A draft of the proposal was publicly released at the end of June 2010 [13]. The identity ecosystem is based on four main principles:

- The system will be secure and resilient;
- The system will be interoperable;
- The system will be privacy-enhancing and voluntary;
- The system will be cost-effective and easy to use.

However today, in the context of PKIs, the situation in the US remains unclear. Users must be able to assess the technical and legal risk resulting from the dependence on various PKIs, which utilise different types of certificates with different levels of technical and juridical qualities.

In other countries, such as the EU, which provide a minimum level of technical and legal protection for their citizens, the clarity of the situation at national level increases with the government's level of intervention. However, the international situation remains unclear. These countries have problems regarding the recognition of foreign certificates managed by foreign PKIs. For example, web browsers imposed the "extended validation" standard as a *de facto* solution for recognizing these certificates. Given the approach that has been followed for developing this standard, the EU countries could find this standard unfair to their citizens. Currently, there are not sufficiently well developed mechanisms to give official recognition to the standards developed outside the EU's borders.

The various attempts that have been aimed at harmonizing the trust frameworks of PKIs between countries have not actually improved the situation. For example, the attempt by the United Nations Commission on International Trade Law (UNCITRAL) to harmonize the laws of different countries for the recognition of electronic signatures has not achieved its objectives. The proposed harmonizing approach is flexible; it allows countries that have adopted it to modify it freely to suit their own needs. But this has led to creating interoperability problems [17].

In the EU, the legal, technical and organizational harmonization through the directive on electronic signatures has not been a huge success. In 2007, a study, at the request of the EC found that the lack of interoperability between EU countries is one of the main factors that have contributed to the slow adoption of electronic signature technology in Europe [18]. In fact, in parallel with the standardization efforts of EESSI, some Member States have developed their own national standards such as ISIS-MTT in Germany, PRIS in France and SEIDE in Sweden. These standards have created additional interoperability problems between European countries. This is legally possible in the EU because CWAs and TSs don't have the same status as formal standards (ENs). Therefore, the obligation imposed on Member States to remove existing national standards that are inconsistent with European standards does not apply in the case of CWAs and TSs [19].

To face this problem, the EC is working on a new proposal to regulate electronic identification and trust services for electronic transactions in the internal market [23]. The objective of this proposal is to enable cross-border secure transactions between European countries, both for the public and private sectors. Whilst directive 1999/93/EC only covers electronic signatures, the new regulation defines a comprehensive framework that encompasses electronic identification, authentication and signatures. It is too early to measure the success of the new regulation. However, the new regulation introduces certainty only for qualified trust services i.e. those that

meet the requirements of the EC, and not other trust services that nevertheless are still authorized to sell their services in the EU market. Thus, uncertainty will still persist for the latter services.

Today, new countries are starting to have an important role in the development of global standards (especially China, India and Korea). For example, Scott Kennedy explains [16] that the investment of China in standards development is to break the domination of western countries in this area. The quality of these standards can vary considerably, depending on the participants and the rules for participation established by the agency that develops the standards.

As a consequence of these major differences, PKIs remain isolated islands in the open model. Each PKI seeks to comply only with the requirements of the jurisdiction where the premises of its root CA are located. Thus, the RPs have to handle this PKI interoperability issue in the end. The various harmonization attempts at regional and international level have not come up with a solution to the PKI interoperability problem. Trust architectures such as Bridge CAs or hierarchical CAs cannot help in resolving the problem in the open model since the main idea of these architectures is to prove the juridical, political and technical equivalence between CAs. However, because of the interoperability problems between countries, this equivalence is not feasible. This is why Web browsers today contain many hierarchical CA roots, and not just one.

4 Handling the Interoperability Problem from the Trust Management Point of View

The persistence of interoperability problems creates a ***trust management problem***, i.e. how can an RP trust one CA or another when certificates have different levels of quality? If there was a compatibility between PKIs at the juridical, organizational and technical levels, there would not exist a ***trust management*** issue because in this case a limited number of classes of globally accepted certificates could be defined, where each class could meet a specific context of use. However, this theoretical solution cannot be implemented in practice because of the reasons presented in section 3.

We propose to handle the interoperability problem by transforming it into a ***trust management problem***. Establishing trust in a certificate requires managing technical, organizational and legal issues. This task is extremely complex, therefore only technical and legal experts can perform it. It is not conceivable to delegate this task to the RPs which generally are unskilled people.

In the closed PKI model, the administrators of the CAs and the lawyers of each organization play the roles of technical and legal experts to help the employees of the organization in dealing with certificates coming from other organizations. RPs and the experts, being part of the same organization/company, have a trust relationship which is naturally created. The trust of the RPs in their administrators is not only related to the quality of the certificates they are issued with but also to the CAs they are recommended or allowed to trust. In addition, interconnection topologies are often built for

a predefined number of services related to the nature of the collaboration between the organizations. Thus, the trust decisions of the RPs can be automatically configured.

In the open model, the situation is far more complex than the closed model for several reasons (Fig. 3). There is no explicit and balanced predefined trust relationship between RPs and experts. Web browsers implicitly play the role of expert as they manage the list of trusted CAs, but there is no agreement between the RPs and the browsers' manufacturers to make them responsible for the information they provide.

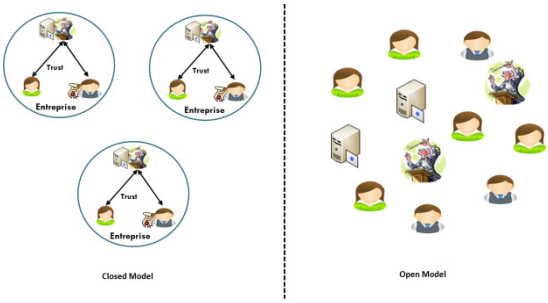


Fig. 3. Differences between the closed model and the open model

Secondly, the scope of the certificate usage is more open (i.e., not limited to predefined specific services). The consequence is that Web browsers don't provide enough information to make an informed decision. The recommendation is binary (trusted or not recognized, e.g. an icon in the URL bar is blue or not). Trusted CAs are all stored in the same trusted list. CAs with different levels of quality are equally trusted regardless of the use of the certificate.

All these **ad-hoc** solutions, either for the open (e.g. Web browser approach) or for the closed model (e.g. interconnection topologies), include **implicitly** the role of expert. The differences lie in the nature of the entities playing the role of expert, the type of trust linking the expert with the RPs, and the nature of the information that the expert supplies to RPs. We propose to clarify this situation by adding **explicitly** the role of a trusted expert to the X.509 trust model, in the form of a **trust broker**. RPs need to rely only on the trust broker and not on each and every CA issuing certificates to their holders. In this case, the X.509 trust model is fairer for the RPs. The trust broker evaluates objectively the CA and its certificates, and sends recommendations to RPs that helps them to make informed decisions about these certificates (Fig. 4-A).

The relation between the trust broker and the RPs must be regularized by **explicit** agreements. In such agreements, the trust broker recognizes its **responsibility** to the RPs about the provided recommendations and requires itself to respect and to protect the privacy of the RPs. On the other side, the trust broker must be **independent** from the CAs. Its relationship with CAs must also be regularized by **explicit** agreements, so that the trust broker can transfer the responsibility to a CA when a false recommendation is made resulting from incorrect information provided by the CA.

The contractual agreements between the RPs and the trust brokers create trust communities. The role of trust broker could be provided by:

- Commercial organizations which make a business from giving recommendation about certificates;
- National governments which wish to facilitate e-commerce in their countries;
- An international body like the UN in order to facilitate international trade.

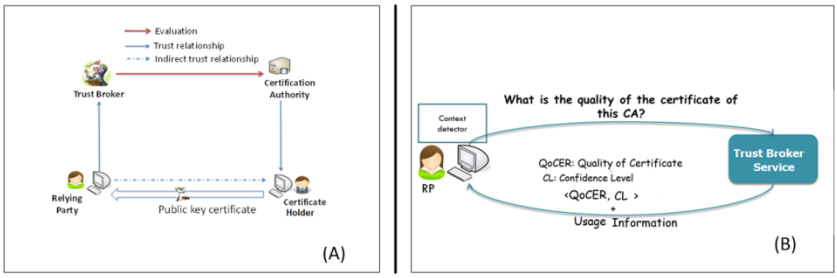


Fig. 4. The Trust Broker

Finally, to help RPs to make informed decisions about certificates, the trust broker must provide **contextual recommendations**. For example, recommendations about a certificate that authenticates an email server should be different from recommendations about a certificate that authenticates an e-commerce server. This is because the information sent by the RP to the certificate holder (login/passwd or credit card information) and the consequences of these transactions are different. In the first case, the critical information is the quality level of the certificate and the financial and juridical protection if the certificate is false. In the second case, this information should be supplemented with the maximum transaction amount that can be used in order to stay covered by the financial protection offered in the CP/CPS.

We have already proposed that the next version of X.509 contains the trust broker as a new trusted third party for RPs, and the current working draft of X.509 (2016) [24] contains the four cornered model shown in Fig 4-A. We have also started an implementation of a trust broker service and protocol. We call it the "unified approach" because it is applicable to both the open and closed deployment models of PKIs (Fig. 4-B). When an RP receives a certificate, its client sends a query to the trust broker asking it about the trustworthiness of the certificate. The trust broker responds by providing three types of information:

- Quality of Certificate (QoCER): a score between 0 and 1 representing the level of trust that can be placed in the certificate;
- Confidence Level (CL): a score between 0 and 1 that indicates to what extent the trust broker is confident in the QoCER recommendation sent to the RP;
- Usage information about the recommended or allowed uses of the certificate.

The RP's proposed certificate's use is only provided to its client rather than to the trust broker for privacy reasons. Consequently the trust broker has to enumerate all the allowed uses for the certificate. This list should be structured enough to allow the client to match the appropriate use and present this to the RP. For example, the list could contain: {"Bank Server authentication", "E-mail server authentication",

"Buying a product with 5000$ maximum", "multimedia server authentication", etc.}. Part of our future research is to determine the way this information should be structured in order to allow efficient matching. If there is no intersection between the proposed use and the trust broker's list, then the client will recommend the RP not to use the certificate. Further information about the calculation of OCER, CL and the usage parameters can be found in [22]. Once we have finished the pilot implementation we propose to offer the protocol to a standards body such as the IETF of OASIS.

A direct application of our work could be to help RPs to decide about the juridical validity of a digital signature apposed on a document. The juridical validity of a digital signature depends in part on the quality of the CA's management procedures of the certificate used to validate the signature. The score of QoCER represents in this case the juridical validity of the signature and can help the RP to decide whether to accept the signed document or not.

In previous research, Jon Olnes [21] introduced a new entity, called a "Validation Authority" (VA), to help RPs take decisions about certificates. It is similar to our concept of a trust broker. The relationship between a VA and RPs must be regularized through contractual agreements. However, the interoperability differences between countries are not explained and thereby the role of the VA is not completely justified. Additionally, the author doesn't provide information about the nature of recommendations to send to RPs. Finally, the concept of contextual recommendations is not considered.

5 Conclusion

X.509 certificates have been widely adopted today for the realization of different security services. However, many problems still slow the adoption of this technology by (mainly human) RPs, one of them being the interoperability problem. One of the objectives of this paper was to clarify the interoperability problem and we have shown that juridical, organizational and technical differences between countries are the main reasons for this problem. We have proposed to solve this from a trust management perspective, by extending the X.509 trust model to include a new trusted third party called the trust broker. We have also started to implement this role as a new TTP service to be offered to RPs.

References

1. Hanna, S.R., Pawluk, J.: Identifying and Overcoming Obstacles to PKI Deployment and Usage. In: 3rd Annual PKI R\&D Workshop. NIST, Gaithersburg (2004)
2. Smith, P.: Internet Based Payments Application - Trust and Digital Certificates. In: 16th Payment Systems Internatoinal Conference (PSIC), Bruges, Belgium (May 2000)
3. Organization for Economic Co-operation and Development (OECD): The OECD report on regulatory reform: Synthesis Paris (1997), http://www.oecd.org/dataoecd/17/25/2391768.pdf
4. PKI Assessment Guidelines of the American Bar Association, http://www.abanet.org/scitech/ec/isc/pagv30.pdf

5. United Nations Commission on International Trade Law: Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods (2009) ISBN 978-92-1-133663-4
6. Susanna, F.F.: Saving Rosencrantz and Guildenstern in a virtual world? A compara-tive look at recent global electronic signature legislation. Journal of Science and Technology Law 7 (2001)
7. Deffains, B., Winn, J.K.: Governance of Electronic Commerce in Consumer and Business Markets. Social Science Research Network (2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1099516
8. Moringiello, J.M., Reynolds, W.L.: Survey of the law of CyperSpace Electronic Contracting Cases 2007-2008. Business Lawyer 64 (2008)
9. Winn, J.K., Bix, B.H.: Diverging Perspectives on Electronic Contracting in the US and EU. Clev. St. L. Rev. 54, 175 (2006)
10. Winn, J.K.: What protection do consumers require in the information economy? Law Ethics & Society 4, 84–102 (2008)
11. Winn, J.K., Yuping, S.: Can China Promote Electronic Commerce through Law Reform-Some Preliminary Case Study Evidence. Colum. J. Asian L. 20, 415 (2006)
12. Winn, J.K., Jondet, N.: A 'New Approach' to standards and consumer protection. Journal of Consumer Policy 31(4), 459–472 (2008)
13. National Strategy for Trusted Identities in Cyberspace, Daft (2010)
14. Winn, J.K.: Information Technology Standards as a Form of Consumer Protection Law (2008), http://www.law.washington.edu/Directory/docs/Winn/Info_Tech_Stds.pdf
15. Guidelines for the issuance and management of extended validation certificates (2007), http://www.cabforum.org/EV_Certificate_Guidelines.pdf
16. Kennedy, S.: The political economy of standards coalitions: Explaining China's involvement in high-tech standards wars. Asia Policy 2, 41–62 (2006)
17. Martínez-Nadal, A., Ferrer-Gomila, J.L.: Comments to the UNCITRAL Model Law on Electronic Signatures. In: Chan, A.H., Gligor, V.D. (eds.) ISC 2002. LNCS, vol. 2433, pp. 229–243. Springer, Heidelberg (2002)
18. European Commission: The study on the standardisation aspects of eSignatures (2007), http://ec.europa.eu/information_society/eeurope/i2010/docs/esignatures/e_signatures_standardisation.pdf
19. Van Eecke, P., Pinto Fonseca, P., Egyedi, T.: EU Study on the specific policy needs for ICT standardisation: Final report (2007)
20. Winn, J.K.: US and EU regulatory competition and authentication standards in electronic commerce. Journal of IT Standards and Standardization Research 5(1), 84–102 (2006)
21. Ølnes, J.: PKI Interoperability by an Independent, Trusted Validation Authority. In: 5th Annual PKI R&D Workshop 2006 (2006)
22. Wazan, A.S., Laborde, R., Barrère, F., Benzekri, A.: A formal model of trust for calculating the quality of X.509 certificate. Security and Communication Networks 4(6), 651–665 (2011)
23. Draft Regulation on "electronic identification and trusted services for electronic transactions in the internal market" (2012)
24. ITU-T Rapporteur Q.11/17. Rec. ITU-T X.509 (2012) | ISO/IEC 9594-8 : 2012 Information Technology - Open systems Interconnection - The Directory: Public-key and attribute certificate frameworks – Working Draft for Adm. 2: Directory-IdM support. TD0241, Geneva, April 17-26 (2013)

The Power of Hands-On Exercises in SCADA Cyber Security Education

Elena Sitnikova[1], Ernest Foo[2], and Rayford B. Vaughn[3]

[1] University of South Australia
elena.sitnikova@unisa.edu.au
[2] Queensland University of Technology
e.foo@qut.edu.au
[3] Mississippi State University
vaughn@research.msstate.edu

Abstract. For decades Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) have used computers to monitor and control physical processes in many critical industries, including electricity generation, gas pipelines, water distribution, waste treatment, communications and transportation. Increasingly these systems are interconnected with corporate networks via the Internet, making them vulnerable and exposed to the same risks as those experiencing cyber-attacks on a conventional network. Very often SCADA networks services are viewed as a specialty subject, more relevant to engineers than standard IT personnel. Educators from two Australian universities have recognised these cultural issues and highlighted the gap between specialists with SCADA systems engineering skills and the specialists in network security with IT background. This paper describes a learning approach designed to help students to bridge this gap, gain theoretical knowledge of SCADA systems' vulnerabilities to cyber-attacks via experiential learning and acquire practical skills through actively participating in hands-on exercises.

Index terms: industrial control systems, SCADA, critical infrastructure, cyber-security, experiential learning, security laboratory, curriculum.

1 Introduction

Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) are used for remote monitoring and control physical processes in many critical industries including electricity generation, gas pipelines, water distribution, waste treatment, communications and transportation. Increasingly today, these systems are being interconnected with corporate networks via the Internet. This makes them vulnerable and exposes them to the same risks as those experienced in cyber-attacks on a conventional network.

In recent years, research and education in the area of cyber security of ICS and SCADA systems has attracted interest within academic institutions. With the Australian

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 83–94, 2013.

Prime Ministerial directive recently announced by the Hon Julia Gillard and the launch of a new Cyber Security Centre [1], more researchers will begin to investigate the problem set associated with such systems and their critical roles in monitoring and control of Australian Critical Infrastructures. There is also a high industry demand in cyber security training for ICS and SCADA systems. However, many existing research centres are limited by the lack of testbeds or models capable of representing actual instantiations of ICS applications and an inability to observe an entire SCADA system. The reasons are usually high costs and limited space for such laboratories.

The Idaho National Laboratories (INL) SCADA Testbed Program is a large scale program dedicated to ICS cyber security assessment, standards improvements and training [2]. For several years Australian operators of critical industrial control systems have been attending one week training provided by INL in the US. The Australian government Attorney General's Department has subsidised attendance for selected attendees. This training which balances theory and practice is valuable. However from an Australian perspective the benefits are limited, because the time available limits the areas covered and it is a 'one off' opportunity, with substantial costs for the fortunate few attendees. These factors create an urgent need for locally based educational programs which aim to build awareness and relevant skills across the critical infrastructure industries. Local programs would also allow the curriculum to be customised, reflecting specific Australian directives and best practices. It would also cover a broader range of topics and delve more deeply into them. Local training capability also scales up better allowing an increase in the volume of students for a better return on investment.

This paper describes the authors' experience in designing and developing hands-on practicals in the two university courses listed below and their value in discovering vulnerabilities in SCADA systems. The cost of travelling overseas to undertake this kind of training is prohibitive, so locally offered courses such as these minimizes expenses and maximizes opportunities for operators to gain critical education in this area.

- COMP 5062 Critical Infrastructure and Process Control Systems Security (Masters level) course at the University of South Australia (UniSA)
    - At UniSA, hands-on practicals are presented during a one week intensive study workshop that balances the content of lectures with hands-on practicals delivered in our security laboratory set up temporarily on equipment provided by industry collaborators.
- Cyber-security 5 days training at the Queensland institute of Technology (QUT)
    - At QUT, the curriculum for a 5 day Cyber-security training is focused on providing education and local training for professionals working in the control system industry, as well as for graduates hoping to enter the field.

By way of background, researchers at both UniSA and QUT established a cross-institutional collaboration in 2011 when they first met at the Idaho INL training facilities. This initial connection was expanded internationally through strong

collaborations with Mississippi State University (MSU) in the United States. This involved exchanges of faculty members, the establishment of SCADA laboratory facilities at QUT similar to the MSU laboratory and the exchange of virtual SCADA testbed software with UniSA. This collaboration has already resulted in several joint papers in the field [3,4] and plans for an international research and educational project between the three universities involved, MSU, QUT and UniSA.

The paper is organised as follows. Section 2 describes the needs of education in SCADA and ICS systems and highlights the challenges of educating both IT personnel and SCADA engineers. Section 3 examines tailoring reflective practice and active learning pedagogical approaches. In Sections 4 and 5 we provide details on the practical laboratories that we developed at QUT and UniSA and comment on the value that they provided to the students. Section 6 outlines some benefits, limitations and preliminary findings of how students responded to courses with a focussed on hands-on practical component. We conclude this paper by reviewing our contributions and future work.

2 The Need

According to an international commentator and INL's infrastructure protection strategist Michael Assante, for managers and engineers responsible for control systems, physical security has always been a priority [5]. For many also, IT security is a new field. They have to understand the importance of these systems' cyber security requirements, associated risks and thus deploy proper security measures. Assante in his testimony to the US government on process control security issues, criticises the last decade's considerable body of research in implementing yesterday's general IT security approaches into today's ICS and SCADA systems. He asserts it has "proven ineffective in general IT systems against more advanced threats". He also notes that as more technological advancements are introduced to ICS and SCADA, more complexity and interconnectedness are added to the systems, requiring higher levels of specialty skills to secure such systems. Training managers and process control engineers in the field will help to meet this skills need gap.

Other literature states that SCADA and process control systems vulnerabilities can increase from a lack of communication and/or trust between IT and engineering departments [6]. This is because very often SCADA networks services are viewed as a specialty subject, more for engineers than standard IT personnel. Control system operators are often mistrustful of IT maintainers because ICS has a 24/7 uptime requirement whereas IT maintenance often requires system outages. Previously [7,8,9, 10] authors have recognised these cultural issues and highlighted the gap between specialists with ICT engineering skills and the specialists in network security with IT background.

The gap between these two disciplines needs to be bridged to recognise, identify and mitigate against vulnerabilities in SCADA and process control systems networks. Broader awareness and the sharing of good practices on SCADA security between utility companies themselves is a key step in beginning to secure Australia's critical Infrastructure.

Industry-trained professionals and qualified learners, today often working in process control services and government organisations, bring to class their

fundamentally different skills, objectives and operating philosophies to the concept of security in an enterprise IT context. Thus, the authors are challenged to develop a curriculum that aims to address both discipline-specific engineering and IT issues and bridges the educational gap between IT network specialists and process control engineers, but within the post-graduate cyber security and forensic computing nested programs. To address these issues, the curriculum is designed to accommodate both process control engineers (with no or limited IT skills) and IT specialists (with no or limited engineering skills). This in itself is a difficult balance to achieve.

3 Learning and Teaching Aspects

3.1 Reflective Practice

Our students' diverse skill set has motivated educators at UniSA to implement a reflective practice approach to the hands-on exercises as a part of their assessment task. According to the literature, reflective practice enables students to: 1) understand what they already know; 2) identify what they need to know in order to advance their understanding of the subject; 3) make sense of new information and feedback in the context of their own experience and 4) guide choices for further learning [11]. Considerable literature attests to its benefits. In the mid-late 80s, researchers Kolb, Schon and Boud et al. [12-14] highlighted the major benefit of reflective practice as enabling learners to make sense of their practical experiences and develop critical thinking skills which are essential for decision making and problem solving, especially in the workplace. It has been argued [15] that reflection can be used as a tool to help learners through their studies by encouraging and fostering a deep learning approach. Unlike many other professions and disciplines, especially those in science, health and medicine, that have long adopted this pedagogical practice, engineering and ICT education have only recently begun to adopt this practice [16].

A reflective practice pedagogical approach has been introduced in the COMP 5062 Critical Infrastructure and Process Control Systems Security 4.5 unit course at the University of South Australia. Using well-structured hands-on practical exercises, students experience the technical details of what they have learned from the associated lecture topics. They then reflect on the skills gained, in the form of a written report by the end of the intensive week. Below, we discuss how hands-on practicals are aligned with a 4 step reflective practice process that enables students to

1) *understand what they already know;*

Prior to the intensive week, students have to complete a brief questionnaire on what they know about SCADA systems security. This allows instructors to identify students' backgrounds, work experience and knowledge in control systems. It also provides information for making informed decisions on how to form groups where diverse skills complement each other's skills to aid collaborative work.

2) *identify what they need to know in order to advance understanding of the subject;*

This step requires planning intensive week activities to balance theory and practice. Every daily session presents theory to students with active discussion, addressing focussing questions. This gives students knowledge prior to laboratory practicals.

3) *make sense of new information and feedback in the context of their own experience;*

The Intensive workshop is constructed to be informative and active, with timely feedback and support from instructors. Reflection on new gained knowledge is demonstrated during active participation in group discussions, oral presentations and written reports on the results from practicals.

4) *guide choices for further learning*

Building on knowledge during the intensive week, students reflect on comments and suggestions provided and then write their further assignment component - a SCADA Security Plan (SSP). The plan takes a form of the academic paper that includes a literature review on the topic and is based not only on theoretical scholarly knowledge, but also on the technical knowledge that students have gained.

QUT educators also implement a reflective practice approach to students' learning. For most of the courses there is an endeavour to ensure that there are three types of sessions. The intent is to provide a theoretical basis for the material, reinforce this with practical application and finally, encourage students to integrate the learning by actively reflecting on the sessions.

- *The first session* is a lecture type session where students are introduced to the theoretical aspects of the material. Students learn where issues fit into the bigger picture. Often, cyber security training courses concentrate on particular vulnerabilities without teaching the background theory. This makes it difficult for students to adapt when faced with a new attack or other scenario.
- *The second session* is a practical hands-on exercise relevant to the topic. Some courses provide only theory or lecture based courses. These are good for awareness issues, but it is not until students successfully complete a hands-on exercise that the impact of the security issue hits home. The use of complex full system hands-on exercises such as a red team, blue team exercise is particularly good at providing an impact to students.
- *The third 'debrief'* session, occurs after the practical session. Here, the course instructor encourages students to discuss the impact of the previous exercise and relate it to their industry experiences. These open discussion sessions allow students to share their insights. Ideally, course instructors arrange for a break between the practical session and the debrief session. This allows students to reflect internally and synthesise the application of the hands on exercise that they have just completed. We have found in previous cyber security courses that the debrief sessions are often described by students as the most useful aspect of the course.

The authors next describe a set of hands-on exercises that are designed to help students to overcome the ICS/IT gap, gain knowledge through experiential learning of SCADA systems vulnerabilities to cyber-attacks and reflect this knowledge by actively participating in hands-on cyber security exercises.

4 Intensive Hands-On Practicals at UniSA

UniSA has developed a new Master of Science (Cyber Security and Forensic Computing) one and a half year full time equivalent program. It offers a pathway through

a suite of nested programs including Graduate Certificates, a Graduate Diploma, Masters and possible continuation into PhD level program. These are designed to attract a diverse group of learners traditionally coming from two cohorts of industry practitioners: one with engineering (SCADA practitioners) and the other (ICT personnel) with IT background. It also enables industry-trained and qualified learners without undergraduate degrees, to gain the security qualification required though their access to tertiary study [8]. Within the program students have to complete eight core courses before they study a Minor Thesis 1 and 2. The COMP 5062 Critical Infrastructure and Control Systems Security course is one of the eight courses the program offers.

As the majority of these students are working and studying part-time, we need to accommodate their needs. To maximise flexibility, availability and convenience, the CICS course is offered to part-time students in online distance study mode (external class) – 1 virtual online class per course per week over 12 weeks plus one week half day intensive study in-class per course (15 hours).

The intensive face-to-face component is not mandatory for external students, but highly recommended. It is a cornerstone of the curriculum and it always occurs in week 4 of the study period. Students from both external and internal classes have an opportunity to attend a face-to-face workshop in Adelaide and participate in hands-on practicals, guest speakers' presentations and also networking opportunities among peers. During an intensive study week when students attend a half day face-to-face session at Mawson Lakes campus at UniSA, they attend lectures and guest speakers' presentations from industry, police, and law enforcement agencies. Students receive the majority of the course materials and hands-on exercises in class. Exercises are based on operational world situations run by industry practitioners. A brief overview of the intensive week is described in Table 1.

5 A Continuing Professional Education (CPE) Training Program at QUT

QUT has developed a Continuing Professional Education (CPE) training program teaching cyber security for industrial control systems. This course is mainly designed for control systems engineers to raise awareness of the impact of cyber attacks on the systems that are under their control. The course also caters to IT security professionals who wish to gain an understanding of control systems and the issues that face control system designers. The course is taught at a postgraduate level, as participants are mainly experienced engineers or IT professionals. Figure 1 (2-4) shows the QUT's laboratory module. The pioneer of the SCADA laboratory was Mississippi State University which first established the lab through support from the US National Security Agency and the US Department of Homeland Security. QUT purchased their lab from the same engineering company used by MSU to insure compatible configurations that will support future research experimentation between the two institutions.

As Control Systems become integrated with IT systems, engineers and IT professionals are now expected to understand the vulnerabilities and threats that affect industrial control systems under their protection. As a result they need to be familiar with general system exploitation techniques and tools that may be used against their system services and applications.

Table 1. A brief overview of the intensive week at UniSA

	Day 1	Day 2	Day 3	Day 4	Day 5
Short Lecture	SCADA control systems fundamentals	SCADA Specific Protocols Modbus and DNP3			**Recap and the summary** Students present on what they have learned during intensive week. During this session students reflect on the knowledge they have gained during the week.
Practical Lab	Programming and testing of PLC.	Modbus Communications	SCADA Vulnerability assessment Part 1	SCADA Vulnerability assessment Part 2	
Lab Configurations	Virtual machine pre-installed with PLC programming software with emulation ability; HMI programming software with runtime ability, SCADA development and runtime software.	Virtual machine pre-installed with ModScan, MovServ software; Hex editor; Wireshark open source ; Hyper Terminal communication software; serial port capture, Modbus RTU parser	System is deliberately configured to be highly vulnerable with network in a "bad" condition. Different platforms are used (NT3.5, NT4, Win98) with un-patched software installed	System configured to be less vulnerable with network in a "good" condition. Tasks included: blue/red team exercise with red as attackers and blue as defenders. Students are provided with Backtrack software.	
Task	Students have to write a PLC program starting from a single traffic light operation, adding later multiply traffic lights and include pedestrian lights and extending PLC program to include external control for emergency such as fire and ambulance. With SCADA running and its graphical control through HMI, students have exposure to detect PLC faults and fix them to ensure SCADA operates in correct way.	Students study Modbus RTU and Modbus TCP serial packets using ModScan and ModSim; forming of a Modbus packet to inject and manipulate of the traffic PLC.	The Blue/Red team exercise with red as attackers and blue as defenders of the traffic control system (Fig.1). Students are provided with Backtrack software.	The Blue/Red team exercise with Red as attackers and Blue as defenders. Students are provided with Backtrack software.	
Assessment	Worksheet completion with the comments /solutions demonstrated	Worksheet completion with the comments /solutions provided	Group presentations and discussions on Day 5	Group presentations and discussions on Day 5	

This course aims to give an understanding of the fundamental concepts and major issues in the area of industrial control system cyber security. Students will be able to identify critical application and system service vulnerabilities and determine the information security implications of those vulnerabilities upon completion. The course introduces of a range of techniques for exploiting and mitigating the impact of threats and vulnerabilities to networks and systems.

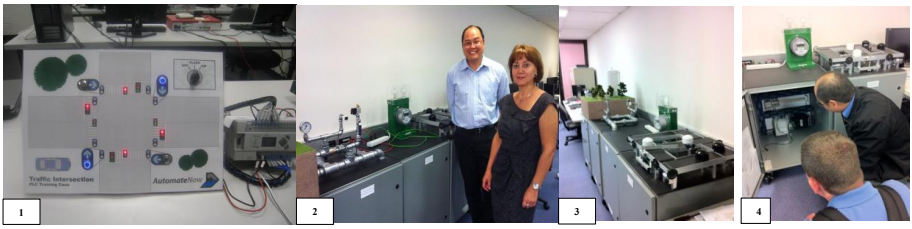


Fig. 1. A SCADA Traffic Control System Lab at UniSA (1), Pipeline, Smart Meter and Conveyer Laboratory Simulators at QUT (2-4)

It is important to point out that this course discusses design and testing principles that produce secure applications. During this course techniques and tools are introduced that demonstrate how to exploit system services and applications. Each day of class consists of several information style presentations followed by a relevant practical exercise.

The course is an intensive five-day course delivered in one week. Students must travel to Brisbane to participate. The course has seen representation from students from a wide range of industrial sectors including transport, power, gas and water treatment. Students have travelled from all around Australia to attend the course even though a similar course is held in Western Australia.

The cornerstone of the QUT program is an 8 hour practical exercise. The course participants are divided into a blue team and a red team. The Blue team must defend a corporate network that is connected to a real industrial control system process. The Red team must attack and disrupt the industrial process. The QUT program employs small scale industrial process systems that use industrial PLCs to control them. These systems are also used to conduct research in the area of industrial control system vulnerabilities and the testing of mitigation strategies.

The following is a brief overview of day to day content included in the QUT's five-day course (Table 2)

Table 2. A brief overview of the content of the CPE training program at QUT

Day 1	Day 2	Day 3	Day 4	Day 5
The first day begins with an introduction to cyber security and control systems. Definitions of threats and vulnerabilities are covered and a round up of recent security incidents is discussed. It culminates with a practical demonstration of a MODBUS control system being compromised.	The second day looks at common web application vulnerabilities such as cross site scripting, cross site request forgery and SQL injection. In the afternoon we look at authentication systems. The practical exercises involve demonstrating common password cracking strategies.	The third day looks at network vulnerabilities and exploit frameworks. We start the day by discussing network discovery techniques. The final section of the day looks at network mitigation strategies and the use of firewalls and intrusion detection systems.	The fourth day of the course is the key learning event for the course. The Red Blue team exercise is an eight hour event where the blue team must defend their industrial process from the red team.	The fifth day is a closing day where the students reflect on the week they have completed. Student from the red team and blue team give presentations that reflect on the processes and incidents that occurred in the Day 4 exercise. The instructors conclude the day by emphasising key points, as well as revealing any components of the Red Blue Team exercise that could have been handled better by the respective teams.

6 Discussions

Experience on running of hands-on practicals and the lessons we have learned could be categorised as benefits, limitations and observations.

Benefits. IT personnel together with control systems engineers have to encounter non-standard IT systems and learn how to protect SCADA and ICS and make them less vulnerable to cyber-attacks.

Limitations. Unlike QUT, UniSA does not have its own laboratory. For this reason academics rely on local industry practitioners to design, establish and run the lab once a year for a week. UniSA provides licences for required software, but hardware equipment is generously provided by industry collaborators.

Observations. At UniSA Students demonstrated good results (grades for hands-on practicals), they also summarised and reflected on what learned during the week during their oral presentations in class, but they were informally assessed by educators and fellow students. It would be better to include this activity in a formal submission with appropriate weighting.

One of the major goals of the course is the applicability of knowledge gained to students' work environments. We received positive feedback from students to this effect:

> *"It's been so much more than I expected - a good balance of technical along with practical skills that will hopefully help me gain employment" (Student #1, 2011, Adelaide)*

> *"The subject matter covered throughout the course was generally directly relevant to the industry I work in. The assignments were very helpful and relevant. Data collected during the first assignment and the report generated as part of the second assignment was able to link directly with issue within my own enterprise and been able to submit internally within the enterprise for further action". (Student #2, 2011, Adelaide)*

QUT Course Structure

The QUT training course has its origins in coursework adapted from normal coursework security classes that are offered to postgraduates and undergraduates. As a result the lecture presentations were quite theoretical and lengthy. There has been a concerted effort to streamline these presentations and to allow more time for students to explore and experiment in the practical exercises associated with each topic. This is also important for preparing students for the Day 4 Red/ Blue Team exercise.

Course Content

The content of the QUT training course is based on several classes that make up the undergraduate and postgraduate degree courses. This content previously had a strong focus on web vulnerabilities. While this has been very educational and interesting for

students, the relevance to industrial control systems is less clear. It should be noted that some industrial control systems do employ a web interface. There are other relevant areas of security that have been previously omitted from early courses because of time constraints. These topics, such as the effect of social engineering and phishing attacks will be included in the next iteration. Also, basic introductions to malware functionality, operation and analysis will be included. These two main topics are more relevant to control system engineers, as they are the threat most likely to be encountered in their daily operations.

Red/Blue Team Exercise

The QUT course development team spent a large amount of time and effort in creating the Red/Blue Team exercise on the 4th day of the course, aiming to produce an environment as detailed and as realistic as possible. This complexity enables students to immerse themselves in the scenario and really invest in their tasks. Overall this has been a great success, with some students becoming too emotionally involved in the scenario. The many ingredients include a realistic corporate network and DMZ, physical separation of red and blue teams into their own areas, CCTV monitoring systems and localized VOIP communications. One of the key areas that has added to the realism of the exercise is the use of real control systems, combined to produce an industrial process that the Blue team must monitor and operate throughout the day. A complex sequence of events must be completed for one instance of the process to be completed. The Blue team is rewarded with points for every time the sequence is completed. The industrial process involves three of the simulators available at the QUT SCADA security research laboratory. These include a water reservoir, conveyer system, and gas pressure system.

While the Red/Blue Team exercise was successful, aspects of the exercise can be improved. Besides fixing bugs in the system, it is important that both teams are monitored closely. We employed CCTV cameras to monitor the teams as well as network monitoring software, to ensure that Blue team servers continued to function. However the QUT development team realized that a closer monitoring of the network is required, in particular the monitoring of password changes by both the attacking and defending team. In the next course iteration, custom software will be used to monitor password files.

Another important aspect for the Red/Blue team exercise that links with monitoring students is that organisers should ensure that scripted events occur during the 8 hour length of the exercise. The Red Team should not be able to beat the Blue team in the first hour, but should not be stuck for hours on a particular problem either. The Red Team should have to meet a set of achievable goals within certain time restrictions. These do not necessarily need to match or oppose the goals of the Blue team. For example the Red team can be tasked with exfiltrating company secrets while the Blue team's main goal is maintaining the industrial process. Contingencies should be made by the course organizers to ensure that key learning outcomes are made for both the Red and Blue teams equally.

One option for running the Red/Blue exercise is to only have students participate as part of the Blue team as that is where industry will require them to operate. However since the teaching staff have set up the exercises and know all the avenues to access the Blue team network, the exercise would seem too artificial to the students. Ideally, past students should be invited back to play different roles such as the Red Team if they have participated originally as the Blue team. However this scenario is currently difficult, because students travel from all over Australia. It might be possible if the exercise were offered to local students in other award courses such as a Bachelors or Masters degree.

Experiences at UniSA and QUT have shown that large complex practical exercises for cyber security training have a deep impact on students' learning, enabling students to reflect on newly learnt theory and apply new skills and insights to following assignments and later to their workplaces.

7 Conclusion and Future Work

This paper has described two courses developed in two Australian universities – the University of South Australia (UniSA) and the Queensland University of Technology (QUT). From an Australian perspective, our work in developing courses in SCADA systems security aims to educate locally SCADA practitioners with engineering backgrounds and ICT personnel.. Establishing a local facility both to provide training and research into industrial control systems security should have substantial benefit. Establishing these course curriculum and practical laboratories in Australia gives more opportunity for local systems owners and operators to provide feedback so that local conditions can be more easily taken into account.

Another aim is a collaborative effort of two Australian universities - University of South Australia (UniSA) and Queensland Institute of Technology (QUT) towards an international project with Mississippi State University (MSU) in the United States. Plans are underway to engage our respective students in this project which will attempt to implement a trans-Pacific red team/blue team exercise.

Our future plans include expanding our research and education in the area of SCADA and ICS security by developing

- an external penetration hands-on exercise from the UniSA to a QUT laboratory;
- a remote vulnerability testing between laboratories in Australia (QUT) and United States (MSU);
- a working simulation model of ICS that provides accurate responses to sets of inputs (thus allowing some research experimentation to take place without using a physical laboratory)

Acknowledgements. The authors would like to acknowledge Mr Cameron Sands and Mr Ben McInerney of AutomateNow for their assistance in developing hands-on exercises for COMP 5062 course intensive week practicals at UniSA described in this paper and Dr Patricia Kelly from UniSA for editorial advice.

References

[1] Julia Gillard - Cyber Centre PMC's announcement (January 2013), http://www.theaustralian.com.au/national-affairs/defence/julia-gillard-announces-cyber-security-centre-warning-a-long-fight-lies-ahead/story-e6frg8yo-1226559907481 (viewed April 6, 2013)

[2] Common Cyber Security Vulnerabilities Observed in Control Systems Assessments by INL NSTB Program. Idaho national Laboratory. Idaho Falls, Idaho 83415 (November 2008)

[3] Morris, T., Vaughn, R., Sitnikova, E.: Advances in the Protection of Critical Infrastructure Improvement in Industrial Control System Security. In: Morris, T., Vaughn, R., Sitnikova, E. (eds.) Australasian Computer Science Week, January 29-February 1. University of South Australia, Adelaide (2013)

[4] Vaughn, R., Morris, T., Sitnikova, E.: Development and Expansion of an Industrial Control System Security Laboratory and an International Research Collaboration. In: 8th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW8), Oak Ridge, TN, January 8-10 (2013)

[5] Assante, M.J.: Testimony on Securing Critical Infrastructure in the Age of Stuxnet. National Board of Information Security Examiners (November 17, 2010)

[6] ITSEAG, Achieving IT Resilience Summary Report for CIOs and CSOs, http://www.tisn.gov.au/Documents/ITSEAG+Resilience+Paper+CIO+Report+(PDF).pdf (viewed 6 April, 2012)

[7] Slay, J., Sitnikova, E.: Developing SCADA Systems Security Course within a Systems Engineering Program. In: Proceedings 12th Colloquium for Information Systems Security Education, Dallas, US (2008)

[8] Sitnikova, E., Slay, J.: Pathway into a Security Professional: a new Cyber Security .... ADFC Richmond, Virginia (2012)

[9] Sitnikova, E., Hunt, R.: Engaging Students through Reflective Practice Assessment within SSLS course, Orlando, US (2012)

[10] Foo, E., Branagan, M., Morris, T.: A Proposed Australian Industrial Control System Security Curriculum. In: 2013 46th Hawaii International Conference on System Sciences (HICSS), January 7-10, pp. 1754–1762 (2013)

[11] Hinett, K.: Developing Reflective Practice in Legal Education. UK Centre for Legal Education (2002)

[12] Kolb, D.: Experiential learning: experience as the source of learning and development. Kogan Page, London (1984)

[13] Schon, D.: Educating the Reflective Practitioner. Jossey Bass, San Francisco (1987)

[14] Boud, D., Keogh, R., Walker, D.: Reflection: turning experience into learning. Kogan Page, London (1985)

[15] Philip, L.: Encouraging reflective practice amongst students: a direct assessment approach, GEES Planet Special Edition- Issue 17 (2006), http://www.gees.ac.uk/planet/p17/lp.pdf (viewed February 27, 2012)

[16] Kaider, F.: Introducing undergraduate electrical engineering students to reflective practice. In: Proceedings of the 2011 AAEE Conference, Fremantle, WA (2011)

"Business Continuity and Information Security Maintenance" Masters' Training Program

Natalia Miloslavskaya, Mikhail Senatorov, Alexandr Tolstoy, and Sergei Zapechnikov

National Research Nuclear University MEPhI,
31 Kashirskoe Shosse, 115409, Moscow, Russia
{NGMiloslavskaya,MJSenatorov,tolstoy,SVZapechnikov}@mephi.ru

Abstract. The experience of preparing for the "Business Continuity and Information Security Maintenance" (BC&ISM) Masters' program implementation and realization at the "Information Security of Banking Systems" Department of the National Research Nuclear University MEPhI (NRNU MEPhI, Moscow, Russia) is presented. Justification of the educational direction choice for BC&ISM professionals is given. The model of IS Master being trained on this program is described. The curriculum is presented.

Keywords: Information Security, Business Continuity, Standard, Model, Curriculum, Bachelor, Master, Specialist, Higher Education, Master's Program.

1 Introduction

In current conditions the critical infrastructure companies are faced with the challenges of their activities disruption or interruption. The reasons differ significantly: disruptions in an energy supply and services delivery, dysfunction of the information and telecommunication systems, presence of the information security (IS) threats in their information sphere and intentional actions or errors of their personnel, resignation of their key personnel, as well as fires, floods, man-made disasters etc.

The "business continuity" (BC) term has appeared in the second half of the 90ties. It was used in connection with the uninterrupted operation of a whole company, including first of all its main (key) and auxiliary business processes.

The BC maintenance process is to ensure the restoration of the company's functioning in the event of any unexpected or undesirable incident that could negatively affect the continuity of the critical business functions and their supporting elements, with a threat of losing the entire business.

In the framework of this process it is important for every company to address issues of IS maintenance. Accidentally the best practices experience shows (e.g., ISO/IEC 27002) that IS maintenance serves a common goal of business development and ensuring its continuity, since the information assets protection against various types of the IS threats can minimize the IS risks and maximize ROI (Return On Investment).

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 95–102, 2013.

The IS management international standards' (27000 series) analysis has allowed to justify the urgency of the BC&ISM training program. Therefore it becomes evident at present that for the success of any business it is necessary to have knowledge in two interconnected areas – BC and IS. Thus the professionals with integrated knowledge, skills and abilities in these areas are in more demand than ever. That is why relevant staffing for the stakeholders is a very actual problem.

Analysis of the training programs, implemented by the various educational institutions of Russia and related to BC and IS, shows that a substantial dissatisfaction of the labor market needs in the professionals of this profile exists. That fact can be explained by the following reasons. Firstly, BC and IS maintenance (BC&ISM) refers to a fairly new area of a professional activity. Secondly, the dynamics of this area is such that the existing Russian educational system with its high inertia lags behind the labor market needs.

The situation is complicated by the fact that the national system of higher education has lack of BC&ISM professionals' comprehensive training. The BC issues are completely absent in the curricula of the existing IS training.

Partial satisfaction of the labor market needs is met at the level of an additional vocational training via implementation mainly of a few improvement courses and certification programs being implemented with an assistance of the BSI, the Disaster Recovery Institute, the BCM Institute etc. [1-3].

The article presents the experience of preparing for the implementation and realization of the "Business continuity and information security maintenance" (BC&ISM) Masters' program at the "Information Security of Banking Systems" Department of the National Research Nuclear University MEPhI (NRNU MEPhI, Moscow, Russia).

2 Choice of Educational Direction for BC&ISM Professional Training

The national system of higher education in Russia includes the following educational levels:

1) Bachelor (4 years' full-time training period, on the basis of the school education);
2) Master (2 years, continuing education after "Bachelor" qualification or the second higher education);
3) Specialist (5-5,5 years, on the basis of the school education).

There are two lists:

- a list of the training directions related to the implementation of the various profiles of bachelors and the various programs for masters;
- a list of the specialties.

For each training direction and each speciality there is the developed and approved basic national Federal state educational standard (with abbreviation FGOS from the Russian title of the standard) and corresponding approximate (so-called recommended) curriculum.

Taking into account the above-mentioned features of the professional activities related to BC&ISM, it is possible to consider the applicability of a particular level of education for the professionals training.

Firstly, a long-term training on the basis of higher education (bachelors, masters and specialists) cannot provide the required adaptation of the training content to the dynamically changing field of the graduates' professional activity.

Secondly, the strict framework for the training content, set by FGOS for bachelors and specialists, does not allow to take into account adequately the companies specifics under which BC&IS challenges are addressed and where the graduates of the educational institutions will work.

Thirdly, among the training directions and specialities there is no FGOS directly related to BC&ISM.

To our opinion the most appropriate way of addressing this challenge is to select an educational direction related to Masters' training. This approach has the following advantages:

- short training time (only 2 years);
- variability of the curriculum formation (up to 50 % of training time can be given to the subjects, developed by an educational institution itself and directly related to the chosen field of their graduates' professional activity);
- flexibility of the curriculum implementation (up to15 % of training time can be given to so-called "optional (selected by the students themselves from the proposed set, at their own choice) disciplines" when the students choose to study the particular subjects, reflecting the specific objects of their professional activity, with which they may work during their further employment);
- practical orientation of training (up to 25 % of training time can be given to the different types of practices (practical work), the implementation of their scientific and research works and preparation of a final qualifying work – PhD dissertation);
- curriculum adaptability (an educational institution must provide the students with a real opportunity to participate in their training program development themselves, including possible development of their individual educational programs).

The outlined above features enable to make a reasonable choice of the level of higher education "Master" as a base for the BC&ISM professionals' training.

The Master's program development involves its binding to a specific educational direction. BC management in the presence of the IS threats in the information sphere relates directly to IS management. Therefore it is expedient to choose the 090900 "Information Security" educational direction and the corresponding FGOS [4].

3 Model of a Graduate Trained on BC&ISM Master's Program

The model of a Master, trained on the BC&ISM program, should define the areas, objects and types of a graduate professional activity and also the professional tasks, which he/she can solve in a company, where he/she will work after graduation.

The modern Russian education is based on the so-called competence approach: the training outcome is stated as a list of the professional competencies that a student must acquire and that will determine its ability to apply his/her knowledge, skills and personal qualities to be successful in a particular area. Therefore the model should be supplemented by the appropriate professional competencies.

It should be noted that FGOS [4] contains the definition of the areas, objects and types of the professional activities, and also the professional tasks and the corresponding professional competencies related to basic IS Masters' training. These definitions were taken as a basis for describing the Master's model, adjusting them to a specific subject area of BC&ISM.

The professional activity's area for the BC&ISM Master's program graduates is the following: the areas of science, engineering and technology, covering the wide range of problems related to ensuring BC&IS of the key company's business processes in conditions of presence of the IS threats in the information sphere.

The professional activity's object for the BC&ISM Master's program graduates are the following:

- information resources and IT; computer, automation, telecommunication, information and analytical systems that ensure the key company's business processes;
- technologies ensuring BC&IS of the key company's business processes;
- methods and tools for designing, modeling and experimental testing of systems, ensuring BC&IS of the key company's business processes;
- management processes for ensuring BC&IS of the key company's business processes.

The professional activity's types for the BC&ISM Master's program graduates are the following:

- organizational and managerial;
- design;
- control and analytical;
- scientific and research;
- scientific and pedagogical.

The professional activity's types are related directly to a particular company's activities. At present the following companies' types that may need the BC&ISM professionals can be outlined:

1) companies that create and operate systems ensuring BC&IS of their business processes (such as banks);
2) companies developing such a systems (for example, system integrators);
3) companies engaged in control for assessing BC&ISM level of the key company's business processes (for example, auditors);
4) companies carrying out scientific research and providing education (such as scientific and research centers and educational institutions).

The professional activity's tasks for the BC&ISM Master's program graduates are the following:

1). BC&ISM systems' creation and operation relate to an organizational and managerial activity. Company's personnel are involved in addressing the following professional activity's tasks:

- participation in the projects on creating the BC&ISM systems for the key company's business processes;
- preparing some methodical and legal documents' drafts, proposals and activity for the BC&ISM systems for the key company's business processes;
- organization and implementation of a control activity for effectiveness assessment of the BC&ISM systems for the key company's business processes;
- organization of an activity on improvement, modernization and unification of the BC&ISM systems for the key company's business processes in compliance with the legal documents and requirements.

2). The BC&ISM system for the business processes development relates to a design activity of the company's personnel and includes addressing the following professional activity's tasks:

- system analysis of an application area, identification of the IS threats and vulnerabilities in the company's information systems, development of the BC&ISM requirements and criteria for the key company's business processes;
- conceptual design of the complicated systems, tool sets and technologies for BC&ISM for the key company's business processes;
- justification of a choice of the functional structure, organizational principles for hardware, software and information management of the systems, tools and technologies for BC&ISM for the key company's business processes;
- development of the BC&ISM systems and technologies for the key company's business processes;
- adapting of the modern BC&ISM techniques for the key company's business processes to a particular company on the basis of the domestic and international standards.

3). Implementation of the control functions on an assessment of the BC&ISM level for the key company's business processes is related to a control and analytical activity, addressing the following professional activity's tasks:

- development of the control and analysis activity's programs;
- effectiveness control of the measures being used for BC&ISM of the key company's business processes;
- implementation of the auditing programs for BC&ISM of the key company's business processes;
- composing of a control and analytical activity's documentation.

4). In carrying out the scientific research and educational activities the universal tasks listed in FGOS are addressed [4].

The BC&ISM Master's program is aimed at developing *the graduates' specific professional competencies*. At the end of the training they should be able:

- to analyze and explore the BC&ISM models and systems;
- to use in practice the BC&ISM standards;
- to analyze the IS risks in order to ensure BC;
- to conduct synthesis and analysis of the design decisions on a company's BC&ISM;
- to ensure the effective application of a company's information and technology resources to meet the BC&ISM requirements;
- to participate in design and operation of a company's IS incident management;
- to participate in design and operation of a company's BC&ISM systems;
- to conduct an instrumental IS monitoring in a company;
- to develop the proposals for a company's BC&ISM systems;
- to develop and effectively implement a complex of the BC&ISM measures (including rules, procedures, practical techniques, methods, guidelines, tools).

These professional competencies are established during a particular curriculum implementation.

4 BC&ISM Master's Program Curriculum

The BC&ISM Master's program curriculum (Table 1) has been created in 2011. It is a list of the disciplines with their labor content in credits and academic hours. All the disciplines are grouped in two training cycles:

- M1 - general scientific;
- M2 - professional.

Each training cycle has a basic part with a list of the disciplines determined by FGOS [4] and a variable part with the disciplines, identified by each educational institution itself and reflect the features of a particular Master's program.

The successful development of the professional competencies during the BC&ISM Masters' training is impossible apart from the specific objects. Therefore in each variable part there are some optional disciplines, reflecting the specifics of such an objects. In the given curriculum (Table 1) each optional discipline matches two disciplines related to the Russian credit and financial sector (e.g. banks) and to the Russian nuclear industry (corresponding to the specifics of the NRNU MEPhI). During training within each optional discipline a student studies one of these disciplines considering a company's specifics, in which he/she will work after the graduation.

With the development of the Master's program the number of the disciplines related to a specific optional discipline can be increased, thereby extending the range of the professional activity's objects.

The curriculum has another two cycles that determine the time required and the labor content of the practice (internship), scientific research works (M3) and final state certification (M4). This part of the curriculum involves the students into implementation of some specific projects related to the BC&ISM systems of a particular company's business processes.

This allows to create graduates' practical skills to apply the existing regulatory framework, to implement the IS risks (related to disasters) analysis, to establish the

proper criteria for evaluating the possibility of an IS incident transformation into a disaster, to determine the IS related disaster scenarios, to choose the strategies and tools to ensure IS during the disaster and to develop the coordinated BC&ISM programs.

Table 1. The BC&ISM Master's Program Curriculum

№	Cycles, modules and disciplines	Labor content	
		Credits	Hours
M1	**General scientific cycle (FGOS)**	**24**	**864**
	Basic part (FGOS)	**8**	**288**
	Humanitarian module (FGOS)	***3***	***108***
M1.B1	Economics and Management. Part 1 (Economics)	3	108
	Mathematical and natural sciences (FGOS)	***5***	***180***
M1.B2	Special sections of mathematics	3	108
M1.B3	Special sections of physics	2	72
M1.V	**Variable part (program)**	**16**	**576**
	Humanitarian module	***2***	***72***
M1.V1	Economics and Management. Part 1 (Management)	2	72
	Mathematical and natural sciences	***8***	***288***
M1.V	System analysis and system engineering	2	72
M1.V	Applied theory of reliability	2	72
M1.V	Decision making	2	72
M1.V	Knowledge-based analysis of data and processes	2	72
M1.VO	**Optional Disciplines**	**6**	**216**
M1.VO1	***Optional discipline 1:***	***2***	***72***
M1.VO1.1	Psychology and Pedagogy		
M1.VO1.2	Research and development management		
M1.VO2	***Optional discipline 2:***	***2***	***72***
M1.VO2.1	Banking system of the Russian Federation		
M1.VO2.2	Fundamentals of nuclear non-proliferation		
M1.VO3	***Optional discipline 3:***	***2***	***72***
M1.VO3.1	Banking basics		
M1.VO3.2	Fundamentals of nuclear technology		
M2	**Professional cycle**	**35**	**1260**
M2.B	***Basic (general professional) part (FGOS):***	**9**	**324**
M2.B1	Protected information systems	3	108
M2.B2	Objects' IS maintenance technologies	3	108
M2.B3	IS management	3	108
M2.V	**Variable part (program)**	**26**	**936**
M2.V1	Computer systems' security	5	180
M2.V2	BC&ISM basics	3	108
M2.V3	IS incident management basics	2	72
M2.V4	IS risks management basics	2	72
M2.V5	Information systems' disaster recovery	2	72
M2.V6	IT security assessment	2	72
M2.V7	BC maintenance management	2	72
M2.VO	**Optional Disciplines**	**8**	**360**
M2.VO1	***Optional discipline 1:***	***2***	***72***
M2.VO1.1	IS of credit and financial sector's companies		
M2.VO1.2	IS of nuclear objects		

Table 1. (*continued*)

№	Cycles, modules and disciplines	Labor content	
		Credits	Hours
M2.VO2	***Optional discipline 2:***	***3***	***108***
M2.VO2.1	Fundamentals of bank cards' security maintenance		
M2.VO2.2	Physical security of nuclear objects		
M2.VO3	***Optional discipline 3:***	***3***	***108***
M2.VO3.1	Electronic documents interchange security		
M2.VO3.2	Safety criteria and risk assessment		
M3	**Practice and Scientific Research Works**	**50**	**1800**
M4	**Final State Certification**	**11**	**396**
	Totally	**120**	**4320**

5 Conclusion

The IS management international standards' analysis has allowed to justify the urgency of the BC&ISM training program.

The experience of preparing for BC&ISM program implementation and realization at the "Information Security of Banking Systems" Department of the NRNU MEPhI shows that this program is more suitable to implement for Masters. Justification of the educational direction choice for the BC&ISM professionals is given.

The BC&ISM Master's program is designed for the applicants with the "Bachelor" qualification (for continuation of their higher professional education) or "Specialist" qualification (for the second higher education).

The model of IS Master being trained on this program is described. The model defines the areas, objects, types and tasks of a graduate professional activity.

The presented curriculum has been launched in the NRNU MEPhI from 2012. The first group of Masters (15 students) has started their training from fall 2012 and they still have not finished their first year.

Our findings may be useful for the tutors and managers of the similar training programs.

References

1. http://www.bsigroup.com/en-GB/iso-22301-business-continuity/iso-22301-training-courses
2. https://www.drii.org/education/education.php
3. http://www.bcm-institute.org/bcmi10/en/education
4. http://www.edu.ru/db-mon/mo/Data/d_09/prm497-1.pdf (in Russian)

Cyber Safety for School Children
A Case Study in the Nelson Mandela Metropolis

Johan van Niekerk, Kerry-Lynn Thomson, and Rayne Reid

Nelson Mandela Metropolitan University
{Johan.VanNiekerk,Kerry-Lynn.Thomson}@nmmu.ac.za,
s208045820@live.nmmu.ac.za

Abstract. Protecting the youth against the dangers posed by cyber space has become a matter of national priority. Parents often lack the necessary cyberspace know-how, to teach their own children how to be safe online. It has thus become the responsibility of society at large to educate the youth. This paper reports on a cyber safety poster creation campaign in the Nelson Mandela Metropolis in South Africa.

1 Introduction

For many nations, protecting the youth whilst they use cyber space, has become a matter of national importance. The UK National Cyber Security Strategy [1, p. 26] lists "tackle cyber crimes like online bullying..." as one of its "priorities for action". Klimburg [2] provides an overview of more than 20 National Cyber Security Strategies (NCSS), and notes that "Cyber security at the national level will fail when there is an inappropriate level of cyber security awareness and education" [2, p. 133]. Such awareness and educational campaigns should include all members of society and should range from primary and secondary school level, to awareness campaigns aimed at adults and the elderly [2].

The protection of national interests in cyber space has received a lot of focus in recent years. More than half of the NCSS examined in Klimburg [2] were introduced since the start of 2011. In fact, the international standard ISO/IEC 27032 [3], which differentiates cyber security from other forms of security, was first published in 2012. To a large extent, this urgency to address cyber security related issues stems from the speed with which the use of the World Wide Web has diffused through society.

The system that makes the World Wide Web possible was first created by Berners-Lee in 1990 and the first Web server became operational in 1991 [4]. Today, barely two decades later, an estimated 2.4 billion people uses the Web on a regular basis [5]. Use of the Web has permeated every aspect of many people's daily lives. The Web is used to play games, to do research, to conduct business, to perform personal financial transactions, and for many other daily tasks. Unfortunately the adoption and diffusion of many technological innovations often has undesirable and unanticipated consequences [6]. One such consequence is that the parents of the current generation of children mostly grew up before the Web

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 103–112, 2013.

existed. These parents are thus ill equipped to teach their children how to use the Web safely. It has thus become the responsibility of society at large to try to create awareness amongst children regarding the dangers posed by cyberspace.

This paper presents a case study of a cyber safety awareness campaign conducted amongst school children in the Nelson Mandela Metropolis. The researchers hosted a cyber safety awareness poster creation competition as part of a larger national cyber security awareness week. This paper presents the lessons learned during this campaign and also discusses some interesting observations made by the researchers during the campaign.

2 Methodology

The paper is structured according to the guidelines for a Case Study as presented by Creswell [7]. Creswell suggests the following structure:

- Entry vignette
- Introduction
- Description of the case and its context
- Development of issues
- Detail about the selected issues
- Assertions
- Closing vignette

In the context of this paper, the abstract and introduction to the paper respectively serves as the case study's entry vignette and introduction. The next section will describe the case and its context.

3 Description of the Case and Its Context

The South African Cyber Security Academic Alliance (SACSAA) was formed in 2011 by researchers from three South African universities, namely the University of Johannesburg (UJ), the University of South Africa (UNISA), and the Nelson Mandela Metropolitan University (NMMU). "The main objective of SACSAA is to campaign for the effective delivery of Cyber Security Awareness throughout South Africa to all groupings of the population" [8].

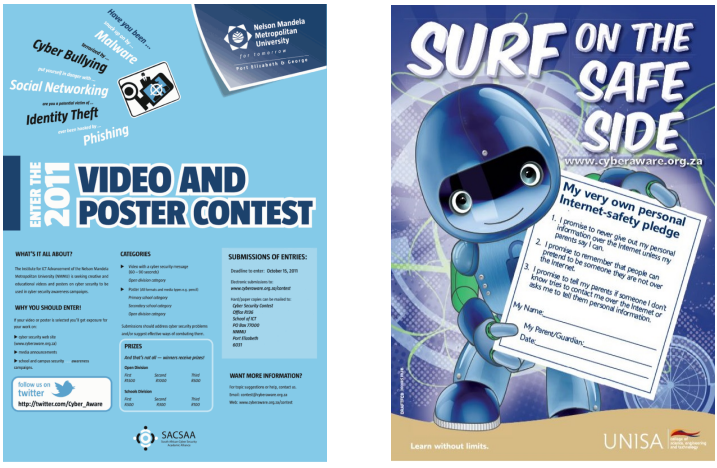
As part of its cyber security awareness activities, SACSAA hosted South Africa's first national cyber security week in October 2012. Preparations for this first national cyber security awareness week started in 2011. The initial plan was to host such a week in 2011. However, due to logistical reasons it was decided to postpone the first national week to 2012. Each of the three founding institutions committed to conducting at least one major cyber security awareness initiative as part of the activities for this national event. The NMMU researchers decided to host a cyber security awareness poster creation competition. This poster competition forms the focus of this case study. The case study will present a brief overview of the hosting of this competition and will report on the lessons learned by the researchers conducting this event.

4 Development of Issues

A 'trial run' of the planned poster creation competition was held in 2011. This was followed in 2012 by the first fully fledged competition. The following subsections will briefly describe how the hosting of the 'trial run' differed from the first fully fledged awareness competition in 2012.

4.1 The 'trial run' in 2011

The 2011 'trial run' started in the 3rd term of 2011. During this term hundreds of professionally created and printed promotional flyers, which advertised the competition, were distributed via 'snail mail' to schools in the Nelson Mandela Metropolis. Flyers were also posted on noticeboards across the NMMU campus. Figure 1a shows an example of the 2011 competition flyer.



(a) Competition Advertising Flyer

(b) Cyber Safety Pledge

Fig. 1. Examples of material distributed to schools

The 2011 'trial run' called for entries in the form of either awareness raising posters or videos. The posters could be submitted in either digital form or physical copies could be mailed as entries. The competition asked for entries in one of three categories, namely:

- A primary school division
- A secondary school division
- An open school division, which anyone could enter, irrespective of age

The competition offered cash prizes to the winners. These prizes were reasonably generous in the South African context.

Despite a lot of effort in the advertising of the contest during this year, only three posters and one video were received as entries for this 'trial run' competition.

4.2 The First 'official' Competition in 2012

In 2012 the first 'official' competition was hosted as part of the national cyber security awareness week. A lot of effort went towards not repeating the mistakes that were made during the previous year's 'trial run' competition. The following changes were made:

- Flyers to call for participation in the competition was printed during the first term of the year and immediately distributed. This was done because many school teachers who received flyers via the mail the previous year responded with concern that the third term was too late in the year for them to meaningfully encourage learners to participate.
- The competition was more focused. Only poster entries was called for and the previous year's video category was removed.
- Entries were restricted to the school children only. There was thus just a primary school and secondary school division call. The previous year's open division was removed because the researchers felt that this category did not meaningfully contribute to the actual raising of awareness amongst the entrants.
- The researchers visited several schools and delivered competition flyers in person. Whilst delivering these flyers effort was made to explain the context and purpose of the competition to the teachers involved.
- Following the hand delivery of competition flyers the researchers were invited to present cyber security talks at some schools. During these talks copies of an awareness flyer developed by the researchers entitled "Cyber Safety 101" were distributed to teachers and participating learners. These awareness flyers are discussed in depth in a later section.
- The competition received radio and media exposure as part of the larger national cyber security awareness week campaign. Following this exposure, many sets of competition flyers and accompanying basic awareness flyers were distributed on request to schools in several provinces.
- The competition was supported by the activities of other SACSAA member institutions. Of specific interest to this case is the distribution of a cyber security pledge form to learners in participating schools. This pledge form was signed by learners and signified that they pledge to 'surf on the safe side'. The pledge form listed three promises which all reinforced specific messages that also formed part of the messages on the "Cyber Safety 101" flyers. The pledge form and other awareness material distributed as part of the larger national campaign were branded with a 'mascot' in the form of a robot figure with a lock on its chest. The pledge form is depicted in Figure 1b.

The 2012 campaign had considerably more participants that the trial run in 2011. A total of 217 poster entries were received. Of these entries 94 were from

primary school children and 123 were from secondary school children. However, despite having many requests from schools located all across South Africa for competition flyers, educational material and additional information regarding how to enter, all entries received were from the Nelson Mandela Metropolis. In fact, all entries were received from schools that were visited in person by a member of the research team to advertise the competition and explain its purpose to learners and teachers.

The following section will provide more detail regarding the awareness message given during our visits at schools and will present the results of a content analysis performed on the poster entries received.

5 Detail of Selected Issues

5.1 Educational Flyer

During the initial 'trial run' in 2011 many teachers who were asked to encourage their learners to participate stated that they did not know enough about cyber safety and/or security to give advice to children regarding poster topics. This lead to the creation of an educational flyer by the researchers which were send to schools with the 2012 poster contest flyer. The flyer lists seven basic cyber safety 'rules' that children can follow to help them stay safe online. The contents of this flyer also formed the basis of the cyber safety talks presented at the schools by the researchers.

The following is a verbatim copy of the listed 'rules' on this flyer:

1. Protect your computer - As a minimum every computer should run an anti-virus program and a firewall. Very good antivirus and firewall software is available free of charge. Visit our website for more info.
2. Have a good password - A good password should contain UPPER and lower case alphabetic characters, numbers, and some special characters. Try using the first letter of every word in a sentence combined with a few twists like using the last word in full. For example: My name is Bob and I like to eat = MniBaIl2e@t.
3. Never share personal details online - One of the biggest online dangers is that criminals can find your personal information like your ID number, date of birth, address, or cell number and use it to steal your identity. Never post either your own, or anyone elses personal information online!
4. Dont trust anyone online - People you meet online are rarely who they say they are. Never believe that someone you met online is telling you the truth. Be especially wary of gifts, competitions, and other prizes. How can you win if you never entered?
5. Dont break the law - Illegal software, games, or music often contains hidden malware. Why would someone go through all the effort to crack the copy protection on a file if there is nothing in it for them?
6. Dont be a bully - Everything you post online stays there forever, even if you delete it. Do you really want the people you are going to work for one day to know how nasty you were to someone else today?

7. Trust someone - It is a good idea to have at least one adult you can trust who knows who you are talking to online and what you do when you are online. This could be a parent, uncle, aunt, teacher, or even a brother or sister.

The above mentioned flyer was handed out at all schools that were visited in person during 2012. Schools that requested that additional information be mailed to them via 'snail mail' also received copies of these flyers. Due to available time and logistical issues, schools that were initially visited and invited to participate did not receive copies of these flyers unless they were also visited a second time for the researchers to present a cyber safety talk to the learners.

5.2 An Analysis of the Poster Entries

All 217 poster entries in the 2012 competition came from only four schools, one was a primary school with most learners between the ages of 6 and 13 years of age. The remaining three were secondary schools with learners predominantly aged between 13 and 18 years old. All of these schools were amongst those visited in person by the researchers. However, only the primary school received a cyber safety talk and the accompanying copies of the "Cyber Safety 101" flyers. In all cases the researchers were contacted by the teachers of the entrants and asked to collect the poster entries for the entire school in a batch. The primary school children thus each had a copy of the topics suggested by this flyer, whilst the secondary school children's entries were primarily based on their own, or possibly their teacher's, perceptions of what would be relevant topics.

The authors performed a qualitative content analysis on all the poster entries that were received. For this analysis the following questions were asked for each poster:

1. What topic(s) is covered by the message(s) in the poster?
2. Is the poster specific to one category (form factor) of device?
3. How well has the cyber safety message been internalized (in the researchers opinion)?

Each of the above questions will be briefly elaborated on in the following subsections.

Posters per Topic. This question was asked to firstly determine how well the message contained in the 'Cyber Safety 101' flyer was received by the learners. Secondly the researchers wanted to know which specific topic(s) was seen as more important by the learners and whether or not there was a difference between the topics primary school children and secondary school children considered important. Figure 2 shows the results of this part of the analysis. As can be seen in Figure 2 the primary school children predominantly based their posters on messages contained in the "Cyber Safety 101" flyer, whilst the secondary school

entries also included the topics of social networking, phishing, and identity theft. Secondary school entries on the "Protect your computer" topic also covered a much wider range of malware and were not restricted to anti-virus or firewall related messages, while most primary school entries were restricted to topics on the educational flyer. Of interest to the researchers was that the most popular messages for primary school children were to not trust strangers, or give out personal information online. For secondary school learners the most popular message by far was not to be a cyber-bully. Very few children chose the message that related to not using illegal software or media as the topic for their posters.

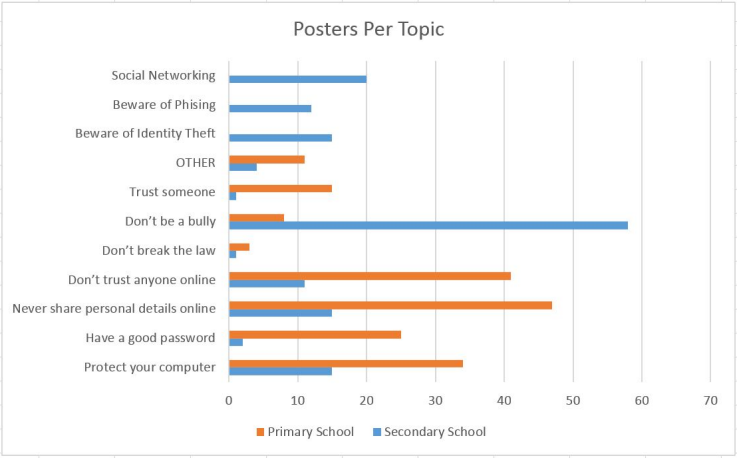


Fig. 2. Number of Posters per Topic

Also of interest to the researchers was that many (20 out of 94) of the primary school posters used the robot 'mascot' in the poster design. In many cases where the robot was used, the message stated that the robot will help protect you against the dangers of cyber space.

Posters per Category of Device. The purpose of this question was to determine whether the children associated the Web with a more 'traditional' computer, or with a mobile device, or whether they made no distinction between computers and mobile devices like smart-phones. The results of this analysis is shown in Figure 3. From this analysis it appears that the primary school children tend to associate Web use with a single device whilst secondary school children do not make such a distinction.

Internalization of Cyber Safety Message. The final question asked in the analysis attempted to judge how well the child internalized the message(s) portrayed in the posters. If the poster just re-iterated a message from the flyer in more or less the same words as it were given to them it was rated as "As given".

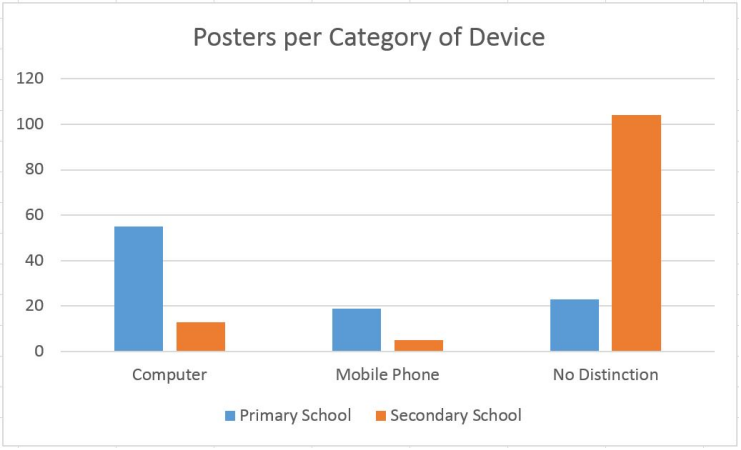


Fig. 3. Number of Posters per Category of Device

If however the message was expressed in the child's own terms it was rated as "Rephrased in own terms". Finally if there was clear evidence that the child also understood the implications and/or consequences of not adhering to the message's advice it was rated as "Fully internalized". An example of a poster considered "Fully internalized" is depicted in Figure 4. In the poster shown in Figure 4 one can clearly see how the child interpreted the concept of cyber-bullying. A character called Sam sent an untrue message claiming "Jo said she likes Mike". Jo is crying because she never said this and Mike is confused because he was unaware that Jo likes (has a crush on) him. The poster shows that the child understood false messages about others to be cyber-bullying; she also understood that such action could hurt others, hence Jo's tears, and by showing the same message on all depicted character's devices she demonstrated that she understands that such bullying is often via a public forum and not limited to one-on-one communication.

An initial analysis compared primary to secondary school children. However, it was found that almost all the secondary school entries were rated as "Fully internalized". The primary school sample was then sub-divided into children aged 6 to 9, and those aged 10 to 13 for a secondary analysis. This analysis, as depicted in Figure 5 showed that the younger children internalized the safety messages to a lesser degree than the older group.

6 Lessons Learned

During the 2012 poster competition the researchers have learned many lessons, which can hopefully assist in making similar campaigns in future more successful. The following is a brief summary of the lessons learned:

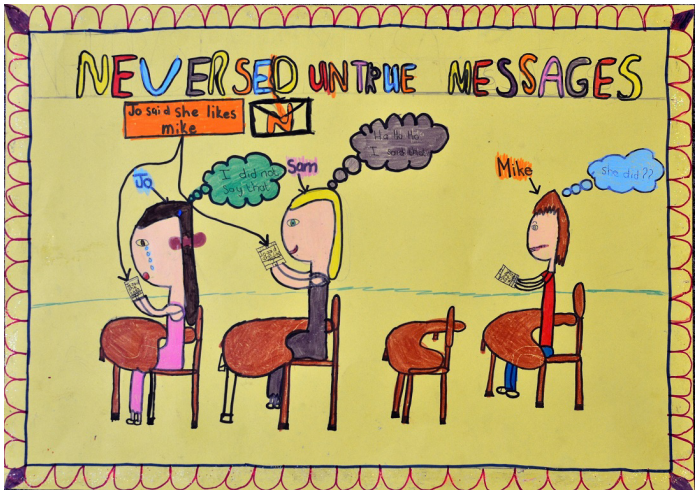


Fig. 4. Example of internalized poster

1. Schools will only participate in campaigns like these if they are notified of the campaign early in the school year.
2. Personal visits to schools are a lot more effective than mailed invitations. No entries were received from schools that were not visited in person. Even schools that specifically requested entry information via the mail did not participate.
3. Teachers play a vital role in such campaigns and need to understand the relevance of the campaign.
4. Prizes should be distributed across many categories. Initially the researchers planned to have prizes split into only two categories, namely primary and secondary school categories. However, many primary school teachers expressed concerns that it would not be fair to judge/compare poster entries by 6 year olds against those entered by 13 year olds.
5. Guidance regarding judging criteria should be specific enough to ensure desired outcomes. The intention of the poster creation campaign was to use the best poster entries received as awareness raising posters in future campaigns. Unfortunately a lot of the entries had a lot of text and were in the format of informational brochures, rather than that of awareness posters.
6. Mascots and other branding should be chosen with care. Children do relate the mascots to the topic.
7. Hand drawn or painted entries should be encouraged. The majority of entries that were created with the aid of a computer were of a 'cut and paste' nature. The researchers believe that the hand drawn posters provided a better indication of actual assimilation of the subject matter.

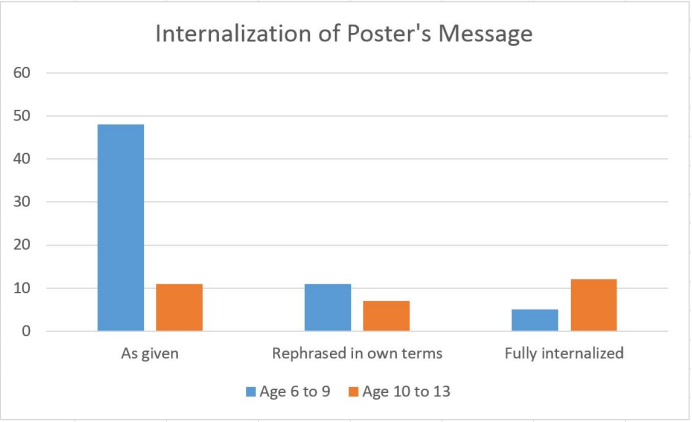


Fig. 5. Internalization of poster's message

7 Conclusion

Protecting the youth in cyber space has become the responsibility of society at large. Without an appropriate level of cyber security awareness and education national cyber security strategies cannot work. This paper reported on a cyber safety awareness campaign conducted in the Nelson Mandela Metropolis in South Africa. The paper described how a poster creation campaign was used to raise awareness about cyber safety related issues amongst both primary and secondary school children. The paper briefly presented the researcher's observations during this campaign and some lessons learned which could help contribute towards the success of future campaigns.

References

[1] Minister for the Cabinet Office and Paymaster General: The UK Cyber Security Strategy Protecting and promoting the UK in a digital world (2011)
[2] Klimburg, A. (ed.): National Cyber Security Framework Manual. NATO CCD COE Publications (December 2012)
[3] International Standards Organization: ISO/IEC 27032:2012(E) Information technology - Security techniques - Guidelines for cybersecurity (2012)
[4] Chen, H., Crowston, K.: Comparative diffusion of the telephone and the World Wide Web: An Analysis of rates of adoption. In: Lobodzinski, S., Tomek, I. (eds.) Proceedings of the WebNet 1997 World Conference of the WWW, Internet and Intranet, Association for the Advancement of Computing in Education, pp. 3–7 (1997)
[5] World internet users and population stats, `www.internetworldstats.com`
[6] Rogers, E.M.: Diffusion of Innovations, 5th edn. Simon and Schuster (2003)
[7] Creswell, J.W.: Qualitative inquiry and research design: Choosing among five approaches, 2nd edn. Sage, Thousand Oaks (2007)
[8] SACSAA: South african cyber security academic alliance, `http://www.cyberaware.org.za`

A Review of IFIP TC 11 WG 11.8 Publications through the Ages

Lynn Futcher[1] and Louise Yngström[2]

[1] Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
Lynn.Futcher@nmmu.ac.za
[2] Stockholm University & The Royal Institute of Technology, Sweden
louise@dsv.su.se

Abstract. IFIP WG 11.8 established a series of conferences in 1999 entitled World Information Security Education (WISE). These conferences have been held every second year since then, with the eighth one being held in 2013. Not surprisingly, there has been numerous high quality papers presented and published in the WISE conference proceedings over the years. However, many of these publications are not easily accessible and are therefore not being readily cited. One of the reasons for the inaccessibility of these papers is that they have not been made widely available through either print or a well-known repository on the Web. Furthermore, a need exists to reflect on what has been done in the past in order to realize the future of these conferences and related events. In order to begin the process of addressing this need, this paper presents a review of the IFIP WG 11.8 publications through the ages. It also reflects briefly on the problems relating to the inaccessibility of these publications, the decline in paper submissions and the lack of citations.

Keywords: Information security education, WISE conference publications, content analysis, publication classification.

1 Introduction

'*International Federation for Information Processing (IFIP) is the leading multinational, apolitical organization in information and communications technologies and sciences. It is a non-governmental, non-profit umbrella organization for national societies working in the field of information processing. IFIP is recognized by the United Nations and other world bodies*.' [1].

IFIP began its official existence in 1960, under the auspices of UNESCO, as a result of the first World Computer Congress held in Paris in 1959. Its basic aims are: to promote information science and technology; to advance international cooperation in the field of information processing; to stimulate research, development and application of information processing in science and human activity; to further the dissemination and exchange of information on information processing; to encourage education in information processing [1].

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 113–122, 2013.

IFIP represents Information Technology (IT) societies from 56 countries, covering all 5 continents, with over half a million members. It links more than 3500 scientists from academia and industry. IFIP is structured according to working groups reporting to 13 Technical Committees (TCs). There are currently in excess of 101 working groups. TC11 (Security and Protection in Information Processing Systems) is one such committee. The aim of TC11 is '*to increase the trustworthiness and general confidence in information processing and to act as a forum for security and privacy protection experts and others professionally active in the field*' [2]. TC11 is organized into 13 working groups referred to as WG 11.1 to 11.13 respectively. WG 11.8 (Information Security Education) consists of an international group of people from academia, military, government and private organizations who are dedicated to increasing knowledge in the field of information security education. WG 11.8 was established in 1991 and aims to '*promote information security education and training at the university level and in government and industry'* [3].

In order to meet these aims, WG 11.8 established a series of conferences in 1999 entitled World Information Security Education (WISE). These conferences have been held every second year since then, with the eighth one being held in July 2013. Not surprisingly, there has been numerous high quality papers presented and published in the WISE conference proceedings over the years. However, many of these publications are not easily accessible and are therefore not being readily cited. One of the reasons for the inaccessibility of these papers is that they have not been made widely available through either print or a well-known repository on the Web.

In addition, a need exists to reflect on what has been done in the past in order to realize the future of these conferences and related events. In order to begin the process of addressing this need, this paper presents a review of the IFIP WG 11.8 publications through the ages. It also reflects briefly on the problems relating to the inaccessibility of these publications, the decline in paper submissions and the lack of citations. While Section 2 focuses on a brief background to IFIP WG 11.8 and the first seven WISE conferences, Section 3 presents the approach used to analyse the numerous publications from these conferences. Section 4 provides a 'quick and dirty' analysis and summarises the key findings. This paper is concluded in Section 5 where suggestions for further research within this area are recommended.

2 Background to IFIP WG 11.8 and WISE Conferences

Before the inception of the WISE series of conferences in 1999, a number of Information Security Education workshops were hosted by IFIP WG 11.8. The aim of these workshops was to *'investigate current and future needs, problems and prospects within information security education'* [4].

The first such workshop was held in Cape Town, South Africa, in 1995, in conjunction with the annual IFIP TC11 Information Security and Privacy Conference. Two papers were presented at this workshop. A first paper entitled '*Concepts, Issues and Resources Structuring Ethical Curricula in the Information Age'* was presented by Sarah Gordon from Indiana University, USA; a second paper entitled '*Education in IT security in Europe'* was presented by Louise Yngström from Stockholm University in Sweden. Apart from the authors of these papers, there were 7 other

workshop participants including 4 from South Africa, 1 from Sweden, 1 from China and 1 from the United Kingdom.

In 1996, the second Information Security Workshop was held in Samos, Greece. This workshop was a continuation of the theme from 1995 and attracted 5 speakers who presented the following papers:

- '*Concepts, Issues and Resources Revisited: Structuring Ethical Curricula for Developing Countries'* (Sarah Gordon - Indiana University, USA);
- '*Computer Security Education in South Africa'* (Lynette Drevin – Potchefstroom University, South Africa);
- '*Teaching Privacy as Part of the Computer Science Curriculum*' (Simone Fischer-Hűbner – University of Hamburg);
- '*Teaching Security by Means of Practical Laboratory Experiments'* (Erland Jonsson – Chalmers University of Technology, Sweden)
- '*Holistic Approach to InfoSec Education'* (Louise Yngström – Stockholm University and Royal Institute of Technology, Sweden).

In 1997, the third Information Security Workshop was held in Copenhagen, Denmark. This workshop was a continuation of the theme from 1995 and 1996 and attracted 5 speakers who presented the following papers:

- '*Framework for Information Security Experiments'* (Lech Janczewski – University of Auckland, New Zealand; Erland Jonsson – Chalmers University of Technology, Sweden);
- '*Critical Analysis of Today's Education. New Perspectives'* (Louise Yngström – Stockholm University and Royal Institute of Technology, Sweden).
- '*Education of Data Protection Officials'* (Simone Fischer-Hűbner – University of Hamburg);
- '*The SUSEC school project: Introducing computer security to teachers and pupils'* (Gunnar Wenngren, Sweden);
- '*Teaching IS Security – Theory versus Practice'* (Helen Fillery-James – Curtin University of Technology, Australia).

The fourth Information Security Education Workshop was held in 1998 on a conference boat between Vienna and Budapest. Five papers were presented at this workshop including:

- '*Teaching Information Security to Network Computing Professionals'* Yuliang Zheng, - Monash University, Australia);
- '*What we can and what we should teach within information security education from an ethical point of view*' (Mikko T Sipponen and Jorma Kajava – University of Oulu, Finland);
- '*Information Security Education – a Human Side of the Curriculum'* (Jorma Kajava and Mikko T Siponen - University of Oulu, Finland);
- '*IT related ethics education in Southern Africa'* (Lynette Drevin – Potchefstroom University, South Africa);
- '*Critical analysis of today's IS education, can we create new perspectives*?' (Louise Yngström – Stockholm University and Royal Institute of Technology, Sweden).

All four workshop papers were published by the Department of Computer and Systems Sciences, Stockholm University/Royal Institute of Technology in Sweden. These workshops addressed a number of key issues relating to information security education which are still pertinent today. These include:

- the importance of information security in the Computer Science/Information Systems/Information Technology (CS/IS/IT) curricula;
- the need for a holistic approach to information security education;
- human and ethical aspects of information security education;
- theoretical and practical approaches to teaching information security; and
- information security education for all.

It is therefore clear that these four workshops created a solid grounding for the working conferences which followed.

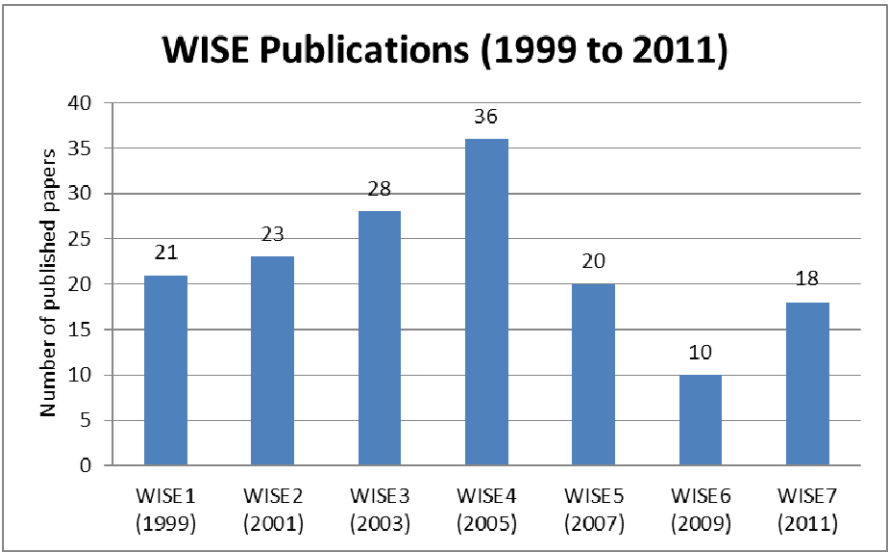


Fig. 1. WISE Publications (1999 to 2011)

The first WG 11.8 working conference (WISE 1) was named 'First World Conference on Information Security Education'. It was held in Stockholm, Sweden in June 1999. The proceedings from WISE 1 were published by the Department of Computer and Systems Sciences, Stockholm University/Royal Institute of Technology in Sweden. The WISE conferences that followed included:

- WISE 2 held in Perth, Australia in 2001 (proceedings published by the School of Computer and Information Science, Edith Cowan University, Perth, Western Australia);
- WISE 3 held in Monterey, California, USA in 2003 (proceedings published by Kluwer Academic Publishers);

- WISE 4 held in Moscow, Russia in 2005 (proceedings published by the Moscow Engineering Physics Institute, Russia);
- WISE 5 held in West Point, New York, USA in 2007 (proceedings published by Springer);
- WISE 6 held in Bento Gonzalves, Brazil in 2009 (proceedings published by the World Conference on Computers in Education);
- WISE 7 held in Lucerne, Switzerland in 2011 (proceedings edited by Lynn Futcher and Ronald Dodge).

Unfortunately, the proceedings for WISE 1, 2 and 4 are inaccessible in practice as they are technical reports; the proceedings from WISE 3 and 5 are accessible as they are published by well-known publishers who have a presence on the Web; and the proceedings from WISE 6 and 7 are difficult to find making them inaccessible in practice. An attempt therefore needs to be made to ensure that all past and future publications are accessible via a well-known repository on the Web.

A further problem is that the number of submissions and publications at WISE conferences has been on the decline in recent years. Figure 1 indicates the number of papers published for each of the first seven WG 11.8 working conferences. From this figure it is evident that the number of papers published increased each year from 1999 (21 papers) to 2005 (36 papers). This reflects an increase of 71%. However, there was a significant drop in 2007 (20 papers) and 2009 (10 papers). The general drop in paper submissions and publications over recent years is of major concern and needs to be addressed to ensure the future of these working conferences. The inaccessibility of some of the previous WISE proceedings may be a significant contributing factor. However, the geographical location of these conferences may also play a role.

As previously mentioned, a need exists to reflect on what has been done in the past in order to realize the future of these conferences and related events. In order to begin the process of addressing this need, this paper presents a review of the IFIP WG 11.8 publications through the ages. The following section describes the approach used to analyze the papers published at each of the seven working conferences.

3 Research Approach

There are various approaches that can be used for analyzing qualitative data (for example research publications). Content analysis has been used in many studies and is commonly used for analyzing written, verbal or visual communications. According to Krippendorff [5], content analysis is a research method for making replicable and valid inferences from data to their context. The pupose is to provide knowledge, new insights, a representation of facts and a practical guide to action [5]. Gerbic and Stacey [6] state that qualitative data analysis software programs can be used to make content analysis more manageable and ordered.

In order to carry out the analysis of the seven working conferences, a list of all published papers was compiled including titles, authors, affiliations and keywords. Abstracts were not included in this initial 'quick and dirty' analysis. Furthermore, a web application called TagCrowd [7] was used to create word clouds for each individual set of WISE publications together with a consolidated view of all WISE

publications. TagCrowd is a web application for visualizing word frequencies in any text by creating what is commonly known as a word cloud, text cloud or tag cloud. It was created in July 2006 by Daniel Steinbock, while a PhD student at Stanford University. TagCrowd [7] specializes in making word clouds easy to read, analyze and compare, for a variety of useful purposes including the visual analysis of qualitative data. The text included in this initial analysis included titles and keywords. Although this initial 'quick and dirty' analysis focused primarily on individual words, TagCrowd does allow for the analysis of key phrases, for example '*information security'* which appears 99 times throughout all the WISE publications.

In order to highlight the issue of citations, the authors have chosen to use Harzing's [8] '*Publish or Perish'* software that retrieves and analyzes academic citations. It uses Google Scholar to obtain the raw citations, then analyzes these and presents various statistics including: total number of papers; total number of citations; average number of citations per paper; average number of citations per author; average number of papers per author; and average number of citations per year. For this initial analysis, only WISE 6 publications were analyzed for citation frequencies.

The analysis of previous WISE publications was performed in order to reflect on what has been done in the past. This is deemed necessary in order to realize the future of these conferences and related events. The following section highlights some of the key findings relating to the analysis of previous WISE publications.

4 Analysis and Findings

Using TagCrowd [7] to perform a 'quick and dirty' analysis of previous WISE publications provided some interesting findings.

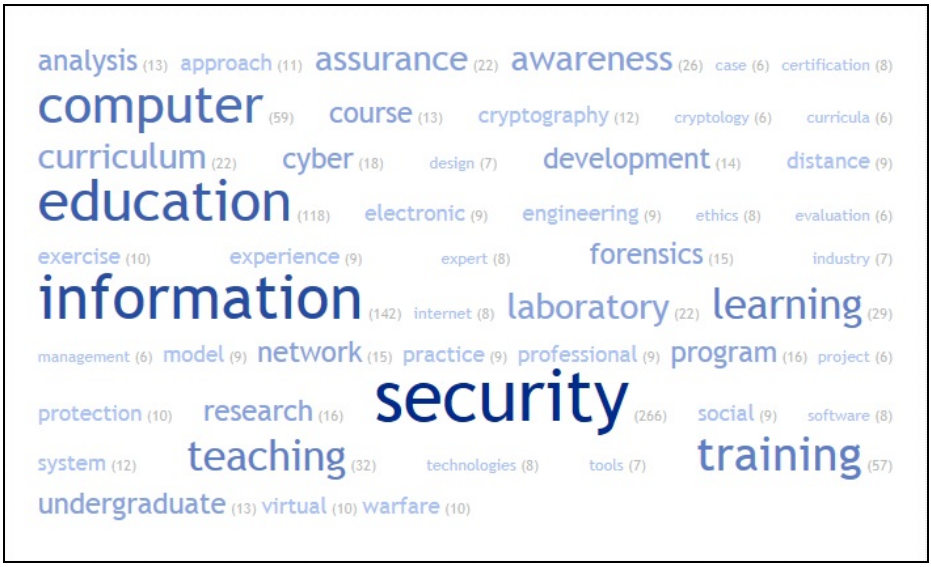


Fig. 2. Titles and Keywords Word Cloud: All Papers for all WISE Conferences

As can be seen in Figure 2, TagCrowd clearly highlights the words that occur most frequently by increasing the font size and its boldness. In addition, words are placed in alphabetical order and the frequency is indicated in parentheses after each word. This improves the ease of analysis of the word clouds created using TagCrowd. In addition, TagCrowd caters for synonyms. However, since this 'quick and dirty' analysis only included paper titles and keywords, it was not deemed necessary at this initial stage.

Figure 2 is a consolidated word cloud for all papers presented at all WISE conferences based on titles and keywords. It clearly shows that the word '*security'* appears the most number of times (266), followed by '*information'* at 142 and '*education'* at 118. This confirms that the primary focus of these publications is information security education. Similar word clouds were created for all papers published at each individual WISE conference based on titles and keywords. However, due to space limitations, this paper does not present the actual word clouds for each individual working conference. Instead, the findings from these word clouds are summarized in Table 1 which depicts the top 20 words used in the titles and keywords of the papers presented at the various individual WISE conferences.

Table 1. Top 20 Words based on Word Frequency (WISE 1 to WISE7)

No.	Word	WISE1	WISE2	WISE3	WISE4	WISE5	WISE6	WISE7
1	security	40	27	54	60	31	17	34
2	information	21	19	28	32	14	8	20
3	education	21	14	30	26	17	7	20
4	training	7	9	8	12	12	4	5
5	computer	16	3	9	10	10		6
6	teaching	5	7	8	6	4		3
7	learning	3	12	4	3	4		3
8	awareness	6	3	2	8	2	4	
9	laboratory	3		7	9		2	
10	curriculum/curricula	3	4	3	9			4
11	assurance			14	3			2
12	cyber			7	4	2		5
13	system	2	4	3	7			2
14	network		2	6	3	3		2
15	professional	5			9	2		
16	course	2	2		5	2		4
17	forensics			2	4	7	2	
18	research			4	4	4		2
19	cryptography				9	4		
20	development	2	3	3	4			

Table 1 clearly confirms that the primary focus of these individual conference publications relate to information security education, training and awareness together with teaching and learning. This is addressed within the CS/IS/IT curricula including specific examples of practical implementations through various laboratory experiments. In addition, cyber, system and network security are addressed throughout the various years of publications. Furthermore, forensics and research aspects are introduced as important topics from WISE 3 onwards, while cryptography is introduced in WISE 4 and 5.

While Table 1 only highlights individual words, a similar analysis can be done for key terms. As previously mentioned, the term 'information security' occurs 99 times, '*security education'* occurs 69 times, '*network security'* occurs 9 times and '*cyber security'* occurs 6 times. This type of 'term analysis' can therefore be useful to develop a folk taxonomy for IFIP WG 11.8 publications, similar to that of Botha and Gaadingwe [9]. Such a taxonomy is based on a particular group's 'language' that is vernacular in nature [9]. Botha and Gaadingwe [9] specifically reflected on 20 IFIP SEC conferences totalling 802 papers.

Similarly, Bjorck and Yngström [10] presented a classification model for research in information security based on an analysis of 125 papers from the IFIP World Computer Congress/SEC 2000. This model suggested categorising information security research on three dimensions namely X, Y and Z. Dimension X addresses the level of abstraction ranging from theories and models to empirical world; dimension Y addresses the domain ranging from technical, via formal to informal; and, dimension Z addresses context in order to cater for time and space. A similar classification model could be used to analyse the various WISE publications. However, this would require a more in depth analysis which is planned for the near future.

Table 2. Total Number of Citations for WISE 6 (2009)

Paper Title	**Authors**	**Citations**
Reaching Today's Information Security Students	Helen Armstrong, Ron Dodge, Colin Armstrong	0
Some 'Secure Programming' Exercises for an Introductory Programming Class	Matt Bishop	2
A SWOT Analysis of Virtual Laboratories for Security Education	Alan Davidson, Javier de La Puente Martinez, and Markus Huber	1
Determinants of password security: some educational aspects	Lynette Drevin, Hennie Kruger, Tjaart Steyn	1
Improving Awareness of Social Engineering Attacks	Aaron Smith, Maria Papadaki and Steven Furnell	0
A Risk-Based Approach to Formalise Information Security Requirements for Software Development	Lynn Futcher and Rossouw von Solms	0
Two Case Studies in Using Chatbots for Security Training	Stewart Kowalski, Katarina Pavlovska, Mikael Goldstein	5
Information Security Specialist Training on the Basis of ISO/IEC 27002	Natalia Miloslavskaya, Alexander Tolstoy	0
Using Bloom's Taxonomy for Information Security Education	Johan Van Niekerk and Rossouw Von Solms	0
Advancing Digital Forensics	Katrin Franke, Erik Hjelmås, and Stephen D. Wolthusen	0
TOTAL NUMBER OF CITATIONS		**9**

As discussed in Section 3, Harzing's [8] '*Publish or Perish*' software was used to highlight the issue pertaining to citations. As an example, Table 2 presents the number of citations for the WISE 6 publications according to Harzing [8].

Of the 10 papers published, only four of these have been cited, with 9 citations in total. These figures indicate the general lack of citations for WISE publications. An obvious explanation for this may be the general inaccessibility of WISE papers and the fact that the WISE conferences may not be well known in the relevant communities. This is a further concern for the IFIP WG 11.8 which needs to be addressed.

5 Conclusion

This paper presents a review of the IFIP WG 11.8 publications including the four workshops held from 1995 to 1998 and the seven working conferences held from 1999 to 2011. In addition, it highlights a number of key issues that are pertinent to the future of the working group. These include the lack of accessibility of the various publications, the meager number of citations of these publications and the decline in the number of submissions and publications at the various working conferences.

Further research is being considered to develop a folk taxonomy for IFIP WG 11.8 publications by carrying out a more in depth study of all previous WISE publications. The development of a classification model for information security education publications is also being considered. These further developments could be useful in understanding the publications from previous publications. In addition, such a detailed analysis could assist in identifying any potential gaps in the research previously carried out and in so doing highlight opportunities for future possible research.

References

1. International Federation for Information Processing. About IFIP. International Federation for Information Processing (IFIP) (2013), `http://www.ifip.org/` (retrieved March 18, 2013)
2. International Federation for Information Processing. IFIP TC-11 WG 11.8. IFIP TC-11 WG 11.8 (2013), `http://www.ifiptc11.org/` (retrieved March 18, 2013)
3. International Federation for Information Processing. IFIP TC11 Working Groups IFIP TC11 (2013), `http://www.ifiptc11.org/` (retrieved March 18, 2013)
4. Yngström, L.: IFIP TC11 Wroking Group 11.8 Information Security Second Workshop. Information Security Education - Current and Future Needs, Problems and Prospects. Samos, Greece: DSV Department of Computer and Systems Sciences (1996)
5. Krippendorff, K.: Content Analysis: An Introduction to its Methodology. Sage Publications, Newbury Park (1980)
6. Gerbic, P., Stacey, E.: A purposive approach to content analysis: designing analytical frameworks. Internet and Higher Education 8, 45–59 (2005)

7. Steinbock, D.: TagCrowd (2006), http://tagcrowd.com/ (retrieved March 15, 2013)
8. Harzing, A.: Publish or Perish (2007), http://www.harzing.com/pop.htm (retrieved April 4, 2013)
9. Botha, R.A., Gaadingwe, T.G.: Refelcting on 20 SEC conferences. Computers & Security 25, 247–256 (2006)
10. Bjorck, F., Louise, Y.: IFIP World Computer Congress/SEC 2000 Revisited. In: IFIP TC11 WG 11.8 Second World Conference on Information Security Education, pp. 209–222. School of Computer and Information Science, Edith Cowan University, Perth (2001)

Preparing Our Undergraduates to Enter a Cyber World

Dino Schweitzer, David Gibson, David Bibighaus, and Jeff Boleng

Department of Computer Science, United States Air Force Academy, Colorado, 80840, United States

Abstract. Today's students have grown up with computer-based technology and need to be prepared to enter a career in a digital world. This includes an understanding of the broader implications of technology such as the growing threat of cyber-crime and cyber-terrorism, cyber-ethics, the legal and social implications of technology, and the local and global impacts. At our institution, we have taken a broad look at ways of integrating cyber awareness and education across the curriculum to reach all levels of students, irrespective of their major. We have identified core cyber issues that are taught to all freshmen, developed awareness training that is regularly completed, provided opportunities for interested students to gain more cyber knowledge through a student club and summer program, and developed an in-depth educational program for technical students to graduate with an emphasis in cyber-warfare. This paper will describe our various cyber programs and future plans.

Keywords: cyber-education, cyber-training.

1 Introduction

A key priority in the National Strategy to Secure Cyberspace is to increase security training and awareness through enhanced education programs [1]. As a result of this emphasis on security education, more courses and programs are being offered at the undergraduate level in security-related topics such as cryptography, information security, network security, and information warfare. These courses have benefited from an increasing number of textbooks, curriculum development, and student competitions such as the Collegiate Cyber Defense Competition [2].

While much of the focus of cyber education has been on the creation of a professional cyber workforce, at the United States Air Force Academy (USAFA), we feel it is critical for all students to have awareness of the issues and threats associated with cyberspace. In addition, students who have a strong interest in cyber topics, but are not technical majors, should have the opportunity to explore cyber-related areas in greater detail without taking highly technical computer science or engineering courses. Finally, our students who will be starting their careers as cyber professionals need to be able to explore, in depth, both the conceptual aspects of cyberspace as well as receiving hands-on experience in the tools and techniques of the field. This paper will examine these three levels of cyber education and training as implemented at USAFA.

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 123–130, 2013.

2 Cyber for All

While many recognize the importance of developing the cyber skills of all students, finding a place in the curriculum for cyber education and training can be a challenge. At USAFA, all students receive cyber education in the core curriculum and cyber training in their *First Year Experience* course.

A large core curriculum at our school provides an ideal opportunity for cyber education in the *Introduction to Computing* (CS110) course offered by the Computer Science department and taken by all students as freshman. CS110 consists of 40 lessons covering information representation (5 lessons), algorithmic reasoning (13 lessons), computer system capabilities (7 lessons), computer ethics (1 lesson), software applications (7 lessons), cyber security and warfare (5 lessons), plus a midterm exam and course review (2 lessons). While cyber security topics naturally arise in discussions throughout the course, the 5-lesson cyber security and warfare block is dedicated to cyber education.

CS110's five cyber block topics are: information security, cryptography, cyber warfare and crime, offensive cyber operations, and defensive cyber operations. In addition to introducing the growing importance of cyber security and the prospect of cyber warfare, the information security lesson focuses on the principles of confidentiality, data integrity, availability, and authenticity. The cryptography lesson introduces students to basic symmetric encryption techniques as well as asymmetric public key encryption and digital signatures. CS110's cyber warfare and crime lesson provides students with a political, economic, and military context for cyber warfare and cyber crime before discussing current threats, vulnerabilities, and common cyber attack vectors. The offensive cyber operations lesson explains to students how individuals and organizations conduct cyber attacks with a focus on password attacks and attacks using social engineering. Students do not learn about specific cyber attack tools and techniques in CS110. Finally, the defensive cyber operations lesson focuses on strategies for defending against the attacks described in the previous lesson with a focus on how students can protect themselves and their own computers.

All of our students also learn about cyber topics in several other required core courses. For example, in *Principles of Air Force Electronic Systems* offered by the Electrical and Computer Engineering department, all students learn about circuit and packet switching networks and their respective vulnerabilities to cyber attacks. In *Military Theory and Strategy*, offered by the Military Strategic Studies department, students learn about military cyber capabilities and strategies. In *General Physics II*, students learn about the electromagnetic spectrum which underlies all cyber technologies.

Few colleges and universities have a large core curriculum like USAFA's. Nevertheless, opportunities exist at many schools for introducing cyber topics to a broad group of students in general education elective courses. One target of opportunity may be the first year experience course required for all freshmen at many schools. At USAFA, one of the first lessons of the *First Year Experience* class teaches cadets how to access and use the institution's computer network safely and securely.

3 Cyber Training

In addition to the exposure to cyber topics provided all students in the core curriculum, our department has created opportunities for greater hands-on cyber training to interested students outside of the classroom. We accomplish this through two primary mechanisms: a summer cyber training program and an active Cyber Warfare Club.

3.1 Basic Cyber Training

This summer, we will offer our newest training course in Cyber Warfare – Basic Cyber (Cyber 256) which was first prototyped in the summer of 2009. The course is a ten-day introduction to cyber operations and is open to all sophomores. The goal of the class is to "explore … cyber … with hands-on training designed to teach the fundamentals of establishing, operating, attacking, defending, and exploiting computers and networks." The course was modeled on our USAFA's basic sailplane course. There are three distinctive aspects of the basic sailplane course that we are incorporating into the Cyber 256:

- Light on Theory – heavy skills training. In soaring, students receive very little classroom learning (just enough to keep them safe) and spend most of their time in the cockpit. The goal is to provide enough real-world exposure early in their experience with the subject to allow students to intelligently decide if they are motivated to delve deeper into the subject (which will naturally require a more in-depth classroom experience). Likewise, our cyber class is designed to give them enough hands-on training with real world tools in a carefully controlled environment to allow them to decide if they want to pursue the discipline at a deeper level.
- Student Led – One of the amazing things at our institution is to watch the hundreds of glider flights that occur safely every week and realize that they are being taught by undergraduate instructors. This has two benefits: for the student, it makes the skills seem not so far "out of reach" and removes some of the mental limitations that students often place on themselves. For the student instructor, it not only builds a deeper level of competency in the subject area, but also develops the ability to lead and communicate effectively about their discipline. Since cyber warfare is often perceived as a dark art, having students lead the training is important to make the topics appear more accessible to the students. In addition, the nation needs young men and women who can effectively communicate and lead in cyber matters.
- Task Oriented – The soaring program is centered on students being able to perform a series of tasks needed to safely and effectively fly an aircraft. For the Cyber course, students will be presented with a series of scenarios that require them to perform specific tasks and will be evaluated on whether or not the student performed them satisfactorily.

The Cyber 256 class will expose students to cyber-warfare primarily from an attacker's point of view. Students will begin by exploring some of the basics of establishing a network and then quickly proceed to use some of the more commonly used network security tools. The idea is not to provide in-depth training on these tools, but rather provide enough exposure for the students to understand the basic process and appreciate some of the avenues of attack. In addition, the course is designed to be cross-disciplinary. Special emphasis is placed on the larger context of cyber warfare including social engineering, the legal aspects of cyber warfare, current threats, and how the Air Force is organizing itself to address them. Table 1 shows a list of the topics taught during the Basic Cyber Warfare course.

Table 1. Topics in Cyber 256

	Morning Topic	**Afternoon Topic**
Day 1: Establish	Basic Network Training	Advanced Networks
Day 2: Cyber Intel	Network Mapping	Denial of Service
Day 3: Penetrate	Computer Penetration	Web Vulnerabilities
Day 4: Operations	Air Force Cyber Mission	Cyber Threat
Day 5: Social Aspect	Social Engineering	Law
Day 6: Wireless	Wireless Vulnerabilities	Password Cracking
Day 7: No Training		
Day 8: Forensics	Forensic Tools	Hard Drive Analysis
Day 9: Advanced Threats	Root Kits	Intrusion Detection
Day 10: Capstone	Capstone Part I	Capstone Part II

The Cyber 256 course has some similarities to the Advanced Couse in Engineering Cyber Security Boot Camp (ACE) course that was developed by the Air Force Research Laboratory and administered to Air Force ROTC students [4]. Our course has several important differences. First the course is offered to all rising sophomores. This is one year earlier than the ROTC program and therefore cannot be limited to students of a particular major. In addition, it is a ten-day course as opposed to the current ten weeks for ACE. Because of the compressed timeline and less-restrictive pre-requisites, the course is, by design, much more training-focused as opposed to education-focused.

3.2 Cyber Warfare Club

The Cyber Warfare Club at USAFA was created as a multidisciplinary club with members from all academic majors. It is similar to the club described at the United States Military Academy [5]. Among the current 100+ club members, there is a diversity of academic majors, to include aerospace engineering, biology, chemistry, computer science, economics, electrical engineering, English, military strategic studies, physics, political science, space operations, and systems engineering. One of the goals of the club is to make it inclusive and attract a diversity of students. This decision was based on the realization of the importance of cyber education to all of our graduates.

In September of 2008, we began to survey the interest of students at our institution in cyber warfare by demonstrating some simple Backtrack tools at semi-annual majors nights where we typically recruit young students into the computer science major. The response was overwhelming. Several planning meetings were held with many of the interested students leading to a vote for student leadership in January of 2009. The club was officially recognized by the institution club regulatory body at the end of March the same year. In the short history of the club, we have had many successful training opportunities, invited talks, and members have participated in several competitions learning a great deal along the way.

We have had to carefully design club activities to ensure opportunities for all members because of the diverse nature of our membership. One way in which we have done this is through talks given by experts from the field. One of our first talks was given by the Director of Communications and Information at our institution and detailed a plan for the future network architecture. Since that first talk we have had others including a presentation on current trends in cyber warfare by the Research Director at Gartner, threats and case studies by the NSA Information Assurance Directorate Technical Director, and Public Key Infrastructure by the Air Force PKI Team. Recent talks include a discussion of Microsoft's work to mitigate threats by a senior Microsoft Security specialist and a discussion of the policy, law, and ethics of cyber attack by the Chief Scientist of the Computer Science and Telecommunications Board, National Academy of Sciences. By providing a mixture of technical and policy discussions we have been able to entice a mixture of all of club members to attend and participate.

Hands-on training in network attack and defense is another major goal of the Cyber Warfare Club. Development of the appropriate level of hands-on labs has been challenging. One of the approaches we have used is to introduce security concepts through web-based simulations of cyber threats such as buffer overflow and SQL injection which do not require a highly technical background to understand [6]. We identified the following topics as a starting point for hands-on lab development:

- vulnerability analysis and penetration testing,
- the hacker methodology,
- incident response,
- forensics,
- reverse engineering,
- networking fundamentals, and
- service fundamentals

A key concept in our hands-on labs is the idea of a "check ride". In aviation, a check ride is where a student takes control of a plane (under the close supervision of a qualified pilot) and demonstrates techniques and is either verified as being qualified or needing additional training. We utilize our senior club members to provide cyber check rides to the more junior students. We are pursuing the development of multiple training modules in parallel. Additionally, there are several opportunities to leverage work being done in various cyber organizations to provide additional training to club members. Several organizations have expressed an interest in collecting club materials and training modules developed at our institution.

Besides the training opportunities, we have used the club as an opportunity to select students for additional training provided commercially. Over spring break in 2009 and 2010, we sent ten students to Certified Ethical Hacker training. This course was well received by the students.

In its short history, students from our Cyber Warfare Club have participated in multiple cyber competitions. Two of these competitions had the students on blue teams protecting systems and services while another allowed them experience on a red team in a capture the flag event. We recently competed in the 2010 International Capture The Flag (ICTF) competition and had a respectable placing in the top 20 of all teams worldwide [7]. These competitions serve as capstone events and tie all of the education and hands-on training together to provide students an opportunity to integrate all their skills and get a feel for the bigger picture.

4 Cyber in Depth

Along with the cyber education given to all students, and the cyber training providing additional experience to interested students, we offer students the opportunity to explore cyber topics in much greater depth through the cyber warfare track of our computer science major, through the cyber instructor course, and through cyber research opportunities.

4.1 Cyber Warfare Track

Our Computer Science major has been recognized by NSA and DHS as a Center of Academic Excellence (CAE) in Information Assurance Education. We have integrated computer security principles in several of our major courses where appropriate. In addition, all CS majors are required to take the Information Warfare course which is a concepts course in cyber security.

For students that want to focus on cyber warfare, we offer two additional courses, a cryptography course and a network defense course. Students that complete both of these as optional courses in the major receive a designation on their diploma as having completed the cyber warfare track of the Computer Science major.

4.2 Cyber Instructor Course

As stated earlier, undergraduate students are the primary instructors of the Cyber 256 class. Each 10-day offering will have fifteen students and three undergraduate

instructors. These student instructors have been hand-picked by the faculty because of their leadership potential and demonstrated proficiency in the cyber warfare club. As previously described, this instructor model draws heavily from the sailplane instructor paradigm. For each skill, student instructors will demonstrate a skill, allow students to practice the skill with instructor help and finally have the student perform the skill for evaluation. If the sailplane program is any indication, the biggest challenge for these instructors will be to restrain themselves from correcting student mistakes too quickly.

The Cyber Instructor Course fulfills a very important and often underappreciated need within the cyber warfare discipline, namely to develop cyber leaders. Too often cyber warfare courses emphasize the technical nature of the discipline. Yet what is in demand are people who not only understand the technical challenges cyber warfare presents, but can communicate those challenges to non-technical people. Student instructors will be required to train their non-technical peers to use sophisticated cyber security tools to perform basic tasks. In the process, they will develop both their technical and leadership skills. In fact, USAFA is allowing these cyber instructors to teach the cyber warfare class in-lieu of other leadership requirements.

4.3 Cyber Research

Although we are an undergraduate-only institution, we believe that research is an integral part of the undergraduate experience. Students have the opportunity to explore a cyber-research topic in-depth through an independent study course which matches the student with a faculty mentor conducting research on a specific project. In addition, our institution offers a 5-week summer research program made available to the top students in each major. Between their junior and senior years, students in this program attend institutions such as NSA, NRO, MITRE, Intel, and research organizations to work on a real-world research problem. The program is highly rated by students and gives them an excellent exposure to the cyber world outside of academia.

We believe that research should not be relegated to just the top students. In our Information Warfare course required of all computer science majors, we have created a final course project that provides a research experience [8]. Students pair up with a faculty mentor to work on a current research topic throughout the semester. The project is broken into the phases of a research effort where students have to conduct background investigation, develop a research plan, collect data, perform analysis, and document their findings in both a research poster and a conference-level research paper. Several of the projects have been published in various conference proceedings.

5 Future Plans

Our current program is successful in providing all of our graduates a fundamental exposure to important issues they will be facing in their professional careers. Students with an increased level of interest have access to training opportunities that

take into consideration the fact that they may not be technical majors. Our graduating cyber professionals have a high rate of accomplishment in their careers and a proven track record of successful performance.

To continue our success, however, requires evolving our program as technology changes and as the demands of our students future career field change. We are constantly updating our educational cyber curriculum and have faculty actively involved in cyber-education working groups. We also have faculty who actively participate in defining training standards and programs for the Air Force cyber career field. We try to take the lessons learned to improve our cyber training opportunities for students. As we gain more experience with Cyber 256 and the associated student instructors, we will need to tweak the program to keep it fresh, challenging, and relevant. Similarly, we are constantly in touch with our peers in the commercial and research sectors to understand the current challenges and find interesting projects for our students to work on. By maintaining currency, we hope to keep our broad-based program at the forefront of cyber education and best prepare our students to enter the cyber world.

References

[1] Critical Infrastructure Protection Board, National strategy to secure cyberspace, http://www.whitehouse.gov/pcipb

[2] Conklin, A.: The Use of a Collegiate Cyber Defense Competition in Information Security Education. In: Proceedings of the 2nd Annual Conference on Information Security Curriculum Development, pp. 16–18 (2005)

[3] The National Centers of Academic Excellence in Information Assurance Education Program, http://www.nsa.gov/ia/academia/caeiae.cfm

[4] Jabbour, K., Older, S.: The Advanced Course in Engineering on Cyber Security: A Learning Community for Developing Cyber-security Leaders. In: The Sixth Workshop on Education in Computer Security (2004)

[5] Conti, G., Hill, J., Lathrop, S., Alford, K., Ragsdale, D.: A Comprehensive Undergraduate Information Assurance Program. In: Irvine, C., Armstrong, H. (eds.) Security Education and Critical Infrastructures, pp. 243–260. Kluwer Academic Publishers, Norwell (2003)

[6] Schweitzer, D., Boleng, J.: Designing Web Labs for Teaching Security Concepts. Journal of Computing Sciences in Colleges 25(2), 39–45 (2009)

[7] The UCSB iCTF, http://ictf.cs.ucsb.edu/

[8] Schweitzer, D., Boleng, J., Hadfield, S.: Providing an Undergraduate Research Experience in a Senior Level Security Course. In: Proceedings of the 13th Colloquium for Information Systems Security Education (2009)

How to Secure the Cloud Based Enterprise Information System

– A Case Study on Security Education as the Critical Foundation for a MS-EIS Program

Yanzhen Qu

Colorado Technical University, 4435 N. Chestnut Street,
Colorado Springs, CO 80907, USA
yqu@coloradotech.edu

Abstract. This paper presents a case study for a new Master of Science in Enterprise Information Systems program created at Colorado Technical University in which security courses occupy over 20% of all classes within the program. Should there be such a high emphasis on security courses? Through reviewing the performance of the first class of students in the Enterprise Information System Capstone course of this program, we can conclude that the investment on the security education is absolutely necessary. These courses have laid down the critical foundation for students to correctly handle today's ever growing real world Enterprise Information Systems' challenges.

Keywords: Enterprise Information System, Security, Security Education, Cloud Computing, Service Oriented Architecture.

1 Introduction

As Enterprise Information System (EIS) becomes an integral part of any modern business, the need to train more qualified IT professionals who can take a business problem and find an EIS solution to address business requirements of the enterprise has become more urgent. To meet such needs, Colorado Technical University (CTU) created a new master program named Master of Science in Enterprise Information Systems in the late of 2008. This program has set up the following core outcomes [1]:

- Plan, implement and use technology within a broad business and real world perspective
- Demonstrate the ability to critically analyze and solve technical issues as they are related to the enterprise
- Demonstrate the ability to design, implement and manage technology solutions to achieve enterprise goals
- Exercise strong interpersonal and team communication skills
- Demonstrate the skills necessary to perform all actions within an ethical framework

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 131–139, 2013.

The program consists of the following courses:

- Computer Networking
- Security Management
- Database Systems
- Enterprise Systems Architecture
- Enterprise Information Systems
- Information Technology Systems Development
- Project Management Process in Organizations
- Schedule and Cost Control Techniques
- Enterprise Information Systems Capstone
- 2 elective courses from the list course listed below:
  - Software Information Assurance
  - System Security Certification and Accreditation
  - Software Project Management
  - Applied Managerial Decision-Making
  - Project Planning, Execution and Closure Impact on Design & Production

Among all fourteen courses, three courses are related to security. Obviously the security is the heaviest emphasis in this new program. This results from the combination of the market trend research and the recommendation from the CTU's industrial advisory board. Because security issues are associated with every component of the EIS, every application, and every business process, it is no longer enough to just provide students with some basic concepts and common practice knowledge in security management. It is very important to make students understand the root cause of all the security issues, the essence, principles and methods of security management, and the impact of security to every decision made by an EIS designer or developer. In fact, as a "National Center of Academic Excellence in Information Systems Security Education" designated by the US National Security Agency and the Department of Homeland Security, CTU has always placed a high emphasis on security education in its Computer Science and Information Technology degree programs in all levels from Associate, Bachelor, and Master to Doctor.

In January 2010, the first cohort of students enrolled in this new program was about to take their EIS Capstone course. The students were to be tested on how well they could solve real world problems by applying the knowledge and skills they had acquired from the new program. At the same time this new program was also to be tested on how effective its courses were. Having taught several courses with this cohort, recommended by both the school and the students, I was selected as the instructor for this first EIS Capstone course.

In the following sections I will present a case study of the EIS Capstone course so that we will have some evidence to answer the question: "Is the emphasis on security in this new program a right decision?"

Interestingly enough, the answer to that question is closely related to the answer to another more technical question: "How to secure the Cloud based Enterprise Information System".

The rest of this paper will help relate those two questions.

2 What Are the Real Requirements?

This first EIS Capstone course was sponsored by the global Information Technology (IT) department of a multi-national enterprise. For convenience, in the rest of this paper, we will call this enterprise "the Company." The EIS Capstone course was scheduled for 11 weeks, and this cohort had total of 12 students. During the first week of the class, we went through the requirements of the EIS Capstone class and also reviewed various key concepts of Service Oriented Architecture and Cloud Computing [2], [3]. During the second week of the class, our sponsor met with all the students, and issued a written task specification as shown below (minor wording modifications have been made correspondingly) [4]:

"The Information Technology (IT) department serves the global technology infrastructure needs of the Company through the stewardship of scarce financial, human, software and machine resources. The Company has set as its goal to double its service to the targeted customers by the year 2015 and double again by the year 2020. In anticipation of supporting this goal, IT will complete installation of a global technology infrastructure upgrade by June 2010.

In addition to internal Company's resources, IT envisions leveraging an agile global pool of technical resources to assist in the construction and deployment of our technical service offerings. Service offering outcomes may include technologies that link suppliers to customers, address specific community needs, and enable real time responses from venders or suppliers to global needs.

Task Description

In consideration of Vision 2020, global technology infrastructure upgrade, the current IT architectural and investments, will establish an executive level plan to establish a global developer network that:

- *Articulates a global vision, outcomes and benefits*
- *Describes the objectives and scope of the plan*
- *Frames and describes the required technical infrastructure, standards and processes required*
- *Outlines the sequence of proposed activities and dependencies*
- *Documents risks and mitigation strategies*
- *Provide a rough order of magnitude costs to implement*
- *List assumptions that bound the scope and delivery of the project "*

After reading through this task specification, all students asked the same question: "What are the real requirements?" This was because they were lacking the working knowledge regarding the Company's As-Is IT systems, the daily real challenges and restrictions that the Company's IT department faced, and the root cause of these problems. Therefore, the students decided that they first needed to start the system life cycle development process to make more in-depth investigations, and to exercise more due diligence to find out the real requirements.

Through a sequence of email communications and several face to face meetings, much more information was collected, as summarized in the following:

- The Company was helping more than 1 million customers in 25 countries with an ever growing need. It was essential that the Company expands its system-wide IT communication capability to automatically translate, store, secure, update, and rapidly retrieve large amounts of data.
- The protection of the Company's business databases which include the financial information of their partners, vendors, suppliers, and customers, was a crucial requirement.
- The Company's existing IT systems were developed by multiple vendors and introduced at different times for different purposes. The Company's As-Is IT systems were really the Silos systems as described in [5]. All the IT functions had been independently structured to meet local application demands with only a secondary consideration on how to connect a global community. The IT functions also did not readily share information outside of their respective infrastructures.
- With the limited IT budget that the Company could offer, developing any new integrated EIS would require a very innovative and non-conventional solution. And the Company was willing to look into any new technical solutions that could save costs while still achieving its' final goals.

It was very clear that the real requirements could be concluded in one statement:

"***The Company needs to develop a Service Integration Architecture Framework to enable existing and new functionalities and resources continuously integrated in a fast, secure and cost efficient manner.***"

This statement was quickly reviewed and endorsed by the sponsor. It then not only provided the project direction for students, but also became the only criteria to assess the final result of the students' work created through the project.

3 A Solution Meeting the Requirements: Service Integration Architecture Framework Based on Cloud Computing [6]

After fully understanding what the real problems of the As-Is IT systems were and what real needs the Company had, the students quickly focused their effort onto creating a new Service Integration Architecture Framework (SIAF). The SIAF would help the Company not only to move from the Silos systems to an integrated Service Oriented Architecture (SOA) based system, but also to take advantage of Cloud Computing Services wherever appropriate.

As shown in Fig. 1, the proposed SIAF addressed the pre-requisite considerations and risks associated with external Cloud Computing Services and/or platforms to include newly evolving issues, constraints, efforts, technical advances, and the latest industry standards pertains to the Company's global operations.

In the proposed SIAF, the discussions were focused on the following five aspects:

(1) Pros and Cons of Various types of Cloud Computing Services
(2) Security in the Context of Cloud Computing:
    - Identity and Access Management
    - Data Security
(3) Communication in the Context of SOA and Cloud Computing:
    - External Enterprise Service Bus (EESB)
    - Internal Enterprise Service Bus (IESB)
(4) Application Programming Interface
(5) Business Process Manager

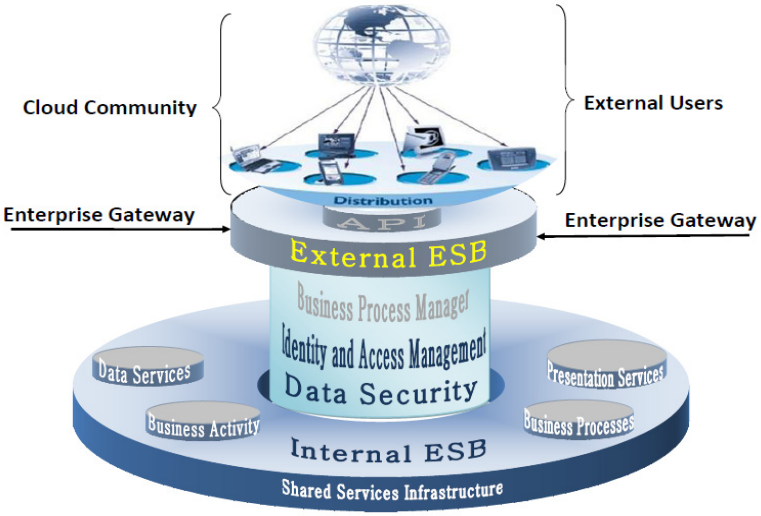


Fig. 1. Service Integration Architecture Framework

Below is the simplified version of students' proposal.

3.1 Pros and Cons of Cloud Computing Services

The students provided a through analysis on the Pros and Cons of various types of Cloud Computing Services regarding the needs of the Company, as summarized in the Table 1.

The students concluded that although public Cloud Computing Services could provide cost savings on both IT Application and Data Management, the cost to maintain the required security and privacy as well as data accessibility would reduce that benefit. The entire IT Operation cost would only be reduced to a certain level depending on what type of Clouding Computing Service was really used.

3.2 Security in the Context of Cloud Computing

Security functionality is the central part of in this SIAF. It is managed through two subsystems: Identity and Access Management (IAM) subsystem and the Data Security subsystem.

Table 1. Comparisons of Various Types of Cloud Computing Services

Type of Cloud Computing Service	Private Cloud (On Premise)	Public Cloud–IaaS (Infrastructure as a Service)	PublicCloud-PaaS (Platform as a Service)	PublicCloud–SaaS (Software as a Service)
Control Computing Resources	Organization Control	Shared Control	Vendor Control	Vendor Control
Data Security and Privacy Risk	Low	Medium	High	High
Data Management Cost	High	Medium	Low	Low
Existence and Standards for Cloud Identity and Access Management (IAM) Tools	Matured (ISO/IEC27002)	Reviewed (ISO/IEC27002 (2005))	Proposed (Cloud Security Alliance established in 2008)	Proposed (Cloud Security Alliance established in 2008)
Requirements for Federation IAM Tools	Lowest	Low	Medium	High
IT Application Development Cost	Highest	High	Medium	Low
Security and Privacy Management Cost	Low	Medium	High	Highest
IT Operation Scalability	Low	Medium	High	High
Overall IT Operation Cost	High	Medium(high end)	Medium	Medium (low end)

IAM Subsystem

The IAM subsystem includes the following components:

- Access control based on business requirements
- User Access Management
- User Responsibility validation and enforcement
- Network access control
- Operating system access control
- Application access control
- Information access control
- Mobile computing and teleworking access control

The IAM's purpose in the context of the Cloud Computing is to extend and blur the lines of boundary and trust. It must achieve the following security functionalities:

- Timely and secure managing of on-boarding and off-boarding users in the cloud.
- Authenticating users in trustworthy and manageable manner and addressing credential management, delegation, and managing trust across multiple types of Cloud Computing Services.
- Federation to enable organizations to use selected Identity provider (IdP) to exchange identity attributes across allied organizations.
- Authorization and user profile management to establish and manage profiles and policies to control access in auditable manner.

Data Security Subsystem

In addition to the conventional data security functions that are usually associated with the specific data management systems (such as databases, or data warehouses) in the context of Cloud Computing, the data security subsystem must also support the following functionalities:

- Arranging different data stores and accessing measures based on the security level, availability and integrity requirement of the data.
- Effectively supporting the responsibility in terms of Physical Administrative Access, Logical Administrative Access, Object Sharing and Maintenance of the data which are well defined in the Service Level Agreement (SLA).
- Being able to test and verify the capabilities of the Secured and Virtual Storage, Disaster Recovery or Continuity of Operation declared by the cloud service providers.
- Being flexible enough to smoothly switch among the various mode of an IT application's lifecycle such as "application development mode", "application testing mode", "application operation mode", "application maintenance mode", and "application retiring mode", etc.

3.3 Communication, API and Business Process Manager

The Internal ESB is responsible for managing and interacting with the Company's current information at its Core IT Infrastructure. For example, the Internal ESB can manage and increase capability to communicate with Field Offices and Partners.

The External ESB is responsible for managing Cloud Computing Services in the future and the connection to external APIs to utilize the Cloud Computing based applications.

As a component allowing the external users or applications to integrate with the Company's applications, the Application Programming Interface (API) is a critical "gateway" between the external world and the internal Core IT Infrastructure.

The Business Process Manager subsystem is responsible for invoking Business Processes defining the work flows for both internal and external communication.

3.4 Final Recommendations

Finally, the students recommended the Company to carefully examine the following actions to develop their next generation IT system infrastructure.

- Until the Cloud security management matures, consider migration of only non-sensitive data and low risk applications as a logical first step.
- Develop more mature Identity and Access Management capabilities within the enterprise while the Cloud Computing Service community coalesces.
- Utilize ESBs to route and translate messaging for both internal and external users, which sets the stage for the Company to adapt to Cloud Computing.

4 Conclusion

After the SIAF was presented to the executives and IT management of the Company, it received high praise from the audience. It was commonly acknowledged that the most impressive achievement by the students was that they had correctly considered security at every level of the system. They also successfully balanced the benefits and risks involved in the Cloud Computing. The most attractive feature of their proposal was that it enabled the Company to gradually replace future applications development with Cloud Computing Services, while, smoothly and securely integrating these results with the Company's own Core IT Infrastructure. The students work had fully met the requirement. And the objectives of the program were also met completely.

During the final discussion on the project, most of the students had credited their success back to the security courses taught in the program, which had prepared them well for dealing with the security related issues in the project.

Therefore when the students correctly answered the question: "How to secure the Cloud based Enterprise Information System", and succeeded in their EIS Capstone project; our question: "Is the emphasis on security courses right?" had also been clearly answered. Indeed, the security education in the MS in EIS program played a critical role in our students' success.

Acknowledgement. The author sincerely thanks all the students who participated in the EIS Capstone class described in this paper. Much of the technical content and the conclusions made in this paper about the Service Integration Architecture Framework project are directly based on their excellent work.

References

1. Colorado Technical University: 2009 Course Catalog (2009)
2. Linthicum, D.S.: Cloud Computing and SOA Convergence in Your Enterprise. Addison-Wesley (2010)

3. Mather, T., Kumaraswamy, S., Latif, S.: Cloud Security and Privacy Enterprise. O'Reilly (2009)
4. Qu, Y.: Internal Communication Note (2010)
5. Goyal, B., Lawande, S.: Enterprise Grid Computing with Oracle. Oracle Press, USA (2006)
6. Windom, S., Hasse, M., Chaney, L., Salinas, M., Rademacher, T.: Service Integration Architecture Framework. Colorado Technical University Technical Report (2010)

Robust Programming by Example

Matt Bishop[1] and Chip Elliott[2]

[1] Dept. of Computer Science, University of California at Davis
Davis, CA 95616-8562 USA
bishop@cs.ucdavis.edu
[2] GENI Project Office, BBN Technologies, 10 Moulton Street
Cambridge MA 02138 USA
celliott@bbn.com

Abstract. Robust programming lies at the heart of the type of coding called "secure programming". Yet it is rarely taught in academia. More commonly, the focus is on how to avoid creating well-known vulnerabilities. While important, that misses the point: a well-structured, robust program should anticipate where problems might arise and compensate for them. This paper discusses one view of robust programming and gives an example of how it may be taught.

1 Introduction

The results of poorly written software range from the merely inconvenient to the catastrophic. On September 23, 2010, for example, a software error involving the mishandling of an error condition made Facebook inaccessible for over 2 hours [7]. Medical software, electronic voting systems, and other software [1,2,13] also have software problems.

Problems in software often appear as security problems, leading to a demand that students learn "secure programming". While laudable, this focuses the discussion of programming on *security* rather than good programming style. The reason this difference is important lies in the definition of "security".

Security is defined in terms of a security policy, which describes those states that the system is allowed to enter [3]. Should the system enter any other state, a breach of security occurs. "Secure programming" therefore ties programming to a particular policy (or set of policies). As an example, consider a program in which a buffer overflow on the stack will not be caught. The attacker overflows the buffer, uploading a changed return address onto the stack. This causes the process to execute code that the attacker desires. If the program adds privileges to the attacker, for example as a setuid-to-*root* program on a Linux system, the ability of the attacker to perform arbitrary tasks by exploiting this buffer overflow is a violation of any reasonable security policy. So, "secure programming"—in which one focuses on those programming problems that cause security violations—would cover this case.

Consider the same program, but it does not add privileges to the attacker. The attacker can exploit the same buffer overflow flaw as before, but that code

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 140–147, 2013.

will execute with the attacker's *original* privileges. As there is no increase in privileges, exploiting the buffer overflow flaw usually does not violate a security policy. Hence this is not a "secure programming" problem.

But it is a robustness problem. Such a buffer overflow can cause the program to act in unexpected ways. Robust code would handle the input causing the overflow in a reasonable way. In this case, a robust program would gracefully terminate, telling the user about the invalid input that caused the problem.

In what follows, we refer to "code" when we mean a program or a library. The reader should make the obvious generalization to terms. Thus, "input to code" means any input that the user or environment provide to a program or a library, including the parameters passed and the return value in the case of the latter. "Calling a function" may refer to invoking a program.

The goal of this paper is to discuss the principles of robust programming, and provide an example of how to explain the issues to students. The next section focuses on the principles. We then present an example of non-robust coding, and then show how to write the same library function in a robust way. We conclude with a brief discussion of our experiences using this example.

2 Background

There is amazingly little written about robust coding. Certainly any survey of the literature must begin with Kernighan and Plaugher [9] and Ledyard [10], who provide general rules. Other books focus on specific programming languages [8,11,12]. These books provide detailed rules and examples of the application of the rules. Specific exercises and mentoring [5,6,4] have also been discussed. This paper aims at a broader scope, enunciating some fundamental principles and then applying them to library functions.

3 Principles

Robust code differs from non-robust, or fragile, code by its adherence to the following four principles:

1. *Be paranoid.* The code must check any data that it does not generate to ensure it is not malformed or incorrect. The code assumes that all inputs are attacks. When it calls a function, the code checks that it succeeds. Most importantly, the programmer assumes that the code will have problems, and programs defensively, so those problems can be detected as quickly as possible.
2. *Assume stupidity.* The programmer must assume that the caller or user cannot read any manual pages or documentation. Thus, the code must handle incorrect, bogus, and malformed inputs and parameters appropriately. An error message should not require the user to look up error codes. If the code returns an error indicator to the caller (for example, from a library routine), the error indicator should be unambiguous and detailed. As soon as the

problem is detected, the code should take corrective action (or stop). This keeps the error from propagating.

3. *Don't hand out dangerous implements.* A "dangerous implement" is any data that the code expects to remain consistent across invocations. These implements should be inaccessible to everything external to the code. Otherwise, the data in that data structure may change unexpectedly, causing the code to fail—badly. A side benefit is to make the code more modular.
4. *Can happen.* It's common for programmers to believe conditions can't happen, and so not check for those conditions. Such conditions are most often merely highly unlikely. Indeed, even if the conditions cannot occur in the current version, repeated modifications and later additions to code may cause inconsistent effects, leading to these "impossible" cases happening. So the code needs to check for these conditions, and handle them appropriately (even if only by returning an error indicator).

The defensive nature of robust programming protects the program not only from those who use it but also from programming errors. Good programming assumes such errors occur, and takes steps to detect and report those errors, internal as well as external.

4 The Non-robust Example

This example is part of a queue management library. It consists of a data structure and routines to create and delete queues as well as to enqueue and dequeue elements. We begin with the queue structure and the interfaces.

```
/* the queue structure */
typedef struct queue {
  int *que;   /* the actual array of queue elements */
  int head;   /* head index in que of the queue */
  int count;  /* number of elements in queue */
  int size;   /* max number of elements in queue */
} QUEUE;

void qmanage(QUEUE **, int, int);/* create, delete queue */
void qputon(QUEUE *, int);       /* add to queue */
void qtakeoff(QUEUE *, int *)    /* remove from queue */
```

This organization is fragile. The pointer to the QUEUE structure means the location of the data, and hence the data itself, is accessible to the caller, so the caller can bypass the library to obtain queue values—or, worse, alter data in the structure. So this encapsulation is not hidden from the caller.

Next, consider the queue manager routine *qmanage*. The first argument is the address of the pointer to the QUEUE structure; the second, a flag set to 1 to create a new queue and 0 to delete the queue; and the third, the size of the queue to be created. If the second argument is 0, the third argument is ignored.

```
void qmanage(QUEUE **qptr, int flag, int size)
{
  if (flag){
      /* allocate a new queue */
      *qptr = malloc(sizeof(QUEUE));
      (*qptr)->head = (*qptr)->count = 0;
      (*qptr)->que = malloc(size * sizeof(int));
      (*qptr)->size = size;
  }else{
      /* delete the current queue */
      (void) free((*qptr)->que);
      (void) free(*qptr);
       }
}
```

This routine is composed of two distinct, logically separate operations (create and delete) that could be written as separate functions. Thus, its cohesion is low. Poor cohesion generally indicates a lack of robustness.

Indeed, this code is not robust. The arguments are not checked. Given that the last two are integers, a caller could easily get the order wrong. The semantics of the language means that if the second argument is non-zero, the function creates a queue. Thus the call

```
qmanage(&qptr, 85, 1);
```

allocates a queue that can hold at most 1 element. This is almost certainly not what the programmer intended. Further, this type of error cannot be easily detected. Decoupling the two separate functions solves this problem.

Lesson 1. *Design functions so that the order of elements in the parameter list can be checked.*

Next, consider the *flag* argument. The intention is for 1 to mean "create" and 0 to mean "delete", but the code makes any non-zero value mean "create". There is little connection between 1 and creation, and 0 and deletion. So psychologically, the programmer may not remember which number to use. This can cause a queue to be destroyed when it should have been created, and *vice versa*.

Lesson 2. *Choose meaningful values for the parameters*

The third set of problems arises from a failure to check parameters. Suppose *qptr* is a nil pointer (**NULL**) or an invalid pointer when a queue is being created. Then the first *malloc* will cause a crash. Similarly, if *size* is non-positive, when the queue is allocated (the second *malloc*), the result is unpredictable.

Now consider queue deletion. Suppose either *qptr* or **qptr* is **NULL**. Then the result of the function *free* is undefined and may cause a crash.

Lesson 3. *Check the sanity of the parameters.*

More generally, the pointer parameter poses problems because of the semantics of C. C allows its value to be checked for **NULL**, but not for a meaningful non-**NULL** value. Thus, sanity checking pointers in C is in general not possible.

Lesson 4. *Using pointers in parameter lists leads to errors.*

The function does not check sequences of invocations. Consider:

```
qmanage(&qptr, 1, 100);
  /* . . . */
qmanage(&qptr, 0, 1);
  /* . . . */
qmanage(&qptr, 0, 1);
```

This deallocates the queue twice. The second deallocation calls *free* on previously deallocated memory, and the result is undefined (usually a crash).

Lesson 5. *Check that the function's operations are semantically meaningful.*

In the body of the function, failure of either memory allocation *malloc* call will cause references through nil pointers.

Lesson 6. *Check all return values, unless the value returned does not matter.*

Finally, consider the multiplication. If the system has 4 bytes per integer, and *size* is 2^{31} or more, on a 32-bit machine overflow will occur. Thus the amount of space may be much less than what the caller intended. This will probably cause a crash later on, in a seemingly random location.

Lesson 7. *Check for overflow and underflow when performing arithmetic operations*

We now apply these lessons to construct a robust data structure and queue management routine.

5 The Robust Example

Begin with the queue structure, which is at the heart of the library. That structure is to be unavailable to the caller, so we need to define two items: the structure itself, and its interface. We deal with the interface first. The object that the caller uses to represent a queue will be called a *token*.

If the token is a pointer to a structure, the user will be able to manipulate the data in the structure directly. So we need some other mechanism. Indexing into an array is the obvious alternative. However, simple indices enable the caller to refer to queue 0, and have a high degree of certainty of getting a valid queue. So instead we use a function of the index such that 0 is not in the range of the function. Thus, we will represent the queue as an entry in an array of queues. The token will be the output of an invertible mathematical function of this index.

Also, the code must never reference a queue after that queue is deleted. Suppose a programmer uses the library to create queue A. He subsequently deletes queue A and creates queue B, which has the same index in the array of queues as queue A did. If the token is a function of the index only, a subsequent reference to queue A will refer to queue B. To avoid this problem, each queue is assigned a nonce that is merged into the token. For example, suppose queue A has nonce 124 and queue B has nonce 3086, and both have index 7. The token for queue A

is $f(7, 124)$ and the token for queue B is $f(7, 3085)$. As these values differ, the token will refer to queue A and be rejected.

This simplifies the interface considerably. The type **QTOKEN** consists of the value of the function that combines index and nonce. We must be able to derive the index and the nonce from this token; a moment's thought will suggest several ways to create such a function. Then, rather than pointers, the value of the token represents the queue. The caller cannot access the internal queue representation directly; it can only supply the token, which the library then maps into the corresponding index.

This applies lesson 4. Because we designed the **QTOKEN**s so their values could be easily sanity checked, this also follows lesson 3.

The queue structure and storage then becomes:

```
typedef struct queue {
  QTICKET ticket;    /* contains unique queue ID */
  int que[MAXELT];   /* the actual queue */
  int head;          /* head index in que of the queue */
  int count;         /* number of elements in queue */
} QUEUE;

static QUEUE *queues[MAXQ];   /* the array of queues */
static unsigned int noncectr = NOFFSET;/* current nonce */
```

For simplicity, all queues are of fixed size. All global variables are declared static so they are not accessible to any functions outside the library file. An empty queue has its count eld set to 0 (so the queue exists but contains no elements); a nonexistent queue has the relevant element in the array *queues* set to *NULL* (so the queue does not exist).

We modularize the functions. We define two new functions. *qgentok* generates a token from an index. *qreadtok* validates a given token and, if valid, returns the corresponding index. This enables us to make changes to the mapping between the token and the index in *queues*.

The queue creation and deletion operations are decoupled into two separate functions. Due to space limitations, we examine only the queue creation function:

```
QTOKEN qcreate(void)
{
  register int cur;    /* index of current queue */
  register QTOKEN tkt;/* new ticket for current queue */

  /* check for array full */
  for(cur = 0; cur < MAXQ; cur++)
    if (queues[cur] == NULL)
      break;
  if (cur == MAXQ){
    ERRBUF2("create_queue: too many queues (max \%d)", MAXQ);
    return(QE_TOOMANYQS);
  }
  /* allocate a new queue */
```

```
  if ((queues[cur] = malloc(sizeof(QUEUE))) == NULL){
    ERRBUF("create_queue: malloc: no more memory");
      return(QE_NOROOM);
  }
  /* generate ticket */
  if (QE_ISERROR(tkt = qgentok(cur))){
    /* error in ticket generation -- clean up and return */
    (void) free(queues[cur]);
    queues[cur] = NULL;
    return(tkt);
  }
  /* now initialize queue entry */
  queues[cur]->head = queues[cur]->count = 0;
  queues[cur]->ticket = tkt;
  return(tkt);
}
```

The differences between this routine and the non-robust version are instructive. Creating a queue requires no information beyond the invocation. So if one wanted to allow the user to specify the size of the queue, that size could be passed as the single parameter. Therefore, the parameters cannot be confused with one another—there are no parameters, or (if modified as suggested above) exactly 1 parameter. This applies lessons 1 and 2.

Next, the return values of all functions are checked. If *malloc* fails, an error code and an expository message are returned. This should never happen; the amount of space requested is a small constant, and with virtual memory, it would be very rare for that allocation to fail. Nevertheless, we check for failure (thereby checking for "impossible" cases). Similarly, if a token cannot be generated, an error is returned. This follows the lesson of checking *all* function calls—our own as well as library and system calls. This applies lesson 6.

The routine provides two types of error indicators. The return value is an integer outside the range of the function used to generate the token (so it cannot be confused with a valid token). A header file supplies a macro, **Q_ISERROR**, that takes an integer and returns 1 if the value represents an error, and 0 if it represents a token. In addition, a special error buffer contains a string describing the problem and any limits that were exceeded. A good example of this is in the body of the first *if* statement in the above function. If there were no available space in the array, the queue cannot be allocated. So the routine provides the caller an error indicator, and **ERRBUF2** loads into the error buffer a message giving the maximum number of queues that can be created. This way, the programmer knows the maximum number of queues the library can create.

Lesson 8*. Provide meaningful and useful error indicators and messages.*

6 Conclusion

Teaching robust programming is implicit in every beginning programming course. Unfortunately, as students advance through other computer science courses, they

often do not use the techniques for writing robust programs. Changing this situation requires having the students apply the techniques they have learned, and are learning, rather than treating the subject as an abstract exercise in analysis.

A similar statement holds for "secure programming". A focus on security, though, is misplaced—while it is a critical element of software, its exact definition varies from system to system and site to site. Programming robustly provides the basis for adding security elements to the program; but without robust programming, secure programming will never achieve the desired effect.

The above example was constructed many years ago to illustrate the problems of non-robust code, and how library routines written robustly overcome the problems. When teaching this lesson, having the students find the problems in the non-robust library challenges them to think of what can go wrong—in computer security terms, to think like an attacker (except that the "attacker" may not be malicious). This is the key to robust programming, and indeed all code reviews—a mode of thought in which problems are anticipated by examining the structure of the code and asking, "What if . . . ?"

References

1. Infusion pump improvement initiative. Tech. rep. Center for Devices and Radiological Health, U. S. Food and Drug Administration (April 2010), http://www.fda.gov/downloads/MedicalDevices/ProductsandMedicalProcedures//parGeneralHospitalDevicesandSupplies/InfusionPumps/UCM206189.pdf
2. Bilton, N.: Bug causes iphone alarm to greet new year with silence (January 2, 2011), http://www.nytimes.com/2011/01/03/technology/03iphone.html
3. Bishop, M.: Computer Security: Art and Science. Addison-Wesley, Boston (2002), http://www.amazon.com/gp/product/0201440997
4. Bishop, M.: Some 'secure programming' exercises for an introductory programming class. In: Proceedings of the Seventh World Conference on Information Security Education (July 2009)
5. Bishop, M., Frincke, D.: Teaching secure programming. IEEE Security & Privacy 3(5), 54–56 (2005)
6. Bishop, M., Orvis, B.J.: A clinic to teach good programming practices. In: Proceedings of the Tenth Colloquium on Information Systems Security Education, pp. 168–174 (June 2006)
7. Johnson, R.: More details on today's outage (September 2010), http://www.facebook.com/note.php?note_id=431441338919&id=9445547199&ref=mf
8. Kernighan, B.W., Pike, R.: The Practice of Programming. Addison-Wesley Professional, Boston (1999)
9. Kernighan, B.W., Plauger, P.J.: The Elements of Programming Style, 2nd edn. Computing McGraw-Hill (1978)
10. Ledgard, H.F.: Programming Proverbs. Hayden Book Co. (1975)
11. Maguire, S.: Writing Solid Code. Microsoft Programming Series. Microsoft Press, Redmond (1993), http://www.amazon.com/dp/1556155514
12. Seacord, R.C.: Secure Coding in C and C++. Addison-Wesley Professional, Upper Saddle River (2005), http://www.amazon.com/dp/0321335724
13. Zetter, K.: Serious error in Diebold voting software caused lost ballots in California county—Update (December 8, 2008), http://www.wired.com/threatlevel/2008/12/unique-election/

An Approach to Visualising Information Security Knowledge

Colin James Armstrong

Curtin University,
Perth, Western Australia
Colin.Armstrong@cbs.curtin.edu.au

Abstract. This paper discusses the application of international standards and guidelines together with vendor sponsored accreditation programs in the development of information security curriculum and an approach for visualising that knowledge.

Keywords: ISO27000, COBIT, SFIA, ITIL, information security, curriculum, visualisation.

1 Introduction

Global information communications demand effective and appropriate information security. Teaching information security effectively and appropriately requires incorporating two main dimensions: internationally agreed methods and approaches, and a close organisational fit. Although the majority of organisations have deployed information security capacities, these are not always as effective as organisations would wish. A CSI Survey [1] reports large increases in the incidence of financial fraud, malware infection, denials of service, password sniffing and Web site defacement. In order to better address security management 43% of respondents suffering security incidents changed their organisation's security policy following the abuse [2]. The CISO report published by ISC2 suggests that organisations, like Socrates, need to 'know thyself', being aware of their challenges and opportunities in information systems security management [3]. This report confirms that half of the respondents feel they have a significant ability to impact the security posture of their organisation yet continue to see vulnerabilities and incidents. Emerging new challenges include adoption of social networking applications to improve business processing, and 'cloud' technologies as an alternative repository for corporate information.

Information security curriculum needs to possess the capacity to demonstrate how it addresses these contemporary and other traditional objectives within the much broader encompassing information and communications technology (ICT) arena. Internationally agreed methods and approaches are established through international standards and professional bodies to provide guidance in what to do, how to do it, and who will do it. In the current age of global organisational structure and communications a baseline is

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 148–155, 2013.

essential in order to determine levels of security management between business partners. When organisations consider venturing into, and extending their business information over the internet, they don't necessarily have the means for quickly and accurately measuring their vulnerability and the risks they offer to other organisations. Compliance with international standards gives some predictability and evidence of compliance provides reassurance that the organisation is probably managing security at an appropriate level for the desired engagement. Business organisations trading in global economic markets require security appropriate to their risk exposure. International standards and guidelines provide the baseline for security requirements and to address these requirements organisations need firstly employees with the essential skills and knowledge and secondly the necessary organisational policies and procedures, to maximise security of their systems. The core body of knowledge recognised by professional associations and certification bodies provides the framework for the necessary skills and knowledge which are delivered by recognised educational institutions. Providing the means of visualising information security subject matter facilitates seeing how well curricula match industry requirements and potential staff capabilities.

2 Standardising Information Security

The need to ensure information is protected and secure is well established. The roles and tasks performed to secure and protect information communications falls upon those working in the ICT sector. Compliance with expected competencies within this sector is a major undertaking and these competencies should be aligned with internationally agreed standards. There is as yet no clear single agency responsible for overseeing the alignment of internationally agreed standards. The generally accepted core body of knowledge is no longer disputed yet there is a proliferation of organisations offering solutions to the vexed challenge of securing information. Those responsible for managing information security turn to a number of possible solutions. Solutions to securing information focus on what task should be done, how those tasks should be performed, and who is appropriate to perform these tasks. Seeing the relationships between various information security stakeholders and having the means to visualise competencies and capacities associated with information security roles and tasks is also part of the solution.

The ICT stakeholders identified include professional standards organisations, businesses, governments, educators, academic institutions, students, and the community at large. The community at large is a necessary stakeholder because information is exchanged between members of the public and other traditional ICT stakeholders.

Information technology service management relies on professional standards organisations to provide leadership and direction. Professional standards organisations include International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and special interest groups such as Information Systems Audit and Control Association (ISACA), International Professional Practice

Partnership (IP3), and the International Information Systems Security Certification Consortium, Inc. (ISC²).

One might observe that the ISO/IEC 27000 series and ISACA's CoBIT define 'what' should be done, ITIL defines 'how' it should be done, SFIA defines 'who' should do it, and the various other bodies offer systems of accreditation ensuring 'what', 'how', and 'who' compliance. Two groups; one reflecting the organisation's requirements, the other a practitioner's potential capabilities and the interrelationships between 'what', 'how', and 'who' may be represented, as an information security network as shown in Figure 1.

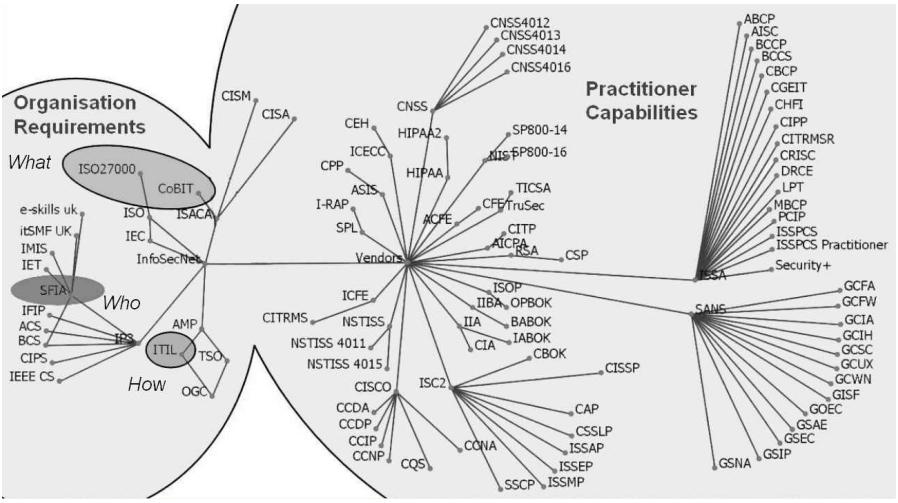


Fig. 1. Information Security Network

The ISO/IEC 27000 Series is that most relevant to information security. The comprehensive nature of the ISO/IEC 27000 Series is intended to address every activity considered necessary for managing information security. The generally accepted view is that standards define what must be done and that guidelines explain how to conduct the necessary activities to be compliant with those standards. The Information Systems Audit and Control Association (ISACA) Framework COBIT addresses 'what' should be done by providing technical guidance [4].

How to convert the divergent high level guidance provided by ISO and COBIT into a coherent set of practically implementable tasks suggested in ITL is not obvious. Kulkari [5] discusses the challenges management faces when business processes undergo rapid environmental change and are forced to modify policies to addresses redefined business goals. The COBIT Framework facilitates management of change by addressing the three primary information control topics; security, quality, and fiduciary[6]. Help [7] offers a model of the transition from higher level requirements guidance offered in ISO and COBIT to practical application implementation. The arrangements of the frameworks in Help's model clearly shows the relationship and

overlapping between not only each model but also the transitions for 'What' and 'How' in regard to their relationship to standards and guidelines.

The Skills Framework for the Information Age (SFIA) is intended to address a perceived lack of agreement on an appropriate framework to describe graduate skills [8]. Organisations employing ICT professionals can use SFIA to write position descriptions, manage risks and improve the ICT function [8]. It has also been used to identify skills attained by graduates of an academic program [9]. The SFIA matrix, that provides skills grouped by categories and subcategories on one axis, while the other axis offers seven levels of responsibility and accountability, is shown as a network in Figure 2. The seven levels are generically described, commencing at the lowest level, as 'Follow' ascending through 'Assist', 'Apply', 'Enable', 'Ensure, advise', to 'Instantiate, influence', culminating at the highest level with 'Set strategy, inspire, mobilise' [10]. Currently, IP3 assumes an ICT professional capacity operating at levels equivalent to SFIA Level 5, and that a university degree program graduate would be able to assume Level 4 responsibilities [10].

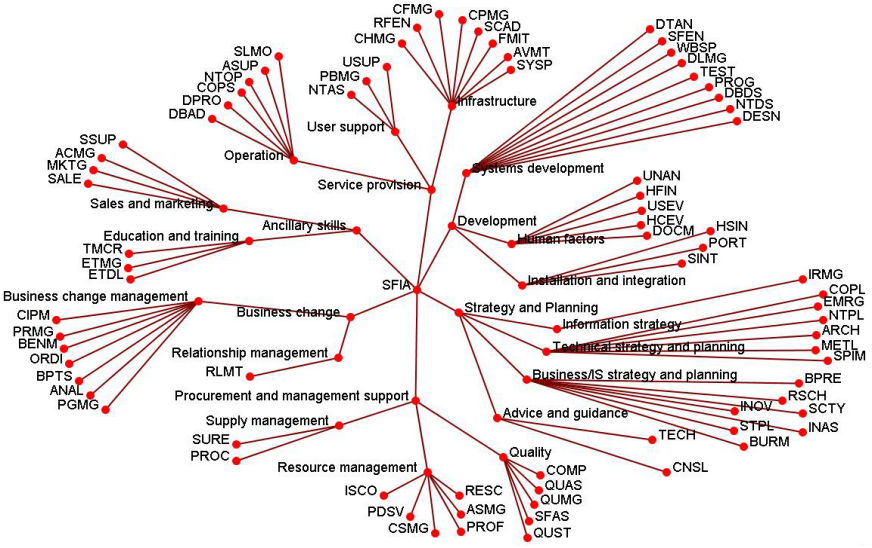


Fig. 2. SFIA Skills Network. Adapted from Source: [10].

The crucial issue after determining 'what' should be done is addressing 'how' tasks should be conducted. The Information Technology Infrastructure Library (ITIL) sets out the requisite IT service management concepts and practices for meeting the criteria established in the ISO/IEC 27000 Series and by COBIT. Rudd [11] provides an introductory overview of ITIL explaining the interconnections between ICT management and service delivery, and support mechanisms. Cartlidge et al. [12] furthers Rudd's introductory overview discussing the ITIL service lifecycle in regard to; strategic planning, integrating and aligning business goals, continual improvement, measuring effectiveness and efficiency, optimising costs, achieving a return on

investment, developing partnerships and relationships, improving project delivery, outsourcing, gaining a competitive advantage, delivering required services, managing change, and demonstrating governance.

Because the primary focus of ITIL is the provision of business IT service, security is sometimes seen as an additional process. ITIL does provide for information security, primarily as a service.

3 Curriculum Development

The preceding overview shows the nature of contributions to information security curriculum development drawn from the ISO 27000 Series, COBIT, SFIA, and ITIL as used by academic institutions developing course materials. Armstrong and Jayaratna [13] discuss the structure of required information security skills, distinguishing between generic, specialist, and practical skill sets inculcated into a postgraduate internet security management curriculum design. Kim and Surendran [14] offering a Korean perspective discuss four main areas of information security management curriculum design focussing on security policy, risk management, safeguard implementation and training, and safeguard management and conclude with the twelve necessary information security topics.

The Bogolea and Wijekumar [15] survey concluded that curriculum developers should utilise already existing government resources. Armstrong and Armstrong [16] examine alignment of information security education curricula by mapping core body of knowledge and learning outcomes to fifteen national and international accreditation standards. The Theoharidou and Gritzalis [17] review confirms design of academic curricula to conform with CISSP's ten domains meets industry requirements. Dodge, Hay and Nance [18] argue aligning cyber security exercise outcomes assessment to include mapping core body of knowledge in selected standards facilitates measuring student performance.

Examination of core body of knowledge and learning outcomes recommended by academic, government, and vendor publications suggests adopting the CISSP ten domain structure. It is apparent that the core body of knowledge and learning outcomes for information security is well defined. The extent and depth of information to be taught is not disputed but there is a challenge in how best to demonstrate that necessary materials are presented to students and that students have studied the required topics. The apparent lack of a ready means to clearly see the various components of information security is therefore a problem. This problem is not restricted to academia and is exasperated in the business world when non security aware personnel are required to decide organisational requirements, outcomes, and appropriate allocations of resources for meeting information security objectives.

4 Visualising Information Security Criteria

Information security education and training organisations look to business needs, emerging ICT developments, and build products to sell to those seeking to meet

employment opportunities. As pointed out by von Konsky et al. [9], aligning prospective employee capacity, graduate students in particularly, with job criteria is beneficial to both employer and employee. The end objective of curriculum development is graduates succeeding in the workplace. A method facilitating seeing alignments more readily seems a logical next step.

The process for visualising information security curricula alignment to industry standards and guidelines such as SFIA and CISSP learning outcomes, and core bodies of knowledge is modelled in Figure 3. The visualisations are constructed by taking the listed information security categories and attributing them with a value based on the SFIA levels of autonomy and responsibility.

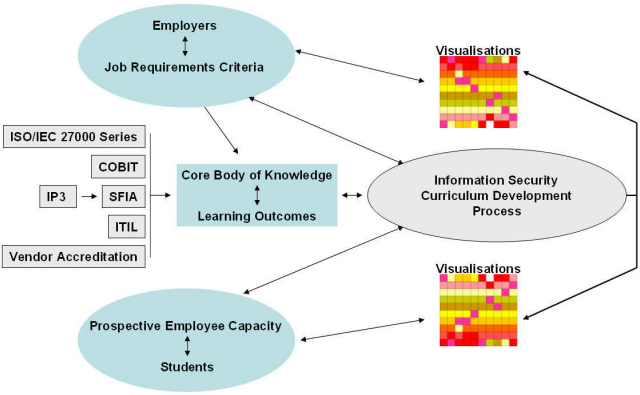
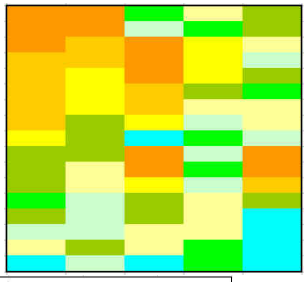


Fig. 3. Information Security Curriculum Development Model

A matrix of 78 SFIA categories as shown in Figure 4, each with seven possible levels equates to 546 distinct patterns.

ACMG	COPS	INAS	PRMG	SLMO
ANAL	CPMG	INOV	PROC	SPIM
ARCH	CSMG	IRMG	PROF	SSUP
ASMG	DBAD	ISCO	PROG	STPL
ASUP	DBDS	METL	QUAS	SURE
AVMT	DESN	MKTG	QUMG	SYSP
BENM	DLMG	NTAS	QUST	TECH
BPRE	DOCM	NTDS	RESC	TEST
BPTS	DPRO	x	RFEN	TMCR
BURM	DTAN	NTOP	RLMT	UNAN
CFMG	EMRG	NTPL	RSCH	USEV
CHMG	ETDL	ORDI	SALE	USUP
CIPM	ETMG	PBMG	SCAD	WBSP
CNSL	FMIT	PDSV	SCTY	x
COMP	HCEV	PGMG	SFAS	x
COPL	HFIN	PORT	SFEN	x
x	HSIN	x	SINT	x



Score Card Values						
Follow	Assist	Apply	Enable	Ensure / Advise	Initiate / Influence	Set Strategy
1	2	3	4	5	6	7

Fig. 4. SFIA Coded Matrix Example with Score

Colouring or shading each cell provides an almost unique picture making it a simple matter for the stakeholder, a staff member from human resources department, an academic, or a prospective employee, to develop score card visualisations addressing a set of information security requirements shown in Figure 5.

Fig. 5. Example of Required SFIA Skills Compared with Best Available Applicant Skills

Unlike the SFIA framework that provides an alpha code for each skill, the coding used for CISSP relies on a numbering system. This numbering system was derived from the table of contents to CISSP Guide to Security Essentials by Gregory [19]. From the ten chapters, one for each domain, sections and subsections lead to the provision of 78 topics in Chapter 1, 28 topics in Chapter 2, and to eventually provide a total of 680 topics and sub categories.

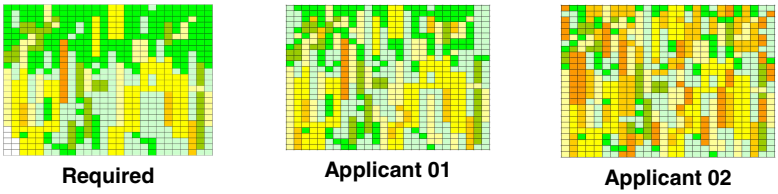


Fig. 6. Example of Required CISSP Skills Compared with Best Available Applicant Skills

5 Conclusion

This paper has provided an overview to some of the influencing factors in the information security curriculum development arena and offered a simple visualisation process for evaluating decision making processes regarding associated skill sets and core knowledge. Adoption of this approach facilitates ready recognition of intricate details to a complex topic independent of external influences. Confirming that this approach using visualisation of information security processes is readily suited to auditing and regulatory compliance purposes is the subject of further current research.

References

1. Peters, S.: 2009 CSI Computer Crime and Security Survey Executive Summary. Computer Security Institute, New York (2009)
2. Richardson, R.: 2009 CSI Computer Crime and Security Survey Comprehensive Edition. Computer Security Institute, New York (2009)

3. CISO Survey Report, The, State of Cybersecurity from the Federal CISOs Perspective – An (ISC)2 Report (2010)
4. COBIT Framework for IT Governance and Control (September 20, 2010), http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
5. Kulkari, M.: Applying COBIT Framework. Information Systems Control Journal 5 (September 20, 2003), http://www.isaca.org/Journal/Past-Issues/2003/Volume-5/Pages/Applying-COBIT-Framework1.aspx
6. Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. A Management Briefing From ITGI and OGC. IT Governance Institute (2008), http://www.itgi.org
7. Help, T.: Case Study: Better to Prevent Than Cure—A New Way to Enhance IT and Business Governance Collaboration. Information Systems Control Journal 4 (September 20, 2008), http://www.isaca.org/Journal/Past-Issues/2008/Volume-4/Pages/Case-Study-Better-to-Prevent-Than-Cure-A-New-Way-to-Enhance-IT-and-Business-Governance-Collaboration.aspx
8. SFIA, Skills Framework for the Information Age Foundation, 3.0. SFIA Foundation, United Kingdom (2005), http://www.sfia.org.uk/
9. von Konsky, B.R., Hay, D., Hart, R.: Skill set visualisation for software engineering job positions at varying levels of autonomy and responsibility. In: 19th Australian Conference on Software Engineering (ASWEC 20008), March 26-28, pp. 26–28. Industry Experience Report, Perth (2008)
10. Gregor, S., von Konsky, B.R., Hart, R., Wilson, D.: The ICT Profession and the ICT Body of Knowledge (Vers. 5.0). Australian Computer Society, Sydney (2008)
11. Rudd, C.: An Introductory Overview of ITIL. itSMT Ltd., Earley (2004)
12. Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I.,, Windebank, J., Rance, S.: An Introductory Overview of ITIL® V3. The UK Chapter of the itSMF, UK (2007)
13. Armstrong, H.L., Jayaratna, N.: Internet Security Management: A Joint Postgraduate Curriculum Design. Journal of Information Systems Education 13(3) (2002)
14. Kim, K.-Y., Ken Surendran, K.: Information Security Management Curriculum Design: A Joint Industry and Academic Effort. Journal of Information Systems Education 13(3) (2002)
15. Bogolea, B., Wijekumar, K.: Information Security Curriculum Creation: A Case Study. In: Proceeding of the 1st Annual Conference on Information Security Curriculum Development, InfoSecCD 2004 (2004)
16. Armstrong, C.J., Armstrong, H.L.: Mapping Information Security Curricula to Professional Accreditation Standards. In: The West Point Workshop, 8th Annual IEEE SMC Information Assurance Workshop. United States Military Academy, West Point (2007)
17. Theoharidou, M., Gritzalis, D.: Common Body of Knowledge for Information Security. IEEE Security & Privacy 5(2) (March/April 2007)
18. Dodge, R.C., Hay, B., Nance, K.: Standards-Based Cyber Exercises. In: International Conference on Availability, Reliability and Security, ares, pp. 738–743 (2009)
19. Gregory, P.H.: CISSP Guide to Security Essentials. Cengage Learning, Boston (2009)

Creating Shareable Security Modules

Kara Nance[1], Blair Taylor[2], Ronald Dodge[3], and Brian Hay[4]

[1,4] University of Alaska Fairbanks, Fairbanks, AK, USA
{klnance,brian.hay}@alaska.edu
[2] Towson University, Towson, MD, USA
btaylor@towson.edu
[3] United States Military Academy, West Point NY, USA
ronald.dodge@usma.edu

Abstract. While there is increased appreciation of the need to provide students with education in computer security, there are significant challenges associated with the creation of shareable computer security modules that can be used by a wide-range of educators. This paper discusses some of the challenges that educators currently face in this area, and presents a means to couple a successful framework and infrastructure environment to address some of the associated issues. Two examples are provided that link the framework and infrastructure followed by suggestions for future research and development in this area.

Keywords: Computer Security Education, Computer Education, Repositories.

1 Introduction

This paper discusses a framework for creating shareable security modules for information assurance. We explain the environmental and pedagogical challenges associated with the creation and sharing of educational resources, followed by a description of two successful projects that can be coupled to facilitate the process - the Security Injections@Towson (SI@T) and the Remotely Accessible Virtualized Environments (RAVE) projects. We provide example labs that demonstrate the coupled framework in action and conclude with future considerations that will facilitate the creation and continued evolution of shareable security modules.

2 Challenges

The benefits to a hands-on learning environment are widely recognized. Access to hands-on environments not only strongly reinforces lecture concepts, but also allows students to experiment with and extend concepts presented in the classroom. However, there is a great deal of effort required for individual instructors to create educational materials that extend course concepts to a hands-on learning environment. The challenges and time requirements can make the exercise prohibitive for many

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 156–163, 2013.

educators. Moreover, when those efforts are successful, there is often not an easy way to leverage the effort of any given teacher to improve the capabilities of the entire community.

2.1 Environmental Challenges

Below is a list of questions instructors may need to address when creating a hands-on computer lab experience:

- Do all of the students have the same configuration?
- Do the students all have the same computing platform?
- Do they all have the same operating system?
- Do their machines have enough resources to run the lab exercise?
- How do I know that they all started from the same configuration?
- If I am not sure that they all started from the same configuration, how can I grade them appropriately?
- When a student has a problem with the lab exercise, how can I provide help to them?
- If I need to make a change to the lab exercise or configuration, how do I distribute that to all students?
- If I am not at my own computer or at the school, how can I work on the lab exercises? [6]

In addition to configuration issues, the instructor needs to worry about student access to the lab resources, load balancing among limited resources (such as software licenses), and managing the instructor time so that individual student needs can be met. While these issues are complicated in a face-to-face laboratory environment, they become even more challenging when the educational environment involves distance education or even an asynchronous local experience.

When the topic being taught is computer security, additional issues arise as the hands-on labs and activities frequently can only be done in an isolated environment. Studying issues such as the malware behavior and cyberdefense exercises would not be safe (or in some cases, legal) on production networks. Yet, the ability to gain hands-on experience with the computer security concepts presented throughout the curriculum is essential if we want students to be able to address the evolving security needs of the nation.

2.2 Pedagogical Challenges

In addition to the environmental challenges faced by instructors, further work is required to produce materials which support a meaningful hands-on educational experience for the student. This includes providing adequate foundational elements to bring all students to a common level, educational content to meet the learning objectives, reflective activities to ensure that the learning objectives have been met, and extension activities to demonstrate how the concepts fit into the big picture.

In addition, the current ad hoc nature of most Computer Science (CS) labs inadequately address synthetic and analytical thinking, Most programming labs are structured towards the goal of "getting the code to run." For example, a lab assignment which requires students to compute the average of three test scores could be tested with the input values of 100, 100, and 100; and submitted with an answer of 233.33. In many cases, students are so relieved that the code ran they give little thought regarding the reasonableness of the answer. To address these challenges and better prepare students as security professionals, there have been increased efforts towards creating information assurance laboratories [1-3]. However, while more instructors recognize the need for incorporating security into the curriculum, many are hindered by the environmental challenges listed above, resource limitations, time constraints, insufficient security training, and lack of effective pedagogical materials.

3 Framework for Security Modules

Based on our own experiences with these challenges, we propose guidelines for creating information assurance resources. Specifically, a framework for shareable security modules should:

1) be broadly applicable across institutions and courses
2) be extendible to meet the needs of diverse audiences
3) be easy to use from a student perspective
4) be easy to identify, access, and implement for instructors
5) encourage active learning
6) facilitate and stimulate development of new modules
7) be largely platform independent

The combination of two successful NSF research projects provides an exciting opportunity to begin to meet these important guidelines. The following sections describe the Security Injections@Towson (SI@T) (NSF Project 0817267) and the Remotely Accessible Virtualized Environments (RAVE) (NSF Project 0123152) and provide two examples of how the project outcomes can be utilized in tandem to begin to meet the requirements for a framework for shareable security modules.

3.1 Security Injections@Towson

For the past five years, researchers at Towson University have worked with instructors across five diverse institutions, to incorporate security into the CS curriculum. The project has targeted the introductory programming courses required of all CS majors: Computer Science I (CS1), Computer Science II (CS2), and the preparatory course in programming logic (CS0); as well as the Computer Literacy course offered to non-majors. The goals of the project were to 1) increase faculty awareness of secure coding concepts 2) increase students' awareness of secure coding issues 3) increase students' ability to apply secure coding principles and 4) increase

the number of security-aware students. Towards this end, they developed and implemented a series of self-contained security injection modules that target key security concepts including integer overflow, buffer overflow, and input validation for the programming courses and phishing, passwords, and cryptography for the literacy course [1].

The process for material development began with an initial set of draft modules that were piloted in local classrooms. To encourage collaboration, researchers held on-site faculty workshops at each of the participating institutions, using the modules as starting points for discussion and review. Revised modules were deployed in a variety of educational contexts. Formal assessment included pre and post-tests, code checks, and faculty surveys to identify factors that worked well across different demographic groups. Feedback from workshop participants, assessment results, and advice from an expert evaluator, shaped the formation of the resulting security injection modules.

The format for the security injection module includes four components as described below:

Background: The purpose of this section is to set the context of the assignment, provide necessary background information for the security lab, and motivate students for future learning. This section includes a brief summary of the targeted security issue, a description of the problem and risk, code snippets which demonstrate the vulnerability, and real-life examples which describe actual occurrences of security incidents that have been documented in the news or other media and are selected to peak students' interest and motivate them to fully understand the concept.

Real-life Example: In December 2005, a Japanese securities trader made a $1 billion typing error, when he mistakenly sold 600,000 shares of stock at 1 yen each instead of selling one share for 600,000 yen. A few lines of code may have averted this error. [7]

Problem-Security-Related Lab: Creating interesting and relevant CS lab assignments has always been challenging. Students today are genuinely interested in security; therefore security-centric labs not only teach important security concepts but can help increase interest and motivation. Dovetailing the traditional CS core concepts with relevant security topics – arrays with buffer overflow, data types with integer errors – has been effective. A model for mapping security topics to primitives, courses - CS0, CS1, or CS2, and learning objectives [4] is easily expanded to other courses.

Checklist: Security checklists, which target a security vulnerability or topic, have been developed using feedback from students, instructors, assessment, and an expert evaluator. Checklists help students check their code and simultaneously learn and internalize important security concepts. Checklists provide a quantifiable list of security criteria to aid in writing secure code and further

reinforce security principles by encouraging self-evaluation and learning reinforcement. The checklist can also be used for peer reviews, collaborative learning, and assessment. Repeated exposure to the checklists and security concepts facilitates use of the checklists and reinforces the security principles. Additionally, as the process of using the checklist becomes routine, the expectation is that students will practice this habit as programmers.

Analysis- Discussion questions: Discussion questions require students to analyze and summarize their results and promote critical thinking, analysis, and reflection. Additionally, students' answers to these questions provide valuable and immediate feedback to the instructor.

The template for the security injection modules was created with an eye towards the learning sciences and borrowing from the more structured laboratory approach employed by the traditional sciences such as biology and chemistry. By motivating students with background information, including self-checks and reflective questions, students are encouraged to analyze the process, the results, and the security implications. The use of a standardized lab format was also found to be beneficial to both students and instructors. Students gained familiarity with the structure and process for completing each assignment. Instructors could pick and choose parts of the labs for inclusion in their own assignments and most importantly, this model proved easy to expand for new courses and new topics.

3.2 RAVE

One common barrier to the utility and adoption of a lab repository is the heavy dependence on infrastructure and support. These requirements include specific hardware and software requirements for the labs, shared computer labs with a fixed number of computers, and to the system administration of the lab facilities.

The model implemented by the RAVE (Remote Access Virtual Environment) project, creates shareable virtual environments built to support many institutions remotely accessing a set of resource clusters. It replicates and builds on the successful prototype ASSERT Lab at the University of Alaska Fairbanks [8]. Many papers have discussed the benefit of virtualization supporting information assurance laboratory exercises. The advantage of RAVE comes from the nature of a shared set of computing recourses; one virtualization resource center is used by many different institutions. The RAVE architecture consists of multiple virtual resource centers. Combining the shareable lab exercises with a standard lab infrastructure removes a significant barrier limiting many institutions.

4 Examples

The two NSF-funded projects described above can provide a catalyst for the creation of shareable computer security modules. In order to demonstrate this concept, two examples are provided. The first takes an existing example from the SI@T suite of

exercises and demonstrates how coupling the exercise with the RAVE environment will address most of the challenges identified in section 2. The second exercise takes an existing RAVE scenario and builds an associated educational component using the SI@T framework.

4.1 Example 1 – SI@T Modules in the RAVE Environment

The SI@T Project has resulted in a collection of valuable resources in a common framework easily utilized by instructors. While many instructors have an infrastructure in place in which students can conduct these exercises, most institutions suffer from some (if not all) of the environmental challenges listed in section 2. As described in section 3, the exercises consist of four sections. Three of the four sections are self-contained. Combining the hands-on or problem section with the RAVE capabilities alleviates all of the environmental challenges listed in section 2.

After completing the background section, the student is given access to a RAVE environment in which to test the applied component. The nine identified issues are addressed through the configuration of the RAVE environment.

- Issues 1-5 have to do with student resources configuration. In this case, all students are given identical virtualization environments; so system components, platform, operating system, machine resources, and starting configuration are all ensured to be uniform.
- Issue 6, handling non-identical configurations, is no longer an issue since all environments are homogeneous.
- Issue 7 is concerned with student assistance. RAVE provides several capabilities to assist in this area including remote access by instructors, permissions to view and assist student accounts and snapshot capabilities to further interact with students.
- Issue 8 is concerned with changes to the configuration and distributing changes. Since RAVE is a virtualized environment and images are created on demand, this issue is easily solved.
- Issue 9 has to do with student accessibility to the environment to complete the hands-on component. Since RAVE environments are remotely accessible and available around the clock, students are free to complete the exercises within the constraints of the timeline required by the instructor.

Thus, using RAVE as an environment for completing the hands-on component of the SI@T suite of exercises addresses many of the identified challenges associated with hands-on computer security labs.

4.2 Example 2 – RAVE Exercise Using the SI@T Framework

As IA course offerings at colleges and universities have increased dramatically over the last 10 years, many institutions have struggled with the issues identified in section

2.1. In the previous section, we identified how current IA modules from the SI@T benefit from utilizing the infrastructure provided by RAVE. Outside of the fiscal and resource management benefits of leveraging the RAVE virtualization resources center model, the greatest curricular enhancement comes from instructors being able to now more easily share IA lab exercises. An enhancement to provide a more reusable set of exercises is to take existing scenarios developed by faculty and rewrite them adopting the framework discussed in section 3.

As an example of this process, we rewrote a lab exercise (described in [9]) instrumented in a RAVE cluster to follow the SI@T model. The module was originally written to permit other faculty to adopt the module for use in their own institutions. Given the variability in infrastructures, 70% of the module focused on how to set up the hardware and software, rather than the learning objectives. The four sections in the new model broke the content into a format that was more easily followed by students.

The *background* section was mostly present in the existing module, however, adding details that tied the objective to a real world event provided more motivation to the students. The second section, *Problem - Security-Related Lab,* was directly ported over. The third section, *Checklist,* required iterating through the lab exercise, identifying key components that tied to the learning objectives, providing a guided walk through of essential concepts of the security topic. The final section, *Analysis-Discussion questions*, was already present in the original lab exercise.

The process of migrating the original lab construction to the SI@T model resulted in an exercise that provides the advantages listed in section 3, providing a more shareable module that can be accessed virtually anywhere in the world.

5 Future Considerations

The framework for the computer security modules described in the previous section, builds on successful NSF research efforts to provide meaningful, hand-on exercises that address many of the identified environmental and pedagogical challenges. What remains is the identification or creation of a repository environment to facilitate the sharing of the modules on a much wider scale. There are currently several efforts underway that are addressing these challenges and coupling the results of this research effort with successful repository development will be essential to ensure that the research efforts are leveraged to minimize duplication of effort and maximize the sharing of resources. The repository must allow instructors to adapt modules to their own environment and then contribute these newly evolved modules back to the repository for others to use. It needs to be scalable so that the topical areas can expand as the technologies to support other areas are identified and utilized.

While there are several repository efforts underway for IA educators, the repository frameworks are each unique, limiting the ability for instructors to locate exercise labs that support their curriculum and infrastructure. The NSF-funded Ensemble Project [5] may be a candidate for a repository, or at least provide a foundational framework to guide the development of a more specialized framework. The project uses a

distributed portal approach intended to coordinate across communities. A second related NSF-funded project (# 0231122 and 0618680) is SEED: A Suite of Instructional Laboratories for Computer SEcurity EDucation [3] which has a growing suite of complete educational laboratory experiences, provides a wealth of experience in the development and deployment of security education modules, but is also in search of a repository. Likewise, PRISM: A Public Repository for Information Security Material [2], provides a repository framework that should be further evaluated as a repository environment for this framework.

While efforts continue, much work remains to be done in order to reach the ambitious framework goals outlined in this paper.

Acknowledgements. This research has been funded in part by the National Science Foundation through the Division of Undergraduate Education (#1023125) and (#0817267).

References

1. Security Injections @ Towson University, `http://triton.towson.edu/~cssecinj/secinj/`
2. Garramone, V., Schweitzer, D.: PRISM: A Public Repository for Information Security Material. In: Colloquium for Information Systems Security Education (CISSE), Baltimore, MD (2010)
3. Du, W., Wang, R.: SEED: A Suite of Instructional Laboratories for Computer Security Education (Extended Version). The ACM Journal on Educational Resources in Computing (JERIC) 8(1) (March 2008)
4. Taylor, B., Azadegan, S.: Moving Beyond Security Tracks: Integrating Security in CS0 and CS1. In: Technical Symposium on Computer Science Education (SIGCSE), ACM (2008)
5. Hislop, G.W., et al.: Ensemble: creating a national digital library for computing education. In: Proceedings of the 10th ACM Conference on SIG-Information Technology Education, p. 200. ACM, Fairfax (2009)
6. Nance, K., Nestler, V.: Unpublished manuscript (2009)
7. Costello, M.: Fat fingered typing costs a trader's bosses £128m. The Times Online (December 9, 2005)
8. Hay, B., Nance, K.: Evolution of the ASSERT Computer Security Lab. In: 10th Colloquium for Information Systems Security Education, Adelphi, MD (June 2006)
9. Hay, B., Dodge, R., Nance, K.: Using Virtualization to Create and Deploy Computer Security Lab Exercises. In: Jajodia, S., Samarati, P., Cimato, S. (eds.) Proceedings of the 23rd International Information Security Conference (SEC 2008). IFIP, vol. 278, pp. 621–635. Springer, Boston (2008)

Towards a Pervasive Information Assurance Security Educational Model for Information Technology Curricula

Lynn Futcher and Johan Van Niekerk

Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
{Lynn.Futcher,Johan.VanNiekerk}@nmmu.ac.za

Abstract. Information Technology (IT) encompasses all aspects of computing technology. The pervasiveness of IT over the past decade means that information assurance and security (IAS) know-how has become increasingly important for IT professionals worldwide. However, South African universities do not get specific curriculum guidelines to ensure that all essential security-related aspects are included in the IT courses offered. With respect to IAS, these universities are therefore required to self-regulate through measuring against international norms and standards. One such norm for the IT profession is given by the ACM/IEEE-CS in the *'Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programs in Information Technology'* document. This paper examines this norm, together with relevant South African curricula policy document, to establish what information security guidance exists to support IT curriculum developers and educators. In addition, it argues that an integrated educational IAS model can help address IAS as a pervasive theme throughout IT curricula.

Keywords: Information security education, information assurance and security model, IT curriculum.

1 Introduction

Over the past decades, four major organizations in the United States have developed computing curricula guidelines for colleges and universities. These include the Association for Computing Machinery (ACM), the Association for Information Systems (AIS), the Association for Information Technology Professionals (AITP) and the Computer Society of the Institute for Electrical and Electronic Engineers (IEEE-CS).

The School of Information and Communication Technology (ICT) at the Nelson Mandela Metropolitan University (NMMU) is responsible for educating Information Technology (IT) professionals for tomorrow. However, it does not get specific curriculum guidelines to ensure that all essential security-related aspects are included in the IT courses offered. The South African curricula guidelines for IT qualifications [1,2,3,4] dictate the instructional offerings which need to be incorporated at each level

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 164–171, 2013.

of the curricula. However, they do not provide in-depth guidance with respect to recommended content. As a South African university, the NMMU is therefore required to self-regulate through measuring against international norms and standards. One such norm for the computing profession is provided by the ACM/AIS/IEEE-CS Computing Curricula 2005 [5]. More specifically, such a norm for the IT profession is offered by the ACM/IEEE-CS in the '*Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programs in Information Technology*' document [6].

The purpose of this paper is to argue that the ACM/IEEE-CS and the South African Council for Higher Education (CHE) curricula guidelines do not provide sufficient guidance to **ensure** that information security is adequately incorporated within the IT curricula of the School of ICT, NMMU. In addition, it proposes an integrated IAS educational model to help address IAS as a pervasive theme throughout IT curricula.

The following sections discuss these guidelines and the extent to which they support IT curriculum developers and educators at South African universities. This is followed by some critical comments and recommendations in this regard.

2 ACM/IEEE-CS Curriculum Guidelines for Undergraduate Degree Programs in Information Technology

IT is the latest academic discipline covered by the ACM/AIS/IEEE-CS Computing Curricula volumes [5,6]. According to ACM/IEEE-CS, the pillars of IT include programming, networking, human-computer interaction, databases, and web systems. These are built on a foundation of knowledge of the fundamentals of IT. Overarching the entire foundation and pillars are information assurance and security, and professionalism [6].

The ACM/IEEE-CS's '*Information Technology 2008, Ccurriculum Guidelines for Undergraduate Degree Programs in IT*' [6] presents a curriculum for a 4-year study in IT. In so doing, it defines an IT body of knowledge that spans 13 knowledge areas. Information Assurance and Security (IAS) is one of these knowledge areas. These knowledge areas are further divided into smaller units, each of which represents individual themes within the respective areas. At the lowest level of the hierarchy, each unit is subdivided into a set of relevant topics.

IAS as a knowledge area is well defined by the ACM/IEEE-CS [6] curricula guidelines. It is recognised as a very integrative knowledge area and one in which all senior IT students should be involved. ACM/IEEE-CS specifically states that '*every student should be involved with some of the advanced security outcomes*' and that '*every student needs some advanced, integrative experience in IAS* ***in the 4th year'***. As a knowledge area, it is divided into various units including *Fundamental Aspects*, *Security Mechanisms*, *Operational Issues*, *Policy*, *Attacks*, *Security Domains*, *Forensics*, *Information States*, *Security Services*, *Threat Analysis Model* and *Vulnerabilities*. Approximately 7.5% of the total core hours defined for the 4-year curriculum should be allocated to IAS. However, since much of the content listed by IAS as a knowledge area may be regarded as primarily aimed at 4th year level, there is

a concern that some university curricula may only address security-related issues at this level. In addition, at some universities it may be regarded as an elective since it is a specialized field of study.

The ACM/IEEE-CS [6] addresses this concern to a certain extent since various security units and topics are defined within other knowledge areas. In general, the knowledge areas of IT Fundamentals (ITF), Information Assurance and Security (IAS), Information Management (IM), Integrative Programming and Technologies (IPT), Networking (NET), Platform Technologies (PT), System Administration and Maintenance (SA), Social and Professional Issues (SP) and Web Systems and Technologies (WS) all address some aspects of information assurance and security. For example, software security practices lies within the Integrative Programming and Technologies (IPT) knowledge area and a security unit is defined for the Networking (NET) knowledge area. In addition, Vulnerabilities is listed as a unit within the Web Systems and Technologies (WS) knowledge area. However, the knowledge areas of Human Computer Interaction (HCI), Mathematics and Statistics for IT (MS), Programming Fundamentals (PF) and System Integration and Architecture (SIA) contain no security-related aspects.

ACM/IEEE-CS [6] also addresses IAS as a pervasive theme as discussed in the following section.

3 IAS as a Pervasive Theme

In addition to having been defined as a key knowledge area, IAS has also been defined as a pervasive theme. ACM/IEEE-CS [6] describes a pervasive theme as those topics which are '*considered essential, but that did not seem to belong in a single specific knowledge area or unit'*. These themes should therefore be woven into the curriculum by being addressed numerous times and in multiple classes [6]. The pervasive themes of the IT curriculum are described under IT Fundamentals (ITF). The ACM/IEEE-CS [6] states that all the IT pervasive themes be covered by the end of the 4-year curriculum and that they must be addressed frequently from 1st to 4th year. However, although IAS is defined as both a knowledge area and a pervasive theme, at some universities it may be overlooked until the 4th year.

According to the IT body of knowledge, as defined by the ACM/IEEE-CS [6], IT Fundamentals (ITF) should take up approximately 8% of the core hours as indicated in the IT curriculum. Of this 8%, '*Pervasive Themes in IT'* should present approximately 68% which equates to roughly 5.5% of the total core hours defined for the 4-year curriculum. However, no further breakdown is provided as to how much time should be allocated to IAS as a pervasive theme. This means that other topics within the '*Pervasive Themes in IT'* unit may be given preference over IAS. This may lead to an IT graduate leaving university with apparent gaps in their security-related knowledge.

According to the IT curricula guidelines of the ACM/IEEE-CS [6], the IT Fundamentals (ITF) knowledge area is intended to be at the introductory level in a curriculum. The purpose of the ITF knowledge area is to develop fundamental skills

for subsequent courses by providing an overview of the IT discipline and how it relates to other disciplines. In so doing, it should instill an IT mindset that helps IT students understand the diverse contexts in which IT is used [6].

The ITF knowledge area is divided into four units. These units include '*Pervasive Themes in IT*', '*History of IT*', '*IT and its Related and Informing Disciplines'* and '*Application Domains'*. IAS is further listed as a topic within the '*Pervasive Themes in IT*' unit. Linked to IAS as a topic is the core learning outcome which is stated as - '*Explain why the IAS perspective needs to pervade all aspects of IT*'.

Many South African universities use these guidelines provided by ACM/IEEE-CS as an informal reference when creating IT curricula. However, it is the opinion of the authors that these guidelines do not adequately address IAS as a *pervasive* theme and that no further guidance exists to assist IT educators in developing curricula to ensure that IAS is effectively integrated into the curriculum at undergraduate level. In support of this argument, Futcher, Schroder and Von Solms [7] question the extent to which information security is incorporated into the IT/IS/CS curricula at South African universities. They raise the concern that information security is not being addressed adequately at undergraduate level and suggest that information security be defined as a critical cross field outcome (CCFO) in South African curricula guidelines. This implies that security-related aspects be integrated into the IT/IS/CS curricula from the 1st year of study. In line with this, the following section provides a critical evaluation of current South African curricula guidelines [1,2,3,4] against the ACM/IEEE-CS [6] guidelines.

4 A Critical Evaluation of South African Curricula Guidelines Against the ACM/IEEE-CS

The South African Council for Higher Education (CHE) provides guidance to tertiary institutions regarding curriculum composition. This guidance currently resides in documents from the Higher Education Qualifications Framework (HEQF), the South African Qualifications Authority (SAQA) and the National Assembly Training and Education Department (NATED). This section examines the guidance provided by the CHE specific to IT qualifications [1,2,3,4] in order to critically evaluate it against the ACM/IEEE-CS [6] curriculum guidelines. The aim is to identify possible weaknesses and areas for improvement with respect to integrating information security into IT curricula.

The HEQF is a qualifications framework for a single coordinated higher education sector. It applies to all higher education programmes and qualifications offered in South Africa by public and/or private institutions. As such, it replaces previous policy documents including '*A Qualification Structure for Universities in South Africa - NATED Report 116 (99/02)'*, '*General Policy for Technikon Instructional Programmes - NATED Report 150 (97/01)'* and the '*Formal Technikon Instructional Programmes in the RSA - NATED Report 151 (99/01)'*. However, some relevant curricula information still resides in the NATED documents.

The NATED Report 151 specifies instructional offerings for a National Diploma [2] and Bachelor of Technology in Information Technology [1]. Although no specific

security-related offerings are stipulated for the National Diploma [2], Computer Security IV and Information Security IV are specified for the Bachelor of Technology [1] qualification. However, these two offerings are not compulsory in any of the nine specialised IT fields as defined by SAQA [3,4]. These IT fields include Business Applications, Software Development, Communication Networks, Web and Application Development, Information Systems and Technology Management, Intelligent Industrial Systems, Support Services, Technical Applications and Hardware and Computer Architecture.

None of these IT fields have any security-related exit level outcomes nor specific outcomes identified for the SAQA registered National Diploma in IT [4]. For all nine IT fields, the SAQA registered Bachelor of Technology in IT qualification [3] defines a security-related exit level outcome that states that '*the qualifying learner should have the ability to apply advanced techniques in the introduction and control of information security in an IT environment*'. However, this is only stipulated as being core for the Business Applications field and as an elective for the other eight IT fields. Linked to this exit level outcome is the associated assessment criterion '*Evaluate the information security environment and design control measures'*. This poses a major concern with respect to addressing IAS as a pervasive theme within South African IT curricula.

In comparison, the ACM/IEEE-CS's curriculum guidelines [6] offers an excellent baseline from which to develop a 4-year IT curriculum. Specifically, at the 4th year level it recommends the inclusion of IAS as an advanced subject area and it provides very clear guidelines on the topics such an instructional offering should be covering [6]. However, specific guidance on *how to* incorporate security concepts as a pervasive theme during the first three years of study, and as part of the remaining 4th year subjects, is lacking.

This could lead to potential problems at several different levels. Firstly, the structure of the 4-year IT curriculum at the NMMU, and several other similar South African universities, is such that the 4th year of study forms part of an optional, more advanced, qualification [1]. It is thus possible for a student to exit the qualification after the 3rd year of study. Secondly, even for students who do decide to enroll in the optional 4th year qualification, the "Information Security" instructional offering is not considered compulsory in the South African curriculum guidelines, and is thus an elective subject [1]. Students could thus elect to not receive the requisite information security education. This means that the lack of *specific* guidance on how information security-related concepts should be incorporated *as a pervasive theme* into the curricula of subjects during the first three years of study could lead to IT curricula that do not adequately address information security, despite the relative importance assigned to this topic by the ACM/IEEE-CS's [6] curriculum guidelines.

Even though it cannot reasonably be expected from the ACM/IEEE-CS to provide subject specific guidance on these topics, it could be argued that a minimum "standard" for each topic area could be more clearly delineated by the curricula guidelines. Such delineation could possibly be done with the assistance of the information assurance model suggested in the ACM/IEEE-CS guidelines [6], to provide the context for information security knowledge, and the use of a learning taxonomy like Bloom's taxonomy, as suggested by Van Niekerk & Von Solms [8] to provide guidance on the "depth" of topic coverage at a specific year of study.

As an example it could be argued that the topic of "buffer overflow attacks/prevention" should not simply be relegated to form part of an *optional* 4th year subject. Instead it should be integrated into programming subjects throughout the qualification. Thus, with the help of a learning taxonomy, like Bloom's, specific learning objectives could be defined which requires learners at the 1st and 2nd years of study to **remember** and **understand** material relating to this topic, and which requires 3rd year students to be able to **apply** the relevant knowledge.

This integration of the topic into the programming curriculum could also provide security context through the incorporation of the suggested information assurance model. Relevant topics could thus still refer to the underlying information states, security services and/or security countermeasures relevant to the context in which these topics are being taught. Table 1 provides brief examples of sample learning activities for the topic of "buffer overflow attacks/prevention" for the lowest three levels of Bloom's taxonomy only. Similar examples could also be constructed for the remaining levels but were omitted due to space constraints.

Table 1. Abbreviated example of Learning Activities based on Bloom's Taxonomy for Information Security, adapted from Anderson, et al. [9]

Level	*Verb*	*Sample Activities*
Apply	execute	Write error prevention code to ensure that your methods iterating through the given list of stored items cannot overstep the boundaries of this list. (Security Countermeasure)
Understand	discuss	Explain how the integrity of the data in the computer's memory could be negatively affected if your code tries to access an array element outside the boundaries of the current array. (Security Services)
Remember	define	In terms of the underlying memory used/allocated, define what an array of 32 bit integers is. (Information States)

The information assurance model suggested by ACM/IEEE-CS [6] can also be adapted to reflect this incorporation of Bloom's taxonomy into the intended curriculum design process. Such an adaptation is illustrated in Figure 1. This is similar to an earlier adaptation by Maconachy, Schou, Ragsdale & Welch [10], where "Time" was added as a fourth dimension to the model. The addition of a time dimension was not used as "*a causal agent of change, but a confounding change agent*" [10]. This catered for the need to modify other dimensions to cater for new technologies which are introduced over time.

The adaptation depicted in Figure 1 similarly is not a causal agent, but rather serves to illustrate the increasing "depth" of the student learner's mastery of the underlying, pervasive security concepts, in terms of Bloom's taxonomy, as such a student progresses through his/her studies. A student might therefore initially only deal with a specific concept at the "remember" dimension of the cognitive domain but should, over time, progress towards the "create" dimension.

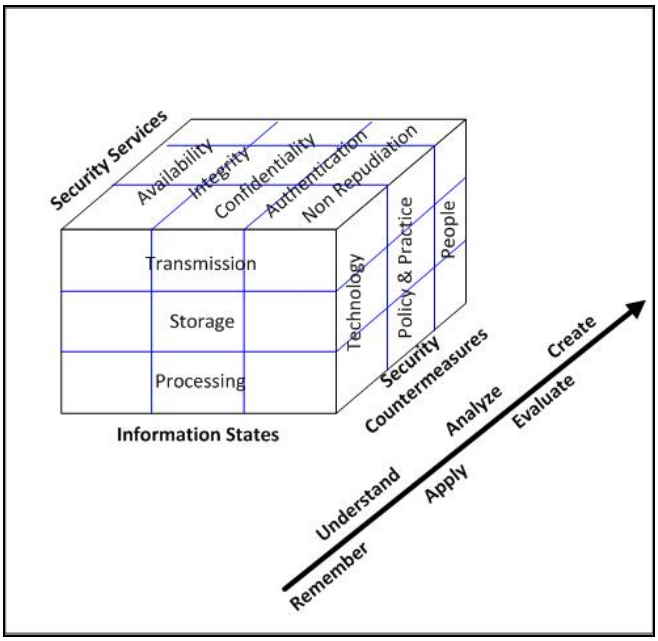


Fig. 1. Model for Pervasive Information Assurance and Security Education (adapted from Maconachy, Schou, Ragsdale, Welch [10])

Weaving many of the IAS concepts into the curriculum provides challenges unique to the IT profession. It is this challenge which this proposed model for pervasive information assurance and security education, as depicted in Figure 1, could help to address.

5 Conclusion

Although the ACM/IEEE-CS advocates IAS both as a knowledge area and as a pervasive theme, there is little guidance provided with respect to assisting IT educators in incorporating information security as a pervasive theme into their various offerings. More guidance should be given by either the ACM/IEEE or at national level with respect to IAS as a pervasive theme. In order to integrate IAS pervasively into IT curricula, it would be sensible to use a learning taxonomy to "phase in" concepts. By utilizing the proposed pervasive information assurance and security model for IT education, curriculum developers and educators can determine the fundamental, core and elective security-related aspects to be incorporated from the 1st to the 4th year of the IT qualification. Whereas fundamental aspects should form the essential basis required for the proposed qualification, core aspects should include the compulsory learning required in situations contextually relevant to the particular instructional offering. Elective aspects should include any additional optional security-related aspects that could enhance the qualification. Incorporation of the

proposed model could benefit the guidelines provided by both the ACM/IEEE-CS and the CHE.

Finally, CHE does not provide detailed subject level guidelines. It is the authors' opinion that IT educators in South Africa could benefit from formally adopting ACM/IEEE-CS guidelines since extensive guidance is provided. However, from a security perspective the authors believe that even more guidance specific to the incorporation of security as a **pervasive** theme is needed. However, future research is required to determine whether security-related aspects are specified within institutional learning programme guidelines.

References

1. South African Council for Higher Education (CHE), Nated Document 151: Baccalaureus Technologiae: Information Technology (2005)
2. South African Council for Higher Education (CHE), Nated Document 151: National Diploma: Information Technology (2005)
3. South African Qualifications Authority (SAQA), Registered Qualification: Bachelor of Technology: Information Technology, (2007), http://regqs.saqa.org.za
4. South African Qualifications Authority (SAQA), Registered Qualification: National Diploma: Information Technology (2007), http://regqs.saqa.org.za
5. ACM, AIS & IEEE-CS, Computing Curricula 2005: The Overview Report (2005)
6. ACM & IEEE-CS, Information Technology 2008: Curriculum Guidelines for Undergraduate Degree Programs in Information Technology (2008)
7. Futcher, L., Schroder, C., Von Solms, R.: Information security education in South Africa. Information Management & Computer Security 18(5), 366–374 (2010)
8. Van Niekerk, J., Von Solms, R.: Using Bloom's taxonomy for information security education. In: Education and Technology for a Better World. 9th IFIP TC 3 World Conference on Computers in Education, WCCE 2009, Bento Goncalves, Brazil (July 2009)
9. Anderson, L., Krathwohl, D., Airasian, P., Cruikshank, K., Mayer, R., Pintrich, P., Raths, J., Wittrock, M.: A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Complete Edition. Longman (2001)
10. Maconachy, W.V., Schou, C.D., Ragsdale, D., Welch, D.: A Model for Information Assurance: An Integrated Approach. In: Proceedings of the 2001 IEEE Workshop on IAS. United States Military Academy, West Point (2001)

Two Approaches to Information Security Doctoral Research

Helen Armstrong

School of Information Systems, Curtin University, GPO Box U1987,
Western Australia, 6845 Australia
h.armstrong@curtin.edu.au

Abstract. Researchers embarking upon doctoral research in information security face numerous challenges at the commencement of their studies. Students often face confusion as they consider where to start and how to progress. The objectives of the research need to be clearly defined before commencing the project. The research questions, methodology, data and analysis are inextricably tied to the objectives, and as such a top-down approach is recommended. This paper discusses two approaches to doctoral research, top-down and bottom-up. The paper is designed to guide students at the commencement of their information security doctoral research. These guidelines may also be of value to the supervisor.

Keywords: information security education, doctoral research.

1 Introduction

Research in the area of information security is moving at a fast pace. The rise in security breaches, which has been a keen driver of research in the field, has the propensity to negatively impact not only an organization's reputation, but also its profitability and overall economic growth, plus the risk of legal action [1]. Unlike the pure sciences, the information security field is young, and PhD researchers do not have the wealth of past research and knowledge available to the sciences. New knowledge in the information security field is constantly being developed and there is a race against time to keep up with the pace of technological progress and methods of abuse [2]. It is essential that a thorough investigation of current research in the area is undertaken to ensure the chosen topic has not been already carried out. As the security field advances it is important to carry out the research quickly in order to remain relevant as well as publish the findings before others. Wise doctoral students will be aware of related research being undertaken by other researchers and this requires constant investigation of the state of the art throughout their research journey. A well-integrated research project in information security will display some essential flows and links in the research process. The thesis should clearly indicate that a coherent piece of research has been completed. Theses that show good integration indicate to examiners that the student understands and has carried out a well-structured research process. As this area is poorly covered in research methods texts generally, this paper

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 172–179, 2013.

presents two approaches to doctoral research in Information security; the top-down approach where the data definition is drawn from the research objectives and research questions, and the bottom-up approach where the research questions are driven from previously collected data. This paper is designed to be of use to students new to research and may also provide a valuable resource for supervisors.

2 Top-Down and Bottom-Up Research Processes

Many who are new to research will not be familiar with the process and expectations involved in doctoral research. As the demand for advanced qualifications in information security grows, more students are seeking out doctoral studies to increase their knowledge in the area and make a significant contribution to theory by carrying out leading edge research. Guidance and good planning is needed in the early stages of doctoral research to ensure a coherent piece of research is completed. Figure 1(a) illustrates how the research progresses using a top-down approach and (b) bottom-up approach.

The top-down approach requires careful consideration and definition of the topic, scope and aims as well as investigating prior research in the field prior to defining the research questions and the desired end product of the research. This ensures that the research has not already been undertaken, and that the proposed research fills a gap in knowledge. This is linked to defining the information security problem to be addressed. The next step in the top-down approach is determining the theoretical and practical contribution to the field; a major area of consideration for examiners later in the doctoral process. The choice of an appropriate research method then guides the data collection, analysis and evaluation of achieving the research goals. This approach gives the researcher clear goals to work towards, a structured plan and a well integrated approach to the project as a whole. The researcher has several phases where the integration of key factors is essential to ensure a coherent piece of research is achieved: The research questions must be driven by the aims and scope and the proposed contribution to the theory and knowledge in the specific security field. The research questions determine the data to be collected and the analysis required to answer the research questions. The evaluation phase determines how well the aims have been achieved, whether the research questions have been answered and if a significant contribution has been made to the field of knowledge.

The bottom-up approach, on the other hand, commences with data that has already been collected and a desire to produce a significant contribution from analysis of that data. The data is then the instrument that dictates the formulation of research questions. An investigation is made of the literature to ascertain what research has been completed in this field to date and whether the proposed research actually addresses a problem and fills a gap, or can be moulded to fit a gap in the body of knowledge. The aims, scope and end product of the actual research can then be determined and the contribution to theory and knowledge defined. Although the bottom-up approach is a commonly applied in doctoral research several difficulties have been identified with this approach, including time-consuming diversions due to

lack of direction, the need to change focus or collect more data if the research has already been undertaken, the end product of the research may not be considered doctoral contribution level, plus there is a risk that the research questions could be flawed or biased. The author's experience in supervision of doctorate research has shown that researchers adopting the bottom-up approach have immense difficulty in producing a coherent, integrated piece of work that has sound theoretical and conceptual foundations. The move from raw data to conceptual thinking is a complex step and such an abstraction is frequently hard to achieve. On the other hand, the top-down approach is a structured guide, providing the researcher with an ordered set of activities designed to aid in the production of logical and sound results. Using a top down approach the first part of planning involves deciding upon a topic, setting the objectives and aims and defining the scope. As a PhD in Information Security requires a substantial contribution to the body of knowledge the topic chosen should be one in which the student already has significant knowledge. It is not sufficient to choose a topic the researcher currently know little about but would like to investigate further, as doctoral enrolment assumes that he or she is already a master in the chosen topic area. The sections that follow describe this approach in more detail.

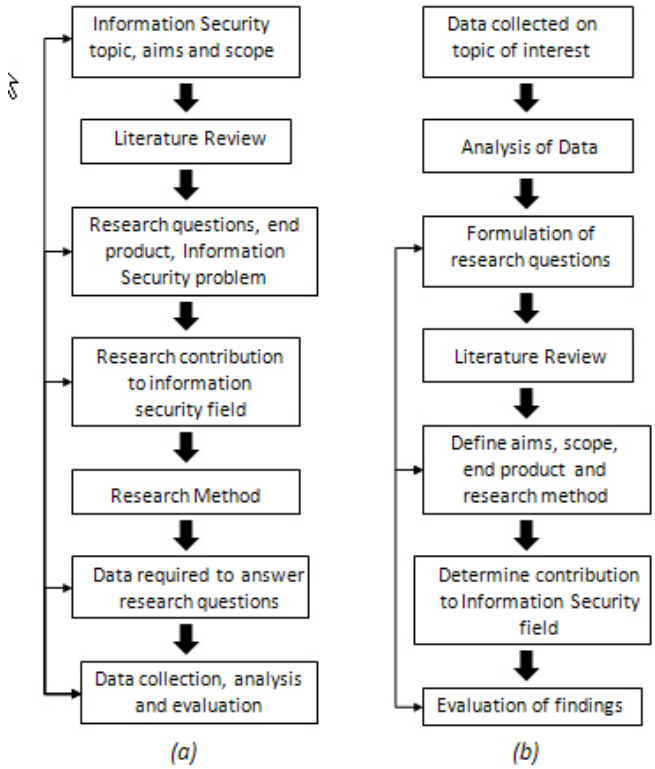


Fig. 1. (a) Top down approach (b) Bottom-up approach

2.1 Research Topic, Aims and Scope

Making a substantial theoretical contribution is difficult if the researcher has no foundation upon which to build. For example, just because you think digital forensics is an interesting area it should not be the focus of your research if you have not studied it as part of a prior degree. A sound knowledge of computer forensics is necessary to be able to discover and formulate new knowledge in the discipline. Passion in the chosen topic area is also desirable. The process of doctoral research can be a lonely place as the researcher moves further into areas not yet studied. Many give up as their topic is not one that drives them to discover more knowledge; there is no passion for the research so the impetus fades. Doctoral students eat, breathe and live their research for 3-4 years so it needs to be one the student enjoys. The topic should also be one the student wishes to carry further once the PhD is complete as the doctorate is akin to verification that they are able to carry out further research. In many cases the PhD is to further employment opportunities, so the research needs to be carried out in a field associated with desired future employment. The main reasons a doctorate is undertaken are to make a significant contribution to knowledge and obtain the qualification that recognizes such a contribution. Other personal motivations also drive a desire to complete doctoral research such as aspiring to make a difference, solve a problem, or gain a qualification to harness employment opportunities. The desire to be recognized as an expert in the chosen security field should not be underestimated, as this often is the driving force that makes a researcher continue when the going gets tough. If a student undertakes the research for someone else (for example, parents, employer, etc.) then the motivation to complete decreases as difficulties arise. Ownership of the research is not to be underrated as the student has more commitment to perform the research if it is something he or she wishes to do, rather than meeting the expectations of others.

The next step is to clearly define the research aims to be achieved. The aims should state the overall achievement sought and then detail outcomes necessary to achieve the general aim. The research needs to generate a result, it is not a process undertaken in order to achieve that result. For example, *investigating* a topic area is not an aim, it is one of the steps in the process the researcher carries out in order to achieve a stated outcome such as the design or development of a tool or method. It is useful to consider the outcome of the research as an end-product or artifact that could be applied to solve a problem. In choosing the topic and aims it is useful to identify the problem domain to which the end-product will contribute. The continual advancement of technology poses many security challenges providing a wealth of opportunities for research. Defining a problem area to address will assist in formulating the aims, research questions and criteria for evaluation of the final product, as well as giving credence and significance to the research. Scoping the research can be a challenge in the early stages where investigation of a selected area is large however; the scope provides boundaries within which to operate. Scoping the research involves identifying areas of importance and interest, deciding those areas to be included in the research and drawing a boundary around them. Clearly delineate those areas excluded and those areas residing on the boundary. As progress of the research brings

clarification of the scope, determine the importance and relevance of those topics sitting on the boundary and decide whether or not each will be included. This will limit the risk of becoming sidetracked and wasting time investigating irrelevant areas.

2.2 Prior Research on Topic

Investigating prior research via a literature review is essential in order to set down what has been achieved in the chosen information security field. Such an investigation also clarifies the progress already made in the area, clearly indicating where gaps exist. This provides evidence of the need for the proposed research. For example, a researcher choosing to investigate the area of wireless network security may discover that there is much written on the vulnerabilities and the development of new standards in the area, however gaps exist in the secure management of wireless communications, thus exposing organizations to eavesdropping, theft of intellectual property and potential attack. It is wise to also investigate the research in the chosen area being conducted at other institutions and in other disciplines to ensure duplication is not a concern. Siponen and Oinas-Kukkonen [3] report that many researchers have a poor awareness of the contributions made by researchers in other disciplines which leads to fragmentation in the information security field; resulting in duplication of research and piecemeal rather than holistic research outcomes. It is helpful to develop a table summarizing the contributions from prior researchers in the chosen security field. This table could contain details of the researchers' names, publication dates, together with a summary of the contribution made and its significance. The sequence of entries in the table should follow either chronologically if the contributions were made over time, or in a sequence that builds a particular line of thought or theory. Once the proposed research is complete the contribution made by the doctoral researcher will be added as to the table, and this will be presented in the findings section of the thesis. This clearly indicates where the current research sits within the specified security field, and the significance of the current contribution. New PhD students need to also be familiar with the academic writing style and the expectations of thesis examiners regarding the language and structure of the thesis.

2.3 Research Problem, Research Questions, Research End Product

All doctoral research must make a contribution to knowledge and in many circumstances, the contribution will relate to addressing a problem or harnessing an opportunity. The problem area needs to be well investigated and defined, and the research aims then linked directly to the identified problem or opportunity. For example, security of the cloud has been noted as a top security issue for CIOs [4,5,6,7]. This security issue needs to be investigated in detail to gain a full understanding of the nature of the problem and the risks that it poses. The outcome will then be directly linked to the problem under consideration. Let's take the example of cloud security: the problem of secure storage of data appears to be the greatest concern so this is the problem we wish to address in some form. The proposed outcome could then be the development of a specific approach or tool to

increase the security of data stored on the cloud. The research questions are developed by looking at the problem domain and asking what questions do I need to answer in order to devise a solution to this problem? An investigative study in a new area may need to commence with research themes from which more definite research questions emerge as the research progresses. The research questions also directly relate to the research end-product or outcome. Theoretical outcomes could take the form of a detailed theory, algorithm, conceptual model or a design whilst a device, an application, a prototype, a methodology or a set of guidelines are possible outcomes for application. The relationship between the problem and the outcome as a solution must be clear.

2.4 Research Contribution

The significance of the research will relate to the problem space or opportunity upon which the research is based. Undertaking the research and producing the end artifacts will result in some change, and the impact of this change needs to be identified. An additional way to approach the significance is to identify what would happen if the research did not take place, what are the impacts, or projected implications of this problem if it were to continue unaddressed. The contribution needs to identify who will benefit from the end product and how they will benefit, who will use it, why and how it will be used. The contribution made by information security researchers can take the form of a theoretical contribution, such as a framework or conceptual model based upon theory and/or a contribution to practice, such as a set of guidelines, a software application or a methodology. Applied research commonly makes a contribution to both theory and practice, as new thoughts and designs are based upon the development of hypotheses. For example, the researcher hypothesizes that the proposed structure, sequence or design will improve a given situation or will provide a valuable result. The significance of the contribution needs to be clearly identified early in the research to ensure an acceptable level of knowledge contribution is achieved.

2.5 Research Methodology

A research methodology is a way to systematically solve a research problem by following a set of steps or processes to produce a defined research product. The major research methods used in information security research are positivism, interpretivism and design science; however other approaches can be used depending upon the research objectives. Positivism utilizes the scientific method to verify a hypothesis by empirical means. It commonly uses large scale surveys for data collection and statistical methods to test the hypotheses. Interpretivist methods assist in understanding the phenomenon of interest within contextual situations, in its natural settings and from the participants' perspectives [8]. Design science aims to produce a design artifact to solve a problem relevant for a group of stakeholders. Design artifacts can include constructs, models, methods, and instantiations [9]. The use of interpretivist and design science methods in information security and information systems research is on the increase with the recognition that social as well as technical

aspects can influence security. Studying phenomenon within their normal operating environments enables a much richer study of factors that influence the security of given settings. Take, for example, the study of information security, behavior and culture as proposed by Da Veiga and Eloff [10] where employee behavior and organizational culture relate directly to information security. It must be borne in mind, however, that interpretive research does not in many cases, enable the findings to be generalized to a global population where the study has concentrated on a localized setting. Siponen and Oinas-Kukkonen [3] conclude that there is a great need for empirical studies on the development of secure IS and security management, proposing that such research embraces empirical theory-creating and testing employing qualitative as well as quantitative methods. PhD candidates need to ensure the research method chosen is appropriate to the type of research being undertaken, the desired end product and the generalizability of the findings.

2.6 Data and Analysis

The data that needs to be collected and analyzed in order to answer the questions and produce the proposed end product is derived from the research questions. This process involves the following steps for each research question:

1. What data do I need to answer the research question? Where will I find that data? Who has control of that data? How is this data held and in what format? What is the most appropriate means of collecting this data? What ethics approval is required to collect his data? How sensitive is this data and will it need to be anonymized?
2. What analysis do I need to carry out in order to transform this raw data into meaningful data in order to answer the research question?
3. How will the research end-product be evaluated in relation to the contribution? What milestones, evaluation criteria and measurement methods are appropriate for this evaluation?

The identification of the data to be collected and its source and nature permits the consideration of the best means of collecting that data and the research method will guide in determining the data collection methods and instruments. For example positivist research results are expected to be repeatable, with significant relationships identified between dependent and independent variables hence surveys, databases, simulations, experiments would be appropriate data collection methods, with the data analyzed by statistical testing. Interpretivist studies often collect data via interviews, observations and case studies. Importantly, the data collected and analyzed must be able to answer the research questions. It is helpful therefore to develop a table summarizing the research questions, the data required to answer each question, how the data will be collected and from whom, and the analysis needed on that data in order to answer the associated research question. This succinct précis is a valuable guide in those frustrating moments when focus is lost or distractions lead the student astray.

3 Conclusion

Looking back on the PhD thesis examination process Mullins and Kiley [11] report poor theses commonly displayed "lack of coherence, lack of understanding of the theory, lack of confidence, researching the wrong problem, mixed or confused theoretical and methodological perspectives, work that is not original, and not being able to explain what had actually been argued in the thesis". PhD researchers need to be conscious of such potential problems early in the process and ensure such characteristics do not manifest in their thesis. A top down approach to research planning is an essential starting point for new PhD researchers. The linking of the research questions, research product, data collection and analysis methods is necessary in order to produce a coherent piece of research that makes a contribution significant at the doctoral level.

References

1. Dlamini, M., Eloff, J., Eloff, M.: Information Security: The moving target. Computers & Security 28, 189–198 (2009)
2. Armstrong, H., Yngström, L.: Resubmit my Information Security Thesis? You must be joking! In: Proceedings of WISE5, June 19-21. West Point Military Academy, New York (2007)
3. Siponen, M., Oinas-Kukkonen, H.: A Review of Information Security Issues and Respective Research Contributions. The Database for Advances in Information Systems 38(1), 60–80 (2007)
4. Binning, D.: Top five cloud computing security issues. Computer Weekly (April 24, 2009), http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm
5. Brodkin, J.: Gartner: Seven cloud-computing security risks. Network World (July 2, 2008), http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853
6. Kandukuri, B.R., Paturi, R., Rakshit, A.: Cloud Security Issues. In: Proceedings of Working IEEE SCC 2009: International Conference on Services Computing (SCC 2009 WIP), Bangalore, India (2009)
7. Salek, N.: Revealed: CISO's top security concerns. IT News (May 31, 2010), http://www.itnews.com.au/News/176434,revealed-cisos-top-security-concerns.aspx
8. Orlikowski, W., Baroudi, J.: Studying Information Technology in Organizations: Research Approaches and Assumptions. Information Systems Research 2(1), 1–8 (1991)
9. March, S., Smith, G.: Design and natural science research on information technology. Decision Support Systems 15, 251–266 (1995)
10. Da Veiga, A., Eloff, J.: A framework and assessment for information security culture. Computers & Security 29, 196–207 (2009)
11. Mullins, G., Kiley, M.: It's a PhD, not a Nobel Prize: how experienced examiners assess research theses. Studies in Higher Education 27(4), 369–386 (2002)

Towards Information Security Education 3.0
A Call for Information Security Educational Ontologies

Johan Van Niekerk and Ryan Goss

Institute for ICT Advancement, Nelson Mandela Metropolitan University
{johan.vanniekerk,ryan.goss}@nmmu.ac.za

Abstract. The need for information security "know-how" has permeated to all aspects of modern society. Nowadays, information security is no longer a problem faced by organizational users alone. Individuals often use online services in cyberspace on a daily basis for activities ranging from personal banking to social networking. The need to educate users regarding secure behavior in cyberspace has subsequently also become well established. This paper firstly argues that approaches towards such "cyber-security" education should be based on the same Web 2.0 philosophies and paradigms that made the use of the Web in daily life so popular. Finally the paper briefly discusses the need for future research to enable such an approach towards information security education.

1 Introduction

The advent of the Internet has brought many advantages to humanity. For the first time in history humans are able to communicate and collaborate in almost real-time, with ease, virtually irrespective of national borders and/or time zones. In recent years information technology has become such an intrinsic part of modern business that some authors no longer see the use of information technology as a strategic benefit. Instead, it can be argued that information technology is a basic commodity, similar to electricity, and that the lack of this commodity makes it impossible to conduct business [1].

However, the benefits of information technology and the Internet do not only apply to organizations. Increasingly, the Internet is being used as a tool for personal business, entertainment, communication, and many other activities by individuals at home. Online activities are also not restricted to only the rich, or the educated, or any other specific demographical grouping. According to the World Bank (2010) 8.6% of all South Africans was Internet users in 2008. Amongst urban South Africans this figure is substantially higher. Kreutzer [2] found that 83% of low-income black South African youth in an urban township uses the Internet via mobile phone technology on a typical day. Even amongst school children the use of online technologies and/or platforms has become almost ubiquitous due to the low cost of access using platforms like, e.g. MXit. It can be argued that the Internet, in one form or other, today is being used by all demographic groups, including the young and old, rich and poor, educated and uneducated, urban and rural.

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 180–187, 2013.

Unfortunately, the Internet has not only brought advantages. It has also brought numerous new risks. In an organizational context, typically these risks can be mitigated through the use of various information security controls. For organizations these controls are usually selected with the aid of internationally accepted standards such as ISO/IEC 27002 and ISO/IECTR 13335-1. These information security controls, to a large extent, depends on the actions of organizational users in order to work correctly. Humans, at various levels in the organization, play a vital role in the processes that secure organizational information resources. Many of the problems experienced in information security can be directly contributed to the humans involved in the process. Employees, either intentionally or through negligence, often due to a lack of knowledge, can be seen as the greatest threat to information security [3, p. 3]. Organizations typically address this lack of information security related knowledge through formal information security awareness and educational programs. Many current research publications focus on organizational information security education and many companies specialize in providing such education as a service. Unfortunately, almost no-one currently provides equivalent information security education for individuals using the Internet in their personal capacities.

The need for information security education outside the corporate environment has become widely recognized. Furnell [4] likens the Internet to a jungle, with uneducated users falling "prey" to online "predators". Siponen [5] identifies the need for five "dimensions" of information security awareness education, one of which is the "general public" dimension. Siponen [5] also argues that society as a whole has an ethical responsibility to ensure that its vulnerable groups receive appropriate information security education. As an example; South Africans in general have a well-developed culture of personal security. Most South Africans are used to assessing the risks posed by "normal" day-to-day activities and also know how to mitigate such risks, e.g. through locking the doors at night, avoiding walking through dark alleys, not leaving personal possessions unattended, etc. However, due to the relative newness of Internet access for many citizens a *culture of cyber-security* is still lacking.

Many South Africans, especially from vulnerable groups, such as the elderly, are completely unaware of even the existence of many risks during "normal" online activities and thus can easily fall prey to online "predators". During 2010 alone approximately 4400 cases of identity theft, involving losses of more than R200 million, have been reported to the SAFPS (www.safps.org.za). As the so called "digital divide" is reduced, progressively more South Africans will be put at risk of having their identities stolen. The only way to effectively mitigate this, and other risks posed by Internet access, is through increased awareness of the risks posed by this medium, and education regarding how these risks can be mitigated.

There is a need for information security education for all "cyber-citizens". Furthermore, due to the diverse backgrounds, educational levels and many other factors of the various vulnerable groups, a "one size fits all" approach to such education cannot work. It can thus be argued that information security educational programs would have to be tailored to the specific needs of each target

user group in order for such programs to be effective. The aim of this paper is to argue that there is a need for a freely accessible "cyber-security portal" through which any Web user can access relevant information security educational programs. Furthermore, the paper briefly explores the idea of basing such a portal on a Web 2.0, and hence E-learning 2.0, paradigm and then presents a call for further research towards such educational approaches.

2 Why E-learning 2.0?

The rapid advancement, and global acceptance, of the Internet and World Wide Web has left modern society in general somewhat unprepared for the digital economy we now live, and work, in. In the past the general spread and use of major technological advancements happened at a pace that still allowed society to gradually develop ways of dealing with it. The widespread use of the automobile, for example, happened over more than one generation. This allowed people time to develop ways and means of acting safely in and around cars. This behavior was then passed from one generation to the next allowing the development of a "culture" where all members of society are aware of the dangers motorized vehicles could pose to their personal safety. The rate at which use of the Web penetrated society did not allow the formation of such a "culture". Not only are we still in the first generation of web-users, but the technology used is still changing rapidly.

One of the best examples of the rapid acceptance of new technology in modern society is the recent advent of social networking and other Web 2.0 phenomena. The participatory, collaborative, and dynamic online approach of Web 2.0 is arguably where most serious efforts at Web-based development are currently heading; therefore, it follows that online learning communities would naturally transform to use a similar approach [6]. By following the trends of Internet users, these new learning environments prepare the learner for operating in the real world. While it is true that some aspects and characteristics of the current educational system will most likely prove resilient as the preferred method for learning certain topics [6], it is very likely that Web 2.0 trends will penetrate more of the educational system than one can now imagine.

Web 2.0 provides the learning environment with the tools necessary to enable learners to build their own knowledge constructs and not conform to the generic constructs of information that, for example, traditional education imposes on them. By allowing learners to construct their own knowledge and storing it in a way that is most efficient and effective for their own learning style, educators ensure the best possible outcome to the learning experience. The combination of Web 2.0 and e-Learning methodologies brings forth a new breed of e-Learning systems, known as e-Learning 2.0.

E-Learning has been suggested as a tool which could make education and lifelong learning more effective and efficient. The content driving such systems, however, is often static in nature and many of the e-Learning systems fail in that they simply imitate previous educational paradigms [7]. This is also true

of many IT-based fields as IT itself changes so rapidly with new technological advancements being introduced on a nearly daily basis. Growth of social software on the Internet and the **movement towards open educational content** has had researchers rethink previous models of e-Learning. The term "E-Learning 2.0" was coined in 2005 to describe e-Learning systems, built on social networking software (Web 2.0) and published online [8]. This e-Learning system is a new style of learning deeply rooted within the social constructivist paradigm [9], described as a revolution, converting the Web as a medium, as it is widely known and accepted, into a platform for delivery of data [8].**Content is no longer only delivered to learners, but also authored by learners**. Web 2.0 in the educational environment is considered by several authors as progressive and the driver of educational change which offers new perspectives and challenges to education at all levels.

Some of the features which make Web 2.0 so favourable to the educational sector are its **ease of publication**, **sharing of ideas** and **re-use of study content**. Commentaries and links to relevant resources in information environments that are managed by the teachers and learners themselves also make Web 2.0 favourable in the eyes of educators [7]. The idea of allowing learners the ability to manage and contribute to their learning environment is in contrast to previous education systems, where developers of the system employed creators of study content, who were tasked with building a generic knowledge base from which learners were educated. Forcing all learners to learn in the same way from such a knowledge store is not necessarily the most effective learning approach. It could be argued that Web 2.0 based systems might have more success. Previous information security education systems relied heavily on the use of formal learning techniques, whereas Web 2.0 based tools would allow learners to branch out and explore "informal" learning.

80% to 90% of all learning has been attributed to learning occurring informally outside of the classroom [10]. Informal explanations dominate over formal mathematical proofs and examples of computer applications security were found to be especially well received by learners in information security education [11]. Informal learning design is nothing new, but is something e-Learning designers have previously ignored [10]. The statistics themselves should be enough to force e-Learning design practises to incorporate more informal learning techniques [10]; however, nothing significant has to date been done about it. The possibility of implementing such a system for information security education should thus be investigated in order to ascertain its usefulness in educating all users of computer systems, world-wide.

As argued earlier, the use of computer systems has expanded from typically adults within an organization to include people from all walks of life. It has therefore become necessary for information security education to evolve beyond organizational information security towards **cyber-security education** targeting all of these would-be victims. It can be argued that E-Learning 2.0 systems are ideally suited to this task, as they are built on the Web as a platform, and uses technologies already reaching these would-be learners during other activities. Furthermore,

e-Learning 2.0 systems allow the user to act as both a consumer and a producer, allowing them to "Rip, Mix and Feed" [10]. This process allows for the education content created to be authored by many individuals, instead of being tasked to a single person or team. This means that the creation of the information security education content base becomes a community endevour, *which requires various rating systems to be implemented in order to decern the credibility of the authors and the works which are produced as a result of such a community endevour.* By allowing learners to not only draw from, but also contribute to the content base, the learner is assured a sense of ownership for the content they produced. Providing a sense of ownership creates an appetite for further learning, the learners within a system are thus **motivated** to continue their education and further themselves. This motivation stems from the system actively engaging the learner in the learning process, by requiring them to integrate and maintain the social software tools which allow the learning to happen [12].

The advantages of e-Learning 2.0 systems are extensive and elaborate, allowing these systems to fast become viable options for replacing many of the traditional learning systems in production today. It is thus the assertion of this paper that the use of E-learning 2.0 for "cyber-security education" could be the ideal way to address the growing need to educate learners from all walks of life, enabling them to be "safe" whilst online. Unfortunately, the advantages offered by such "revolutionary" education technology are also accompanied by certain challenges which could hamper the development and success of such systems. The most notable of these challenges will be briefly examined in the next section.

3 Problems with Learner-Generated Learning Material

The promotion of learner-assisted content publishing and creation allows an abundance of information on a number of cyber-security related topics to be generated. The generation of such volumes of information produces yet another potential problem. Firstly, instead of a *lack* of sufficient information security content, learners could potentially suffer from *information overload* [13]. One of the problems with traditional e-Learning systems was that it took a long time and a lot of financing in order to build a suitable knowledge base from which to educate learners. Developers of the coursework of information security education systems are typically experts in the field developing content as part of their jobs. E-Learning 2.0 allows the learners themselves to contribute and build up the learning material, building a system based on "folksonomy" or user-generated taxonomy. Although this can provide many advantages, it also gives rise to the potential for **information overload**. If learners are not limited to the scope of a contribution, certain information security topics may have a large amount of content associated with them, so when a learner searches for a particular topic, too much information is returned and the learner is unable to manage and sift through it to find specifics [13]. Secondly, in order to ensure wide acceptance of learner generated content, a mechanism to ensure the validity

of such content would be needed. The integrity of the information available at sources such as wikipedia is often questioned precisely because of the lack of such mechanisms. Critics of learner-created content in general express concerns about trust, reliability and believability of such content [14].

Any proposed system must allow the large amount of information posted to be managed in an effective way, so that learner searches are optimized and only information pertinent to a specific search are returned. This is currently still difficult to accomplish on e-Learning 2.0 systems, as each typically provides its own proprietary knowledge storage facility, each differing in design from other such applications. This means that for one system to share content with another system, it would need to provide an API to its knowledge store and the receiving application would need to write specific code in order to interact with this API. This type of code would need to be written for all remote knowledge stores that the receiving application wishes to interact with, severely limiting the scope of applications which can interact with one another. One possible solution to this problem that is currently being developed and is fast gaining momentum as the next wave in the evolution of the Web, is the Semantic Web.

4 Towards Information Security Education 3.0

Web 2.0 opened the Web and allowed contribution of information by the average computer user. This contribution facility, although solving the problem of content generation, introduced further problems which needed to be addressed in order to ensure the continued success of the Web and facilitate its large growth. One of the problems with allowing contribution from many sources, is that of information overload. The information posted is generally stored in a format suitable only to human readers, making it very difficult for machine users (or applications) to understand and draw inference from it. This meant that machine users and applications are unable to understand information security concepts and the contributions learners make on the system. **Although information security education concepts would be *machine readable*, they would not necessarily be *machine understandable*** [15]. In order to facilitate searches which filtered through all of this information accurately and effectively, preventing information overload to the users of the system, machine users need to be able to parse the information and have an understanding of its contents.

The Semantic Web can be thought of as a large relational database, joining tagged items and incorporating all topics and concepts, from book chapters to cell phones to the price of laptop computers [13]. By joining these topics in a way which computer applications can understand, the Semantic Web allows information generated by learners on an information security education system to be transformed from a "display only" form, only parsable by humans or software agents written specifically for the task, to a vast database of knowledge, which **computer applications can parse and understand** [13]. This knowledge **allows computers to more accurately search for specific criteria within the information security education system content base** and do much

of the grunt work in information processing and filtering for searches performed by human users of the system. The Semantic Web further allows users to find relationships between tagged items, such as related information security topics [13]. This process is possible due to the Semantic Web's ability to use inference rules and data organizational tools known as "ontologies", which are domain theories, enabling a Web that provides a qualitatively new level of service [13] [15].

An ontology, according to Gruber 2003 is a formal and explicit specification of a shared conceptualization [16]. Formal, meaning it should be represented in a formal representation language and shared, indicating that the ontology describes knowledge accepted by a community [16]. A primary goal of ontologies is to facilitate knowledge sharing and reuse, providing a common understanding of various content that reaches across people and applications on the Semantic Web [15]. The only way learning systems on the Web which share domain and pedagogical knowledge amongst themselves will work is if a large number of ontologies surrounding these systems exist [15]. Currently, this is not the case as there are few domain ontologies in existence and even fewer which cover instructional design and learning theories [15]. For this reason, the learning community in general, and in this case the information security educational community specifically, needs to come together and develop the standard ontologies in a collaborative way, much like the contributions to a wiki, where all users input is valued, condensed and refined by the community working toward a common goal.

One of the main reasons for the lack of such standardized ontologies for learning is the apparent lack of standard vocabulary in the domain of education and instructional design [15]. Many standards groups are in the process of addressing these and other issues. However, no current group are dedicated to the creation of information security educational ontologies.

5 Conclusion

There is a need for information security education beyond the confines of modern organizations. Individuals from all walks of life are using the Internet as a tool for personal business, entertainment, communication, and many other activities. These individuals need to be educated in order to help protect them from the dangers posed by engaging in such activities online. Such education should be in a form that encourage people to engage in it on a voluntary basis. One possibility to explore is the leveraging of the Web 2.0 philosophy in order to engage such learners in the participatory creation of learning content. The idea of such an e-learning 2.0 approach has been suggested by several educational researchers but its effectiveness has yet to be proved. However, before such an approach could become a reality subject specific ontologies for the intended subject matter would be needed. The authors of this paper wish to call on the fraternity of information security education researchers to start exploring the possibilities offered by Web 2.0, e-learning 2.0 and Semantic Web technologies. Furthermore

this paper wishes to call on these, and future, researchers to collaborate, and contribute, towards the needed shared information security educational ontologies needed to make Information Security Education 3.0 a reality. It is thus not the intention of this paper to present completed research, but rather to serve as a catalyst for future research.

References

[1] Carr, N.G.: IT Doesn't Matter. Harvard Business Review, 41–49 (2003)
[2] Kreutzer, T.: Internet and online media usage on mobile phones among low-income urban youth in cape town. In: Beyond Voice? Pre-Conference Workshop at the International Communication Association (ICA) Conference Chicago, Illinois, May 20-21 (2009)
[3] Mitnick, K., Simon, W.: The art of deception: Controlling the human element of security. Wiley Publishing (2002)
[4] Furnell, S.: It's a jungle out there: Predators, prey and protection in the online wilderness. Computer Fraud & Security, 3–6 (October 2008)
[5] Siponen, M.: Five dimensions of information security awareness. Computers and Society, 24–29 (June 2001)
[6] Rogers, P., Liddle, S., Chan, P., Doxey, A., Isom, B.: Teaching social software with social software. Turkish Online Journal of Distance Education 8(3) (2007) ISSN 1302-6488
[7] Geser, G.: Open educational practices and resources. [WWW document] (2007), http://www.olcos.org/ (sited September 27, 2008)
[8] Downes, S.: E-learning 2.0. [WWW document] (2005), http://www.elearnmag.org/subpage.cfm?section=articles&article=29-1 (sited May 25, 2008)
[9] Servitium: Web and learning 2.0: A servitium whitepaper. Servitium White Paper (2008)
[10] Schlenker, B.: What is e-learning 2.0? Learning Solutions. Practical Applications of Technology for Learning, e-Magazine (2008)
[11] Yurcik, W., Doss, D.: Different approaches in the teaching of information systems security. In: Information Systems Education Conference (ISECON), Cincinnati, OH (2001)
[12] Mejias, U.: Teaching social software with social software. Innovate: Journal of Online Education 2(5) (2008)
[13] Ohler, J.: Web 3.0 - the semantic web cometh. University of Alaska (2008)
[14] Mason, R., Rennie, F.: Using web 2.0 for learning in the community. Internet and Higher Education 10, 196–203 (2007)
[15] Devedzic, V.: Education and the semantic web. International Journal of Artificial Intelligence in Education 14, 39–65 (2004)
[16] Gladun, A., Rogushina, J., Garcia-Sanchez, F., Martinez-Bejar, R., Fernandez-Breis, J.: An application of intelligent techniques and semantic web technologies in e-learning environments. Expert Systems with Applications 36, 1922–1931 (2009)

The Use of Second Life® to Teach Physical Security across Different Teaching Modes

Vincent Nestler[1], Erik L. Moore[2], Kai-Yi Clark Huang[3], and Devshikha Bose[4]

[1] Department of Educational Leadership & Instructional Design,
Idaho State University, South 8th Ave., Pocatello, ID 83209, USA
nestvinc@isu.edu
[2] Associate Dean, College of Engineering and Information Sciences,
Devry University, 1870 West 122nd Avenue, Westminster, Colorado 80234 USA
emoore@devry.edu
[3] Department of Educational Leadership & Instructional Design, Idaho State University,
South 8th Ave., Pocatello, ID 83209, USA
huanyung@isu.edu
[4] Department of Educational Leadership & Instructional Design, Idaho State University,
South 8th Ave., Pocatello, ID 83209, USA
bosedevs@isu.edu

Abstract. Teaching physical security can be difficult since classes generally do not have access to physical structures to assess. The purpose of this study was to investigate a new way of teaching physical security using Second Life® and to see if there is a difference in performance related to mode of instruction. The research question sought to determine whether there was a significant difference in student performance based on differences in modes of instruction for students evaluating physical security in virtual world environments. Three groups of participants situated in three geographic locations in the United States and belonging to three different modes of instruction – traditional, online, and hybrid were taught using Second Life®. The results were inconclusive in determining the best mode of instruction. However, the research suggested that Second Life® can be used as a teaching platform to teach physical security.

Keywords: Second Life®, Virtual Reality, Simulation, Physical Security, Avatar, Virtual Learning.

1 Introduction

Simulation is a situation where physical models, computer programs, or a combination of both offers the opportunity to gain experience and assess skills through repeated practice within a safe environment [1]. This study tested the potential for using virtual world technologies for teaching physical security in a variety of learning contexts: online, classroom, and hybrid. Students use avatars and role-play as physical security auditors in a datacenter that is rife with problems and then after a debriefing session, proceed to a second datacenter empowered with more information. The study focuses on comparing student responses to the first and second

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 188–195, 2013.

scenario to determine if this learning method can create significant improvement in response. This study was not able to reach any additional meaningful determination of which contextual mode of instruction better supported simulation-based learning.

2 The Use of Simulation in Teaching and Learning

Teaching and learning through the use of simulation can be especially effective in high risk areas like aviation and medical or surgical training. An important challenge for surgical training lies in providing conditions for effective learning without endangering the patient's life [1]. There are several advantages to using simulation in a field like surgical training. The training program can be determined based on the needs of the learner rather than the patient where learners can focus on complete procedures or particular parts depending on their needs. They can practice as often as required to meet their educational objective because a simulation environment when compared to a real life situation is a safe environment. Simulators provide excellent opportunities for formative and summative evaluation of learning through their built-in tracking and usage recording devices. Moreover, the ability of most simulators of providing immediate feedback has the potential to facilitate individual and collaborative learning.

Educational simulations share key characteristics with games including the common use of a virtual environment and the focus on a particular goal [2]. However, simulations additionally include strategies to guide participants to develop particular behaviors and competencies which may be highly desirable in the intended professional activities. In this research, the use of virtual world technology to teach physical security builds on both of these elements.

A virtual world of teaching-learning appears to be the ideal bridge between the innate interactivity afforded by online courses and the intense absorption offered by immersive role-playing video games [3]. Virtual worlds can act as digital learning objects and can provide an arena for constructivist learning. It can facilitate more student engagement than is possible through simple discussion boards in most online courses. The primary difference between games and the Second Life® Grid used in this study is that the latter is just the platform for creating objects in a space; the educator needs to develop the scenario, plot, motivations, and interactions that engage students with game-like narrative, context, and content characteristics.

A 2009 case study report published on the Linden Lab website mentions how the Customs and Immigration students at Loyalist College used Second Life® to experience the daily routine of their future job [4]. Worldwide terrorism related security issues have made it difficult for the students to get access to sensitive real life locations. The virtual border crossing simulation facility in this project replaced real life geographic border crossing experiences for the students. There was a significant improvement in grades on the students' critical skills test, raising the scores from a 56% success rate in 2007 to a 95 % success rate in 2008 after the simulation program was used.

A central issue of concern amongst those who use simulators for professional training is whether the skills learnt in an artificial environment can be translated into real life situations [1]. A study conducted to demonstrate the effectiveness of virtual reality training in the transference of technical skills to the operating room environment demonstrated that while there was no difference in the baseline assessment scores between the control and the experimental groups, the latter group which had received Virtual Reality based training as a component of their preparation, were able to perform a gall bladder dissection 29% faster than those who did not receive training. Those who did not receive training were found to be 9 times more likely to make less progress and five times more likely to injure the gall bladder. Hence, it was seen that Virtual Reality surgical simulation training significantly improved the performance of the operation room performance of surgical residents.

Dental education has been using simulation since the 1990's for training and development of psychomotor skills [5]. Activities within Second Life® can provide a way to combine new simulation technologies with role-plays which can be used to enhance instruction in diagnosis and treatment planning. Case-studies and role plays have been used as effective evaluation mechanisms to foster decision making and to learn problem-solving strategies. Synchronous distance communication made possible through Second Life® can result in resource sharing and collaboration, thus promoting the globalization of dental education .

3 Purpose and Research Design

The purpose of this study was to investigate the effectiveness of teaching physical security using virtual world scenarios. Particularly, the study objective was to determine any difference in learning performance in relation to accompanying modes of instruction.

The following research question was the focus of this project: Is there a significant difference in student performance based on differences in accompanying modes of instruction for students evaluating physical security in a virtual world?

A quasi-experimental research design was used for this study because the research participants were not randomly assigned to the experimental groups [6]. It was not a true experiment because the researchers did not have complete control over all experimental conditions. The three group pretest-posttest design used in this study can be graphically represented as follows:

Group(s)	*Pretest*	*Treatment*	*Posttest*
A	O_1	X	O_2
B	O_3	X	O_4
C	O_5	X	O_6

Fig. 1. The Three Group Pretest-Posttest Design

The experimental group (A, B & C) participants were asked to visit the Second Life® website and to download the program. They created an avatar and spent an hour in the Help Island going through the tutorial. In class, they were given a scenario and a building to evaluate for physical security issues. The objective of this physical security evaluation exercise was to find the maximum number of security flaws within the environment. They had to complete the task within one hour. The scores in this session were treated as the pretest scores for this study. After this the students participated in an hour long debrief session where they shared their experiences. The objective of this debriefing session was to share their individual findings as well as to learn from each other's findings. In the next session, the students were assigned a different building with similar physical security challenges but in a different layout. The objective of this exercise was for the students to find as many security flaws as possible within the virtual buildings. They completed this assignment as an asynchronous homework assignment, limited to one hour again, to be completed within the next one to two weeks. This homework assignment was treated as the posttest for this study.

4 Assumptions, Limitations, and Delimitations

It was assumed that the participants in this study already have basic computer skills. These skills should include activities like accessing the internet, as well as knowledge of how to download and access Second Life®. It was assumed that the participants will answer the pre and post test questions honestly and to the best of their ability. It was also assumed that the participants will be interested to participate and complete the project.

The researchers had to work with intact classes in order to comply with research site requirements. Hence, it was not possible to randomly assign the participants into the experimental groups. Also, instructional differences may have occurred as a result of difference in the quality and content of the debriefing sessions at the three different sites.

The study sample consisted of three groups of students participating in three different mediums of instruction - traditional face-to-face, completely online, and hybrid (with face-to-face as well as online course components). The researchers had no control over the prior knowledge, skill, and backgrounds of the students in the experimental groups. Depending on individual circumstances, some participants may have had more or less background knowledge and skills.

This study being quasi-experimental, its participants were not randomly selected. Hence, its findings may not be generalizable to all students. The pre and post tests were developed by the researchers and may not be reliable and valid.

5 Significance of Study

Physical security auditing takes a special kind of perspective. The physical security auditor tries to find and correct the risks and flaws of an organization's physical

facility, before any untoward event happens. To do this work effectively, auditors must develop the skill of walking through a place and seeing what is dangerous, what is misplaced, and what things are missing. Some auditors get this by experience working with others, but these are rare opportunities. Picking it up from books is hard because it is hard to get a sense for "casing a scene."

Teaching physical security in any setting can be a tricky thing to do, especially if one wishes to allow the students to have a meaningful "hands-on" experience. Physical security is one of the most important aspects of the overall security posture of an organization. A well configured firewall and locked down workstations are insufficient protectors when someone can easily access the network from the inside and simply pull cables or attach key loggers. While there are many concepts that can be discussed in a course on physical security, developing a spatial appreciation for physical security in a three dimensional space should be enhanced by actually inspecting a structure.

Finding a "classic case" is not an easy thing to do in the real world. First, it may not be possible to find a single building that contains all the attributes and feature one would like ot discuss. This is especially true if what one would like the student to see is a building constructed with serious security flaws. Even if one did find a building with all the teaching points, and even if the building owner/manager didn't mind exposing vulnerabilities through an educational audit of the space, (semester after semester), it may be an impractical idea to accommodate the entire class physically into the premises under consideration. Or the weaknesses might be remediated.

The researchers developed a scene with virtual buildings on which students can perform physical security audits. Students were given a scenario that required them to identify the features of the building that presented security issues. This included items such as, blind spots in surveillance camera coverage, poor lighting, inappropriate fire suppression equipment, and poor access controls.

The project is in the Second Life® Grid, so that it is both accessible to the students remotely on their schedule and also has the power to host large events "in-world". If people would like to see the facility they can download the Second Life® browser. Initially the facility was on Science Island III, just north of the National Public Radio Science Friday radio show set in Second Life®. Currently it is hosted on 3D Learning Island by the MASIE Center. Please contact the researchers to obtain appropriate permissions to enter the space.

6 Participants and Procedures

The total number of participants in this study was 43 (N= 43). The participating groups were located in three geographically disparate parts of the United States – Idaho (Idaho State University), Maryland (Capitol College), and Colorado (Regis University). The hybrid classroom group at Idaho had 17 students, the completely online group at Maryland had 19 students, and the traditional group at Colorado had 7 students. Ten participants from the Maryland group did not submit their posttests.

Pretest and posttest data were collected from each group. The results were subjected to a descriptive procedure which is used to depict the commonly-used statistics that summarize key properties of distributions of quantitative variables [6]. Due to the huge difference among the number of students in the three groups, a one-way ANOVA was not used in this case. Here the "score difference" refers to the score differences between the pretest scores and the posttest scores. The dependent variable is defined as the posttest score minus the pretest score.

7 Instrument Development, Reliability, and Treatment

In order to answer the research question for this study, the researchers constructed two scenarios for use during the pre and posttest situations. They further made a list of security issues in a template format using Microsoft Word. They derived the security issues from security examinations and government documents. The document template contained 30 items. The items were not weighted according to their difficulty index. The students were required to identify the physical security issues they observed in the areas they visited within Second Life® and fill in the template based on their observation.

One of the researchers developed pre and post tests based on each of the scenarios. However, the testing instrument was not formally analyzed to determine reliability.

The treatment was a period of instructional debriefing and discussion of the students' findings on the pretest and was administered prior to the posttest.

8 Results

The sample sizes were unequal. Group 1 (a hybrid classroom of 17 students), group 2 (a traditional classroom of 7 students), and group 3 (an online classroom of 9 students). The posttest score data was collected after the treatment/instructional debriefing session.

Minimum, maximum, means, and standard deviations of the dependent variable, the differences between the pretest scores and the posttest scores, are shown in Table 1. Of the 33 samples collected, the total score difference (n = 33) averaged to be 13.82 (*SD* = 16.46), the mean of score difference in the posttest (*M* = 49.70) is higher than the mean of score difference in the pretest (*M* = 35.88).

Table 1. Descriptive Statistics of the security flaw numbers for all samples

Item	*N*	*Minimum*	*Maximum*	*Mean*	*Standard Deviation*
Pretest	33	8.00	77.00	35.88	15.84
Posttest	33	14.00	98.00	49.70	18.52
Difference	33	-19.00	50.00	13.82	16.46

Comparing Table 2 to Table 1, it was found that the mean score difference of the hybrid group (M = 21.00) is higher than the total mean score difference (M = 13.82). In contrast to the hybrid group, the mean score differences of the other two groups, the traditional group (M = 9.43) and the online group (M = 3.67) were lower than the total mean score difference.

Table 2. Descriptive statistics of the security flaw number differences for the three groups

Classroom Conditions	N	Minimum	Maximum	Median	Mean	Standard Deviation
Hybrid	17	-4	50	15.00	21.00	17.91
Traditional	7	-7	24	13.00	9.43	11.27
Online	9	-19	17	6.00	3.67	10.21

Table 3 shows the percentage of students in each classroom condition that made progress after the treatment/instruction. There were 94.12% students in the hybrid group, 85.71% in the traditional group, and 77.78% in the online group who made progress.

Table 3. The student performance improvement rate for the three groups

Classroom Condition	***N***	***Positive Difference Number***	***Percentage***	***Negative Difference Number***	***Percentage***
Hybrid	17	16	94.12%	1	5.88%
Traditional	7	6	85.71%	1	14.29%
Online	9	7	77.78%	2	22.22%

9 Discussion

The original intent of the researchers was to identify whether there was an improvement in student performance based on the related instructional mode. However, the results of this study were inconclusive in determining any difference between the modes of instruction. This research might have yielded more representative results with better control measures on the online group and if there was a larger sample in the traditional group.

The data from the research also revealed that the participants were able to identify more physical security flaws within the Second Life® environment than were consciously built in by the creators of the environment. Some of these were related to artifacts of the modeling process. Never the less, this encourages the researchers' belief that a 3-D interactive environment has the potential to provide a learning environment that allows the opportunity for students to make a comprehensive and open-ended evaluation of scenarios. The Second Life® environment allows for a greater amount of learning to take place than what was represented in the intended

text-based outcomes. The performance of most students improved irrespective of the mode of instruction used. The data showed that 87.88 % of the students improved in their posttest performance.

10 Conclusions and Suggested Further Research

This study suggests that it is difficult to isolate the many factors related to the larger learning context that determined student achievement related to virtual world scenario learning. Therefore, better onsite control measures as well as larger and equal sample sizes are required for more conclusive results. Also, the participants in this research study were graduate students. Further research with undergraduate as well as high school students may be helpful to establish the generalizability of the findings across a broader range of ages and backgrounds.

An interesting area of further research may be in comparing the number of items found in a virtual building with those found in a similar actual physical building. The purpose would be to discover meaningful differentials between spatial analysis in virtual and real world experiences. This would help clarify the validity of virtual world training in preparation for real world security. If so, this platform might demonstrate value as an additional feature in information assurance competitions like the National Collegiate Cyber Defense Competitions (NCCDC).

Second Life® has the potential to support the information assurance curriculum. While the results of this study were inconclusive in determining a difference in performance attributable to modes of instruction, the students' posttest results show a general improvement in performance across all three instructional modes.

References

1. Kneebone, R.: Simulation in surgical training: Educational issues and practical implications. Medical Education 37, 267–277 (2003)
2. Aldrich, C.: Virtual worlds, simulations, and games for education: A unifying view. Innovate: J. of Online Education 5(5), http://www.innovateonline.info/pdf/vol5_issue5/Virtual_Worlds,_Simulations,_and_Games_for_Education-__A_Unifying_View.pdf
3. Cheal, C.: Student perceptions of a course taught in Second Life®. Innovate: J. of Online Education 5(5), http://www.innovateonline.info/pdf/vol5_issue5/Virtual_Worlds,_Simulations,_and_Games_for_Education-__A_Unifying_View.pdf
4. Linden Lab. Virtual World Simulation Training Prepares Real Guards on the US Canadian Border: Loyalist College in Second Life®, http://secondlifegrid.net.s3.amazonaws.com/docs/Second_Life_Case_Loyalist_EN.pdf
5. Phillips, J., Berge, Z.L.: Second Life® for dental education. J. of Dental Education 73(11), 1260–1264 (2009)
6. Gall, M.D., Gall, J.P., Borg, W.R.: Educational Research: An introduction, 8th edn. Pearson Education, Inc., Boson (2007)

An Enterprise Anti-phishing Framework

Edwin Donald Frauenstein[1] and Rossouw von Solms[2]

[1] Walter Sisulu University, School of Computing, East London, South Africa
[2] Nelson Mandela Metropolitan University, School of ICT, Port Elizabeth, South Africa
efrauenstein@wsu.ac.za, rossouw@nmmu.ac.za

Abstract. The objective of this paper is to report back on an organizational framework, which consisted of human, organization and technology (HOT) dimensions in holistically addressing aspects associated with phishing. Most anti-phishing literature studied either focused on technical controls or education in isolation however; education is core to all aspects in the above-mentioned framework. It is evident, from literature, that little work has been conducted on anti-phishing preventative measures in the context of organizations but rather from a personal user-level. In the framework, the emphasis is placed on the human factors in addressing phishing attacks.

Keywords: Information Security, social engineering, human factors, phishing, email scams, spam, spoofed-websites.

1 Introduction

It is evident that as more organizations provide greater online access to their customers, phishers are successfully using social engineering techniques and technology advantageously to steal personal information and conduct identity theft on a global scale [20]. Organizations financial information is at risk, because most information-workers are vulnerable to social engineering techniques as the organizations possess financial information [29]. Fraudulent emails, such as phishing, can harm their victims as well as organizations resulting in financial losses, damaged reputation [27] and identity theft. Given a predicted increase in the tools available to fight phishing, it is expected that future attacks will continue to be more refined in targeting users i.e. spear phishing [24] incorporating greater elements of context to become more effective and thus more dangerous for society. Hence, by understanding the tools and technologies that phishers use, organizations, users and their customers can take a proactive approach in defending themselves against future phishing attacks [20]. Although this paper presents a holistic framework which requires all dimensions to be of key importance however, education is indeed a major component of protection against phishing. Thus, the objective of this paper is to emphasis how education, awareness and training are required to effectively strengthen the dependencies between the dimensions in the framework. The rest of the paper is structured as follows: In Section 2, we give a background of phishing and explain its effectiveness. In Section 3, we illustrate the need for a holistic framework. In Section

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 196–203, 2013.

4, we demonstrate the anti-phishing framework focusing on human factors. Finally, conclusions are drawn in Section 5.

2 Phishing Explained

"Phishing" is a hacker's term that originated from fraudsters whom are "fishing" for confidential information, mostly conducted through using fake emails and spoofed websites acting as the "bait", and the victim's accounts as the netted "phish" [27]. Phishing is a component of social engineering through which an individual attempts to solicit and steal confidential information from a user or employee by masquerading as a legitimate entity, usually from well-known financial or e-commerce institutions [27] as the primary of objective is to fraudulently obtain money. PayPal™, eBay™, American Online™, ABSA™, Standard Bank™, Google™, Microsoft and the South African Revenue Services are a few popular cases of organizations, and its clients, that have financially been affected through phishing attacks. Although most cases are financial related, phishing includes unauthorized access to all types of data e.g. social security number. Besides email, there are a number of other phishing variations such as spear phishing, wi-phishing, vishing, baiting, whaling and pharming. Phishing techniques have become more sophisticated [27], making use of a range of modern technologies such as: Internet Relay Chat (IRC), instant messengers (IM's), social networking sites (e.g. Facebook, MySpace) [10],[17],[19] and Trojan horse [6],[27]. The effectiveness of using social engineering techniques do not require much prior technical knowledge or education into hacking information systems; instead human emotion, deceit and manipulation are tools used to trick victims into giving up their personal information.

From the description of phishing above, typically five main processes are used to carry out a phishing attack:

Planning: Phisher determines who and how to attack and the information to be obtained from the victim. According to Orgill [21], social engineering attacks usually entail two facets namely: the physical aspect (e.g. workplace, online) and the psychological aspect or a combination using both aspects to gain desired information.

Email Design: The illusion based by email appearance (e.g. email address structure, subject header and content), is made to appear more legitimate by using institution logos, terminology etc. to create authenticity in the mind of the victim.

Fabricated Story: Is used to gain the victims attention, supposedly in their best interest, that a problem exists e.g. customer accounts has been hijacked. The email can also perceive to have a friendly tone e.g. thanking you for your co-operation. Using reverse social engineering, before the problem is resolved, the target feels indebted to the attacker.

Threatening Tone or Consequence: The user is lured by the fake warning and enticed to click on a hyperlink which is usually disguised as text or an image e.g.

Click here for verification. The tone, together with reverse psychology, is used e.g. the user fears that if they choose not to verify, consequently result in their account being automatically deleted. Ironically, it is "human nature" not to want any further undesired consequences or hassles e.g. renewing accounts etc.

Spoofed-Website: After the user selects/clicks the hyperlink embedded within the email message, they are directed to a spoofed-website which also appears authentic and legitimate in design, and subsequently the victims personal details are captured unsuspectingly.

3 The Need for a Holistic Anti-phishing Framework

Organizations are at risk caused through their employees' actions and behavior [28]. If human behavior could be understood, one may suitably address why humans fall for victim to phishing emails [1],[5]. According to Hinson [13], it can be argued that technical flaws themselves are the product of human errors. Even so, companies concerned with information and data security are increasingly dedicating more *technological* resources to evaluate and protect their information systems [13] thus ignoring employees as the source of their most prevalent exposure. It is often easier for attackers to exploit human and social weaknesses of the defences than to defeat the technological countermeasures [18]. This is also evident in anti-phishing literature as most research focused on technical solutions such as: developing browser toolbars/plug-ins [23] preventative measures, characteristics and email structure [6],[20],[22], algorithms for detecting, identifying and measuring phishing emails and sites [8],[11],[32] and evaluating the effectiveness of web browser toolbar warnings/indicators [4],[7],[12],[31]. Many employees cannot identify the difference between a genuine and a spoofed website [4],[21]. Furthermore, many users are too preoccupied with their primary work duties that they hardly remember to pay attention for web browser security indicators [19]. Information security is far more than applying a range of physical and technical controls [13] and technically knowledgeable specialists often make the mistake of believing that technical measures succeed in protecting them and average consumers [14]. Social engineering attacks and lack of compliance of organizational security policies are increasingly cited as security concerns. Technical solutions are only as good as the people that use and operate them because information security is a multi-dimensional issue and only be achieved if a holistic approach is taken [3].

Generally information security threats exploit human behavior and thus, in an organizational context, require a framework consisting of human, organizational and technological dimensions (HOT) to address against such threats [9]. Illustrated in Fig 1, HOT dimensions are operating in isolation of one another *(dotted lines)*, caused from limited communication and interaction between each of them thus forming only a 'single layer' oriented defense. As a result, if one of the dimensions is weakened, phishing attacks may proliferate compromising the other dimensions respectively. Ideally, it is suitable to move towards an 'in-depth' defense oriented model (see Fig. 2), thus allowing several barriers to serve a defense.

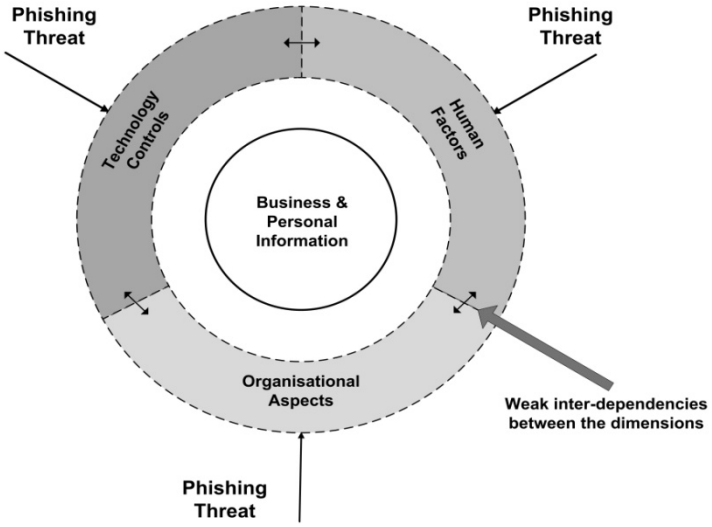


Fig. 1. Organizational dimensions targeted by phishing

4 Anti-phishing Framework: Phishing for a Solution

Technology controls have proven to be inadequate in protecting against phishing especially when applied in isolation of other organizational aspects. While technology is important, organizational and human factors also form a crucial role in achieving information security [1]. Understanding of how different human, organizational, and technological elements interplay could explain how different factors lead to sources of security breaches and vulnerabilities within organizations [15],[30]. Since each dimension has human involvement, even if the organizational dimension is added, protection may not be sufficient as both the organizational and technology dimensions depend on the H dimension. In the organizational dimension, best practices, policies, procedures and international standards (e.g. ISO 27002, King III, COBIT 4.0); fully depend on humans obeying them. Furthermore, they need to be in place to guide the other dimensions. Technology dimensions would typically involve any technical controls such as: anti-phishing browser plug-ins, anti-virus software, spam filters, web browsers, network firewalls, etc. and is dependent on humans to follow the procedures to ensure the technical controls are functioning and applied correctly. The human dimension calls for effective *awareness*, *education* and *training* to assist in strengthening the 'human firewall' and to ideally cultivate information security behavior in the organization. Of these dimensions, the human dimension is the area that phishing exposes the most and as a result, compromises the technology and organizational dimensions. Thus, there is a need for the education element to be present in *all* of the above-mentioned dimensions to ensure that all HOT dimensions are functioning optimally. In doing so, this should provide for adequate overall risk mitigation against phishing attacks (see Fig.2). Further research will validate these findings through an expert review.

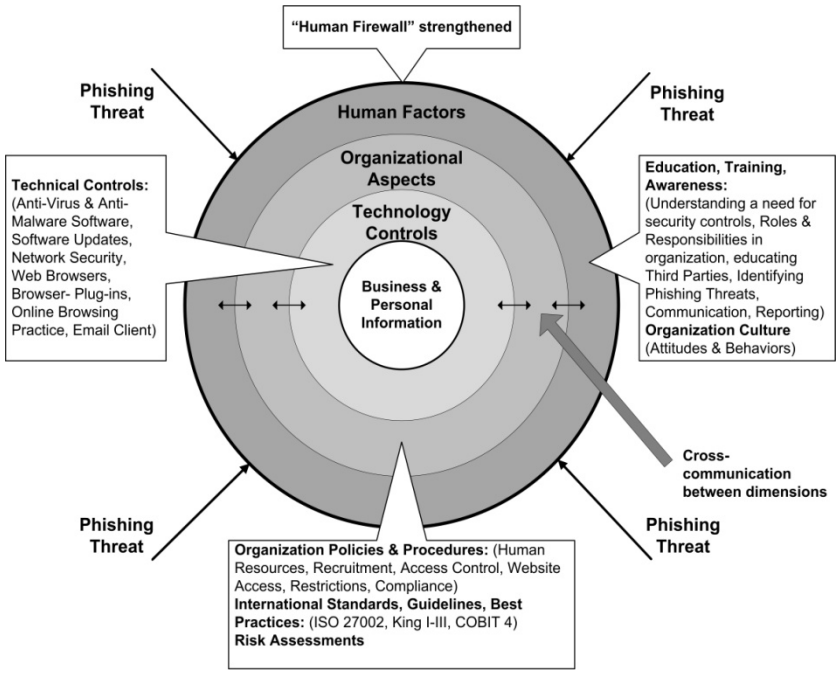


Fig. 2. Aspects in an organization, holistically related to an anti-phishing framework

Illustrated in Fig 2, continual communication *(concentric circles & arrows)* between the HOT dimensions serves a stronger defense. The human dimension is the entry point for phishing attacks and the common link (the glue) which influences all the other dimensions. It requires education to strengthen the interdependencies between the other areas e.g. staff must be knowledgeable enough of policies and technical aspects to ensure that operational procedures are obeyed and implemented correctly. The following section focuses on the components required to address the human factor dimension.

Information Security Management & Culture: Information security management requires, as a minimum, participation by all employees, shareholders, suppliers, third parties, customers or other external parties [25]. It is the responsibility of all employees to protect information thus defending the reputation and financial well-being of the business [2]. Effective interactions and communications are required to reach a mutual understanding about security risks among different stakeholders [30]. An information security culture needs to be adopted to ensure that information security becomes a natural aspect in the daily practice of every employee.

Educate Staff in Recognizing Phishing Emails and other Online Threats: Staff security education and training is one of the most important aspects of an

organizations security posture and perhaps the greatest non-technical measure available and cost-effective solution for human factors and security [2]. Security topics and requirements need to be integrated into normal business behaviour, through clear policy and staff education [2]. Through a regular and comprehensive user education programme, staff can resist and be made more aware of the design (e.g. the address bar, SSL icon, web browser warning indicators, fake websites), activities and dangers involved in a phishing attack [14],[16],[26] and to report such attacks. This is substantiated by Ohaya [19] that many users do not have the underlying knowledge of how operating systems, e-mails and websites work as employees cannot tell the difference between a genuine and spoofed-website. In some cases, users frequently ignore phishing warning messages from anti-phishing tools [7],[19],[31]. For effectiveness, the training could have some incentive, fun (e.g. gameplay [26]) or humour to gain participation from staff. An added benefit, through training, allows employees to also learn other current and future threats of information security aspects e.g. scams, viruses instead of phishing attacks alone especially since attack methods are evolving. Third parties may also require education equivalent with full time employees however, effective education may prove difficult in outsourced environments where providers are growing rapidly [2]. It is essential for all employees to be an above-average computer user, especially in using email and internet, as it exposes the user and organisation to other potential threats. This requirement can be enforced in the recruitment policy (*Organisation Aspects*).

Awareness Programmes: According to ISO/IEC 27002 [25], critical success factors, based on experience, have shown that information security awareness is important. Awareness programmes should aim to enhance levels of trust between employer and employee by developing an understanding of the reasons for the security policies and controls that have been applied, as it will help staff be more aware of the issues [3] thus reducing the likelihood of accidental breaches and increase the probability of malicious activity being detected and reported. Staff needs to understand the implications of not obeying such policies.

Staff Lack in Security Behaviour: Unacceptable, non-malicious behaviour by staff should be taken seriously. Organisation policies can ensure that employees cannot plead ignorance to the rules as many insider problems stem from ignorance rather than malicious motivation [2]. However, mere accidents can potentially cause large implications e.g. social networking sites are a playground for social engineers [10] thus, if staff are spending excessive time on social network sites during office hours, this may put the organisations reputation and financial well-being at risk.

Technical staff must be educated in their duties and define proper technical procedures and apply the relevant technological controls to implement those procedures e.g. prevent users from accessing risky sites.

Monitoring: Some organisations emphasise that monitoring can benefit staff where employees are reassured that the organisation is safeguarded against confidential leaks and hence possible damage to its reputation or financial loss.

5 Conclusion

It has been established that HOT dimensions in an organization require strengthening to address phishing [9]. Human factors have been mentioned to be the greatest risk and as such require the most focus. Much research has been placed either on education, training and awareness [14],[16],[21],[26] or technical controls. Although each HOT dimension has its own weaknesses or vulnerabilities, as all encompass some human involvement, education can close the gap between all the dimensions (e.g. should the technical controls fail; humans can be aware and knowledgeable in addressing a phishing attack) thus resulting in a multi-level defense model.

References

1. Beznosov, K., Beznosova, O.: On the imbalance of the security problem space and its expected consequences. Information Management & Computer Security 15, 420–431 (2007)
2. Cobb, M.: Preventing phishing attacks: Enterprise best practices. SearchSecurity.co.uk. (2010)
3. Colwill, C.: Human factors in information security: The insider threat - Who can you trust these days? Information Security Technical Report 30, 1–11 (2010)
4. Dhamija, R., Tygar, J.D., Hearst, M.: Why phishing works. In: SIGCHI Conference on Human Factors in Computing Systems, pp. 581–590. ACM, Montreal (2006)
5. Downs, J.S., Holbrook, M., Cranor, L.F.: Behavioral response to phishing risk. In: Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit, pp. 37–44. ACM, Pittsburgh (2007)
6. Drake, C.E., Oliver, J.J., Koontz, E.J.: Anatomy of a Phishing Email. In: Conference on Email and Anti-Spam (CEAS). Citeseer (2004)
7. Egelman, S., Cranor, L.F., Hong, J.: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In: 26th Annual SIGCHI Conference on Human Factors in Computing Systems, pp. 106–1074. ACM, Florence (2008)
8. Fette, I., Sadeh, N., Tomasic, A.: Learning to detect phishing emails. In: 16th International Conference on World Wide Web, pp. 649–656. ACM, Banff (2007)
9. Frauenstein, E.D., von Solms, R.: Phishing: How an organisation can protect itself. In: Information Security South Africa, Johannesburg, South Africa, July 6-8, pp. 253–268 (2009)
10. Frauenstein, E.D., von Solms, R.: The Wild Wide West of Social Networking Sites. In: South African Information Security Multi-Conference, Port Elizabeth, South Africa, May 17-18, pp. 74–88 (2010)
11. Garera, S., Provos, N., Chew, M., Rubin, A.D.: A framework for detection and measurement of phishing attacks. In: 2007 ACM Workshop on Recurring Malcode, pp. 1–8. ACM, Alexandria (2007)
12. Herzberg, A., Jbara, A.: Security and identification indicators for browsers against spoofing and phishing attacks. ACM Trans. Internet Technol. 8, 1–36 (2008)
13. Hinson, G.: Human factors in information security (2003), http://www.infosecwriters.com/text_resources/pdf/human_factors.pdf

14. Jakobsson, M.: The Human Factor in Phishing. Privacy & Security of Consumer Information (2007), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.68.8721&rep=rep1&type=pdf
15. Kraemer, S., Carayon, P., Clem, J.: Human and organizational factors in computer and information security:Pathways to vulnerabilities. Computers & Security 28, 509–520 (2009)
16. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., Hong, J.: Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology 10, 1–31 (2010)
17. Leavitt, N.: Instant Messaging: A new target for hackers, pp. 20–33. IEEE Press (2005)
18. Mitnick, K.D., Simon, W.L., Wozniack, S.: The Art of Deception: Controlling the Human Element of Security. Wiley, New York (2002)
19. Ohaya, C.: Managing phishing threats in an organization. In: 3rd Annual Conference on Information Security Curriculum Development, pp. 159–161. ACM, Kennesaw (2006)
20. Ollman, G.: The Phishing Guide, white paper (2008), http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf
21. Orgill, G.L., Romney, G.W., Bailey, M.G., Orgill, P.M.: The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In: 5th Conference on IT Education, pp. 177–181. ACM, Salt Lake City (2004)
22. Patel, D., Luo, X.: Take a close look at phishing. In: 4th Annual Conference on Information Security Curriculum Development, pp. 1–4. ACM, Kennesaw (2007)
23. Raffetseder, T., Kirda, E., Kruegel, C.: Building Anti-Phishing Browser Plug-Ins: An Experience Report. In: 3rd International Workshop on Software Engineering for Secure Systems. IEEE Computer Society (2007)
24. Robila, S.A., Ragucci, J.W.: Don't be a phish: steps in user education. In: 11th Annual SIGCSE Conference on Innovation and Technology in Computer Science Education, pp. 237–241. ACM, Bologna (2006)
25. SANS, Information technology-Security techniques-Code of practice for information security management. ISO/IEC 27002:2005. Standards South Africa (2008)
26. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., Nunge, E.: Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. In: 3rd Symposium on Usable Privacy and Security, pp. 88–99. ACM, Pittsburgh (2007)
27. Sophos, Phishing and the threat to corporate networks (white paper). (2005), http://www.sophos.com/whitepapers/sophos-phishing-wpuk.pdf
28. Thomson, K.-L., von Solms, R., Louw, L.: Cultivating an organizational information security culture. Computer Fraud & Security (2006)
29. von Solms, S.H., von Solms, R.: Information Security Governance. Springer, New York (2009)
30. Werlinger, R., Hawkey, K., Beznosov, K.: Human, Organizational and Technological Challenges of Implementing IT Security in Organizations. In: Human Aspects of Information Security and Assurance, Plymouth, England, pp. 35–48 (2008)
31. Wu, M., Miller, R.C., Garfinkel, S.L.: Do security toolbars actually prevent phishing attacks? In: SIGCHI Conference on Human Factors in Computing Systems, pp. 601–610. ACM, Montreal (2006)
32. Zhang, Y., Hong, J.I., Cranor, L.F.: Cantina: a content-based approach to detecting phishing web sites. In: 16th International Conference on World Wide Web, pp. 639–648. ACM, Banff (2007)

Teaching Computer Security with a Hands-On Component

Narayan Murthy

Pace University, New York
nmurthy@pace.edu

Abstract. To address national needs for computer security education, many universities have incorporated computer and security courses into their undergraduate and graduate curricula. Our department has introduced computer security courses at both the undergraduate and the graduate level. This paper describes our approach, our experiences, and lessons learned in teaching a Computer Security Overview course.

There are two key elements in the course: Studying computer security topics from a current textbook and online and experimenting with security tools. While the textbook and online material expose students to current security topics, projects that involve experimenting with security tools motivate students to explore computer-security techniques, providing a framework for a better understanding of the security topics and strengthening students' ability to put what they learnt in the classroom into practice in their organizations tomorrow.

1 Introduction

We all have seen the dramatic development of new and improved technologies. In July 2010, Facebook reached over 500 million active users, there were 85,500 iPhone apps, and 2 billion downloads occurred. Fifty-six percent of Americans say that they have at some point used wireless devices such as laptops, cell phones, and game consoles for online access.

There has also been an increase in the number, and sophistication, of Internet threats being produced by cyber criminals. According to an Internet security software and service provider Trend Micro study on Threat Predictions for 2011, threat researchers have found that more than 80% of the top malware uses the web to arrive on users' systems, and every second, 3.5 new threats are released by cyber criminals [8]. The Verizon Business website gives an excellent list of recent data breach statistics [9].

The annual CSI/FBI computer crime and security survey has shown that information security has continuously been a top priority in many organizations. This trend brings a great demand for qualified Information Assurance (IA) professionals [4].

In the field of computer security, malicious actors seem to outsmart the good guys. The offenders always seem to be one step ahead of the defenders. We believe that

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 204–210, 2013.

students have to learn defensive techniques by learning how the offense works. Learning successful defensive techniques in sports means observing the offensive tactics of the opponent. On the same lines, students should first be made to appreciate hacking techniques before moving on to defensive roles.

Our Overview of Computer Security course has been developed with this philosophy in mind. The purpose of this paper is to provide our experience in designing information assurance courseware that combines theory with practice. Using well-designed hands-on laboratory exercises, we allow students to experience the technical details of what they have learned [3]. There are two key elements in the course: studying computer security topics from a current textbook and online and experimenting with security tools. In addition to learning pedagogies and theories from the textbook, the course will focus on the use of technology to help students gain insight into the usefulness of what they have learned from the textbook.

Each lesson includes both lecture and hands-on labs to reinforce concepts. Students practice their craft either on their own machines or on the university machines in a controlled real-world environment. The university security lab is a local area networked lab, which is an isolated environment without any connection to the outside world. This isolation enables us to provide an increased level of threat. Students conduct both defensive and offensive experiments in this lab.

Some people argue that labs are so much more engaging than reading and study that they tend to drive out the latter. Given that a course such as this one requires a huge amount of reading and understanding topics such as encryption algorithms, network protocols, software security, and so on, such people say that this course should be light on the labs and strong on essential theory.

We believe that this argument is valid for students with math and programming backgrounds. By definition, the course in question is open to non-computer science majors. We strongly believe that computer security is too important to make this program available only to computer science majors.

2 Our Institution

For more than 100 years, Pace University has been preparing students to become leaders in their fields by providing an education that combines exceptional academics with professional experience and the New York advantage. Pace has three campuses in New York City, Westchester, and White Plains. A private metropolitan university, Pace enrolls approximately 13,500 students in bachelor's, master's, and doctoral programs in the Dyson College of Arts and Sciences, Lienhard School of Nursing, Lubin School of Business, School of Education, Seidenberg School of Computer Science and Information Systems, and School of Law.

Pace University, through the efforts of the Seidenberg School, was redesignated a National Center of Academic Excellence in Information Assurance Education for the academic years between 2007 and 2012. The original designation was awarded in 2004. The National Centers of Academic Excellence in Information Assurance Education (CAEIAE) Program is an outreach program designed and operated by the

National Security Agency (NSA) and the Department of Homeland Security (DHS) [5]. The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education in information assurance (IA) and graduating a growing number of professionals with IA expertise in various disciplines.

To attain certification, an institution must demonstrate commitment to academic excellence in IA by meeting rigorous requirements in areas such as curriculum, faculty qualifications, research efforts, laboratory and library resources, and partnerships. Pace is currently one of only about 120 institutions nationwide to be recognized as a Center.

Students attending these designated schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. Designation as a Center does not carry a commitment for funding from NSA or DHS.

3 Our Programs

IA academic programs have faced several challenges recently. As a way to broaden the appeal of their graduates as well as expand the scope of their computing programs, many computing programs have either integrated the IA curriculum into existing information technology, information systems, or computer science programs or have at least designed a single course to cover IA topics [3]. However, educators have proposed changes in the IA curriculum to cover both technical and nontechnical aspects of information security in order to keep up with the fast-changing security requirements for the public, industry, and the government [3].

At the undergraduate level, our department offers an interdisciplinary minor in collaboration with the Department of Criminal Justice.

At the graduate level, we offer a concentration in information assurance in a master's in information systems program.

The programs are by design not programming focused (we don't offer a software security course) so that it is open to non-CS majors.

3.1 Undergraduate Minor: Information Assurance in the Criminal Justice System

This minor was developed in response to faculty in the Criminal Justice Department who maintained that their students would benefit from information security courses. They might not necessarily plan to work as security professionals but need to deal with security problems in their own field.

The Minor Consists of the Following Six Courses:

CRJ 150 Introduction to Criminal Justice
CRJ 247 Introduction to Private Security

CRJ 346 Terrorism and Society
IT 300 Computer Security Overview
IT 304 Network and Internet Security
IT 308 Computer Forensics

Of these six courses, the first three (with the CRJ prefix) are offered by the Criminal Justice Department, and the last three (with IT) are offered by the Computer Science Department.

All three IT courses are a combination of textbook study and hands-on lab work. The course this paper is discussing is IT 300.

3.2 Graduate Concentration: Security and Information Assurance

This is one of the concentrations available to students in the MS in Information Systems program. Here is a description of the concentration: As organizations become more aware of computer and information security requirements, there is a growing need for IT professionals who understand the technologies and concepts of information assurance, including encryption, threat analysis, access control, and social engineering.

Concentration Courses:
IT 603 Overview of Information Security
IT 660 Network Security
IT 662 Web and Internet Security
IT 664 Computer and Internet Forensics
IT 666 Information Security Management
The course discussed in the paper is IT 603.

3.3 Topics in IT 603 Overview of Information Security

The textbook used is *Corporate Computer and Network Security* By Raymond R. Panko.

Topics covered (from the book) are Access Control and Site Security; Review of TCP/IP Internetworking; Attack Methods; Firewalls; Host Security; The Elements of Cryptography; Cryptographic Systems: SSL/TLS, VPNs, and Kerberos; Application Security: Electronic Commerce and E-mail; and Incident and Disaster Response.

3.4 Hands-On Security Experiments

For each of the hands-on experiments, the instructor provides a document with background material on the experiment to be done.

- **Steganography**

Students learn various steganography techniques, including the LSB method. They work on three careers (an image file, a sound file, and an HTML file) to retrieve hidden messages using a standard steganography tool.

- **Windows password hashes**

Students learn about the following topics: how Windows stores passwords—LAN Manager hash and NTLM hash; SAM file; and how password hacking programs work—dictionary method, brute force method, and hybrid method. Students use one of LC4, a combination of **Proactive System** and **ophcrack or LCP** by LCPSoft v5.04, to extract several passwords of various complexities (very simple to very complex).

- **MBSA**

Students learn to use Microsoft Baseline Security Analyzer (MBSA), an easy-to-use tool designed for the IT professional that helps small- and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. It is possible to improve the security management process by using MBSA to detect common security misconfigurations and missing security updates on computer systems. For the sake of experimenting, students introduce several loopholes and run MBSA. Students fix all the loopholes identified by MBSA and run MBSA again to make sure everything is fixed.

- **PGP**

Students learn about key ideas of encryption. They gain a detailed understanding of symmetric key encryption and public-key (asymmetric-key) encryption.

Students download and install PGP on their computers, generate a key pair, publish their public key on the PGP Global Directory, take the instructor's PGP public key from the PGP Global Directory, and create a small text file (making sure to include their full names in it). They save the file as their last name, encrypt the file using instructor's public key, and submit the encrypted file as an email attachment.

- **Nessus**

Nessus is a free (distributed by GNU), powerful, and easy-to-use remote security scanner developed and maintained by Tenable Network Security. Nessus is a vulnerability scanner that scans a target network to seek vulnerabilities in the network such as software bugs, backdoors, and so forth. The program is developed by Renaud Deraison. This is a very useful tool for network and system administrators to identify problems and security loopholes in their systems.

Students install Nessus and experiment with it. They run Nessus against any server and generate a report.

- **Nikto**

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 3,200 potentially dangerous files/CGIs, versions on over 625 servers, and version-specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated if desired (see http://www.cirt.net/code/nikto.shtml).

Students install Nikto, run it against a server, and submit a report of vulnerabilities on the server.

- **Web: Security, Cookies and History**

Students learn about web insecurity on various levels, addressing digital certificates, browsers' encryption strength, application security, cookies, index.dat file, and browser history. Web Historian is a program that is used to analyze browser history. Students download and install Web Historian and analyze browser history.

- **Phishing**

Students learn about identity theft and phishing. They see several examples of phishing emails. They learn to analyze phishing emails. They also learn email spoofing using port 25.

4 Conclusion

We administer course evaluations by students at the end of the semester. Judging from these evaluations, it is clear that the students enjoyed the hands-on component of the course.

> The following is a sample of comments by students on the evaluation forms:
> "The weekly lab assignments were extremely relevant and current. I learned a great deal by working through the labs."
> "The lab assignments were great. Learned new techniques."
> "Lab assignments gave exposure to the tools used to scan for vulnerabilities."
> "The lab assignments helped to understand the material better."
> Most valuable: "… having us work hands-on with different software."
> Most valuable: "Lab assignments."
> "The labs made me understand the material."
> "All lab assignments were very helpful to understand the objective of this course."
> Most valuable: "The hands on projects."

I believe that the hands-on component helped students appreciate and understand computer security.

References

1. Jeff, B., Schweitzer, D.: A Hands-on Approach to Information Operations Education and Training. In: 14th Colloquium for Information Systems Security Education. Baltimore, MD, June 7-9 (2010)
2. Centers of Academic Excellence—Institutions. National Security Agency (February 3, 2011), http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml

3. Chen, L.-C., Lin, C.: Combining Theory with Practice in Information Security Education. In: 11th Colloquium for Information Systems Security Education, June 4-7. Boston University, Boston (2007)
4. Lin, C., Chen, L.-C.: Development of an Interdisciplinary Information Technology Auditing Program. In: 13th Colloquium for Information Systems Security Education, Seattle, WA, June 1-3 (2009)
5. National Centers of Academic Excellence. National Security Agency (February 3, 2011), http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml
6. Riabov, V.V., Higgs, B.J.: Running a Computer Security Course: Challenges, Tools and Projects. River Academic Journal 6(1) (2010)
7. Sharma, S.K., Sefchek, J.: Teaching Information Systems Security Courses: A Hands-On Approach. Computers & Security 26, 290–299 (2007)
8. Trend Micro Threat Predictions for 2011 (February 3, 2011), http://affinitypartner.trendmicro.com/announcements/trend-micro-threat-predictions-for-2011.aspx
9. Verizon Business. Anatomy of a Data Breach (February 3, 2011) , http://www.govinfosecurity.com/external/rp_2009-data-breach-investigations-supplemental-report_en_xg.pdf

The Strengths and Challenges of Analogical Approaches to Computer Security Education

Matt Bishop[1] and Kara Nance[2]

[1] University of California Davis, Davis, CA, USA
bishop@cs.ucdavis.edu
[2] University of Alaska Fairbanks, Fairbanks, AK, USA
klnance@alaska.edu

Abstract. When teaching concepts such as computer security, with which students cannot easily identify, it is frequently helpful to use analogies to attempt to map a complex concept to an idea with which the student can identify. While this method works particularly well in the computer security domain, there are associated challenges and limits that must be considered when creating appropriate analogies. This paper defines analogies, provides some specific examples in the computer security realm, and discusses the challenges and limits associated with this approach.

Keywords: Computer Education, Computer Security Education, Analogies.

1 Introduction

Computer security is a complex subject, one requiring both an understanding of broad concepts and an attention to fine detail. Students of computer science understand this, because much of systems work in computer science has the same properties. One must understand the concepts, and then design and implement systems with great attention to detail; to be sure they perform at the requisite level. But this complexity can be very difficult to convey to non-computer scientists and new computer scientists.

Even more difficult to convey are certain basic ideas that, while clear to practitioners, are counter-intuitive to most people. As an example, consider the definition of "security" itself. The dictionary definition is "the state of being free from danger or threat"[1]. Some people feel secure in their homes, because their sanctuary has never been invaded by malicious people. Others feel differently, especially victims of home invasion crimes. Some people feel secure giving merchant web sites their credit card information, to make shopping easier (and to avoid re-entering the credit card information each time); others want the security of not leaving that sensitive data in the hands of another. In life, security is largely a matter of perception, culture, environment, individual desire, and can vary from moment to moment. Thus, the notion of security varies among people, and varies in ways that people seldom investigate, realize, or appreciate.

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 211–217, 2013.

This paper discusses an approach to conveying computer security concepts to non-technical audiences through the use of analogies. We provide some background in the next section, and then present some example analogies. A discussion of the challenges associated with finding good analogies, and teaching students how far analogies can be taken, make up the fourth section. We conclude by suggesting other techniques based on analogies that may prove useful.

2 Background

Educators, political organizers, marketing personnel, and parents are well aware of the importance of communicating in the language of the audience. Saul Alinsky wrote, "People only understand things in terms of their experience, which means you must get within their experience" [2, p. 81]. As an example, consider the number of stars in the universe. Presenting the concept mathematically by telling an audience there are 9,000,000,000,000,000,000,000,000 stars in the observable universe conveys little meaningful information about the magnitude of the number of stars, because most people cannot think of anything within their own experience to associate that number with. Alternatively, when the audience hears there are more stars in the observable universe than there are grains of sand on all the beaches of the world, their eyes light up. They have been to a beach, and probably to many beaches. They know how much sand is on those beaches. Now, they have a better understanding of the number of stars in the universe because the concept has been mapped to something with which they can identify.

This is particularly important when students are thrust into environments with which they are unfamiliar—such as using a computer. In order to bridge the distance between the instructor and the student, the instructor needs to find a way to help the students to identify with the concept. An identification of common ground between the instructor and student can be used to introduce a seemingly unrelated concept that is easy for the student to understand or identify with. This idea can then be transformed or bridged into the specialized realm that the instructor is teaching to share the idea with the students. An effective tool for accomplishing this bridging activity is an analogy.

3 Analogies

An analogy presents a concept or idea in the language of the target audience. It maps a concept from one world-view into the experience with which the audience can identify. Once a connection is made between the audience and the presenter, follow-on concepts are much easier to present as the audience has a vested interest in and relationship with the idea being presented. The following two analogies relate computer security issues to concepts in which new students are more likely to be comfortable. Most individuals understand, use and rely on vehicles to meet their transportation needs. While they are likely not auto mechanics or engineers, they all recognize the need for and potential use of vehicles. The same is true with locks.

People interact with locks, choose when to use them, and recognize that different locks are appropriate to protect different assets. They do not need to be expert locksmiths to understand the basics of how a lock functions and how it should be used. The use of these analogies is to bring each student's level of comfort with the new concepts to be consistent with the analogical equivalent. The analogies allow this progression as a sequence of steps, rather than as a new concept.

3.1 Security Is Like a Vehicle

Suppose we must communicate the basic notion of "security" to the average person. The definition of "security" depends upon a security policy, and so differs from site to site. We can use an analogy to demonstrate that different sites have different security needs.

Consider someone who needs to buy a new car. What is the best car to buy? The answer depends on the purchaser's needs. If the purchaser is a gardener who needs to haul a lawn mower, wheelbarrow, rakes, shovels, and other gardening tools as well as plants, he will need a pickup truck. A car for a family with five children, on the other hand, needs to hold more people than a pickup truck—perhaps a minivan or station wagon would work. An adventurous soul who enjoys driving off trails in the mountains would get an all-terrain vehicle. So "the best car to buy" is not the same for everyone. It depends upon the intended use.

Even when the purchaser decides upon the type of vehicle, he must select options. Which minivan should the family get? The expensive one has air conditioning; none of the others do. A manual transmission saves $1,000 over an automatic transmission. The Wobbler is very expensive to repair, unlike the Poodle; but the Wobbler's safety record is considerably better than that of the Poodle. All these differences must be considered.

Computer security is like that vehicle. There is no definition that applies to everyone, or every place. Just as different people interpret the idea of "best car", different people and sites interpret "secure" differently.

A writer may consider a computer to be secure if, when the computer crashes, he restarts it and is able to recover what he typed. The writer doesn't connect to the Internet, and never receives electronic mail. So he doesn't worry about people breaking in. But if he loses 10 pages of his latest novel, he will have to reconstruct it, and the result may be substantially less electrifying than the original effort.

A law firm probably defines "secure" along the lines of keeping information secret. The lawyer does not want her clients' secrets available to anyone on the Internet. She wants her clients to be able to talk to her in confidence, so they can be sure the information will remain confidential. Without that confidence, people will stop coming to her firm, and her practice will fail. So this is a good definition of security from her point of view.

But a university has different goals, and so may define "secure" as "only authorized people can change the data on the system". As a university disseminates research results publicly, it doesn't keep its ideas and results secret. But if anyone can change the results of research that the university posts on the web, the research (and

the university) will lose credibility. Thus, this too is an environmentally appropriate definition of “secure”.

Further, if the university adopted the writer’s definition of “secure”, the research results would be inaccessible because the systems would not be connected to the Internet. Similarly, if the lawyer adopted the definition that the university uses, she would lose her livelihood because the client’s information would be visible—but only the lawyer can change it. Just like the notion of a “best car”, the notion of a “secure system” changes with the needs of the user.

As most people either have bought a car, or know people who have, this analogy uses an everyday conundrum (what car to buy?) to illustrate a seemingly unrelated point that most people find difficult to grasp. Rather than follow the technical terms, by equating security to a security policy and then expounding on that concept, it focuses on the heart of the definition: that security is defined differently, for different needs.

3.2 Passwords Are Like Door Locks

Let’s consider the effort involved in attempting to convince a group of students that the strength of their passwords is fundamental to protecting their associated digital assets. Many instructors approach the concept of password strength with a discussion of combinatorics. As the instructor delves more deeply into the mathematics of a strong password, students' eyes begin to glaze over. If the importance of password strength has not been presented convincingly, the students are not likely to understand the “why” behind the concept. If students don’t understand the “why”, they are not as likely to be interested in the “how”. An analogy using locks can guide them towards the “why” and increase interest in the “how”.

Most individuals understand that locks vary greatly. In general, the more secure a lock is, the more challenging it is for unauthorized users to gain entry. There is an associated tradeoff as there is also increased difficulty in gaining authorized access. Home bathroom and bedroom doors frequently use privacy function locks. These locks are easy to unlock with a paper clip as they only require pressure applied through a hole in the lock in the doorknob. This is an appropriate strength for a lock in the interior of many homes, where the intent is to protect privacy rather than to protect assets. When choosing a lock for a front door—the main entry to the home—this sort of lock is rarely considered. Homeowners are likely to choose a lock and deadbolt combination that increases the challenge of gaining unauthorized entry. They are willing to face the additional challenges (carrying keys, locking the doors when leaving, etc.) as an acceptable tradeoff for the increased lock strength and associated sense of security. Now we can extend the analogy to an embassy in a hostile area, or a bank vault, and discuss what additional locking mechanisms would be appropriate to protect assets in these cases.

Passwords are like door locks. If someone gains access to your NY Times Online account, you are unlikely to experience a significant violation. Thus a weak password — a privacy lock password — can be appropriate in this case. We can extend the analogy to the password used to log into your online banking system. Now you want a

stronger password, as the assets you are protecting are more valuable to you, and unauthorized access would be viewed as a significant violation. The analogy can even be extended to equate using the same password for many accounts to the using the same key to open all the outside doors in your house. If someone has a key to just one of these doors, then she can open all the doors that use the same lock.

Most individuals will more readily identify with a lock analogy than with the underlying combinatorial mathematics regardless of how nicely is it presented. A good analogy creates a relationship between the concept and the learners and can quickly guide them towards understanding.

4 Challenges

While using analogies provides definite benefits to students, it also poses risks. In some sense, the analogy presents a model of a different situation, framed in a "language" or using concepts that the student understands. The benefit is that the analogy explains the problem in the student's terms. However, any model has discrepancies with the reality it represents, and the student must understand what this delineation. Thus, the point of the analogy must be clear, and the teacher must identify and clarify aspects of the analogy that are based on assumptions. In other words, the teacher must clearly delineate the point at which the analogy (the model) deviates significantly enough to no longer be considered an effective analogy.

Consider the analogy in Section 3.1. The point of the analogy is that the requirements that the "best vehicle" must meet are different; one is for ferrying tools, another for driving a family, a third for off-road travel. This maps into the point that the requirements that the "secure system" are to meet are also different: one preserves data across a system crash, another keeps data from public view, a third prevents unauthorized changes to publicly available data. So, drawing an inference about security from the different needs of the would-be purchasers fits into the model. However, drawing inferences such as there being one specific definition for transporting programs (the gardener driving tools), one for data (the family driving children), and one for miscellaneous uses (the all-terrain vehicles) would be incorrect. So the student must be warned that the analogy does not carry through to comparing the different types of cars to different uses of computers, and the requirements of the purchasers to security requirements.

A good rule of thumb is that the student should find the theme, or the main point, of the analogy and use that, and *only* that, in the inferences drawn. This emphasizes the need for the teacher to make that theme explicitly when presenting the analogy.

As another example, consider the analogy between locks and passwords in Section 3.2. That analogy focuses on the relationship between the lock (password) and the asset being protected. When the protection is for privacy in a situation where someone (a parent) may need to gain access, the lock (password) is weak. When the protection is for security, to protect the things guarded by the lock (the password), the lock (password) is strong. So the student is made aware of the consequences of choosing

weak passwords, and can decide under what circumstances to use strong passwords, or to use the same password to protect different things.

The analogy fails when extended to cover other aspects of protection. For example, if the object being protected is a file, the owner of the file can change permissions. But in real life, the owner of the *lock* determines whether access can be changed, by changing the lock. Thus, the heart of the analogy—the equating of strength of the password with the strength of the lock—does not extend to other parallels. The instructor must make this very clear.

One of the greatest challenges in teaching through the use of analogies is coming up with the appropriate analogies that are meaningful to the students and that relate to the course concepts being presented. The experiential diversity of the audience can greatly complicate this effort. Challenges include cultural differences, language barriers, experiential continua, personal biases, and relationship between the instructor and the students.

An example will make this point. On an I.Q. test, students were shown a picture of a cup and asked to identify the object, from a set of 5 pictures, that was most closely related to the cup. The pictures were of a cat, a table, a chair, a saucer, and a kite. Many of the students taking the test selected the table, which was the wrong answer (the saucer was correct). The reason was that the students came from poor backgrounds, where saucers were never used; so they thought the picture of the saucer was a picture of a plate, and chose the table as what they put the cup on.

A faculty member once taught a course in computer security that required students to read Machiavelli's *The Prince*, Sun Tzu's *The Art of War*, and similar books. The point that the faculty member wanted to convey to the students, which he stated explicitly and repeatedly, was that these books showed the reader how to think about systems (military systems, cultural systems, and other societal systems) in order to disrupt, confuse, and ultimately conquer or ruin them. The analogy with how attackers look at sites and systems is clear to anyone who has attacked a system or defended a system. Some students immediately got the point. But other students were so focused on the technical information involved about computer security, they complained that the instructor was turning a technical class into a literature class. Generalizing from books about cultural conflict and manipulation to social engineering and systems analysis was outside their experience.

Key to the use of analogies is the ability of the instructor to determine what the students will relate to. The analogy between the different meanings of security and the different types of automobiles in section 3.1 works with adults who know about cars, especially those who have purchased vehicles. It would not work with children in grade school, though. For them, an analogy involving games or toys would work better, because most children have played games; the analogy could relate the identification of the "best game" to the requirements of security.

Analogies also are affected by cultural norms. Even a concept such as privacy discussed in the lock analogy could potentially have very different meanings to people from Germany (informational self-determination), Japan (constitutional guarantee), and the US (no explicit constitutional right of general privacy). Further, consider an analogy between a system security officer and a police officer. In the

United States, where the power of the police is tied to possible violations of the law, the analogy suggests that a system security officer requires some reason to believe that a user is violating the site security policy to monitor the user. In a country where the power of the police includes the ability to monitor people randomly, the analogy suggests something very different. The key to analogy is to map a new concept to a concept that one understands. If an instructor attempts to maps a concept to a concept that has different meanings for individuals in the class, the understanding of the new concept will be mapped to the diverse worldviews of the students in the class.

5 Conclusion

While a potentially valuable method for identifying with the collective worldview of computer security students, analogies can be tricky. They must be chosen carefully, and explained carefully, because of the associated cultural and societal baggage they may carry. Largely heterogeneous groups are likely to have heterogeneous worldviews. These views are based on assumptions. Likewise, all analogies are founded on assumptions. Further, the assumptions involved are generally not technical. They are human—cultural and societal—and vary with the students' backgrounds. Thus, even in the same class, the students may draw different lessons from the same analogy. This emphasizes the need for the instructor to make explicit the point of the analogy, and also the *limits* of the analogy. Often, the instructor making the analogy is unaware of the assumptions that the students will make. As a result, the analogy fails to teach the students what the instructor believes it should. Thus, there is a failure in the communication network.

While analogies provide an excellent means to map a new concept to the worldview of a learner, this method has some associated challenges. An instructor is a sender who wishes to share an educational message with a student receiver. A good analogy decrypts the message for the student receiver so that the message makes more sense and the student can more easily understand the intent of the message. A poor analogy, or one with which the student receiver cannot identify, effectively encrypts the educational message, making it even more difficult or impossible for the student receiver to understand.

References

1. Definition of Security from Oxford Dictionaries Online. (n.d.), `http://www.oxforddictionaries.com/definition/security?view=uk` (retrieved February 4, 2011)
2. Alinsky, S.D.: Rules for Radicals. Vantage Books, New York (1972)

Reaching Today's Information Security Students

Helen Armstrong[1], Ron Dodge[2], and Colin Armstrong[1]

[1] School of IS, Curtin University of Technology, Australia
h.armstrong@curtin.edu.au,
colinarmstrong@gailaad.com
[2] IETD, USMA, West Point, New York, USA
Ronald.dodge@usma.edu

Abstract. Classes at university today comprise students from the Baby Boomers, Generation X and Y. The different outlooks on life of these generations affect their choice of education options and their learning preferences. There are numerous ways academics can innovatively deliver Information Security learning materials that meet the needs of these generations, whilst still achieving the educational goals. This paper discusses some observations of students in the different generations in information security courses and methods that may be used to ensure a more meaningful learning experience for both the teacher and the learner.

Keywords: information security education, Generation X Y, Net Generation.

1 Introduction

Information Security approaches and techniques are constantly shifting and new approaches emerge as technology progresses and society changes. It is important to continually update information security teaching and learning methods as well as the content of education and training in line with these new directions. However, education encompasses both teaching and learning and methods of achieving the learning objectives must be sufficiently flexible to cope with a changing body of learners. We, as information security educators need to be cognizant of the characteristics of the students we teach, as well as being aware of the different learning styles of different generations. This paper describes the characteristics of our current student body and discusses pedagogical requirements to best engage them. We then present some methods by which academics teaching information security at tertiary level can make the learning experience both meaningful and fun for the learner.

2 Characteristics of the Generations

Three main generations are represented in our information security student body today: Baby Boomers, Generation X and Generation Y. It is very easy to assume that

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 218–225, 2013.
IFIP International Federation for Information Processing 2013

all students born within a particular time frame will exhibit characteristics of their stylized generation and the authors are aware that this is not always the case – each student is an individual and they cannot all be the same, however they will have values and traits in common due to their shared social and historical experiences. The characteristics discussed in this paper are general and as such can only be used as a guide. It should be noted that the years forming the boundaries of each generation differs slightly between authors. It is also important to consider that some students will sit on the cusp between generations and may thus exhibit traits of more than one generation.

2.1 Baby Boomers

Baby Boomers were born during the period 1946-1954, just after WWII. They are confident of themselves and distrustful of authority, questioning the relevance of social structures. Their numbers are great, due to the increase in births encouraged to build the population after the two world wars. Demographics show a greater number of women than men, and the emergence of the quest for equality of the two sexes took a turn in favor of the females. Most families needed to have two incomes in order to survive and progress, initiating the concept of the 'latch-key child'. Baby boomers sought a college education, resulting in a boom in the tertiary education sector. Examples are Richard Branson, the entrepreneur who established the Virgin group of companies, and Bill Gates of Microsoft. Baby boomers are also familiar and comfortable with technology and computers.

Baby boomers see the instantaneous list of results from an Internet search engine an improvement on the extended time previously required to gather and analyze information from disparate sources. The lecture was the most efficient and cost effective means of getting information to a large number of students. The reading of books, analyses of the information gathered and then determination of the relevance of the information gathered, were necessary steps in the learning process. These are the oldest group of students in our classrooms, now being 55 to 63 years old. In many cases these students are attending to gain specialized skills and knowledge, driven by the need for qualifications for promotion or new employment. A small number are there for just the learning experience. These street-wise students bring a wealth of experience and knowledge into the classroom. On the downside, this generation can also be staid in their ways, believing that their way is the only way.

2.2 Generation X and Y

Generation X was born in the period between about 1965 and 1980. Gen Xers have been described by the media as practical skeptics and entrepreneurial free agents who fueled the dot-com boom [1]. Xers have also been called the MTV generation due to their short attention span. They are emotionally secure, informal, and have distain for corporate politics and bureaucracy, and company loyalty holds less importance than

to Baby Boomers. Nagle suggests this generation saw their workaholic parents downsized and restructured out of their chosen careers [2]. Although Gen Xers view work as something they have to do to live (but not to define their life) they will work hard for something they believe in, something that challenges them, or something that will build new desirable skills. Currently aged between about 30 and 45, Gen Xers return to college primarily to complete unfinished business, for career advancement, career security, a career change, or to pursue hopes and dreams [3]. Examples of well known Gen Xers are Nicole Kidman and Heath Ledger.

Generation Y students were born between the mid 1970's and 2001, with Baby Boomer and Gen Xer parents. This group is accustomed to constant change. Also known as Millennials these students first appeared on campuses near the turn of the millennium. They are sometimes called the *trophy generation* as each one is recognized for participating and everyone gets a trophy. They 'graduate' from all levels of schooling including kindergarten. They are achievement oriented, very technically savvy and want to make an immediate impact with little effort. Each child is recognized as 'special' with individual wants and needs, to which custom-designed solutions are applied. They are team players and are socially aware, with a desire to solve society's problems. Millennials see colleagues as a resource for tapping for important and influential information rather than investigating and finding out via their own research efforts. They harness new social technology to the maximum, constantly time sharing across a number of electronic forums such as email, FaceBook and MySpace whilst attending to other tasks. They have a fundamental need for structure from within and without for guidance [2], preferring small goals with tight deadlines and seek to be guided, and advised of, all boundaries so as not to waste time. They seek to add as much to their portfolio as they can. Breadth is more important than depth and the journey is only a means to get to their destination [4]. They move quickly on to the next task. This group expects instant gratification because their needs have always been met immediately. Examples of this generation are Paris Hilton and Brittany Spears.

2.3 Post Modern Students

The majority of American students in Generations X and Y with normal media exposure have postmodern social characteristics [5]. These characteristics include: a leveled view of authority and the importance of their own opinion, belief that experience is more important than knowledge, avoidance of pursuit for deeper meanings, preference for passiveness, and a consumer orientation to almost everything. Conflict is likely to arise in situations where current teaching methods and curricula are predominantly modernist as is the case in many universities [5]. As our student body today is comprised of mainly Gen Xers and Yers, academics teaching information security courses need to harness postmodern approaches to effectively educate students with the characteristics summarized in Table 1.

Table 1. Characteristics of Post Modern Students

General	Learning Related
Short concentration span	Desire a challenge
Desire individual recognition	Want to build skills quickly
View own opinion is important	Prefer small goals with tight deadlines
View the destination as more important than journey	Share information readily and use each other as a source of information
Passive	Prefer limits and structure, and need clear guidance
Desire immediate impact with little effort	Choose breadth rather than depth in researching new topics
Gather trophies and accolades	Only retain information deemed relevant
Use social technology constantly	Information needed is gathered just in time

As new students progress through their tertiary education they are required to adjust to the different expectations and learning activities associated with a higher learning environment. The need to research (rather than Google search) and think (rather than having an answer given) are features of higher learning. As the majority of tertiary learning environments are still based upon the values and beliefs of the Baby Boomer generation many new tertiary students become frustrated and withdraw from their courses. It must be borne in mind that university education is not offered to solely provide skills and training (which more closely meets the needs and expectations of these generations), but an education in its richest sense. An education encourages thinking, and research; the building of concepts and theory, and the application of such theories into practice. Many current students do not see the value in their degree studies as they are not able to convert their learning into immediate practical skills. In order to provide such an education academics need to not only manage the expectations of new students but also adjust their methods of teaching so more value is obtained by the students at the same time deeper learning takes place.

3 Pedagogy Approaches and Information Security

Many approaches have been postulated to engage today's college-aged students, one of which is the Postmodern Pedagogy. This approach recognizes that students require engaging experiences to fully capture their interest and encourage learning. This is the first step in transformational or adult learning models [6]. The description of Postmodern Pedagogy in Taylor [7] identifies that the traditional student – instructor relationship is significantly different from the generations before Gen X. Students are no longer driven by a situation where they are expected to please the instructor; instead, instructors are required to compete for student enrollments as a service provider. Faculty success is measured by the pass rate of students. When a course has an exceedingly low grade average, the thought is not, "why aren't the students learning", it is "why is the instructor not reaching the students". In addition to the relationship and the faculty role changing, the expectation of students is also different. Students are enrolled in Bachelor and Masters programs with a goal of post education employment. They demand applicable curriculum that will enable them to be

immediately effective in their chosen career field. In the IT field, this typically involves the certification preparation where detailed technical, "hands on" skills are required.

Postmodern Pedagogy further defines methods instructors may use to construct curriculum to meet the demands of the new teaching environment. We group these into two broad categories, assessing the student's learning paradigm and constructing a learning conducive environment. In the former, instructors must identify the goals of the students and help the students realize the importance. In the latter, the learning environment must use techniques and technologies beyond lecture. Specifically called for is an increased activity in learning. Studies have concluded that experiential based curriculum strategies result in a higher degree of learning [8,9]. In IT fields, this commonly involves hands-on laboratory exercises. Material should be delivered in multiple formats and the instructor should be available via several mediums (office hours, email, SMS, and the like). Finally, the assessments used must be meaningful. For students memorizing principles and theorems holds no importance to them. We must find a way to embed them into learning goals where the assessments require the student to demonstrate an understanding of the principle – not merely repeat it.

Information security education requires that students have a fundamental understanding of many computer science foundational topics. That, however, is not enough. This knowledge must be applied against a constant changing landscape of aggressor and technology. The skillful attacker is really the kind of student that we would all like to have. He/she is engaged in hacking because they truly are engaged at the base level by a desire to assess a technology and predict how it will fail under specific circumstances (for a variety of motivations). To create and defend our systems against this motivated adversary, our students must be similarly engaged in the process. This level of learning is commonly referred to in Bloom's Taxonomy [10] as the Evaluation level. This is in conflict with the general trend of the post modern generations to understand only what is needed for short term objectives. The good news is that the requirement for information security education at colleges and universities is a relatively recent growth. Instructors are more and more coming to the task of educating with experience managing the very systems their students will be working with upon graduation. This common understanding of the market requirements provides a link not shared in other disciplines. Although teachers in information security programs are predominantly baby boomers, and some Xers they are progressive enough to willingly adapt teaching strategies, however, more than likely they still harbor much of the "lecture" mentality they experienced in education.

4 Closing the Gap

Experiential learning [11], or learning by doing is very important for this generation. Engaging the student in discussions and collaborating in hands-on exercises facilitates a better understanding of the concepts and motivates the student by applying knowledge in a recognizable manner. This interaction allows them to build the skills they pursue. The goal of information security education should be to develop a

learning environment where students are required to apply knowledge and seek answers from group members or other students rather than relying on teachers for *the* answer. When developing an information security course, faculty should consider various ways to engage the student inside and outside of lecture. Several examples utilized successfully by the authors for reducing the gap and achieving objectives in information security include:

Experiential: Design classes so they are practical in nature and require students to actively participate early in each class. Get students actively participating early in each session. Introduce the topic through a real world example. For example if the topic deals with social engineering use social engineering before class to demonstrate the ease at which the student would fall prey to the very topic of the lesson. Experiential learning enables students to concrete their learning and gain skills and understanding. Their concentration span can be extended as they learn and apply new concepts. Walk through practical tasks with them as the theory is being presented. For example, when teaching security policy implementation via firewall rules set the students an exercise to specify the firewall rules as the table is developed, and implement and test it. Another example is giving computer forensics students a set of screwdrivers, a couple of surplus hard drives to dismantle, and an hour to explore at their own pace provides them with insights about the technology they would not achieve by reading a text book or viewing lecture slides.

Task Size: Break the learning session into small tasks allocating a short burst of time for each task. Information security is very open to teaching in smaller sections, with each section or task building on previous tasks. For example students could use password cracking software to gain access to passwords, and then use more secure methods to protect passwords.

Relevance: Show the relevance of the pedagogical materials to the course objectives and subsequent employment. Students respond positively when they can see the applicability and relevance of what they are learning. Understanding how security concepts apply in differing fields and situations is also helpful for students to see relevance in what they are learning. Using technologies the students know to reinforce lack of security in their Facebook and MySpace accounts brings home the need for certain security measures and an opportunity to explain how these work. Linking courses to external certification and standards also reinforces the relevance of the knowledge and skills being learned.

Examples and Instructions: For more complex tasks give unambiguous, concise instructions, clearly presenting what is required of the students, and the end product they are expected to produce. This links closely to making the material relevant. The end product needs to be something where the student can come away with a more clear understanding of what the objective was and whether they achieved it. Present examples to demonstrate key points. Students should be led through basic examples and then challenged to solve more complex ones that build from in-class examples.

Contemporary Tools: Use interactive media and interaction and provide multiple ways to access the material. Rich interactive media engages students and holds their interest. This content should be available in multiple formats. For lectures, the

material can be recorded for "pod cast" or videotaped. Labs or exercises should be accessible from multiple endpoints. Several universities have developed technologies to enable student access from almost anywhere. Multiple formats of the learning materials also provide access to those students with disabilities. Use new technologies as teaching and learning tools, i.e. set assessments and exercises so that students can use the technologies they know, i.e. Second Life, games, etc. Use online references and sources of information. Students should be able to seek additional information when not in class. Instructors can assist by providing links to current additional references that students can use to investigate further.

Groups: Undertake exercises in small groups to encourage confidence. Students are comfortable with this approach as they gather in small groups to discuss assessments and to study. Network security can be presented in such a way that students establish a small network (a virtual environment using tools such as VMWare works really well), then attack each other's networks to test robustness.

Non-assessment: Set practical exercises that are not assessed. This encourages the students to participate and learn without the fear of not succeeding. For example a moot court exercise enables computer forensic students to demonstrate concepts and processes and thus be able to credit themselves with a specific set of skills without undergoing what they see as a formal academic assessment or examination.

5 Conclusion

Educating a mix of information security students from different generations means teachers and students need to interact in a common space. This requires an understanding of the characteristics and learning styles of each generation, plus the flexibility to adjust methods to achieve the learning objectives to the benefit of all. However, it also requires a full understanding of the learning objectives and their relevance to the world the students will enter on completion of their studies. Postmodern students respond positively to relevant and practical learning and the information security field is well placed to set these students up for success in their learning journey.

References

1. Rickes, P.C.: Make way for millennials! How today's students are shaping higher education space. Planning for Higher Education 37(2), 7–17 (2009)
2. Nagle, T.: Coaching Generation X (2007), http://www.coachingandmentoring.com/Articles/x's.html (retrieved January 31, 2009)
3. Black, J.: Gen Xers Return to College: Enrollment Strategies for a Maturing Population, Aacrao, Washington DC (2003)
4. Howe, N., Strauss, W.: Millenials go to College, 2nd edn. LifeCourse Associates, Great Falls (2007)

5. Payne, S.L., Holmes, B.: Communication challenges for management faculty involving younger Generation. Journal of Management Education 22(3), 344–367 (1998)
6. Tsao, J., Takahashi, K., Olusesu, J., Jain, S.: Transformative Learning. In: Orey, M. (ed.) Emerging Perspectives on Learning, Teaching, and Technology (2006), http://projects.coe.uga.edu/epltt/ (retrieved January 05, 2009)
7. Taylor, M.: Generation neXt comes to college: 2006 updates and emerging issues (2006), http://www.taylorprograms.org/images/Gen_NeXt_article_HLC_06.pdf (retrieved January 13, 2009)
8. Greenberg, J.E., Delgutte, B., Gray, M.L.: Hands-on learning in biomedical signal processing. IEEE Engineering in Medicine and Biology Magazine 22(4), 71–79 (2003)
9. Mountain, J.R.: Work in progress - applied process control systems design: hands-on laboratory experiences for multiple disciplines and academic levels. In: 34th Annual Frontiers in Education, FIE 2004, vol. 1, pp. T1D 3–4 (2004)
10. Bloom, B.S.: Taxonomy of Educational Objectives. In: Handbook I: Cognitive Domain. Green & Company, Longmans (1956)
11. Kolb, D.: Experiential Learning: Experience as the Source of Learning and Development. Prentice-Hall, Inc., Englewood Cliffs (1984)

Some "Secure Programming" Exercises for an Introductory Programming Class

Matt Bishop

Dept. of Computer Science, University of California at Davis, Davis, CA 95616-8562, USA
bishop@cs.ucdavis.edu

Abstract. Ideally, computer security should be an integral part of all programming courses. Beginning programming classes pose a particular challenge, because the students are learning basic concepts of programming. Thus, teaching them about buffer overflows as security problems, requiring an explanation of concepts such as "smashing the stack," will confuse students more than motivate them to check array bounds. Advanced concepts such as race conditions require more background than the students have, or will have, when taking introductory programming classes. An alternate approach is to teach the underlying concepts of robust programming; preventing crashes or errors is central to such a course. This paper presents some exercises that illustrate this approach, and some thoughts on what constitutes "secure programming".

Keywords: secure programming, robust programming, introduction to programming.

1 Introduction

Secure programming is a misnomer. A program may be secure under one set of conditions, and yet be woefully non-secure under a different set of conditions. As an example, a program that limits access to a resource to a few specified, authenticated users is secure when the goal of the system is confidentiality, but not when the goal is accessibility and the resource intended to be publicly available. For this reason, introductory programming classes should focus on much more concrete properties of programs: *robustness* and *correctness*. One can then introduce "security" in a later class as a collection of necessary (or desirable) properties for correctness, and the students will have the background to be able to focus on the *security* issues, knowing the robustness and correctness issues.

A second aspect of secure programming lies in design. When presented with a problem, students often try to program the most direct solution. Sometimes, a few minutes' thought will lead the student to a much simpler, easier program. The trick is learning how to look beyond the statement of the problem to what the problem is trying to solve. Like understanding unstated meanings in talking with other humans, being able to see the essence of a problem may make the problem much easier—or point to a deeper problem that must be solved.

Section 2 discusses several programming exercises for introductory classes. These exercises illustrate various aspects of robust programming. Section 3 presents a

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 226–232, 2013.

problem that appears straightforward, but has an interesting subtlety of design. Section 4 discusses some aspects of a programming language suitable for introductory programming classes. Section 5 presents some concluding thoughts.

2 Robustness

Robust, or *bomb-proof*, programming is a style that prevents programs from acting unexpectedly, for example terminating abnormally. The basic principles of robust programming are:

- *Paranoia*. If your program or library doesn't generate it, don't trust it.
- *Stupidity*. Assume the user or caller won't understand your interface, and will send anything through it.
- *Dangerous implements*. If any data structure is visible to the user or caller, assume it will change between references.
- *Can't happen*. If you are sure it can't happen, check for it and return or print an error.

These basic principles underlie a myriad of security problems. As an example, the CWE/SANS Top 25 Most Dangerous Programming Errors [1] cites 9 weaknesses that arise from insecure interaction between components—in other words, by sending incorrect data through the interface, violating the principle of stupidity. The OWASP Top Ten project [2], which identifies the most serious web application vulnerabilities, cites cross-site scripting as the top problem and injection flaws (such as SQL injection) as the second most common problem. Both of these involve ignoring the principle of paranoia because it is trusting data that the program did not generate or check. Students who learn these principles and practice them are much less likely to create software with these problems.

The problems below were given to several classes during a first course in C programming. They can easily be adapted to work with other languages.

2.1 Demonstration of the Problem

One of the ways to impress upon students how important these principles are, and how often they are violated, is to give them an exercise that demonstrates problems with standard functions and libraries.

Problem. Please write three programs that use functions from the standard I/O library. You are to call the functions in such a way that they cause the program to crash, or generate unpredictable results. To demonstrate crashing, use output from *gdb*(1) to show that the crash occurred within the standard I/O library. To demonstrate unpredictable results, run your program without changes on at least two different types of computers in the student laboratories. Note that you ***must*** supply the correct type of argument for the function. You may not, for example, pass a character pointer when a file pointer is expected.

This problem is typically given near the end of the first course in programming, when the students have a basic knowledge of debugging, have used *gdb* to find bugs in programs, and have worked with the standard I/O library.

The (admittedly anecdotal) responses to this question are interesting. At first, the students are nervous because they don't believe they will find anything. Then one or two students will find something, and suddenly many of the students will become excited, and tackle the problem. It generates quite a bit of discussion, especially about the assumptions that the authors of the library made, and the environment for which the library was designed.

About 10 years ago, this problem was surprisingly easy; calls with **NULL** file pointers, or negative numbers, worked like a charm. Recently, though, the robustness of many versions of the standard I/O library has improved, increasing the difficulty of this problem. Thus, now this problem would probably be more suited for a second course in programming. For the introductory course, other libraries provide the (lack of) robustness required for this exercise.

The complement of finding errors is preventing them. This is the topic of the next exercise.

2.2 Handling Procedure and Function Errors

This problem puts the students in the position of the programmer, and has them program defensively. It deals with converting a string to an integer, a topic that causes problems because the students must deal with many possible errors.

Problem. The function *atol*(3) takes a pointer to a character string as an argument and returns the integer value corresponding to that string. Unfortunately, it has several problems:

- Overflow is not detected;
- If the string is not a valid integer, it converts as much of the string as it can and then stops; and
- Most implementations do not handle a leading "+" sign.

Implement a new function called *natol* (for *n*ew atol) that handles all these problems. Your function must have the interface:

```
long natol(char *numstr, int *errcode)
```

where *numstr* is a pointer to the string whose integer value is to be returned, and *errcode* is a pointer to an integer variable which, when *natol* exits, has one of the following values:

0. no error has occurred; or
1. *numstr* points to something that is not a valid decimal integer (this includes *numstr* being **NULL**); or
2. overflow occurred, and the number being read was positive. The result of the function is undefined (that is, you can make it return anything you like, but it must return *something*); or
3. overflow occurred, and the number being read was negative. The result of the function is undefined.

This problem teaches students how to handle errors within library functions. The functions should communicate the error back to the caller, so the caller can handle the error appropriately. Having the library write an error message to the standard output or error (or some other I/O stream) without documenting that side effect can cause serious problems should the caller be producing output in a particular format.

This problem also has a design aspect to it. Checking for overflow in a language-independent way is not at all obvious, especially to beginning students. The obvious approach, checking succeeding values until the absolute value of one is smaller than the absolute value of its predecessor, doesn't always work. The correct technique uses division. As this routine iterates over the characters in *numstr*, it appends one digit per iteration; thus, the check need only confirm that the digit being appended does not cause overflow. The key idea is not to append the digit; rather, it is to determine the maximum digit that *could* be appended without causing overflow. The students have to be careful programming this to avoid causing overflow when checking for overflow.

2.3 Handling Input Errors

A third problem extends the idea of checking for errors to user input by building on a common exhortation in C programming: avoid the use of *gets*(3), an input function known vulnerable to buffer overflow. Students are taught to use the function *fgets*(3), which requires a parameter indicating the size of the array in which the input line is to be stored. The subtlety of *fgets* is that if the line is too long, only that part of the line that fits into the buffer is read. The next invocation of *fgets* begins reading where the previous invocation left off. This exercise provides a more intuitive interface. The function either provides the entire line, regardless of length, or (for backwards compatibility) can act like *fgets*.

Problem. Write a C function called *dyngets* that reads an input line of arbitrary length from a given file descriptor. The interface to *dyngets* is to be:

```
char *dyngets(char *buf, int n, FILE *fp)
```

On entry, `if buf` is not **NULL**, then this function acts exactly like *fgets*(3).

If `buf` is **NULL**, then it and the second parameter, `n`, are ignored. On exit, *dyngets* returns a pointer to an internal buffer containing the input line. This internal buffer is allocated using *malloc*(3) or *realloc*(3). If the line is too long to fit in the currently allocated internal buffer, the buffer is grown to be long enough to hold the full line. The return value is **NULL** on end of file or error.

You are to allocate the internal buffer for *dyngets*, and you must reuse the internal buffer whenever *dyngets* is called. This buffer should be allocated using *malloc* on the first call to *dyngets*, and as you read longer and longer lines, use *malloc* to allocate a new buffer and *free*(3) to free the old one, or *realloc* (with appropriate error checking) to change the length of the buffer.

This exercise requires students to manage memory in a way that is invisible to the caller. Common mistakes are to make the internal buffer visible externally, violating

the principle of dangerous implements, or not properly handling the internal buffer by either deallocating it at the beginning of each invocation, or failing to check the return value of *realloc*.

A second subtlety arises from the emulation of *fgets*. As the second argument is an integer, students must check that it is a non-negative integer. Although *fgets* should check this, some versions do not, and this causes unpredictable behavior.

2.4 Assuming the Obvious: Does 1 == 1 Always?

Students who first encounter floating point numbers do not realize that they represent a subset of the set of real numbers, and that the differences can adversely affect calculations. Some real numbers can be expressed exactly (such as 1/2), but others have no such floating point representation (such as 1/7). This exercise poses the question of "what does a floating point 1 represent on a computer".

Problem. Every computer is limited in the amount of precision it can represent for floating-point numbers. At some point, where `epsilon` is very small, the following expression will be true:

```
1.0 == 1.0 + epsilon
```

Write a program to find the largest value of `epsilon` on your computer for which the above is true. Note that the value of `epsilon` may be different for floats and doubles. Find both values (and the value for long doubles if your compiler supports them).

This exercise has two effects. The first is to show students why one needs to question assumptions. Unless students understand how floating point numbers are represented (a topic often omitted in introductory courses), the discovery that *epsilon* can be non-zero helps them understand the need to follow the principle of "can't happen". Something that appears to be wrong is, in fact, correct!

The second is an interesting design question. Some students will treat the expression as an *algebraic* expression, and instead attempt to find the smallest value for *epsilon* that is equal to 0.0. That approach fails because very small floating point numbers can be distinguished from 0, but when added to 1, the precision of the floating point number is reduced considerably. That is, most computers can represent the real number 2^{-63} exactly, but cannot represent the real number $1+2^{-63}$ exactly, due to limits on the size of the mantissa. So the algorithm the students design must take this into account.

2.5 Summary

This section presented four problems that require students to take care to avoid non-robust behavior: incorrect results or program crashes. The first demonstrates that system libraries, on which programs rely, may be non-robust. The second and third problems encourage the students to apply the principles of robust programming to make their library routines "solid". The fourth challenges a simple yet common idea

among students taking an introductory programming class: that computers are precise and exact. In fact, they are not, particularly when dealing with floating point numbers.

Two of these problems had design components. We now focus on that aspect exclusively.

3 Design

Robust programming favors simplicity and elegance of algorithm. It is much easier to avoid unnecessary interfaces and poor coding when the program is simple and straightforward. Often, complex or long problems have simple solutions, and when they do, spending time to find that solution is well worthwhile.

The Monty Hall problem is a wonderful problem for teaching principles of robust design. It is based on the old TV game show *Let's Make a Deal*. In that show, the moderator, Monty Hall, would select a member of the audience, and offer them a valuable prize. The prize was behind one of three doors. Behind the other two were joke prizes, like a goat and a can of paint. The member of the audience would select one of the doors (say, door number 2). Monty would then say, "Before I show you what's behind door number 2, let me show you what's behind door number 1." Door number 1 would open, to show the can of paint. Then Monty would ask if the player wanted to change to a different door. The question is, should the player do so?

The intuitive answer is that it doesn't matter. As the door Monty opens always has a joke prize, one of the two remaining doors has a joke prize, and the other has the valuable prize. Hence the valuable prize is equally likely to lie behind either door.[1]

Problem. Write a program to simulate 100,000 iterations of the Monty Hall problem. Use the simulation to demonstrate whether it is to the player's advantage to change doors. Please explain your results.

When given in an introductory programming class at UC Davis, student assignments used essentially the following algorithm (iterated the requisite number of times):

```
choose a random door for the valuable prize
player chooses a random door
Monty shows player a door without the valuable prize
generate a random number between 1 and 2 inclusive
if that number is 1, player changes door
if player's door is same as door with valuable prize, increment counter
```

[1] The correct answer requires the student to remember there are *three* doors, not two. The probability that the initial selection is the door with the valuable prize is 1/3. The probability that the valuable prize is behind one of the other two doors is 2/3. When Monty opens a door, that door cannot contain the valuable prize. Thus, the probability is 2/3 that the unselected, unopened door is the door with the valuable prize. So it is to the player's advantage to change her selection.

At the end, the program divides the counter by the number of iterations for the probability that the player will get the valuable prize should she change doors.

A much simpler solution arises when one notices that the number of the door Monty shows is irrelevant. It will *never* be the one with the valuable prize. So, all that matters is whether the player's initial choice is the door with the valuable prize. If it is not, the switch will give the player the valuable prize. If it is, the switch will give the player a joke prize. Thus, the following algorithm also solves the exercise:

```
choose a random door for the valuable prize
player chooses a random door
if player did not choose door with valuable prize, increment counter
```

The probability is computed as before.

The reason this problem is so useful is because the correct answer is counterintuitive, unless you look at the problem in the right way; and the simulation appears to give the wrong answer. Thus, this problem forces the students to analyze their design in detail.

While this program is not, strictly speaking, security-related, it teaches the students skills they need for secure programming. They learn how to ask what the goal of the problem is and focus on meeting that goal, rather than simply choosing the obvious approach. They also see what happens when the mechanism does not work as expected; they learn to question the expected result and analyze it, to see if it is in fact correct. This skepticism is critical to being able to determine the assumptions that a program relies upon—a key aspect of secure programming.

4 Conclusion

The rudiments of secure programming lie in the first programming classes all students take. By emphasizing careful design, robustness, and correctness, those courses can lay a foundation upon which advanced classes can teach programming that deals with specific security problems. Without such a foundation, all the instruction into how to code securely will do little to improve the state of software security.

Acknowledgements. This paper is an expanded version of a working paper given at the Secure Coding Faculty Workshop sponsored by the National Science Foundation and SANS held in April 2008.

References

1. Christey, S.: CWE/SANS Top 25 Most Dangerous Programming Errors (March 10, 2009), `http://cwe.mitre.org/top25`
2. Williams, J.,Wichers, D.: Top 10 2007 (2007), `http://www.owasp.org/index.php/Top_10_2007`

A SWOT Analysis of Virtual Laboratories for Security Education

Alan Davidson, Javier de La Puente Martinez, and Markus Huber

Department of Computer and Systems Sciences,
Stockholm University/Royal Institute of Technology, Sweden
{alan,jdlpm,mhuber}@dsv.su.se

Abstract. Work is active in many institutes of higher education on utilising virtual computer environments for creating laboratories for practical course-work. Computer Security education is one area where virtual environments are proving to be useful, and where several schools have reported their own schemes for implementing environments for practical exercises. In this study we attempt to take a somewhat broader look at what the use of virtualisation technology can imply terms of a number of factors, i.e. the pedagogy, security, licensing, administration and cost. A simple analysis of the general strengths, weaknesses, opportunities and threats of virtual security laboratories allows us to motivate design choices when implementing yet another of these experimental environments.

1 Introduction

Latest developments in virtual computer environments are encouraging a spate of experiments with building virtual laboratories for use in education. Many of the advantages are clear and oft cited, such as how virtual machines allow for efficient use of hardware, and how they can ease system administration.

Courses in ITC security often have special requirements when it comes to their practical laboratory environments. The tools and environments used many times require a student to have administrator privileges. This can create problems if students, either maliciously or by accident, can cause damage to their own environment or others'. Some educational tools, such as virulent malware, or techniques, such as sniffing and password cracking, can be dangerous things to have in a normal working environment. The kind of virtualisation that has been termed *platform virtualisation* [1] therefore seems especially applicable in solving several problematic issues that are typical for ICT security courses.

An existing sandbox laboratory run by the SecLab group at the Department of Computer and Systems Sciences at Stockholm University has previously been used to allow students a practical test environment. Computers within the sandbox were are fitted with removable hard drive cassettes for the computers' operating systems which allowed students to have administrator privileges for their system without affecting the computers. They simply kept the removable cassettes for the duration of their experiments. The sandbox is segregated from the

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 233–240, 2013.

rest of the department's computer networks with a firewall that allows only outgoing HTTP requests. The firewall machine also implements an operative image server which allows students to recreate their environments from scratch in case they should suffer irreversible problems. Various physical devices such as extra network interfaces, cables and hubs are kept in the laboratory allowing students to build sub-nets and connections as any exercise might require.

A number of standard practical exercises for differing operating systems have been devised for execution in the sandbox laboratory. Apart from these we have had an initiative to allow students themselves to create their own experiments and pass them on to others [2]. Though this laboratory has been successful the possible advantages of running an equivalent virtual laboratory have prompted the authors to investigate further.

Several similar projects to utilise virtualisation for diverse ICT security learning environments have been documented [3,4,5,6,7,8,9,10]. Such experiments are encouraging, yet when it comes to implementing our own virtual version of a laboratory we find that there are several general questions that we can identify and that we hope to address:

- Pedagogy. What kind of pedagogical issues are there when moving from a physical environment to a virtual one? Can students learn the same things in either kind of environment?
- Security. Since we are working with potentially dangerous tools and methods we need to be sure that they are efficiently contained. What additional security advantages or problems can one expect with virtual environments?
- Cost. Virtual environments are often touted as being particularly economical. They allow for maximum use of hardware capacity. But moving to virtualisation will have its own costs, as will running the virtual environment. How can these costs be kept to a minimum?
- Administration. As with cost, ease of administration is often cited as one of the major advantages of virtual environments. How true is this in teaching environments?
- Licensing. Software licenses for physical machines are relatively easy to handle since the number of licenses relates to the number of machines. How does this situation relate to the licensing of innumerable virtual machines? Are the opportunities for pirate copying of university licensed software any different when using virtual machines.

These were the main questions that we bore in mind when studying previous virtualisation projects and when designing our own.

2 A SWOT Analysis

In order to gain some perspective over the issues we attempt to structure them according to a simple SWOT analysis, i.e., the strengths, weaknesses, opportunities and threats of virtual environments. We include in the concept of virtual environments both platform virtualisation and virtual networking. We avoid

general virtual machine issues in order to concentrate on the implications for a security laboratory.

2.1 Strengths

Virtual environments allow us the possibility to give students administrator privileges. This is also possible with the physical laboratory described above. With hard drive cassettes however, one does have to be physically present in the lab to run an individual student machine. One could imagine a system of allowing students to connect to physical machines through VPN connections, thereby freeing them from working in the physical environment. However, the combination of allowing students to control their own image of a system and to be able to work from a distance is only achievable through virtual machines.

Virtual machine implementations invariably have simple means to save the state of the system, and allow roll-back to such states. When students work with administrator privileges and with security tools that manipulate complex systems the opportunities for misconfiguration and accidental damage are many. The safety and ease of administration that virtual machines offer is one of their primary strengths. [8]

It is generally true that virtual machines are scalable for the task at hand. In a security laboratory there can be several situations where this is particularly relevant. Take for example a firewalled network experiment with three machines, a machine representing a network to protect, an attacker machine, and a dedicated firewall machine between the two. Though the protected machine may have a fully fledged operating system, the attacker would only need a minimal system to run attack tools. The firewall would be a run on an absolute minimal operating system. Running such an environment on physical machines would be less than effective use of hardware.

Versatility in networking scenarios and services is a central requirement in networking security education, and can be supported by virtual environments [11]. In a physical environment students can reconfigure networks by moving cables, switches, hubs etc. But this can also be achieved in virtual networks, and what is more, system images with varieties of services can be kept on cheap secondary memory ready to be placed in a network at a moment's notice.

Cost savings are possibly the most commonly cited reason for employing virtual architectures in general. This is a noticeable issue with our physical laboratory where security exercises are not run all year round, and because of sensitive nature of much of the equipment and software that is used in this laboratory, it is unsuitable to run other courses in parts of this laboratory in the interim. Machines lie dormant, whereas if the environments were virtual they could be more easily swapped out to accommodate other laboratory situations. Furthermore, it has been proposed that server based virtual machines can also give a new lease of life to an old and tired machine park as it can effectively be utilised as smart terminals to interface with the server [12].

Cost savings with virtual environments are most often associated with efficient use of hardware. There are however issues of software costs to consider as well. Cost could well be counted as a weakness in that commercial virtualisation solutions come with a commercial price tag. Given that there are a number of fully workable open source and freeware solutions available such as VirtualBox, KVM, Qemu, etc. the cost of software is well within the security laboratory's typically shoestring budget. What the true cost of free software is may be the subject of constant debate, but in practise we have found that these "free" solutions are practically feasible without prohibitive administrative overheads.

2.2 Weaknesses

Virtual machines are good versatile tools in as much as they implement a level of abstraction above specific hardware. This level of abstraction in turn comes with the cost of loss of computing power. A number of typical security experiments such as encryption, key and password cracking, vulnerability scanning, etc. are demanding on computational resources. We could expect such heavy operations to be slower. The problem is mitigated by continuing developments in virtualisation technology, and modern processors may be expected to have hardware acceleration for virtual machines.

Computing environments are general, integrated tools where all manner of uses are concentrated into a single versatile machine. With virtual machines we are creating segregation within that environment. Where communication between tasks is simple on an integrated environment, it can be painful across segregated virtual environments. For the security laboratory this problem is noticeable in the way that results from an exercise should be included in the students hand-in documentation. If the documentation is done within the secure environment then there may be extra effort involved in extracting that documentation to a normal study environment where hand-ins can be accepted. If the documentation is done in a study environment then there will be the problem of extracting result from the secure environment. One might also expect computer screens to become easily cluttered with windows to virtual machines overlapping with text editors, email agents, and other such tools necessary for normal student activities.

Perhaps the trickiest issue is how we with virtual environments are attempting to imitate real environments, and we are attempting to teach lessons about real environments. In some cases the difference will no doubt be negligible, such as if we are only experimenting with the use of a software tool within a single machine environment. But if we replace building networks with cables, switches and hubs with building virtual networks through a software interface, how can we be sure that we are not missing out on vital parts of the learning experience? Furthermore, there will be an overhead involved in teaching the student how to cope with virtual environments that may not be as intuitive as interacting with a physical world.

2.3 Opportunities

Among the strengths that we noted above is the idea that one can both allow students to control their own environments, yet not restrict them to a physical locality. By connecting to a virtual machine server it can be possible to run exercises within a secure environment from a distance. It may also be possible to supply students with a secure environment that could be run virtually completely within their own computers. This would not only free up some of the universities own computers, but also potentially provide a means to hold distance education with practical exercises that would previously have been implausible without requiring the students to occasionally come to the physically secure laboratory.

Some security experiments have been difficult to implement in our physical laboratory. A case in point is a firewall exercise that was developed for a group of some 16 students simultaneously using eight computers. Two more computers in the laboratory were used by staff to act as on the one had the machine under attack and on the other hand the attacker. The students were in turn required to configure each of their machines to act as firewalls between the staff machines. Each attack required constant re-routing of network traffic through each of the firewalls. With virtual architectures, each students machine can be given their own internal network of three machines or more, completely and independently set up to run attacks from one machine to the others, while the student is required to properly configure the virtual firewall. Virtual environments can therefore be used to implement experiments that are difficult, if not unfeasible, in a physical network.

2.4 Threats

The above discussion on the weakness of virtual environments in terms of how they segregate working environments may have greater implications than just the practical difficulties. Some kind of connectivity will always be a practical advantage. In our own physical laboratory we choose to allow limited access to the outside world by opening port 80 for outgoing HTTP requests. This allows the student the ready source of information that they have come to expect in all walks of life, as well as access to security tools, malware and exploits. We find that this amount of access encourages students' individual initiative during exercises. Furthermore we allow students to use removable media to transfer materials to and from the secure environment, in particular to aid in their documentation of their work. There are methods to strongly segregate virtual networks [10] while virtual machines implemented with jails are useful when high level security is preferred, but it will of course be at the cost of connectivity. The ever present desire for connectivity is a potential security hazard as the tools and methods used within the secure environment may be difficult to contain.

We might have included the security of virtual environments as one of the strengths. It is true that in the laboratory environment the student will presumably be running the virtual machine within an unprivileged account, so even if the virtual machine itself is running with administrator privileges, it can presumably do little damage to the host environment, beyond the possible containment

problems discussed above. Nevertheless, the authors believe that the security of virtual machines is today overstated. It is not uncommon to equate the segregation of virtual environments with strong security but we have found no clear evidence that security is a goal of modern virtual machines. We must surely assume that the software that implements virtual machines is not intrinsically more secure than other general purpose software, which indicates that we should not assume that containment can be trusted. On the contrary we do see results that indicate that it is possible to programmatically verify that a process is being executed within a virtual machine [13]. This is surely a precursor to malware types that will be able to detect and to break their way out of virtual environments. We therefore prefer to take a conservative point of view on the security of virtual machines, and suggest that until the opposite can be shown, security laboratories run in virtual environments should be regarded with care and scepticism.

Problems with licensing might also be a reason to hold back on the implementation of virtual laboratories. The very portability of virtual machines means that it is simple to move a virtual image from one host to another. Insofar as licensing agreements that a school enters into require due diligence from the licensee to avoid spreading copies of the licensed software, this may be very difficult to uphold. A virtual image that contains licensed software can easily be copied and used on any number of other hosts. Perhaps the only means of limiting such use is though the enforcement of local security policies.

Another licensing problem is due to the way software companies specify the number of licenses. It is common to specify the number of machines that the software is to be installed upon. With easily copyable virtual environments it becomes far more difficult to calculate and control the number of machines that the software is installed upon, and it is a problem that current licenses specify limits on such numbers [4]. It would surely make better sense to have licenses that stipulate the number of copies that may be used concurrently [12].

3 Yet Another Virtual Security Laboratory

When implementing our own virtual version of our successful physical laboratory the above discussions have steered us to a number of design choices.

For reasons of security, administration and pedagogy, we have steered clear of solutions that involve installing virtual machines on the students own computers. It would be possible to implement administratively simple solutions such as providing so called live CDs i.e. bootable systems contained on a CD that could avoid starting the users own system and instead start a virtual environment. However, without considerable work on validating the security of such environments we regard the possibility of accidents that could violate the security of the students local environment as too high.

Our preferred solution is to have a central server for virtual machines. The virtual network is interfaced with that of our existing security laboratory, allowing the two environments to mix for seamless experimentation. A separate

network interface allows the host server itself is to be accessed via department general purpose network, i.e., students easily access the server from the Internet, but the virtual machines that they start are automatically linked to the security laboratory network. Simple shell scripts allow students to copy, start and connect to their virtual machines via VPNs. There are two alternative ways to access the virtual machines: X-forwarding and VNC, both of them encapsulated in a SSH tunnel. If the user accesses the server from the university's facilities, X-forwarding is the preferred method. On the other hand, if the student accesses the server from a remote location where limited network capacity makes the X-forwarding impractical, VNC has proven to be a workable alternative. The server we are using is an IBM System x3450 running the x86-64 version of Debian GNU/Linux OS.

To avoid licensing difficulties as well as to keep down costs we have chosen virtual environment software that is open source, i.e. KVM (Kernel-based Virtual Machine) and Virtual Quare's VDE (Virtual Distributed Ethernet). KVM provides a core infrastructure for native virtualization and a modified version of QEMU is used to run the virtual machines themselves. VDE is compatible with QEMU and supports the creation of a virtual distributed Ethernet based on virtual switches and virtual crossed cables. The virtual machines themselves are to the larger part based on and configured to use open source software. The notable exception here is the use of Microsoft Windows XP, where the relatively liberal Microsoft educational licensing policy allows us to provide students with an environment that they generally have better experience in.

Our environment is still under development, and has not yet been subject to full class deployment. Our ambitions for the near future are to implement simple web based control interfaces similar to those described in [14] to replace the control scripts that we have today. We are also developing a java based interface to the VDE virtual network software that will hopefully help to bridge the pedagogical gap between handling physical and virtual networks.

We have argued that costs can be kept to a minimum with the use of open source software for administering virtual environments, yet the work involved in designing and implementing this environment has been considerable. In our case we were provided a grant from the Royal Institute of Technology in Stockholm that was equivalent to some two person-months of paid time, as a project to further develop our teaching environment. We suspect that without such an injection of funds it would be very difficult to transition easily to such a solution.

References

1. Ramanathan, R., Bruening, F.: Virtualization: Bringing Flexibility and New Capabilities to Computing Platforms. Technical report, Intel Corporation (June 2004)
2. Davidson, A., Näckros, K.: Practical assignments in IT security for contemporary higher education. In: Futcher, L., Dodge, R. (eds.) World Conference on Information Security Education. IFIP, vol. 237, pp. 25–32. Springer, Heidelberg (2007)

3. Bullers Jr., W., Burd, S., Seazzu, A.: Virtual machines-an idea whose time has returned: application to network, security, and database courses. In: Proceedings of the 37th SIGCSE Technical Symposium on Computer Science Education, pp. 102–106. ACM, New York (2006)
4. Hay, B., Dodge, R., Nance, K.L.: Using virtualization to create and deploy computer security lab exercises. In: Jajodia, S., Samarati, P., Cimato, S. (eds.) SEC. IFIP, vol. 278, pp. 621–635. Springer, Heidelberg (2008)
5. Hu, J., Cordel, D., Meinel, C.: A virtual laboratory for IT security education. In: Feltz, F., Oberweis, A., Otjacques, B. (eds.) EMISA. LNI, vol. 56, pp. 60–71. GI (2004)
6. Hu, J., Meinel, C.: Tele-Lab IT security: A means to build security laboratories on the web. In: AINA (2), pp. 285–288. IEEE Computer Society (2004)
7. Kato, K.: Modeling and Virtualization for Secure Computing Environments. In: Cervesato, I. (ed.) ASIAN 2007. LNCS, vol. 4846, pp. 196–197. Springer, Heidelberg (2007)
8. Keller, J., Naues, R.: A collaborative virtual computer security lab. In: e-Science, p. 126. IEEE Computer Society (2006)
9. Kuczborski, W.: A computer network laboratory based on the concept of virtual machines. In: Proc. 6th Baltic Region Seminar on Engng. Educ., pp. 145–148.
10. Sun, W., Katta, V., Krishna, K., Sekar, R.: V-netlab: An approach for realizing logically isolated networks for security experiments. In: Benzel, T. (ed.) CSET. USENIX Association (2008)
11. Alexander, M., Lee, J.A.: A scalable xen and web-based networking course delivery platform. In: Parker, J. (ed.) Proceedings of the Second IASTED International Conference on Education and Technology, Calgary, Alberta, Canada, pp. 131–134 (July 2006)
12. Nastu, J.: Software virtualization: Virtual desktops offer ed-tech revolution. eSchool News, 21–27 (May 2008)
13. Raffetseder, T., Kruegel, C., Kirda, E.: Detecting System Emulators. In: Garay, J.A., Lenstra, A.K., Mambo, M., Peralta, R. (eds.) ISC 2007. LNCS, vol. 4779, pp. 1–18. Springer, Heidelberg (2007)
14. Kneale, B., De Horta, A., Box, I.: Velnet: virtual environment for learning networking. In: Proceedings of the Sixth Conference on Australasian Computing Education, vol. 30, pp. 161–168. Australian Computer Society, Inc., Darlinghurst (2004)

Determinants of Password Security: Some Educational Aspects

Lynette Drevin, Hennie Kruger, and Tjaart Steyn

Computer Science & Information Systems
North-West University, Private Bag X6001, Potchefstroom, 2520
South Africa
ldrevin@acm.org, {Hennie.Kruger,Tjaart.Steyn}@nwu.ac.za

Abstract. Development and integration of technology give organisations the opportunity to be globally competitive. However, the potential misuse of Information Technology (IT) is a reality that has to be dealt with by management, individuals and information security professionals. Numerous threats have emerged over time in the networked world, but so have the ways of alleviating these risks. However, security problems are still imminent – as highlighted by the plethora of media articles and research efforts. The insider risk is stated as being around 80% of security threats [1] in a company. With this statistic in mind, management has to plan how to allocate resources to counteract the risks. Very often, simple measures such as good password behaviour are overlooked or not rated high enough to include in all security awareness programmes. This paper will focus on a study that assesses password management of future IT professionals. It will be demonstrated how management and educators can use these results to focus their efforts in order to improve users' password practices and thereby enhancing overall IT security.

Keywords: Password management, ICT security awareness, Pareto analysis, cause-and-effect diagrams, password strength and confidentiality.

1 Introduction

With the increased usage of information systems and e-business, it has become important to protect information against a wide variety of threats, such as social engineering attacks leading to phishing and identity theft, viruses, spyware, and denial-of-service attacks. There are users in the networked world who are adequately protected, but many individuals are novice users who are ignorant or simply unaware of these vulnerabilities. They spend hours online on social network groups, online banking applications and other systems. Businesses have also changed work practices. Many e-applications are currently in use, such as e-commerce, e-government and e-health. With the use of these and other applications, the previously mentioned risks also pose challenges to the management of organisations that need to allocate budgets to every aspect of business – including the protection of information resources. Information security includes not only technology solutions but also people [2]. One

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 241–248, 2013.

of the most basic and important aspects of protecting access to applications and information is authentication. Users, employees, and management are all subjected to authentication processes to restrict access to authorised persons only. There are different ways to authenticate users, such as the use of a physical token (e.g. something you have), secret knowledge (e.g. something you know), or biometrics (e.g. something you are) [3]. Commonly used is the mechanism of passwords. Studies have shown that the behaviour of users in this regard is not always of a high standard; therefore, the quality of password security is impeded [4], [5]. Users should be made aware of what good password behaviour entails, how to manage their passwords and what the related risks are.

One could argue that the last word has been said about password management, as much has been published on password usage and behaviour. However, it remains highly topical, as can be seen in recent research publications. Examples include graphical passwords [5], social practice of passwords [6] and improvement of passwords through persuasion [7].

Bearing in mind the increase in the number of information users and online applications and the resulting risks, a study was undertaken to provide some insight into the determinants that may impact the standard of password management and behaviour of users. In this study, a measuring instrument was developed and certain techniques applied in order to identify and prioritise important factors when assessing future IT users' perspectives on password usage.

The important password management determinants that emerge from this study will allow management and educators to expend their efforts in order to improve password practices. The remainder of the paper is organised as follows: In section 2, the background to the exercise is given. Section 3 discusses the methodology used. Section 4 details the results of the study, and section 5 presents some concluding remarks.

2 Background

This study stems from a framework developed during 2006 to evaluate ICT security awareness levels [8]. One of the key areas identified in this framework was the acquiring of appropriate data that could be useful to evaluate knowledge and behaviour of users. Password-related information was part of the required data. It was decided to focus this study on evaluating password management and behaviour of students who are the future IT users and IT business leaders.

The literature gives numerous examples of good password practices [4], [3], [9]. Studies to improve authentication through the use of passwords are also in abundance and guidelines are given to address password insecurities [10], [5], [6].

Users from all backgrounds and educational levels use IT and online applications; therefore, the advice given in literature on how to increase password efficiency can be applied by all. As mentioned, this study focuses on students in a university environment and on the assessment of their password practices. Universities are managed and operated these days in much the same way as other businesses, although

their main activities are education and research. They also rely heavily on ICT resources and should therefore be secured so as to adhere to the confidentiality, integrity and availability principles. Student users are given access to systems and applications mainly via user accounts and passwords. They are restricted to their own systems and networked areas and should not have access to university systems containing marks, examination papers, financial data, etc. Failing to keep passwords confidential and making use of passwords that can easily be guessed could result in considerable financial losses and/or examination irregularities. Apart from the usual dishonest behaviour that should be avoided, it seems appropriate to assess the password behaviour and attitudes of young people. They are the IT users and ICT professionals of tomorrow and should be educated about threats and consequences of inadequate password practices.

We viewed effective password management in terms of two categories – *strong or secure* passwords and *confidentiality* of passwords. It is assumed that these two aspects define "good" and "poor" password practices. The two categories were derived from existing literature that provides guidelines on the use of passwords [4], [12].

Strong or secure passwords include principles such as:

- Choose long passwords
- Change passwords often
- Avoid names or dictionary words

Confidentiality of passwords includes principles such as:

- Do not write them down
- Do not use the same password for all applications
- Do not tell anyone your passwords

To comprehend ineffective password management of users, cause-and-effect diagrams were constructed. Also known as an Ishikawa diagram or a fishbone diagram, a cause-and-effect diagram can be used to represent the relationship between some effect that could be measured and the set of possible causes that produce the effect [11]. The effect or problem is shown on the right-hand side of the diagram and the main causes are listed on the left. The causes can be further divided into a few major categories, depending on the problem at hand. Within each major category, specific causes can be listed as branches or sub-branches. These diagrams are useful when it is necessary to understand processes or to identify core causes of problems. The construction of the cause-and-effect diagrams was guided by the following two questions:

- "What is causing the ineffective password management of students?"
- "What factors affect the ineffective password management of students?"

The next section describes the methodology used, i.e. how the cause-and-effect diagram and the measuring instrument were developed.

3 Methodology Used

3.1 Cause-and-Effect Diagram

It was assumed that the effectiveness of password management is influenced by two main factors, namely *strong* passwords and *confidentiality* of passwords. Two cause-and-effect diagrams were constructed for these two factors, using the following two problem statements: *"Strong passwords are not used"* and *"Passwords are not kept confidential"*.

In order to establish the causes of the problems, the argument of Dark [2] was used, where human performance is described as a function of ability and motivation. This assumption provided a framework of categories that was used in the diagrams. The final cause-and-effect diagrams were developed using research strategies such as brainstorming sessions by the research team, validation against appropriate literature [4], [3], [12] and the use of pilot studies. Figure 1 shows the final cause-and-effect diagram for the confidential password problem [13].

3.2 Development and Validation of the Instrument

The construction of the cause-and-effect diagrams was followed by a data gathering process to determine the significant causes that impact the problem. This was done by converting causes identified on the two diagrams into a questionnaire. The objective was to test and empirically validate the factors that may influence the effectiveness of password management. A list of 23 causes was identified as relevant to secure passwords and the confidentiality of passwords. These causes were then grouped into main categories with the help of validation techniques such as content validation, reliability tests and construct validation. The final result was a 5-factor instrument (questionnaire) consisting of 23 items [13]. The secure/strong aspect was tested by 12 items, and the confidentiality dimension by 11 items.

In order to distribute the questionnaire, a web application was used to reach the students and to capture responses. The next section presents the results.

4 Results

The experiment was conducted at a South African university with three campuses located in three different cities – one of which was selected for the exercise. The campus has a well equipped ICT infrastructure and the students are linked to a central network that gives access to all the necessary applications that they need for their studies. Apart from a compulsory computer literacy module, no official security awareness programme is offered to the students.

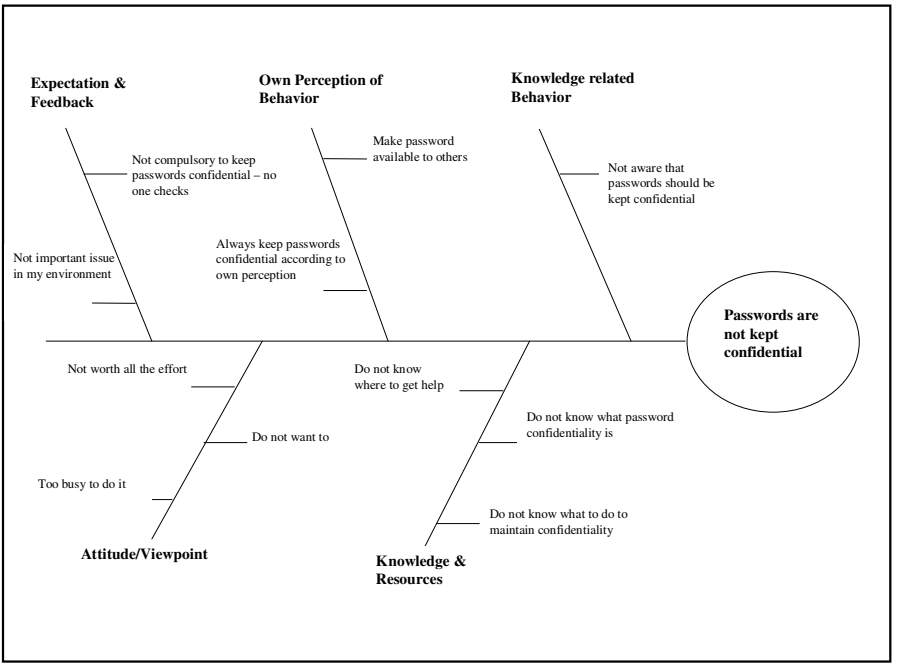


Fig. 1. – Cause-and-effect diagram for confidential passwords

Following a number of pilot studies, e-mail messages were sent to 9 different selected class groups with students ranging from first to fourth year and from different study disciplines. They were requested via e-mail and by their lecturers to complete the web-based questionnaire; 395 responses were subsequently received and completed.

The final results were presented as Pareto charts, which are graphical views with bars that are used to present information in such a way that priorities and relative importance of data can be identified. Pareto charts are often used by managers to direct efforts to the biggest improvement opportunity by highlighting the vital few causes in contrast to the trivial many [14]. The charts are constructed by arranging the bars in decreasing order from left to right along the x-axis, and the cumulative percentages are then used to assist with the analysis of the charts.

Figure 2 contains the Pareto chart for the factors relevant to confidential passwords. More Pareto charts were constructed to present the individual items that contribute to confidential passwords. A similar chart was constructed for the strong password section, which is not presented here.

From figure 2, we can see that the *Expectations and Feedback* factor is the most significant determinant that needs to be addressed in order to improve the confidentiality aspect of password management among students. Two items (“*keeping passwords confidential is compulsory in my work environment”* and *“confidentiality of passwords is an important issue in my work environment”*) were used to measure

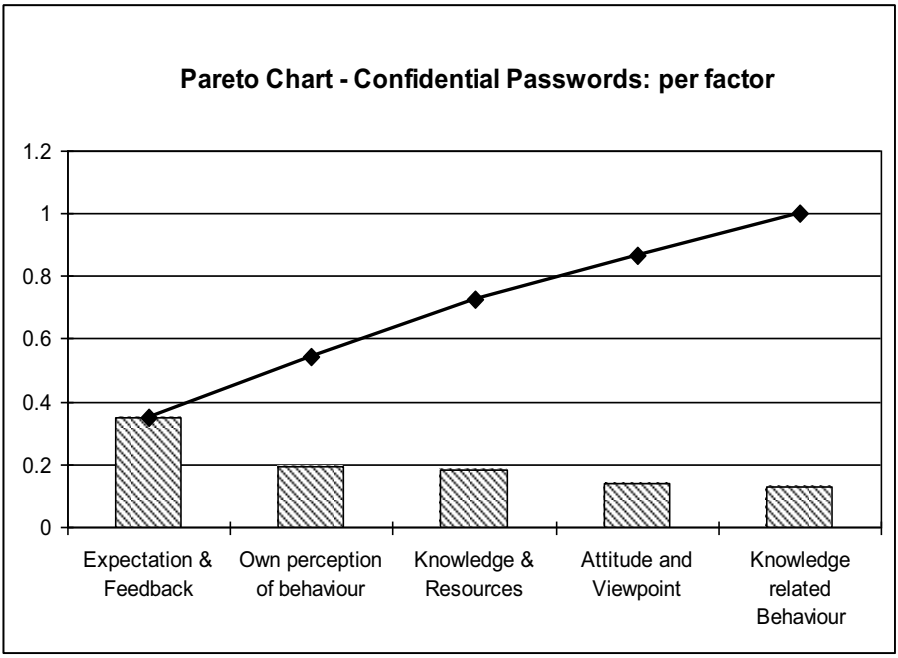


Fig. 2. – Pareto chart per factor for confidential passwords

this aspect. Based on the responses, and as shown on the Pareto chart, the perception is that the current message (feedback) that students receive from management, lecturers, their environment, their peers, etc. is that confidentially of passwords is not really important and also not compulsory. It is not really expected of students to keep passwords confidential and the practice thereof is not verified. When interpreting the Pareto chart for individual items (which is not presented here), the mutual importance of each item can also be established to guide educational efforts. In this survey, the most important individual item, which explains almost 20% of the confidentiality problem, is: "*keeping passwords confidential is compulsory in my work environment – it is regularly checked to see if people keep their password confidential*". The next item, explaining another 18% of the confidentiality problem, is: "*I know where to get help or information regarding the confidentiality of passwords*". These pieces of information determine the important factors, so that management can address specific password behaviour and practices instead of implementing a comprehensive awareness programme. Each of the factors, as well as their related items, can be analysed similarly.

The most significant results that were revealed from this study when interpreting the Pareto charts are as follows:

- Proper use of passwords, including the use of strong passwords and keeping passwords confidential, is *compulsory*.

- Passwords are an extremely *important* aspect of ICT security and improper use will degrade the quality of security and increase the probability of a number of security risks.
- The use of simple passwords that can easily be remembered is not acceptable.
- Users should be made aware of what confidentiality entails and how to get help on this aspect of password management.
- Making passwords available to others is not allowed.

If the above five principles (relating to specific items) could be addressed in security awareness programmes, it would be possible to solve approximately 54% of the problems related to effective password behaviour. The remaining factors and their linked items can be interpreted in the same way. We could also ascertain with this tool that tomorrow's IT users generally have the necessary skills, e.g. they know where and how to change passwords; they generally have a positive attitude or viewpoint towards effective password management, e.g. they think that it is worthwhile to use strong and confidential passwords, and they do not claim to be too busy to concern themselves with strong and confidential passwords.

The above results indicate that educational efforts could be directed more efficiently to focus on problematic aspects of password behaviour.

The following section concludes the paper.

5 Summary and Conclusions

As a result of the increased usage of online applications – where passwords are almost always used in the authentication process – and the accompanying threats in the cyber world, all users need to be aware of good password practices.

This paper addressed the password management problem as an essential element in the information security education arena. A study was conducted at a university to identify the important factors that need to be addressed in order to improve password behaviour. Should an organisation be able to identify and prioritise those significant factors that have an impact on password behaviour, focused awareness programmes can be implemented in such a way that specific issues are addressed. In doing so, financial and other resources can be used more effectively and efficiently. It was shown that tools such as Pareto charts can be valuable. These charts can help identify the important determinants influencing password behaviour among IT users. Educational programmes should include these important factors. [1]

References

1. Walton, R.: Balancing the insider and outsider threat. Computer Fraud & Security, November 8-11 (2006)

[1] This paper is based upon work that was financially supported by the NRF: Grant Number FA200703080000. The opinions expressed in this paper are those of the authors.

2. Dark, M.J.: Security education, Training and Awareness from a Human Performance Technology point of view. In: Whitman, M.E., Mattford, H.J. (eds.) Readings and Cases in the Management of Information Security, pp. 86–104. Thomson Course Technology, Boston (2006)
3. Burnett, M., Kleiman, D.: Perfect Passwords. Selection, Protection, Authentication. Syngress (2006)
4. Pfleeger, C.P., Pfleeger, S.L.: Security in Computing, 4th edn. Prentice Hall, Upper Saddle River (2007)
5. Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., Memon, N.: PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies 63, 102–127 (2005)
6. Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., Furlong, M.: Password sharing: implications for security design based on social practice. In: CHI Proceedings, April 27-May 3 (2007)
7. Forget, A., Chiasson, S., Van Oorschot, P., Biddle, R.: Improving text passwords through persuasion. In: Symposium on Usable Privacy and Security, July 23-25 (2008)
8. Kruger, H.A., Drevin, L., Steyn, T.: A framework for evaluating ICT security awareness. In: Proceedings of the 2006 ISSA Conference, Johannesburg, South Africa, July 5-7 (2006)
9. Gollmann, D.: Computer Security. Wiley (1999)
10. Vu, K.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B.L., Cook, J., Schultz, E.: Improving password security and memorability to protect personal and organizational information. International Journal of Human-Computer Studies 65, 744–757 (2007)
11. Berenson, M.L., Levine, D.M.: Basic Business Statistics. Concepts and Applications, 6th edn. Prentice Hall, Upper Saddle River (1996)
12. Furnell, S.: An assessment of website password practices. Computers & Security 26, 445–451 (2007)
13. Kruger, H.A., Drevin, L., Steyn, T.: Password management assessment. Technical Report. North-West University, South Africa, FABWI-N-RKW:2008-222 (2008)
14. Pareto Diagram, `http://mot.vuse.vanderbilt.edu/mt322/Pareto.htm` (accessed July 9, 2007)

Improving Awareness of Social Engineering Attacks

Aaron Smith, Maria Papadaki, and Steven M. Furnell

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, United Kingdom
cscan@plymouth.ac.uk

Abstract. Social engineering is a method of attack involving the exploitation of human weakness, gullibility and ignorance. Although related techniques have existed for some time, current awareness of social engineering and its many guises is relatively low and efforts are therefore required to improve the protection of the user community. This paper begins by examining the problems posed by social engineering, and outlining some of the previous efforts that have been made to address the threat. This leads toward the discussion of a new awareness-raising website that has been specifically designed to aid users in understanding and avoiding the risks. Findings from an experimental trial involving 46 participants are used to illustrate that the system served to increase users' understanding of threat concepts, as well as providing an engaging environment in which they would be likely to persevere with their learning.

Keywords: Social Engineering, Awareness Raising, Learning Sciences.

1 Introduction

Social engineering relies on techniques such as influence and persuasion to deceive victims into breaching security and divulging their most sensitive information [1]. A successful social engineer is extremely adept at convincing people that he/she is someone he/she is not. Through this method of manipulation, unauthorised entities can gain access to personal information or secured systems that, by rights, they should never have access to. This makes the social engineer an extremely dangerous adversary, who is often able to take advantage of people to obtain information, without the use of technology [2].

The SANS institute, over the last several years has publicised a worrying statistic within the trends of social engineering, the results from several surveys reveal that these techniques at bypassing security measures are on the increase. In most high profile organisations around the world, more and more elaborate security systems are being implemented to protect the perimeter of their networks, making it increasingly more difficult for hackers to gain entry with the traditional technological attacks. These systems, although proving very successful at halting the success rate of traditional attacks, are forcing the hacking community to develop new ways to gain access, thus Paller [3] stated on behalf of the SANS institute, that social engineering seems to be a growing technique of choice for the modern hacker.

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 249–256, 2013.

The influx of success by social engineering is in no small part attributed to the lack of education amongst users of IT systems. Surveys conducted over the last five years have proved that office workers (people who should be trained to understand the importance of security) are more than happy to give away personal information and security credentials when presented with the right reward or incentive [4]. With this being the case for working professionals, it begs the question regarding home and general users, who lack any form of technical training, and their ability to identify and defend themselves against these growing internet based threats.

Due to the flexibility of social engineering, it has been branded by many security consultants as not unlike a disease, which has the ability to morph and disguise itself in new forms every time it is discovered. From this perspective, it shows exactly how social engineering can be a difficult threat to defend against, even if you, as a user are aware of the potential to this threat.

Examples of this can be seen in recent times through the introduction of more complex spam email messages, designed specifically with wording and structure to meet the statistical pass requirements of many spam filters acceptance policies. Even after methods such as this have been discovered, social engineers have shown the ability to mutate their attempt to include compressed archives, or embedded pictures as new techniques to combat the growing success of spam filters. This inability to effectively stay ahead of the growing number of methods has lead to an increasing success rate of these malicious techniques to commit identity theft, fraud and the successful building of botnet farms.

Even with all the current documentation and research that has been performed, social engineering is still not being treated with the respect it deserves. This factor can be attributed at least in part to the sheer number of traditional hacking techniques that have plagued the IT community for decades. Unfortunately this leaves attacks such as phishing, which are growing in number every day, still only being treated as an annoyance by many within the community.

Prevention of social engineering techniques is not only limited by the awareness of users to the threat, but also the effort placed by the social engineer, more than not users are falling for social engineering attacks due to the sheer level of professionalism the effort entails, websites and emails which are so convincing that even the most security conscious expert requires time to uncover the underlying malicious intent of the scheme. Emerging attacks, such as spear phishing (which are individually tailored for specific targets), provide evidence of such trends.

A great deal of the research encountered, leads to the conclusion that the most effective way to prevent successful social engineering attacks, is through the education of potentially targeted users. This defence technique, which falls into the category of semantic learning, teaches the users not only to be aware of the end results or the known attacks, but also to develop a deeper understanding of the principals behind them. This leads to users being able to recognise social engineering attacks that they may not have been originally educated about by recognising the characteristics that are sometimes common to all many techniques.

2 Social Engineering Threats

A review of the literature indicates that a great deal of work has been done by previous authors into defining the term social engineering and tracking new techniques employed by its users. This includes, but not limited to several well-known security organisations that are actively tracking the progress of this technique and attempting to define the damages caused by it. Unfortunately this seems to be the extent of the endeavour, lacking any details regarding progressive defence measures that are being developed by the security community.

Paller [3] has stated that the current levels of awareness amongst home users and businesses is insufficient to combat this growing threat; an opinion which seems to be supported by work of [5] whose efforts demonstrate users' frequent inability to distinguish social engineering attempts from genuine communications (when considered in the context of email and phishing), as well as their tendency to base their judgments upon inappropriate criteria.

Adding to this, research conducted by Greening [6] shows the results of an experiment conducted at the University of Sydney aimed at revealing the awareness of students to the vulnerabilities of social engineering. In this case, out of 338 students targeted using a simplistic email with address spoofing, 138 responded with their correct credentials. Although practical instances of such messages have become much more widespread since 1996, subsequent experiments of a similar nature do not inspire any greater confidence in users' abilities to identify social engineering attacks [7,8].

However, findings results from the Anti-Phishing Working Group show that the volume of the problem remains significant, with an average of over 25,600 unique phishing scams being identified per month in Q2 of 2008 [9]. As such, from just this vector alone, users have a significant potential to encounter social engineering, and a chance of falling victim to it if they are not appropriately attuned to the threat.

3 Promoting Awareness of Social Engineering

Although some have speculated that user education is a pointless endeavour [10], claiming that security is always a secondary concern to end-users and that the true response to enhanced security lies with applications developers, there is significant evidence to suggest that well-designed security education can be effective [11]. Indeed, web-based training, contextual training and embedded training have all been shown to increase users ability to accurately identify an attack.

A study performed by Robila et al. [12] utilised a more direct form of user education, with the introduction of a classroom discussion style environment. Subjects were included in an interactive group study session which focused on the threats of phishing and the attributes to be aware of when dealing with such threat, then allowed to take independent quizzes to test this knowledge, results from this experiment provided favourable results that users were better suited to deal with the illegitimate correspondence after their discussion orientation to the subject material.

Many of the technical social engineering methods revolve around the same techniques of fooling the user into submitting their information, primarily it is only the delivery method which changes, via email, Instant Messaging (allowing a more

persuasive method to be attempted by the attacker) or through pop-up browser windows on legitimate sites (often caused by malware infected servers). Through review of these several other established methods of user awareness, it would seem conclusive that training of user is the most effective way to reduce (but not necessarily eradicate) a users susceptibility to social engineering attacks.

Following the review of previous works and an analysis of their relative success the following elements of content were considered desirable to guide the creation of a new social engineering awareness website:

- Awareness-raising material about a wide range of social engineering techniques
- Links to supporting material such as news reports regarding social engineering trends or techniques
- Quizzes allowing users to test their own ability to recognise and defend against social engineering attacks.
- Online assistance to users who have difficulty in using the material provided (e.g. user guides to explain the general operation of the site)

While it would be fair to say that the power of interactive learning systems has been somewhat doubted in the past, the publication of results from experiments such as the Anti-Phishing Phil game (see http://cups.cs.cmu.edu/antiphishing_phil/new/index.html) and endeavors now being attempted by large organizations to create interactive education games have meant that the true power of these efforts is now becoming evident [13]. As such, some of these concepts were incorporated into this attempt at providing an educational tool, and focused on supplying users with an educational experience based around learning science principles.

In order to further support the user, and to enhance the identity of the site, it was considered useful to incorporate a character that users can turn to for help, or relate the material to. The character in question, named Edward, acts as the user's teacher and mentor during the use of the site, as depicted in Figure 1.

Fig. 1. The main interface of the Social-Ed site

Within the context of this design, the Social-Ed website focused on providing a conceptual educational experience, whereby users are presented with material in a form which they can relate to, adding to this is the availability of interaction through the quizzes which can improve the effectiveness of learning skills [11].

The system is based upon a modular design, in order to allow content relating to additional techniques and trends to be added easily. In the first instance, however, the prototype implementation covered phishing, spam, pop-ups and pretexting. These topics were selected based upon their severity, and their relevance to end-users in an organizational context. For example, phishing is one of the most common online forms of social engineering, manifesting itself through emails and fraudulent websites aimed at fooling a victim into divulging their personal details [14]. Spam is quite possibly one of the original technical social engineering methods, and it is essentially unsolicited email that often promises something to the victim that may not always have a genuine basis. Pop-ups have similar characteristics, but arrive in a web-browsing context and very often seek to trick the recipient by claiming to be an offer or a warning. Spam and pop-ups can be mostly characterized as annoying rather than dangerous to most end users, however they represent threats that are extremely common and difficult to avoid, given the sheer number of examples that are encountered every day [15]. Finally, pretexting is a very common social engineering technique that involves an attacker having a pre-determined target and planning their attack methodically to achieve success. The act of inventing a scenario which can be used by the social engineer to persuade their victim to release the information they require is far more than a simple lie, often background research must take place to build up to the final 'targeted' information [16].

4 Experimental Findings

Once the implementation of the website was complete, and populated with content covering social engineering attacks and defences, an experimental trial was mounted in order to assess the usefulness of the approach in practice. A total of 46 subjects participated in the experiment, with the participant base largely drawn from students and academic staff, and incorporating a mix of technical and non-technical backgrounds.

The website itself was populated with general educational content regarding social engineering threats, and techniques for defending against them, based upon information gathered during the research phase of this project. Several primary quizzes were implemented within the scope of the project using real world examples of social engineering attacks. Proven phishing attack sites, which were retrieved from the Anti-Phishing Working Group (APWG) website were implemented as screenshot questions and annotated for the purposes of these quizzes. Several spam-related quizzes were created using tagged spam mail from personal email accounts and also further examples from the APWG archive. Further quizzes were also developed on the topics of Pop-Ups and Pretexting. However, less emphasis was placed on the populating these aspects, as they are less prominent amongst the deceptions that users might encounter.

Quizzes on the different topics were graded according to the level of assistance available from Edward. In phase 1 and 2 quizzes, users were provided with hints applicable to the question shown, providing them with the valuable 'life line' evidenced in the Anti-Phishing Phil game. Phase 3 quizzes were void of this feature, and consequently users who reached the final phase of the quiz were alone in their efforts to succeed. However, no limit was placed on retakes, allowing subjects to fail any phase quiz and retake it at their leisure, introducing a level of motivation to the user to progress to the next phase.

Each of these subjects participated in several of the available quizzes, resulting in 327 quiz results being logged within the database. This information is presented in Table 1, which also indicates how the activities were distributed across the different topic areas represented within the site.

Table 1. Distribution of quizzes taken during the Social-Ed trial

Quiz category	Phase 1	Phase 2	Phase 3	Total quizzes
Phishing	42	37	34	113
Spam	39	35	30	104
Pop-ups	37	35	NA	71
Pretexting	38	NA	NA	38
Total				327

In terms of the effectiveness, Figure 2 shows a direct correlation between the pass rates of users in relation and their reading the provided educational material. Although users who did not engage in any prior reading were also had some success, there is a noticeable increase between these two sets of results.

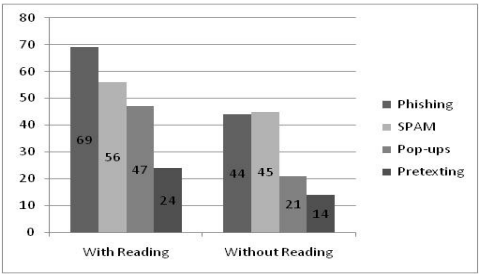


Fig. 2. Social-Ed quiz pass results (with and without reading)

In an effort to determine how successful the goal-oriented design of the quizzes section was, an analysis was performed on these results to determine how many of the users who performed the available quizzes continued through all phases of testing. As can be seen from Figure 3 the overall number completing all the available phases is virtually identical to the number who started the quizzes (people who took a phase 1 quiz), suggesting that the learning sciences principle of goal-oriented design encourages users to seek a satisfactory result once started.

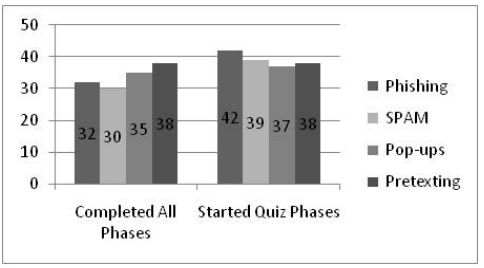


Fig. 3. Commencement versus completion of Social-Ed quizzes

5 Conclusions

A key mechanism for combating social engineering must be the education of potential victims, in order to raise their awareness of the techniques and how to spot them. The research has demonstrated that a web-based approach utilising a goal-orientated system can actively engage users and promote their own desire for success. Further assessment would, however, be advantageous in order to determine the extent to which increased awareness actually reduces the incidence of related breaches.

References

1. Papadaki, M., Furnell, S.M., Dodge, R.C.: Social Engineering: Exploiting the weakest links. In: European Network & Information Security Agency (ENISA), Heraklion, Crete (2008)
2. Mitnick, K., Simon, W.: The Art of Deception: Controlling the human element of security. Wiley Publishing Inc. (2002)
3. Paller, A.: For Questions: Allan Paller, SANS Institute (2007), http://www.tippingpoint.com/pdf/press/2007/SANSTop20-2007_112707.pdf
4. Wood, P.: Social Engineering', Social Engineering (2007), http://www.fbtechies.co.uk/Content/News/PeteSpeak.shtml
5. Karakasiliotis, A., Furnell, S.M., Papadaki, M.: An assessment of end-user vulnerability to phishing attacks. Journal of Information Warfare 6, 17–28 (2007)
6. Greening, T.: Ask and Ye Shall Receive: A Study in 'Social Engineering, vol. 14, pp. 8–14. ACM Press, NY (1996)
7. Dodge, R.C., Carver, C., Ferguson, A.J.: Phishing for User Security Awareness. Computers & Security 26, 73–80 (2007)
8. Bakhshi, T., Papadaki, M., Furnell, S.M.: A Practical Assessment of Social Engineering Vulnerabilities. In: Clarke, N.L., Furnell, S.M. (eds.) Second International Symposium on Human Aspects of Information Security and Assurance (HAISA 2008), pp. 12–23. University of Plymouth (2008)
9. APWG. Phishing Activity Trends Report Q2/2008. Anti-Phishing Working Group (April-June 2008), http://www.apwg.org/reports/apwg_report_Q2_2008.pdf
10. Evers, J.: Security expert: User education is pointless (2006), http://news.cnet.com/2100-7350_3-6125213.html

11. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J., Hong, E.: Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. Institute for Software Research, Carnegie Mellon University (2007)
12. Robila, S.A., James, J., Ragucci, W.: Don't be a phish: steps in user education. In: 11th Annual SIGCSE Conference on Innovation and Technology In Computer Science Education (ITICSE 2006), pp. 237–241 (2006)
13. Havenstein, H.: Video games poised to boost corporate training. Computerworld (August 26, 2008)
14. Rhodes, C.: Safeguarding Against Social Engineering, East Carolina University, Article at (2007), http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_CRhodes.pdf
15. Microsoft. How to Protect Insiders from Social Engineering Threats, Midsize Business Security Guidance (2006), http://technet.microsoft.com/en-us/library/cc875841.aspx
16. Thapar, A.: Social Engineering : An Attack Vector Most Intricate to Tackle, Infosec Writers (2007), http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf

A Risk-Based Approach to Formalise Information Security Requirements for Software Development

Lynn Futcher and Rossouw von Solms

Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
{Lynn.Futcher,Rossouw.vonSolms}@nmmu.ac.za

Abstract. A primary source of information security problems is often an excessively complex software design that cannot be easily or correctly implemented, maintained nor audited. It is therefore important to establish risk-based information security requirements that can be converted into information security specifications that can be used by programmers to develop security-relevant code. This paper presents a risk-based approach to formalise information security requirements for software development. Based on a formal, structured risk management model, it focuses on *how* to establish information security requirements to ensure the protection of the information assets implicated. In this way it hopes to provide some educational guidelines on how risk assessment can be incorporated in the education of software developers.

Keywords: Information security, security requirements, risk analysis, risk assessment, risk treatment, risk-based approach.

1 Introduction

Determining the requirements of a software development project is arguably the most important stage of the lifecycle. Inaccurate, incomplete or vague requirements will result in project failure. In the past, attention was predominantly given to understanding and defining the functional requirements of software development projects – what the system was intended to do, together with its inputs and outputs. Although these functional requirements are still essential for successful software development, developers have recently come to realize the importance of non-functional requirements [1].

Non-functional requirements can be defined as the attributes of the system as it performs its job, including the required usability, performance, reliability and security of the system. Although numerous sources agree that security is a non-functional requirement that needs to be considered when defining the requirements of a system, very few have been able to provide a formal, usable approach to doing this methodically. Various software development methods are typically followed in educating software developers. However, none of these methods provide explicit guidelines on how to establish security requirements. This paper argues that in order to establish these requirements, a risk-based analysis should be performed to

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 257–264, 2013.

determine the risks to the information to be captured, stored, processed and communicated by the software being developed.

The following section describes some important risk concepts, while Section 3 presents a risk-based approach to formalise the information security requirements for a software system. This work is an extension of that published in [2]. Where the focus of that paper was on integrating security into the software development life cycle (SDLC), this paper focuses on *how* to establish information security requirements to ensure the protection of the information assets implicated.

2 Risk Concepts

The various terms relating to risk and risk management are used in many disciplines. This paper supports the formal, structured risk management approach as described in [3] and depicted in Figure 1.

<table>
<tr><td rowspan="8">RISK MANAGEMENT</td><td rowspan="6">Risk Assessment</td><td rowspan="5">Risk Analysis</td><td rowspan="5">“Risk”</td><td rowspan="2">Assets</td><td>Asset identification</td></tr>
<tr><td>Asset valuation</td></tr>
<tr><td rowspan="2">Threats</td><td>Threat identification</td></tr>
<tr><td>Threat assessment</td></tr>
<tr><td>Vulnerabilities</td><td>Vulnerability assessment</td></tr>
<tr><td rowspan="2">Risk Evaluation</td><td colspan="3">Determine risk value or size</td></tr>
<tr><td colspan="3">Prioritise risks</td></tr>
<tr><td rowspan="2">Risk Treatment</td><td colspan="4">Identify suitable controls</td></tr>
<tr><td colspan="4">Implement identified controls</td></tr>
</table>

Fig. 1. Risk Management – a formalized, structured approach (adapted from [3])

From Figure 1 it is clear that risk management comprises two key processes, namely risk assessment and risk treatment. While risk assessment refers to the overall process of risk analysis and risk evaluation, risk treatment is concerned with the process of identifying and implementing suitable controls to mitigate risks.

The main objective of a risk analysis is to identify the risks to which the information systems and its associated information assets are exposed. This can be achieved both formally and informally. Performing a formal risk analysis is a structured process by which the individual information assets, threats and vulnerabilities are identified. However, in order to identify specific risks, the identified information assets need to be related to relevant threats. Having identified all risks by means of a risk analysis exercise, a risk evaluation is required to determine the potential ‘size’ of each risk and for each risk to be prioritized accordingly.

The entire risk assessment process leads to the selection and implementation of appropriate and justified security controls and safeguards in the risk treatment process. It is unwise to implement controls or safeguards simply because they seem to

be the right thing to do, since such implementation may result in serious performance issues [4]. These controls and safeguards should be relative to the information security requirements of the software system in question.

This paper suggests that by following a formal, structured risk assessment, the information security requirements of a software system can be established. The following section briefly describes a risk-based approach to determining these information security requirements.

3 The Proposed Risk-Based Approach

The proposed risk-based approach as described in this section requires that a detailed risk analysis is performed to identify the potential adverse business impacts of unwanted events, and the likelihood of their occurrence. The likelihood of occurrence is dependent on how attractive the information asset is to a potential attacker, the level of frequency or probability of the threats occurring, and the ease with which the vulnerabilities can be exploited. The results of a detailed risk analysis can lead to the identification, assessment and prioritisation of risk that are used to identify and select appropriate controls and safeguards. This can then be used to reduce the identified risks to an acceptable level [5].

3.1 The Identification and Valuation of Information Assets

In order to perform a risk analysis, the key information assets involved need to be identified. These information assets may include, for example, personal information, employee salary information, customer contact information or financial information. The listing of assets, according to [4], based on checklists and judgment, yields an adequate identification of the most important information assets to be considered. This can also be achieved by identifying the information assets that pertain to relevant data gathering questions. These questions could, for instance, refer to those information assets which are the most critical to a company's success, its profitability or its reputation. The aim of this stage is to ensure that the most important information assets that require protection from potentially harmful threats are identified. It is normally sufficient to identify between five and eight key information assets that relate to the software system under development.

The next step in the process is to assign impact values to each of the key information assets identified in Section 3.1. These impact values represent the business importance of the information assets. For simplicity it is recommended that a 5-point Lickert scale, as recommended by [4], be used to establish this impact value. This approach requires that an asset impact value between 0 and 4 (where 0=negligible and 4=critical) is assigned to each of the key information assets, based on its financial value or worth to the organisation. Table 1 illustrates a simple way to map the most critical information assets (rows) against their envisaged asset impact values (columns).

Table 1. Information Asset Valuation

Information Assets	Asset Impact Value				
	0 Negligible	1 Low	2 Medium	3 High	4 Critical
Asset A					*X*
Asset B					*X*
Asset C				*X*	
Asset D				*X*	
Asset E			*X*		

The purpose of this stage of the process is to determine the asset impact value and sensitivity of the information assets in use, being captured, stored, processed or communicated. The next stage requires the identification and assessment of the various threats that may cause harm to these information assets.

3.2 The identification and Assessment of Threats

[6] defines a threat as an undesirable event that could have an impact on the organisation. Software developers therefore need to identify and assess those threats which could negatively impact the information assets associated with their software systems. In order to simplify this process, a checklist of the most common threats is recommended, based on those referred to in [5]. However, since threats are continually changing, software developers are encouraged to add any additional threats to the standard list provided in Table 2. As part of the threat assessment process, it is necessary to determine the level of frequency or probability that a specific threat may exploit some vulnerability thereby negatively impacting the associated information assets.

Table 2. Threat Identification and Assessment

Common Threats (ISO/IEC TR 13335-3:1998)	Level of Frequency/Probability			
	LOW	MED	HIGH	N/A
Theft of information			*X*	
Use of system by unauthorised users		*X*		
Use of system in an unauthorised manner		*X*		
Masquerading of user identity			*X*	
Malicious software attacks			*X*	
User errors			*X*	
Repudiation		*X*		
Technical software failures or errors			*X*	
Other				

This may be performed, as illustrated in Table 2, by assigning each of the threats listed to one of the frequency/probability levels provided, namely low, medium or high.

3.3 The Identification of Risk

Risk can be described as a threat that exploits some vulnerability thereby causing harm to an asset. Risk identification therefore requires that the most critical asset/threat relationships are identified to ascertain which risks are most likely to have a negative impact. This is done by simply considering the most important information assets, as identified in Section 3.1., and the most common threats identified in Section 3.2. Those information assets with high or critical asset impact values (i.e., 3 or 4) and those threats recognised to have a potentially medium or high level of frequency or probability, will contribute significantly to the criticality of the risk.

Table 3. Risk Identification

Common Threats (ISO/IEC TR 13335-3:1998)	**Information Assets**				
	Asset A	**Asset B**	**Asset C**	**Asset D**	**Asset E**
Theft of information	*Risk 1*	*Risk2*			*Risk 5*
Use of system by unauthorised users			*Risk 6*		
Use of system in an unauthorised manner					*Risk 7*
Masquerading of user identity	*Risk 3*				
Malicious software attacks	*Risk 4*				
User errors		*Risk 8*			
Repudiation					
Technical software failures or errors					
Other ……					
Other ……					

Table 3 provides a way to map the most probable threats (rows) against the most important information assets (columns), i.e. identify the specific risks to the software system. Using this table, software developers are required to determine the most critical risks (i.e., asset/threat relationships). It is normally sufficient to identify approximately eight key risks. The risk analysis process, however, is only complete having carried out a vulnerability assessment, since without a vulnerability there would be no risk.

3.4 The Vulnerability Assessment

The purpose of a vulnerability assessment is to determine the degree of weakness that could be exploited. [7] states that in practice, security is not compromised by breaking the dedicated security mechanisms, but by exploiting the weaknesses or vulnerabilities in the way they are used. Therefore, as part of the risk analysis process, it is important to be able to determine the level of vulnerability for each risk (asset/threat relationship) as identified in Section 3.3.

The level of weakness or vulnerability for each risk can be determined by taking the current situation and existing controls into account. This should provide some indication of whether the risk could materialize. Table 4 provides a simple way to map each risk (rows) against the appropriate level of vulnerability (columns), namely

low, medium or high. This completes the risk analysis process, as referred to in Figure 1. Section 3.4 describes the risk evaluation process required to complete the risk assessment process.

Table 4. Vulnerability Assessment

Risks (refer to Table 3)	Level of Vulnerability		
	LOW	MEDIUM	HIGH
Risk 1	*X*		
Risk 2		*X*	
Risk 3	*X*		
Risk 4	*X*		
Risk 5		*X*	
Risk 6			*X*
Risk 7			*X*
Risk 8		*X*	

3.5 The Risk Evaluation

According to [3], the purpose of the risk evaluation process is two-fold. Firstly, it is to determine the value or size of risk and secondly to prioritise risks according to their risk value.

In order to determine the risk value of each risk, the asset impact value of the associated information asset, the level of frequency or probability of the associated threat and the related level of vulnerability must be considered for each risk identified. These relationships can be matched in a table to determine the specific measure of risk on a scale of 1 (low) to 8 (high). These values are placed in a matrix as illustrated in Table 5, according to those recommended by [5]. The appropriate row in the table is identified by the asset impact value of the associated information asset (0 to 4), as identified in Section 3.1. Similarly, the appropriate column is determined by the level of frequency or probability of each associated threat (low, medium or high) and the corresponding level of vulnerability (low, medium or high). The matching cell in the matrix will determine the risk value of the particular risk identified.

Table 5. Risk Evaluation

RISK 1 (as per Asset/Threat Relationship in Table 3)										
		Level of Frequency/Probability of Threat								
		LOW			MEDIUM			HIGH		
		Level of Vulnerability			Level of Vulnerability			Level of Vulnerability		
		LOW	MED	HIGH	LOW	MED	HIGH	LOW	MED	HIGH
Asset impact value	Negligible 0	0	1	2	1	2	3	2	3	4
	Low 1	1	2	3	2	3	4	3	4	5
	Medium 2	2	3	4	3	4	5	4	5	6
	High 3	3	4	5	4	5	6	5	6	7
	Critical 4	4	5	6	5	6	7	6	7	8

The specific risk values, as determined for each risk, are valuable in assessing and prioritising those risks that require individual attention throughout the rest of the software development lifecycle. Furthermore, having followed a formal, structured risk assessment one is able to document appropriate risk-based information security requirements through which these risks may be reduced to an acceptable level.

4 Risk-Based Information Security Requirements

According to [8], information security requirements are generally defined in terms of specific technological mechanisms and tools. However, these can rarely be traced back to a recognised risk. In order to arrive at appropriate information security requirements, this approach proposes a more formalised process whereby a risk assessment is carried out followed by the identification of appropriate security services, as referred to by [9], for each risk. For each key risk, multiple security services can be identified, namely: identification and authentication, access control, data confidentiality, data integrity and non-repudiation. These security services could then be translated into security mechanisms as referred to by [9]. These eight security mechanisms include encryption, digital signatures, access control mechanisms, data integrity mechanism, authentication exchange mechanisms, traffic padding, routing control and notarization mechanisms. This approach should therefore lead to an improved risk treatment process whereby the correct controls are selected and implemented.

5 Conclusion and Future Work

Risk management is an essential tool for the systematic management of information security. It helps identify possible security holes in information systems and assists in providing appropriate countermeasures. For software under development, it is important to have a clear understanding of the information assets that need to be protected, the threats against which those information assets must be protected, the vulnerabilities associated with the information assets, and the overall risk to the information assets from those threats and vulnerabilities.

By following a risk-based approach as proposed in this paper, the controls that are implemented can easily be traced back to specific risks to the information assets implicated in the software under development. It can also assist in motivating which controls, and the strength of the controls to be implemented.

References

1. Britton, C., Doake, J.: Software System Development. A Gentle Introduction, 4th edn., pp. 21–35. McGraw-Hill, Berkshire (2006)

2. Futcher, L., von Solms, R.: SecSDM: A Model for Integrating Security into the Software Development Life Cycle. In: Futcher, L., Dodge, R. (eds.) Fifth World Conference on Information Security Education. IFIP, vol. 237, pp. 41–48. Springer, Heidelberg (2007)
3. von Solms, S.H., von Solms, R.: Information Security Governance, pp. 87–100. Springer, New York (2009)
4. Landoll, D.J.: The security risk assessment handbook: A complete guide for performing security risk assessments. Auerbach Publications, New York (2006)
5. ISO. ISO/IEC TR 13335-3 : Information Technology – Guidelines for the Management of IT Security. Part 3 : Techniques for the management of IT security (1998)
6. Peltier, T.R.: Information security risk analysis. Auerbach Publications, New York (2005)
7. Jurjens, J.: Using UMLSec and goal trees for secure systems development. Communications of the ACM 48(5), 1026–1030 (2002)
8. Tirado, I.: Business Oriented Information Security Requirements Development, Ivan Tirado, CISSP-ISSAP, Kennesaw State University, 1000 Chastain Road, Kennesaw, GA 30144 (2006), http://itiradostudents.kennesaw.edu
9. ISO. ISO 7498-2: Information Processing Systems - Open System Interconnection - Basic Reference Model - Part 2: Security Architecture (1989)

Two Case Studies in Using Chatbots for Security Training

Stewart Kowalski[1], Katarina Pavlovska[1] , and Mikael Goldstein[2]

[1] SecLab, Department of Computer and Systems Sciences,
Stockholm University/Royal Institute of Technology Stockholm, Sweden
stewart@fc.dsv.su.se
[2] migoli, Valhallavägen 130, 114 41 Stockholm, Sweden

Abstract. This paper discusses the result of two case studies performed in a large international company to test the use of chatbots for internal security training. The first study targeted 26 end users in the company while the second study examined 80 security specialists. From a quantitative analytical perspective there does not appears to be any significant findings when chatbots are used for security training. However there does appear to be qualitative data that suggest that the attitudes of the respondents appear to be more positive to security when chatbots are used than with the current traditional e-learning security training courses at the company.

Keywords: Security Awareness Training, Chatbots.

1 Introduction

At the first WISE conference in 1999 Kowalski et al [1] presented in the paper *The Manual is the Message* observations that employees in a company that received security policy and instruction via a paper based medium differed in attitude to security to those that received the same security policy and instruction via an internal webpage. Those that received the information via a paper medium appeared to have a better security attitude than those that received the same information via a web based medium.

In this paper were discuss two new case studies [2, 3] were the medium of communication is the independent variable and the knowledge, attitude and behavior the dependent variable. The paper is divided into five sections. After this short introduction we discuss the current state of security awareness training in corporations. In section two we review the technology of chatbots and how this technology was applied in the case studies. The design and result of these two case studies are presented in section four. We conclude with a general discussion on the potential of chatbots in security education.

2 Quick Overview of Security Awareness Training

The European Network and Information Security Agency ENISA report on current practices in security awareness initiatives in Europe points out that today most

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 265–272, 2013.

European companies have information security policies and instructions set on intranet sites. Most companies also have on-line instruction and 2/3 have some form of mandatory on-line training. [4]

There are those like Nielsen [5] that suggests that awareness and training for security are not an effective way to deal with the web based security problem and only good user design and solid security architecture is the answer. Srikwand and Jakobsson [6] point out often that in an effort to make security messages understandable to the common end user the message is simplified to such an extent that it loses its meaning. Jagatic et al [7] and Kumaragure et al [8] however have performed studies that showed in some case studies that when used in a correct context security awareness training can be effective.

To the authors knowledge no other case studies have been performed to see how chatbot technology can be used to enhance security awareness training.

3 Chatbot Technology

Weizenbaum created the first chatbot in the MIT Artificial Intelligence Lab and called it ELIZA. ELIZA imitated the "active listening" strategies of a touchy-feely 1960s Rogerian therapist [9]. A chatbot or chatterbot can be defined as a computer based program that imitates human (text-to-voice/text) conversation. There is a wide variety of chatbots in use today. They may be used for entertainment, marketing, education and a lists of various chatbots can be found at chatbot.org [10]. These bots can range anywhere from talking to William Shakespeare to speaking with ANNA at IKEA Inc. While some are designed so they are able to compete in a number of different chatbot competitions like the Loebner Prize [11] others are used as a tool for entertainment or for information retrieval. For example, chatbot Sofia [12] can assist in teaching mathematics, VPbot [13] imitates a patient that medical students can interview.

Some chatbots are used in e-business and as a way to communicate to customers. Rita (Real time Internet Technical Assistant) [14] is used in the ABN AMRO Bank to assist customers in doing financial tasks, such as a wire money transfer. In a company called GetAbby, Abby[15] is used to administer customer relationships. The chatbot uses voice recognition techniques during real time phone calls to track and save information from phone calls including customer name, address, and conversations. This allows the company to track customer calls in a cheaper and more efficient way. A chatbot named Anna [16] is used to interact with customers on Ikea's website. It guides and facilitates users in navigation of Ikea's site by allowing them to enter specific questions and then directing them to the appropriate place..

Chatbot Sofia [12] was part of an experiment conducted at the Harvard mathematics department in 2003. The experiment investigated the process of teaching and learning mathematics with the help of a chatbot. Chatbot Sofia has an encyclopedic glossary of mathematics definitions and a general knowledge background, and is able to solve simple mathematical problems. The tool saves all the conversations which can later be analyzed in order to get more information on how

students are learning, what questions they ask, and what mistakes they frequently make. It was concluded that Sofia contributes to a variety of teaching methods and builds an open source knowledge database for different parts of mathematics. In addition, by teaching Sofia and watching how it learns, students may gain a better understanding regarding the process of teaching mathematics.

Computer Simulator in Educational Communication (CSIEC) [17] is a web-based human-computer communication system that uses natural language. This chatbot may be used as a chatting partner for learning the English language. It imitates human emotions and personalities. Moreover, conversations are not limited to any specific subject. The ideal user's input should be acoustic and then converted into text but so far only keyboard inputs are used since the speech recognition program still needs improvement.

It is important to note that when constructing such various chatbots, the goal of what the chatbot should do and the audience to whom the chatbot is for, should be considered and analyzed thoroughly. Tailoring the chatbot for the users and also addressing the appropriate questions/responses of a typical user will produce a more human-like effect. Allowing the chatbot to achieve such an effect may help to improve its overall intention as well as the user's experience of using the chatbot.

4 Design and Result of the Two Case Studies

4.1 End User Case Study

In the first case study [2] selective sampling technique was used to divide the two groups. The selections criteria for the grouping were based on the geographical and operational organization of the company. All the five global sales regions were represented along with two of the three business units in the company were portionaly represented in the two groups. One group was exposed to chatbot (Sally) and e-learning and the other group to e-learning only. Both telephone interviews and email surveys were used to solicit responses from the two groups. The survey consisted of 35 questions which tested various aspects of knowledge, attitude and behavior to security issues. Space does not permit to include the full survey[1] in this paper.

Knowledge questions were concerned with the different information security classes at the company along with examples of typical document types and how they should be classified. Attitude questions covered such aspects as how important information security was over business goals an attitude questions concerning individual responsibilities for classification. Behavior questions ranged from asking how often they changed passwords to how to collect different access rights in the company.

Following the first survey all the respondents of the two groups were sent web links to a training package on Information Security (IS). One group was given an e-learning package only while the other group was given an e-learning package with a

[1] A full copy of the survey and a link to the chatbot can be requested by sending email to the author, stewart@dsv.su.se

voice and text chatbot (Sally). Figure 1 below shows the e-learning package with a chatbot. After about two months a second, identical survey was solicited to the respondents of the two groups.

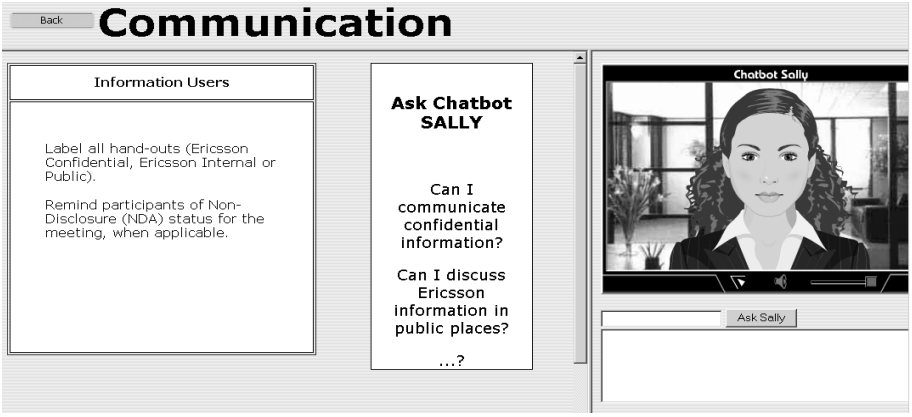


Fig. 1. E-learning package with security information on the left and with chatbot Sally on the right

A Wilcoxon matched pair-single-ranks test was used to assess significance of the quantitative difference in Information Security related knowledge, attitude and behavior between the first and second intervention of the questions for the chatbot and non-chatbot group. There were no significant differences in respondents' responses between the first and second intervention in any of the two sample groups ($p \leq 0.05$, two- tailed test).

The experience of using the chatbot was measured qualitatively by asking the respondents how useful they thought the learning experience had been. As much as 70% of those that used the chatbot found it useful. Over 70% of the respondents agreed that the chatbot had a positive effect on their learning experience and that they would use the chatbot in the future.

To a large extent, the results of this chatbot case study are inconclusive. Quantitatively there does not appear to be any significant difference in knowledge, behavior and attitude improvement using a chatbot. However, the qualitative analysis does indicate positive attitudes by the chatbot users. The restrictive sample size of 16 users of the chatbot can be a contributing factor and the authors suggest that either a large scale analysis be done or a more clinic type of experimental design be used to validate the effects on chatbots on security awareness.

4.2 Security Specialist Case Study

The population consisted of 80 employees that took part in the Information Security Management System (ISMS) Lead Auditor training throughout 2007 [3]. The population was randomly divided into two groups; an experiment group (ISO Alan

chatbot), containing 42 employees, and a control group, containing 38 employees. The experiment group received an e-mail containing a web link to the e-learning package with the ISO Alan chatbot, see Figure 2 below.

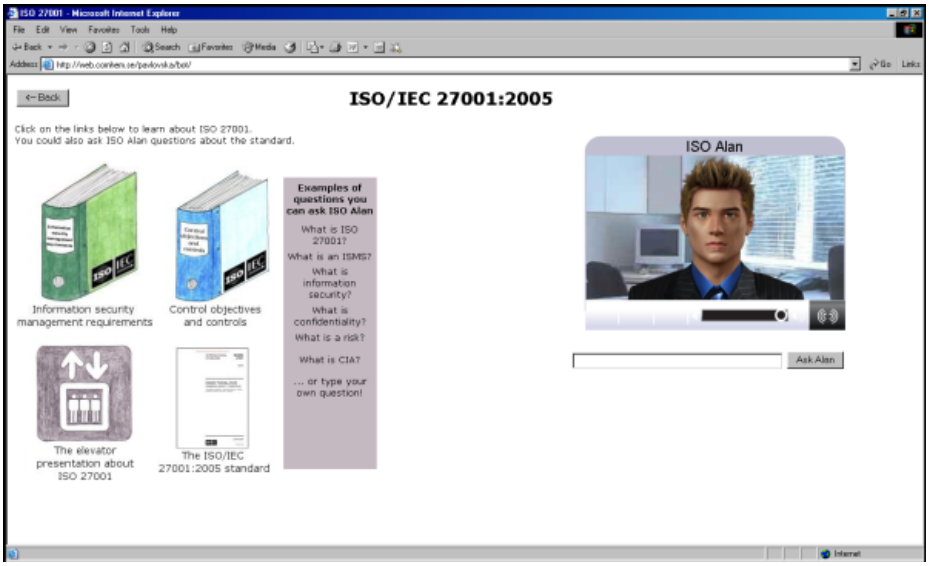


Fig. 2. ISO/IEC 27001:2005 ISO Alan Chatbot with e-learning package

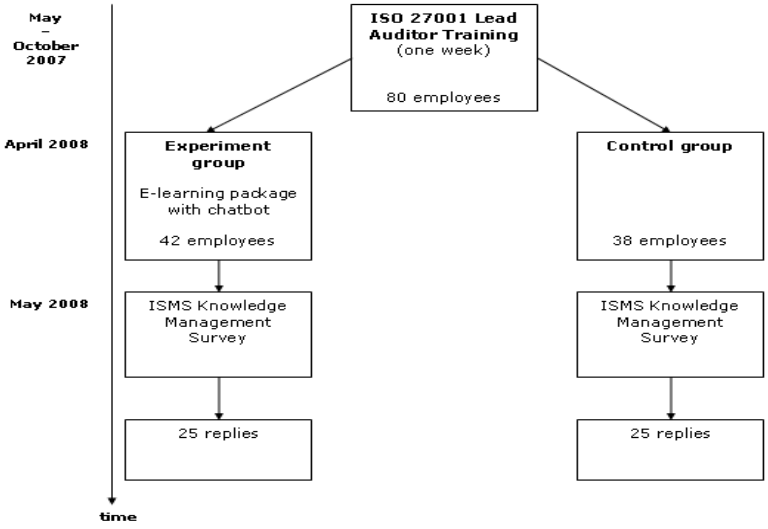


Fig. 3. ISO/IEC 27001:2005 ISO Alan Chatbot Case Design

The employees in the experiment group were asked to spend some time with the e-learning package during the following two weeks. The e-mail also contained the information that when these two weeks had passed they would be asked to participate in a web survey about their feelings regarding their current knowledge of ISO 27001 and ISMS auditing. The control group only received an e-mail with the information about the web survey. Figure 3 shows all the steps of the experiment.

The results from the quantitative analysis show that there was no significant difference between the experiment group and the control group regarding knowledge and attitude. When asked however how useful they thought the learning experience had been, as many as 70% of those that used the Alan chatbot found it useful. Over 70% of respondents agreed that the chatbot had a positive effect on their learning experience and that they would use the chatbot in the future. A selection of comments is presented below;

ISO Alan chat is good, but his knowledge is a bit limited at present time, so when ISO Alan gets more knowledge it will be more useful. The left hand information packages were very good.

Chatbot works quite well once you get used to the idea of simply using key words to get more information - sentences are not needed

As far as I can conclude, the chatbot does not answer questions other than what is. If it is to provide an added value, it must be able to answer questions that would come from the target audience, such as how do I, who should be, etc.

5 Discussion on Way Forward with Security Chatbots

The two cases studies do not provided clear data to validate or falsify the usefulness of using chatbots for security education and training. They do however give some qualitative indication that for particular group of users, chatbots can serve as a complement to computer based training and online awareness training. As Näckros [18] discovered in his work on game based instruction for IT security, different learning styles of individuals prefer different methods of learning. As he points out the majority of computer based learning use sequential learning styles which are designed primarily on serialist learning style. However for those individuals who prefer a holistic approach a serial learning style is often ineffective. A chatbot permits a less serial learning style by design and allows respondents to move in a non-linear fashion in their discovery of knowledge. It is suggested by the authors that if further studies are done with chatbots employed in security training, the respondents should be first screened for their learning style to see if this can be used to predict their appreciation of a chatbot for learning about security issues.

One of the positive side effects of using a chatbot for security awareness training in the organization in the two case studies was a database of questions and issues that both the end user and the specialist ask about security. This database can be used as a knowledge base for future development in the organization. Methods used for

developing, capturing, maintaining and sharing knowledge are usually called knowledge management. Ahmed et. al. [19] defines knowledge management as the combination of processes, technologies, strategies and culture an organization, used together to favor the learning in the organization. The potential of chatbots for security knowledge management in an organization is an area that author see as a potential of future research.

References

1. Kowalski, S., Nässla, H., Karlsson, J., Karlsson, V.: The Manual is the Message: An Experiment with Paper Based and Web Based IT Security Manuals. In: Proceedings of WISE 1999, Stockholm (1999)
2. Kowalski, S., Mozuraite-Araby, R., Walentowicz, S.: Using Chatbots for Security Training of ICT Users. In: World Wide Research Forum 20th Conference Ottawa, Canada (April 2007)
3. Pavlovska, K.: Using Using chatbots to maintain knowledge about ISO/IEC 27001:2005 at Ericsson. Master's thesis, Department of Computer and Systems Sciences (2008)
4. European Network and Information Security Agency, Information Security Awareness Initiatives: Current Practice and the Measurement of Success (July 2007)
5. Nielsen, J.: User education is not the answer to security problems, http://www.useit.com/alertbox/20041025.html (accessed: 2009)
6. Srikwan, S., Jakobsson, M.: Using cartoons to teach Internet Security (2007), http://www.informatics.indiana.edu/markus/documents/security-education.pdf (accessed 2008)
7. Jagatic, T.N., Johnson, M., Jakobsson, M., Menczer, F.: Social Phishing. Communications of the ACM 50(10), 96–100 (2007)
8. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., Nunge, E.: Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. In: Conference on Human Factors in Computing Systems archive. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, San Jose, California, USA, pp. 905–914 (2007)
9. Weizenbaum, J.: ELIZA - A Computer Program For the Study of Natural Language Communication Between Man And Machine. Communication of the ACM 9(1), 36–45 (1966)
10. Chatbot.org, http://www.chatbots.org/ (accessed on April 24, 2009)
11. Loebner Prize, http://www.loebner.net/Prizef/loebner-prize.html
12. Knill, O., Carlsson, J., Chi, A., Lezama, M.: An artificial intelligence experiment in college math education (2004), http://www.math.harvard.edu/_knill (accessed on April 24, 2009)
13. Webber, G.M.: Data representation and algorithms for biomedical informatics applications. PhD thesis, Harvard University (2005)
14. Voth, D.: Practical agents help out. IEEE Intelligent Systems 20(2), 4–6 (2005)
15. GetAbby, http://www.getabby.com/lead_tracking.asp
16. ANNA, http://www.chatbots.org/chatterbot/anna_sweden (accessed on April 24, 2009)

17. Jiyou, J.: CSIEC (Computer Simulator in Educational Communication): An Intelligent Web-Based Teaching System for Foreign Language Learning. In: Proceedings of the IEEE International Conference Advanced Learning Technologies, vol. (30), pp. 690–692 (2004)
18. Näckros, K.: Game Based Instruction within IT Security Education. Department of Computer and Systems Sciences, Stockholm University Royal Institute of Technology, Stockholm (2001)
19. Ahmed, P.K., Lim, K.K., Loh, A.Y.E.: Learning, Through Knowledge Management. Butterworth-Heinemann (2002)

Information Security Specialist Training on the Basis of ISO/IEC 27002

Natalia Miloslavskaya and Alexander Tolstoy

Moscow Engineering Physics Institute (State University), Russia
{milmur,ait}@mephi.edu

Abstract. Information Security (IS) specialists' training for all sectors of trade, industry and government has never been more important as intellectual property and other sensitive or business-critical information becomes the life-blood of many companies today. Analysis of the experience collected within training of IS specialists at the Moscow Engineering Physics Institute (State University) (the MEPhI) at the Information Security Faculty allows forming the basic requirements to the level of their preparation. To form such requirements it is expedient to take a look at the types and tasks of professional activity of the graduates and to formulate their qualification characteristics. This paper formulates these characteristics on the basis of ISO/IEC 27002 (former ISO/IEC 17799:2005).

Keywords: Information Security Education, Specialist Training, ISO/IEC 27002.

1 ISO/IEC 27002

A family of Information Security Management System (ISMS) International Standards, being developed within Joint Technical Committee ISO/IEC JTC 1/SC 27, includes International Standards on ISMS requirements, risk management, metrics and measurement, and implementation guidance. The ISO/IEC 27002 Standard "Information Technology – Security Techniques – Code of Practice for Information Security Management" gives comprehensive guidance on best practice methods for implementing ISO/IEC 27001 "Information Security Management Systems Specification", which specifies requirements for establishing, implementing, maintaining, improving and documenting ISMS for both public and private sector organizations.

ISO/IEC 27001 is the de-facto international standard. It specifies requirements for establishing, implementing, maintaining, improving and documenting ISMS for both public and private sector organizations. It specifies security controls to be implemented by an organization following a risk assessment to identify the most appropriate control objectives and controls applicable to their own needs. This standard forms the basis of an assessment of the ISMS of the whole, or part of an organization and covers the eleven clauses of good IS practice: Security Policy;

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 273–279, 2013.

Organizing Information Security; Asset Management; Human Resources Security; Physical and Environmental Security; Communications and Operations Management; Access Control; Information Systems Acquisition, Development and Maintenance; Information Security Incident Management; Business Continuity Management; Compliance.

ISO/IEC 27002 [1] as a technology independent standard offers a framework to assist any organization to develop a true security minded corporate culture by instilling best practice and detailed guidance regarding all manner of security issues. The guiding principles cover three main aspects: strategic, operational and compliance. ISO/IEC 27002 concentrates on the IS management aspects, defining the controls in enough detail to make them applicable across many different applications, systems and technology platforms without losing any of the benefits provided by standardization. The main characteristics of ISO/IEC 27002 are the following: proven value; widely known and accepted; easy to understand; continuous value; market driven; flexible; adaptable; scalable and so on.

Thus ISO/IEC 27002 provides a stable and comprehensive base for formulating the qualification characteristics of IS specialists, being capable to design, implement and control IS at various types of business organizations. Alignment with the standard also offers a high level of standardization in training worldwide with skills and knowledge set founded upon a uniform, known and acceptable base.

2 IS Specialists' Training and International Standards

Comprehensive security requires secure technologies, organizational processes and people with the necessary background and skills. A large number of certifications are found in the field of IS.

(ISC)² offers the Systems Security Certified Practitioner (SSCP) and the Certified Information Systems Security Professional (CISSP) certifications. The Information Systems Audit and Control Association (ISACA) has a pair of vendor-neutral credentials: the Certified Information Systems Auditor (CISA) and the Certified Information Security Manager (CISM). CompTIA Security+ certification exam covers communication security, infrastructure security, cryptography, access control, authentication, external attack, and operational and organizational security. Software provider Check Point offers a range of security and security management certifications that deal with both general skills and knowledge as well as the company's specific solutions: the Check Point Certified Security Principles Associate (CCSPA), the Check Point Certified Security Expert (CCSE), the Check Point Certified Managed Security Expert (CCMSE). In the Cisco qualified specialist category, there are a few certifications around specific areas of security, including the Cisco Firewall Specialist, the Cisco IDS Specialist and the Cisco Certified Security Professional (CCSP) and so on.

The Global Information Assurance Certification (GIAC) organization, being founded in 1999 by the SANS Institute to validate the real-world skills of IT security professionals, has the main purpose to provide assurance that a certified individual

has practical awareness, knowledge and skills in key areas of computer and network and software security.

The SANS training and GIAC certifications address a range of skill sets and some advanced subject areas such as audit, intrusion detection, incident handling, firewalls and perimeter protection, forensics, hacker techniques, Windows and Unix operating system security.

GIAC currently offers certifications for over 20 job-specific responsibilities that reflect the current practice of IS. At present GIAC certifications cover four IT/IT Security job disciplines: Security Administration, Management, Audit, Software Security.

The SANS training course "SANS 17799/27001 Security & Audit Framework, Mgt-411" implements step by step pragmatic examples to move quickly into compliance with the standard and certification. This track is designed for IS officers or other management professionals who are looking for a how-to guide for implementing the standard effectively. "GIAC Certified ISO-17799 Specialist" (G7799) candidates must demonstrate understanding of the standard and the ability to put it into practice.

Summing up all these certifications it is possible to state that the international perspective of IS specialists' training should be focused on the following international standards: ISO/IEC 27002/27001, Common Criteria, ITSEC and IS bodies of knowledge recommended by professional computing organizations [2].

3 Initial Data for Formulating Qualification Characteristics

"IS specialist" term applies to many positions, responsible for finding and solving security problems in computer systems. What the IS specialist actually does depends on many factors ─ the type and size of the employer, information that needs protection and computers the organization uses.

The basic qualification characteristics of a specialist with higher education are formulated on the basis of his/her special (professional) competences [3] - abilities to solve definite problems and carry out specific work within his/her line. IS specialists must be able to do a number of tasks, to think logically, to pay attention to details and to make sure their work is exact.

Formulating the qualification characteristics is possible only when considering separate typical objects where IS tasks are being carried out. ISO/IEC 27002 analysis shows that there is enough information to formulate the qualification requirements for specialists, ensuring functioning of IS systems of any organization.

The Russian universities allow up to 1 year for practicing and preparing of the graduate qualification paper (diploma project) (for example, the MEPhI students have 10th and 11th semesters). During this period graduates' activities within a specific organization can be divided into three main streams.

1. Forming the goals of ensuring organization's IS (is based upon defining assets to be protected, all types of vulnerabilities, IS paradigm and basic principles, threats' and IS violators' models, implementing risk assessment and forming IS policies).

2. Implementation of these goals (via services/systems/personal).

3. Control of progress in reaching IS goals based upon checks and evaluation of organization's IS (IS monitoring and audit) and defining maturity of organization's IS management processes.

These graduates act as the assistants for organization staff:

- *privacy officers* (develop/implement IS policies and procedures);
- *IS architects* (direct organization-wide security technology);
- *IS analysts* (conduct IS assessments for an organizations);
- *virus technicians* (analyze newly discovered computer viruses and devise ways to defend against them);
- *"red team" testers* (plan/carry attacks on the computer systems);
- *cryptographers* (keep information secure by encrypting it);
- *cryptanalysts* (analyze hidden information);
- *security administrators* (develop/implement protection systems that detect, prevent, contain and deter security risks; update security procedures and establish and maintain access rules);
- *IS incident response team members* (work together to prepare for and provide rapid response to security threats);
- *disaster recovery specialists* (design and implement programs to recover data lost in a disaster);
- *computer crime specialists/computer forensic investigators* (preserve, identify, extract and document evidence if IS incident);
- *IS auditors* (evaluate IS adequacy, effectiveness and efficiency);
- *chief IS officers* (supervise the entire IS department and staff).

Our experience collected since 1995 and ISO/IEC 27002 content analysis allow grouping practice and diploma project topics, incorporating technical, organizational and management aspects (with deeper specification than three main streams), as follows:

- risk management (including development of IS threats' and violators' models, asset management, vulnerabilities assessment);
- IS policies and procedures development;
- business continuity planning and management;
- ISMS design;
- design/development of information protection technologies, tools, means, system/subsystem;
- IS tools and services support and administering;
- physical and environmental security;
- human resources security;
- IS incident management;
- computer forensics;
- IS monitoring and auditing (external, internal, self-assessment against policies, procedures, standards).

To define functions of IS specialists working within concrete objects it is necessary to define IS role for those objects and line of IS specialist activity. Such information could be obtained upon analysis of ISO/IEC 27002.

4 IS Role at Protected Objects

ISO/IEC 27002 defines IS role for any organization as *"…the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. IS is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met."* [1]. Thus when training IS specialists, peculiarities of protected objects should be taken into consideration and they should be reflected in their qualification characteristics.

But it is also important to define subjects that could interact with each other in situations when IS risks could appear. The standard defines the following subjects: *owner of organization's assets and violator trying to influence those assets*. IS role is defined by the tasks being carried out within the conditions of opposition of an owner and a violator for the control over the assets.

While indentifying its security requirements an organization should consider three main sources. The first one *"…is derived from assessing risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated." The second "…is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment." And the third "…is the particular set of principles, objectives and business requirements for information processing that an organization has developed to support its operations."* [1].

IS risks, whose essence is natural vagueness of the future, are an objective reality and they could be lowered only to the level of vagueness of subjects characterizing the nature of business. The remaining part of IS risk defined by the factors of the environment of organization's functioning, for which organization cannot influence at all, should be accepted. In that case ensuring IS at an object should lower risks to a certain level.

After that phase an organization should implement the IS goals – *"appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level… The selection of security controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations."* [1]. The controls can be considered as guiding principles for IS management and applicable for most organizations.

Ensuring IS for an organization is the process that should be efficiently managed. The main IS role is defined by the organization's IS strategy which lies in ISMS deployment, exploitation, check and improve. Along with that IS management is a part of the overall corporate organization's management which is oriented for reaching organization's goals through ensuring protection of its assets. An organization's ISMS is a part of the overall management system based on the business risk approach whose goal is to create, implement, operate, monitor, analyze, support and rise IS of an organization (ISO/IEC IS 27001).

5 IS Specialist Line of Activity

It is possible to formulate the main lines of activity of IS specialist on the basis of the section 0.7 of the ISO/IEC 27002 standard:

"a) IS policy, objectives, and activities that reflect business objectives;

b) an approach and framework to implementing, maintaining, monitoring, and improving IS that is consistent with the organizational culture;

c) visible support and commitment from all levels of management;

d) a good understanding of the IS requirements, risk assessment, and risk management;

e) effective marketing of IS to all managers, employees, and other parties to achieve awareness;

f) distribution of guidance on IS policy and standards to all managers, employees and other parties;

g) provision to fund IS management activities;

h) providing appropriate awareness, training, and education;

i) establishing an effective IS incident management process;

j) implementation of a measurement system that is used to evaluate performance in IS management and feedback suggestions for improvement."

6 Conclusion

Analysis of the experience collected within training of IS specialists with higher education at the MEPhI and of ISO/IEC 27002 allows one to define two types of IS specialist professional activity: technological (ensuring functioning of the main IS technologies) and organizational and technological (ensuring functioning of ISMS).

Qualification requirements are defined by the types of tasks being carried out by the specialists and requirements to the level of knowledge and skills. Three main streams (listed in section 3) define three tasks solved (special competence). The level of knowledge and skills is associated with staff functions (section 3).

IS specialists should –

know:

- normative base, related to ensuring IS;
- the impact which interruptions caused by IS incidents are likely to have on the business;

- principles of ensuring IS;
- methods of IS risk assessment and management;
- IS architectures and infrastructures;
- basic methods of IS management;
- IS effectiveness evaluation methods;
- methods of system IS monitoring and auditing;
- basic methods of IS incident management process;
- business continuity planning and management;
- fundamentals of computer forensics;

be able:

- identifying all the assets involved in critical business processes;
- define models of IS threats and violators;
- develop, review, implement and improve IS policies and procedures;
- conduct IS risk assessment and management at the object (including reducing and avoiding risks);
- develop, deploy, check (and test), improve ISMS;
- administer IS tools (hardware/software) and subsystems of certain information technologies and automated systems;
- review the effectiveness of IS policy and procedures implementation;
- collect evidence for IS incident handling;
- providing appropriate IS awareness, training and education;

have an idea of:

- methods of building object management systems;
- peculiarities of psychology and ethics of team relations;
- defining the resources (financial, organizational, technical and environmental) needed for IS.

These requirements have universality and do not depend upon national and other peculiarities of systems being secured. To conclude, future work should be on the basis of formulated qualification requirements and details of educational course content specified in IS curricula.

References

1. International Standard ISO/IEC 17799. Information technology — Security techniques — Code of practice for information security management, 2nd edn. (June 15, 2005), http://www.iso.org
2. Armstrong Colin, J., Armstrong Helen, L.: Mapping information security curricula to professional accreditation standards. In: Proceedings of the 2007 IEEE Workshop on Information Assurance, US Military Academy, West Point, NY, June 20-22 (2007)
3. Kurilo Andrey, P., Miloslavskaya Natalia, G., Tolstoy Alexander, I.: Information Security Specialist Training for the Banking Sphere. In: Proceedings of the 5th World Conference on Information Security Education WISE5. US Military Academy, West Point, NY, June19-21 (2007)

Using Bloom's Taxonomy for Information Security Education

Johan Van Niekerk and Rossouw von Solms

Institute for ICT Advancement, Nelson Mandela Metropolitan University
{johan.vanniekerk,rossouw.vonsolms}@nmmu.ac.za

Abstract. The importance of educating organizational end users about their roles and responsibilities towards information security is widely acknowledged. However, many current user education programs have been created by security professionals who do not necessarily have an educational background. This paper show how the use of learning taxonomies, specifically Bloom's taxonomy, can improve such educational programs. It is the authors belief that proper use of this taxonomy will assist in ensuring the level of education is correct for the intended target audience.

1 Introduction

The primary aim of corporate information security education is to ensure that each and every employee is instilled with the requisite **knowledge** and/or skills to perform his or her function in a secure way [1]. Most current information security educational programs are constructed by information security specialists who do not necessarily have a strong educational background. Studies have shown that the vast majority of current awareness approaches lacks theoretical grounding [2, pp. 33-56]. The nature of security educational or awareness issues are often not understood, which could lead to programs and guidelines that are ineffective in practice [3]. This paper shows how the use of Bloom's revised taxonomy [4], as a pedagogical framework, can assist the creators of information security educational programs in defining more pedagogically sound learning objectives for the humans involved in information security processes.

The work in this paper is based on qualitative research methods. This paper should thus be seen as "an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem" [5, p. 15]. Since education, as a field of study, is normally seen as a "human science" it was deemed fitting to also "borrow" the research paradigm used in this paper from the humanities. The research presented here does not attempt to define *new* knowledge, but rather to show how an existing taxonomy, Bloom's taxonomy, could be used to improve information security *educational* programs. This paper is an expansion on ideas previously published by the authors in [6]. It is the authors' belief that the use of Bloom's taxonomy could improve the understanding of the pedagogical, or learning, objectives that **should** be considered in any educational program, amongst information security specialists.

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 280–287, 2013.

The rest of this paper will briefly examine this taxonomy, before discussing its possible use in information security education.

2 Bloom's Taxonomy of the Cognitive Domain

Bloom's taxonomy is possibly one of the best known and most widely used models of human cognitive processes. Bloom's model was originally developed in the 1950's and remained in use more or less unchanged until fairly recently [7, p. 249]. A revised version of the taxonomy was published in 2001 [4]. This revised taxonomy has become accepted as more appropriate in terms of current educational thinking [7, pp. 249-260]. Both versions of Bloom's taxonomy consist of six levels which increases in complexity as the learner moves up through these levels. Figure 1 shows both versions of this taxonomy.

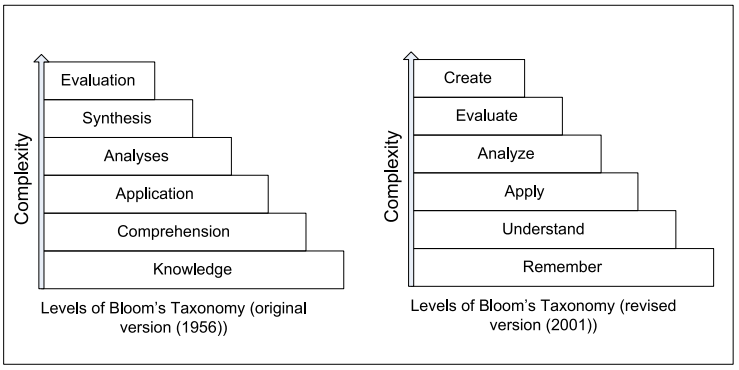


Fig. 1. Blooms Taxonomy, Original and Revised (Adapted from Sousa (2006) pp. 249-250)

There are two main differences between the original and the revised versions of the taxonomy. Firstly, the revised version uses descriptive verbs for each level that more accurately describes the intended meaning of each level. Secondly, the revised version has swapped the last two levels of the original version around. This was done because recent studies have suggested that generating, planning, and producing an original "product" demands more complex thinking than making judgements based on accepted criteria [7, p. 250]. The hierarchy of complexity in the revised taxonomy is also less rigid than in the original in that it recognizes that an individual may move among the levels during extended cognitive processes. This paper will focus on the revised version of the taxonomy. Wherever this paper mentions Bloom's taxonomy, it should be assumed that the revised version is intended, unless otherwise stated. The following is a brief explanation of each of the six levels of this revised taxonomy [7, pp. 250-252]:

- Remember: Remember refers to the rote recall and recognition of previously learned facts. This level represents the lowest level of learning in the cognitive domain because there is no presumption that the learner understands what is being recalled.
- Understand: This level describes the ability to "make sense" of the material. In this case the learning goes beyond rote recall. If a learner understands material it becomes available to that learner for future use in problem solving and decision making.
- Apply: The third level builds on the second one by adding the ability to use learned materials in *new* situations with a minimum of direction. This includes the application of rules, concepts, methods and theories to solve problems within the given domain. This level combines the activation of procedural memory and convergent thinking to correctly select and apply knowledge to a completely new task. Practice is essential in order to achieve this level of learning.
- Analyze: This is the ability to break up complex concepts into simpler component parts in order to better understand its structure. Analysis skills includes the ability to recognize underlying parts of a complex system and examining the relationships between these parts and the whole. This stage is considered more complex than the third because the learner has to be aware of the thought process in use and must understand both the content and the structure of material.
- Evaluate: Evaluation deals with the ability to judge the value of something based on specified criteria and standards. These criteria and/or standards might be determined by the learner or might be given to the learner. This is a high level of cognition because it requires elements from several other levels to be used in conjunction with conscious judgement based on definite criteria. To attain this level a learner needs to consolidate their thinking and should also be more receptive to alternative points of view.
- Create: This is the highest level in the taxonomy and refers to the ability to put various parts together in order to formulate an idea or plan that is new to the learner. This level stresses creativity and the ability to form *new* patterns or structures by using divergent thinking processes.

In addition to these levels of the cognitive domain [4] also places major emphasis on the use of the following categorization of the knowledge dimension [4, pp. 45-62]:

- Factual Knowledge - The most basic elements the learner must know in order to be familiar with a discipline. I.e. Terminology or specific details and elements.
- Conceptual Knowledge - The interrelationships among the basic elements of larger structures that enable these elements to function together. I.e. Classification, categories, principles, theories, models, etc.
- Procedural Knowledge - How to do something, methods of inquiry, how to use skills, apply algorithms, techniques and methods. I.e. Subject specific

skills, algorithms, techniques, and methods as well as knowledge of criteria for determining when to use appropriate procedures.
- Meta-Cognitive Knowledge - An awareness and knowledge of one's own cognition. I.e. Strategic knowledge, Self-knowledge, knowledge about cognitive tasks, including contextual and conditional knowledge.

Activities at these six levels of the cognitive domain are usually combined with the one or more of the four types of knowledge in a collection of statements outlining the learning objectives of an educational program. Usually a *learning objective* statement will be used to create a set of *learning activities*. Learning activities are activities which help learners to attain the learning objectives. A Learning activity consist of a *verb* that relates to an activity at one of the levels of the cognitive domain, and a *noun* providing additional insight into the relationship of the specific learning objective to a category of knowledge [4, pp. 93-109]. The use of a taxonomy often assist educators in gaining better understanding of learning objectives, and activities. However, it is not always clear how this increased understanding can help the educators. [4, pp. 6-10] identifies the following four "organizing questions" as the most important areas in which a taxonomy like Bloom's can assist educators:

- The Learning Question: What is the most important for learners to learn in the limited time available
- The Instruction Question: How does one plan and deliver instruction that will result in high levels of learning for large numbers of learners
- The Assessment Question: How does one select or design assessment instruments and procedures to provide accurate information about how well students are learning
- The Alignment Question: How does one ensure that objectives, instruction, and assessment are consistent with each other.

In most cases, the correct usage of a *taxonomy table*, like the one given in Table 2, which combines elements from both the cognitive and knowledge dimensions, will allow educators to answer these question to some extent.

3 Bloom's Taxonomy for Information Security Education

Learning taxonomies assist the educationalist to describe and categorize the stages in cognitive, affective and other dimensions, in which an individual operates as part of the learning process. In simpler terms one could say that learning taxonomies help us to "understand about understanding" [8]. It is this level of meta-cognition that is often missing in information security education. According to Siponen awareness and educational campaigns can be broadly described by two categories, namely framework and content [3]. The framework category contains issues that can be approached in a structural and quantitative manner. These issues constitute the more explicit knowledge. The second category, however, includes more tacit knowledge of an interdisciplinary nature. Shortcomings

in this second area usually invalidate awareness frameworks [3]. How to really motivate users to adhere to security guidelines, for example, is an issue that would form part of this content category.

Table 1. Abbreviated example of Learning Activities based on Bloom's Taxonomy for Information Security, adapted from Anderson et al., 2001

Level	Verb	Sample Activities
Create	design	Write a new policy item to prevent users from putting sensitive information on mobile devices. **(A6)**
Evaluate	critique	Critique these two passwords and explain why you would recommend one over the other in terms of the security it provides.**(A5)**
Analyze	analyze	Which of the following security incidents involving stolen passwords are more likely in our company?**(A4)**
Apply	execute	Use the appropriate application to change your password for the financial sub-system. **(A3)**
Understand	discuss	Why should non alpha-numeric characters be used in a password? **(A2)**
Remember	define	What is the definition of *access control*? **(A1)**

In order to ensure successful learning amongst all employees, it is extremely important to fully understand the educational needs of individual employees. Managers often attempt to address the security education needs of employees without adequately studying and understanding the underlying factors that contribute to those needs [9, pp. 27-36]. It has been argued before that educational material should ideally be tailored to the learning needs and learning styles of individual learners [10][11, p. 19]. One could also argue that awareness campaigns that have not been tailored to the **specific** needs of an individual, or the needs of a **specific target audience**, will be ineffective. It is in the understanding of these needs, that a learning taxonomy can play an important enabling role.

Information security specialists should use a taxonomy, like Bloom's taxonomy, before compiling the content category of the educational campaign. The use of such a taxonomy could help to understand the learning needs of the target audience better. It could also reduce the tendency to focus only on the framework category of these campaigns. For example, simply teaching an individual what a password is, would lie on the *remember*, and possibly *understand* level(s) of Bloom's taxonomy. However, the necessary information to understand *why* their own passwords is also important and should also be properly constructed and guarded might lie as high as the *evaluate* level of the taxonomy. An information security specialist might think that teaching the users what a password is, is enough, but research have shown that understanding *why* is essential to obtaining buy-in from employees. It is this level of understanding that acts as a motivating factor and thus enables behaviour change [3][10][9, pp. 78-79].

The use of an educational taxonomy in the construction of information security educational programs requires that both the content and the assessment criteria for this program is evaluated against the taxonomy in order to ensure that learning takes place at the correct level of the cognitive domain. The reference point for any educational program should be a set of clearly articulated "performance objectives" that have been developed based on an assessment of the target audience's needs and requirements [9, p. 96]. Correct usage of an educational taxonomy not only helps to articulate such performance objectives but, more importantly, helps the educator to correctly gauge the needs and requirements of the audience.

An example of how Bloom's revised taxonomy could be used in an information security context is supplied in Table 1. This example contains learning activities for a learning objective **(LO1)** that can be briefly expressed as: "Learners should be able to understand, construct and use passwords in the correct context". This example is not intended to be a definitive work, but rather to serve, with taxonomy table Table 2, towards clarifying the use of Bloom's taxonomy in an information security context.

Table 2. Example Taxonomy Table adapted from Anderson et al., 2001

The Knowledge Dimension	**The Cognitive Process Dimension**					
	Remember	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Create**
Factual Knowledge	**A1**				**A6**	
Conceptual Knowledge		**Test1A A2**		**Test1B A4**	**A6**	
Procedural Knowledge			**LO1 A3**		**A6**	
Meta-Cognitive Knowledge				**A5**		

It was mentioned earlier that answering the four "organizing questions" is one of the most difficult things for creators of educational matter to do. The following sub-section will briefly explain how the taxonomy table, Table 2 could be used to assist in answering these question for the learning activities, as shown in Table 1.

3.1 Answering the Four "Organizing Questions"

Each learning activity in Table 1 consist of a *verb* that relates to one of the cognitive domain levels in Bloom's Taxonomy [4, pp 67-68]. Each activity also has a *noun* relating to knowledge that could be categorized as one of the four categories of knowledge. By marking the appropriate spaces in the taxonomy table for each activity, the educator can derive a lot of useful information about

the "coverage" provided by the activities. As an example, the activity marked **A1** Lies at the remember level of the cognitive domain and since it deals with basic subject terminology it deals with the "factual" category of knowledge. This is reflected by its positioning in Table 2. Each of the other activities, **A2** to **A6**, as shown in Table 1 has also been appropriately placed in Table 2. A complete information security educational program will obviously include many more activities, which would result in many more entries in the taxonomy table. Such a table do not always have to deal with an entire program, but could, like the given example, focus on a single learning objective, or even on a few related objectives.

By examining the taxonomy table the educator can easily identify areas of knowledge, or levels of the cognitive domain, that has not been covered by the learning activities. Similarly, areas where multiple activities covers the same levels of cognition and categories of knowledge can be identified. This can assist in answering the so-called "learning question", i.e. "are most important activities receiving the larger share of the available resources?". In order to design activities that will result in maximum learning, thus answering the "learning question", one can look for activities that involves more than just one type of knowledge. For example, in order to create a new policy item (Activity **A6**), the learner will need to know; basic terminology (factual knowledge), how items relate to each other (conceptual knowledge), and which steps to follow to create a policy (procedural knowledge). To answer the "assessment question" the educator could choose to focus on the learning objective itself, and thus, in the example given, only use assessment methods that require the learner to apply procedural knowledge. Or the assessor might decide to focus on one or more learning activities and thus have a wider range of assessment coverage. By noting assessment activities on the same taxonomy table, the educator can ensure that the chosen assessments correspond directly to what he/she intends to assess. For example, that learners must *understand* the concept of a password (**Test1A**) and must be able to *analyze* the relative strength of a given password (**Test1B**). The table will also, at a glance, show which areas are not being assessed. Finally, given a complete taxonomy table, the "alignment question" should be relatively easy to answer. In the given example, a clear "disconnect" between the assessment and the learning objective itself exist. Instead of focusing on the **application, or use,** of passwords the assessments focus on the concept of what a password is, and how to determine its relative strength. Similarly, other "miss-alignments" can be identified with the help of this taxonomy table.

4 Conclusion

This paper suggested that information security educational programs would be more effective if they adhered to pedagogical principles. It was specifically suggested that an educational taxonomy, like Bloom's taxonomy should be used to accurately define the security education needs of organizational users. Through the use of such a taxonomy certain common weaknesses in current security awareness and educational programs might be addressed.

An example of how Bloom's taxonomy might be applied to a learning objective in an information security educational program was provided. The paper used this brief example, to show how a taxonomy table based on this example, could assist educators in addressing the four "organizing questions" faced by educators. The primary weakness of this paper is the lack of empirical evidence to support the suggested use of Bloom's taxonomy. Due to space limitations, the examples are also by necessity, very brief. Future research in this regard should focus on addressing the lack of empirical evidence, and on expanding the examples to be more comprehensive. It has been argued before that security practitioners who engage in research or activities that relate to the human sciences should not re-invent the wheel, but should rather "borrow" from the humanities when appropriate. This paper is one such an attempt, to "borrow" from the humanities.

References

[1] Van Niekerk, J., Von Solms, R.: An holistic framework for the fostering of an information security sub-culture in organizations. Information Security South Africa (ISSA), Johannesburg, South Africa (2005)
[2] Puhakainen, P.: A design theory for information security awareness. PhD thesis, Acta Universitatis Ouluensis A 463, The University of Oulu (2006)
[3] Siponen, M.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security 8(1), 31–41 (2000)
[4] Anderson, L., Krathwohl, D., Airasian, P., Cruikshank, K., Mayer, R., Pintrich, P., Raths, J., Wittrock, M.: A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Complete edn. Longman (2001)
[5] Creswell, J.W.: Qualitative Inquiry and Research Design: Choosing among Five Traditions. Sage, Thousand Oaks (1998)
[6] Van Niekerk, J., Von Solms, R.: Bloom's taxonomy for information security education. Information Security South Africa (ISSA), Johannesburg, South Africa (2008)
[7] Sousa, D.A.: How the brain learns, 3rd edn. Corwin Press (2006)
[8] Fuller, U., Johnson, C.G., Ahoniemi, T., Cukierman, D., Hernán-Losada, I., Jackova, J., Lahtinen, E., Lewis, T.L., Thompson, D.M., Riedesel, C., Thompson, E.: Developing a computer science-specific learning taxonomy. SIGCSE Bull 39(4), 152–170 (2007)
[9] Roper, C., Grau, J., Fischer, L.: Security Education, Awareness and Training: From Theory to Practice. Elsevier Butterworth Heinemann (2005)
[10] Van Niekerk, J., Von Solms, R.: Corporate information security education: Is outcomes based education the solution? In: 10th IFIP WG11.1 Annual Working Conference on Information Security Management, World Computer Congress (WCC), Toulouse, France (2004)
[11] National Institute of Standards and Technology: NIST 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST Special Publication 800-16, National Institute of Standards and Technology (1998)

Advancing Digital Forensics

Katrin Franke[1], Erik Hjelmås[1], and Stephen D. Wolthusen[1,2]

[1] Norwegian Information Security Laboratory, Department of Computer Science, Gjøvik University College, Norway
{katrin.franke,erikh}@hig.no
[2] Information Security Group, Department of Mathematics, Royal Holloway, University of London, United Kingdom
stephen.wolthusen@rhul.ac.uk

Abstract. The diversity of computing and communication systems used as well as the sheer volume of data processed in all aspects of personal, government, and commercial activities poses considerable challenges to law enforcement and particularly compliance officers. While commercial tools exist for a number of common problems, this is, however, not always sufficient in many more complex cases. Moreover, investigators only familiar with such tools may not be aware of limits in scope and accuracy, potentially resulting in missing evidence or placing unwarranted confidence in it. Moreover, not only is it critical to have an in-depth understanding of the underlying operating principles of the systems that are analyzed, there will also at times be a need to go beyond capabilities of existing tool sets, the enabling knowledge, concepts, and analytical skills for which we argue is currently not offered in a concise higher education context but rather tends to be acquired in an ad-hoc manner.

We therefore propose elements of a curriculum for the M.Sc. and particularly the Ph.D. level which provide the necessary rigorous theoretical foundations and perspectives in mathematics, computer science, and engineering combined with a background in forensic sciences which enable both a sound appreciation of existing techniques and the development of new forensic evidence collection and analysis methods. We argue that these abilities are crucial in developing a more rigorous discipline of digital forensics which will both be able to address new challenges posed by evolving information systems and also to satisfy the stringency expected from it given its increasing importance in a broad range of application areas.

Keywords: Digital Forensics, Curriculum Development.

1 Introduction

Digital forensics (also referred to at times as computer forensics) encompasses approaches and techniques for gathering and analyzing traces of human and computer-generated activity in such a way that it is suitable in a court of law. The objective of digital forensics is hence to perform a structured investigation into past and ongoing occurrences of data processing and transmission whilst maintaining a documented chain of evidence, which can be reproduced unambiguously and

R.C. Dodge Jr. and L. Futcher (Eds.): WISE 6, 7, and 8, IFIP AICT 406, pp. 288–295, 2013.

validated by competent third parties. Challenges to such investigation, in addition to legal issues which are beyond the scope of this paper, are practitioner-driven approach currently pursued [1].

A number of programs on digital and computer forensics exist both at the B.Sc. and M.Sc. levels along with a large number of modules integrated in information security and general computer science. The former include offerings by the Universities of Bedfordshire, Bradford, Middlesex, Strathclyde, Teesside and Westminster, UK as well as the John Jay College of Criminal Justice at the City University of New York, Sam Houston State University and the University of Central Florida in the U.S., as well as concentration areas embedded in computer science (e.g. [2]) or forensic sciences in case of George Washington University, Marshall, Purdue, and Stevenson University, the Universities of New Haven and Rhode Island in the U.S. and the University of East London in the UK and the University of Western Sydney in Australia; details (albeit with a U.S. focus) can be found in a recent survey by Taylor *et al.* [3] as well as earlier work by Yasinsac *et al.* [4] and Gottschalk *et al.* [5] with examples of undergraduate programs being described e.g. by Bem and Huebner [6].

Specific offerings at the Ph.D. level are, however, more limited, and although advanced research in the area is not limited to the above-mentioned institutions and a number of specialized publication outlets such as the IFIP 11.9 conferences and SADFE (Systematic Approaches to Digital Forensic Engineering), DFRW (Digital Forensics Research), and Computational Forensics (IWCF) workshops along with publications such as the IEEE Transactions on Information Forensics and Security, the International Journal of Digital Evidence and related research in a number of other outlets, it appears that it is often the application of research to forensics that is acting as the determinant rather than the subject matter itself. However, it is instructive to note that in a recent proposal of a Ph.D. curriculum for digital forensics, Cohen and Johnson stated expert knowledge in the application area as the teleology for higher education at this level rather than research itself [7].

This paper aims to raise three questions with regard to research-oriented higher education in digital forensics, which we think should be the rule rather than the exception at the Ph.D. and M.Sc. levels as opposed to the more vocationally oriented undergraduate and certificate-based offerings. First, we consider it necessary to delineate the scope of digital forensics; here, we concentrate on technical aspects as is suitable for research. Secondly, based on the preceding analysis we identify the topics and areas which we consider unique to digital forensics or at least sufficiently specialized to warrant inclusion in a forensics research curriculum according to the preceding criteria. Finally, we argue that one of higher education's and particularly research's roles in digital forensics should be on the enabling or the development of forensics-friendly mechanisms and systems as this holds the promise of considerable medium- and long-term benefits.

The remainder of the paper therefore addresses the issue of delineation in section 2 followed by a discussion of subjects and topics we consider sufficiently unique to digital forensics in section 3 followed by our arguments for research on systematically enabling forensics in section 4 before a brief summary and conclusions in section 5.

2 Delineating Forensics

While the impetus for digital forensics is originating with legal requirements, we focus here primarily on areas amenable to scientific and mathematical inquiry as this is more likely to be beneficial for the types of investigations and research found in M.Sc. and Ph.D. work. Digital forensics does have an intersection with what may be called conventional forensics in that the underlying physics of information processing devices rather than the logical abstractions formed by computer science and engineering may determine whether evidence can be collected and, if so, how reliable the data captured is to be considered. Beyond these foundations, however, engineering issues will dominate the accessibility for most types of storage (e.g. magnetic, optical, solid-state, and in some cases also considering volatile storage sub-types).

As noted in [7], it is hardly possible to provide students of digital forensics with a solid grounding in all such foundational aspects, and it will be incumbent on students wishing to pursue research in this area to acquire the specialized knowledge and skills from physics and electrical or computer engineering required. When using the abstraction provided as a metric, the issue of extracting, classifying, and visualizing the patterns resulting from the data lies at the other end of the spectrum from device physics. One is, however, confronted with a similarly large area of research as in the case of the physical sciences, and most research involving these areas is more likely to be applied or derivative in nature, although there is clearly considerable room for using domain-specific knowledge to enhance general techniques and approaches. One key characteristic of both individual data items and particularly of any hypotheses and chains of evidence is verifiability, which should become more significant as the field matures from relying on individual expert opinion to objective standards. This requires a rigor and change of emphasis compared to the typical approaches found in information security where the existence of a certain false-positive rate is accepted based on the assumption that analysts will discard such indicators in subsequent steps (e.g. in case of anomaly-based pattern matching and classification used in intrusion detection). Given both the potential adverse consequences of such a false positive match for an individual falsely accused and the likely impact that the detection of a false positive has on the credibility of the forensic mechanism and the expert giving evidence, this clearly provides an impetus for research into verifiable approaches or, if that is not feasible in a given area, ones for which error characteristics can be determined rigorously. This implies not only a sound understanding of statistics and probability as well as of formal models of causality in applying forensic techniques as discussed in section 3, but also imposes constraints on the gathering and particularly on the processing of evidence in such a way that any probabilistic aspects and errors are well understood. This specific aspect of digital forensics is made particularly relevant by the volumes of data which may need to be subjected to analysis and reconstruction both in compliance processes and in discovery or court cases.

Moreover, the combination of potentially large volumes of data to be considered and the need to present the resulting evidence, hypotheses, and chains of reasoning to non-experts in such a way that challenges can still be met rigorously also presents a

number of challenges, beginning with requiring an understanding of the human perceptual system and particularly of the limitations of intuitive reasoning that may bias the perception of evidence by non-experts. In addition — as will also be discussed in section 3 — the pervasive character of information processing systems in all aspects of life also has implications for the potential sources of data and evidence. While traditional information security is often limited to easily accessible and commonly used environments, forensics must consider a large number of unconventional devices such as embedded systems as data sources. Many such embedded systems will be quite limited in their scope and ability, potentially requiring the fusion of a number of data sources to obtain the evidence or accuracy desired. This, however, requires that the individual sources and evidential data be interlinked, which will often be possible only in conjunction with explicit models of an overall system or the external (physical) environment, e.g. in case of vehicular systems. Such models are not necessarily part of either the curriculum or research agenda in information security or, beyond this, computer science and applied mathematics. and hence require a solid grounding in the physical sciences beyond the immediate needs of gathering the evidence from digital systems themselves mentioned above. In delineating digital forensics one must also consider the more general case of *computational forensics* or forensic information technology [8], which is more general in nature and employs computational approaches in support of forensic investigations such as hypothesis generation and validation. However, given that in this case the bounds of the field are determined more by the application area rather than inherent in the field itself, we consider only the immediate intersection with digital forensics proper as relevant for curriculum development.

3 Unique Subjects in Forensics and Limitations

The preceding section has raised the issues of which subject areas are to be part of a curriculum for graduate and postgraduate studies in digital forensics, which are not studied in sufficient depth in computer science and (applied) mathematics curricula [9, 10]. In the following, we therefore describe both *supporting* curricular elements and those of more immediate significance to applications and research, driven in part by the results from the CISSE 2008 report by Nance et al. [1]. As noted by several authors including [7], the most universal supporting modules are indubitably statistics and probability theory, which are also a key element in general forensic science [11]. However, given the requirements outlined above, both practitioners and researchers in digital forensics will typically require a more solid grounding in the creation of models of causality and the limitations of inference models based on incomplete and uncertain information.

[12]. Further, more generally applicable courses and modules will typically encompass the areas of pattern classification, recognition, and matching as well as machine learning and visualization. All of these, together with the often highly optimized algorithms and data structures used will, however, require considerable background in these areas of computer science. Beyond this, however, digital

forensics proper requires familiarity with several aspects of information systems, which are not commonly taught in computer science and engineering or even information security programs. Even in case of conventional computer systems and network systems, the need to cover broad concepts typically results in only an abstract coverage of the principles of operation of digital systems, operating systems, and the interaction of components ranging from storage to peripheral and network subsystems. Moreover, the same desire for abstraction often results in oversimplified models that, while applicable at some point, have long since been superseded; students of digital forensics must, however, typically be familiar with specific implementation characteristics and thus have at least a conceptual framework for studying these rapidly changing models and systems.

Moreover, as noted in section 2, this also extends to information processing and communication systems found in embedded systems that are likely to gain increasing importance as sources of evidence, which not only present different operating environments and constraints (e.g. real-time as well as computational and memory) but also a diversity of capabilities ranging from radio-frequency identification tags via sensors to the rich capabilities of smart phones and vehicular systems. Moreover, such environments also interact with sensors and the physical environment, requiring further consideration. Beyond these topics, however, a review of research activities in digital forensics does not allow the conclusive specification of a set syllabus for courses or even an entire degree program; while areas such as host and network forensics including malicious software mechanisms to be used both for exfiltration of forensic data and as attack mechanisms to be discovered are uncontroversial, neither the depth of coverage nor the systems to be covered are defined clearly. Similarly, while a background in cryptology and particularly cryptanalysis along with ancillary areas such as steganography and steganalysis are highly desirable, they will necessarily be limited in scope. We therefore find it inevitable to structure modules and curricula in such a way that foundational courses described above together with surveys of these topics are augmented by directed individual studies in support of students' research activities.

Finally, another area specific to digital forensics — although similar issues also arise in a more general information security context — is clearly the legal domain. However, this is problematic particularly for highly international programs in that despite recent efforts at harmonization e.g. within the European Union and the EEA, legal systems as well as procedures for gathering, processing, and presenting evidence are substantially different. As with the areas discussed above, it may therefore be more efficient to provide an overview of the legal frameworks in multiple countries, leaving specialization to subsequent individual study rather than focusing exclusively on a single one; this rationale is particularly supported by the observation that not only is research in digital forensics an inherently international endeavor, but also that even practitioners are more than likely to be confronted with multinational environments whether in criminal proceedings or particularly in compliance or discovery procedures.

4 Enabling Forensics

Much as research on intrusion detection and prevention suffers from the limited scope, volume, and trustworthiness of sensor data, digital forensics is often confronted with sources of evidential data that are barely fit for purpose, incomplete, and of questionable reliability [13]. One area of research that holds considerable promise is therefore the development of new or retrofitted systems providing reliable records suitable for use as evidence, and in many cases, these requirements are paralleled by those for auditing found in other areas. However, while auditing is mostly concerned with linking events to authenticated entities for attribution, this is insufficient for forensics purposes as it is frequently not an individual event but rather a sequence of events, potentially originating with multiple event sources, not all of which are attributable or at least have differentiated degrees of confidence in attribution. This not only requires research on the derivation of appropriate metrics and their efficient incorporation into evidential data but also further consideration on preservation mechanisms for such data in the presence of tampering and compromise on one hand and, moreover, approaches to linking individual items into a more comprehensive and coherent whole, often also based on a distributed system lacking a common time base. Thus, in addition to the subjects noted in section 3, research in this area will typically require familiarity with the relevant abstractions from mathematics and computer science such as for distributed algorithms and cryptographic primitives, e.g. for secure multiparty computation, frequently already found in more general information security curricula, but applied to the rather different models of correctness, trust, and reliability than that more commonly found in theoretical computer science and particularly in cryptography.

5 Conclusions

Digital forensics is enjoying considerable popularity as a subject of studies particularly at the undergraduate level owing in no small part to positive employment prospects together with positive connotation derived from media exposure. At the graduate and postgraduate levels, however, the emphasis of degree programs tends to still favor the application of forensics over the generation of new knowledge, also reflecting that the research agenda is still largely driven by practitioners. While the breadth of the subject area is clearly daunting, we strongly suggest that digital forensics professionals will, as in other fields of inquiry, not just require the ability to apply knowledge but to critically challenge concepts, approaches, and also evidence while at the same time being able to obtain, derive, and analyze digital forensic evidence in novel and cogent ways. We consider conducting research (either under guidance in case of M.Sc. dissertations, or largely independently in case of doctoral studies) to be both a proven pathway as well as a necessity given the — steadily growing as technology and its applications move on — number of unsolved research problems. In this paper we have therefore outlined what may be considered a core area of digital forensics, its interrelationship with information security and the broader

context of applying computational methods to forensic science and how these can, at the graduate and postgraduate levels be best supported using both course modules and alternative forms of study with the former of necessity being devoted mainly to theoretical underpinnings from mathematics as well as computer science and engineering. While some areas overlap with other specializations in the field such as general information security, there is still a considerable area of specialization, which must be covered. Moreover, we also assume that the focus of a graduate or postgraduate program in the field will inherently focus on the understanding of existing and development of new forensic techniques and approaches, requiring familiarization with tools and their application through other means. Given the international nature of the programs considered here, moreover, only limited attention is paid to legal considerations that are specific to a particular country or legal tradition; we readily acknowledge that this trade-off clearly requires further specialization in most cases. Ongoing developments and further research will concentrate on the identification of research-driven curriculum development and the trade-offs associated with offering a broader spectrum of specialized elective modules compared to combining a compulsory core area with guided individual specialization at both the M.Sc. and Ph.D. levels.

Acknowledgments. The author would like to thank J. Austen and A. Tomlinson for valuable discussions and comments.

References

1. Nance, K., Hay, B., Bishop, M.: Digital Forensics: Defining a Research Agenda. In: Proceedings of the 42nd Hawaii International Conference on System Sciences (HICSS 2009), pp. 1–6. IEEE Press, Waikoloa (2009); also published as a CISSE report
2. Figg, W., Zhou, Z.: A Computer Forensics Minor Curriculum Proposal. Journal of Computing Sciences in Colleges 22(4), 32–38 (2007)
3. Taylor, C., Endicott-Popovsky, B., Phillips, A.: Forensics Education: Assessment and Measures of Excellence. In: Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2007), pp. 155–165. IEEE Press, Seattle (2007)
4. Yasinsac, A., Erbacher, R.F., Marks, D.G., Pollitt, M.G.: Computer Forensics Education. IEEE Security & Privacy 1(4), 15–23 (2003)
5. Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., Stein, M.: Computer Forensics Programs in Higher Education: A Preliminary Study. In: Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education, pp. 147–151. ACM Press, St. Louis (2005)
6. Bem, D., Huebner, E.: Computer Forensics Workshop for Undergraduate Students. In: Proceedings of the Tenth Conference on Australasian Computing Education, pp. 29–33. Australian Computer Society, Wollongong (2008)
7. Cohen, F.B., Johnson, T.A.: A Ph.D. Curriculum for Digital Forensics. In: Proceedings of the 42nd Hawaii International Conference on System Sciences (HICSS 2009), pp. 1–8. IEEE Press, Waikoloa (2009)

8. Franke, K., Srihari, S.N.: Computational Forensics: An Overview. In: Srihari, S.N., Franke, K. (eds.) IWCF 2008. LNCS, vol. 5158, pp. 1–10. Springer, Heidelberg (2008)
9. Foster, K.R., Huber, P.W.: Judging Science: Scientific Knowledge and the Federal Courts. MIT Press, Cambridge (1997)
10. Aitken, C.G.G., Taroni, F.: Statistics and the Evaluation of Evidence for Forensic Scientists, 2nd edn. John Wiley & Sons, New York (2004)
11. Taroni, F., Aitken, C., Garbolino, P., Biedermann, A.: Bayesian Networks and Probabilistic Inference in Forensic Science. John Wiley & Sons, New York (2006)
12. Pearl, J.: Causality: Models, Reasoning, and Inference, 2nd edn. Cambridge University Press, Cambridge (2009)
13. sDeane, W.: System Event Monitoring as a Security Control. Master's thesis, Royal Holloway, University of London, Egham, Surrey, UK (September 2008)

Author Index