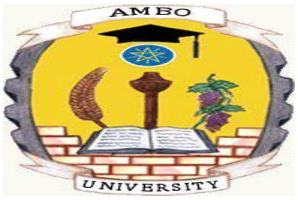


AMBO UNIVERISTY

WALISO CAMPUS

COLLEGE OF TECHNOLOGY AND INFORMATICS

DEPARTMENT OF INFORMATION TECHNOLOGY

Information Assurance and Security Handout

By

AYANTU GUYE BERISA

Woliso, Oromia, Ethiopia

June, 2020

Chapter 1

Cryptography and Network Security

Introduction

- Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit.
- Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

What is the difference among Computer, Network and Internet Security?

1. ***Computer Security*** *- generic name for the collection of tools designed to protect data and to thwart hackers.*
2. ***Network Security*** *- measures to protect data during their transmission.*
3. ***Internet Security*** *- measures to protect data during their transmission over a collection of interconnected networks.*

Security Attacks, Services and Mechanisms

- To assess the security needs of an organization effectively, the **manager** responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements.
- One approach is to consider **three aspects of information security**:
    1. **Security attack** – Any action that compromises the security of information owned by an organization.
    2. **Security mechanism** – A mechanism that is designed to detect, prevent or recover from a security attack.
    3. **Security service** – A service that enhances the security of the data processing systems and the information transfers of an organization. The

services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

Basic Concepts

Cryptography The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form

- ***Plaintext*** *The original intelligible message*
- ***Cipher text*** *The transformed message*
- ***Cipher*** *An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods*
- ***Key*** *Some critical information used by the cipher, known only to the sender& receiver*
- ***Encipher*** *(encode) The process of converting plaintext to cipher text using a cipher and a key*
- ***Decipher*** *(decode) the process of converting cipher text back into plaintext using a cipher and a key*
- **Cryptanalysis** The study of principles and methods of transforming an unintelligible message back into an intelligible message *without* knowledge of the key. Also called **code breaking**
- **Cryptology** Both cryptography and cryptanalysis
- **Code** An algorithm for transforming an intelligible message into an unintelligible one using a code-book

Cryptography

Cryptographic systems are generally classified along 3 independent dimensions:

1. **Type of operations used for transforming plain text to cipher text:** All the encryption algorithms are based on two general principles:
   A. ***Substitution****, in which each element in the plaintext is mapped into another element, and*
   B. ***Transposition****, in which elements in the plaintext are rearranged.*
2. **The number of keys used**
   - ☞ If the sender and receiver uses same key then it is said to be **symmetric key (or) single key (or) conventional encryption**.

- ☞ If the sender and receiver use different keys then it is said to be **public key encryption**.

3. **The way in which the plain text is processed**
   A. A **block cipher** processes the input and block of elements at a time, producing output block for each input block.
   B. A **stream cipher** processes the input elements continuously, producing output element one at a time, as it goes along.

Cryptanalysis

- The process of attempting to discover X or K or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.

There are various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

A. **Cipher text only** – A copy of cipher text alone is known to the cryptanalyst.
B. **Known plaintext** – The cryptanalyst has a copy of the cipher text and the corresponding plaintext.
C. **Chosen plaintext** – The cryptanalysts gains temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.
D. **Chosen cipher text** – The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key.

Steganography

- A plaintext message may be hidden in any one of the two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.
- A simple form of steganography, but one that is time consuming to construct is one in which an arrangement of words or letters within an apparently innocuous text

spells out the real message. e.g., (i) the sequence of first letters of each word of the overall message spells out the real (Hidden) message. (ii) Subset of the words of the overall message is used to convey the hidden message.

Various other techniques have been used historically, some of them are

- **Character marking** – selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held to an angle to bright light.
- **Invisible ink** – a number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
- **Pin punctures** – small pin punctures on selected letters are ordinarily not visible unless the paper is held in front of the light. Typewritten correction ribbon – used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Drawbacks of steganography

1. *Requires a lot of overhead to hide a relatively few bits of information.*
2. *Once the system is discovered, it becomes virtually worthless.*

Security Services

The classification of security services are as follows:

1. **Confidentiality:** Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. E.g. Printing, displaying and other forms of disclosure.
2. **Authentication:** Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
3. **Integrity:** Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
4. **Non repudiation**: Requires that neither the sender nor the receiver of a message be able to deny the transmission.
5. **Access control**: Requires that access to information resources may be controlled by or the target system.

6. **Availability**: Requires that computer system assets be available to authorized parties when needed.

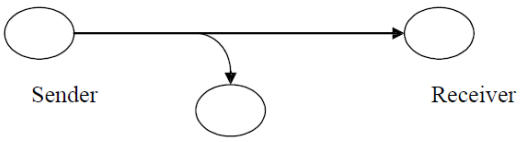
Security Mechanisms

- One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security.
- Some of the mechanisms are
    1. Encipherment
    2. Digital Signature
    3. Access Control

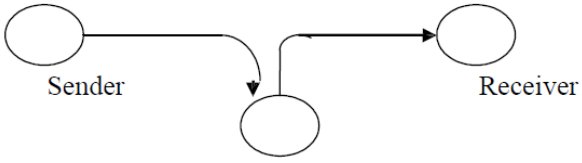
Security Attacks

There are four general categories of attack which are listed below.

1. **Interruption: -**An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.
2. **Interception: -**An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer. e.g., wiretapping to capture data in the network, illicit copying of files

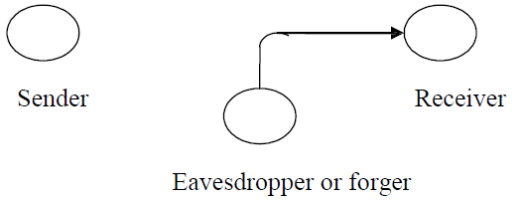


3. **Modification: -**An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.



Eavesdropper or forger

4. **Fabrication: -**An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file.



Cryptographic Attacks

Passive Attacks: -Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive attacks are of two types:

A. **Release of message contents:** A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

B. **Traffic analysis**: If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.

Active attacks: -These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:

1. **Masquerade** – One entity pretends to be a different entity.
2. **Replay** – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.
3. **Modification of messages** – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.
4. **Denial of service** – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire

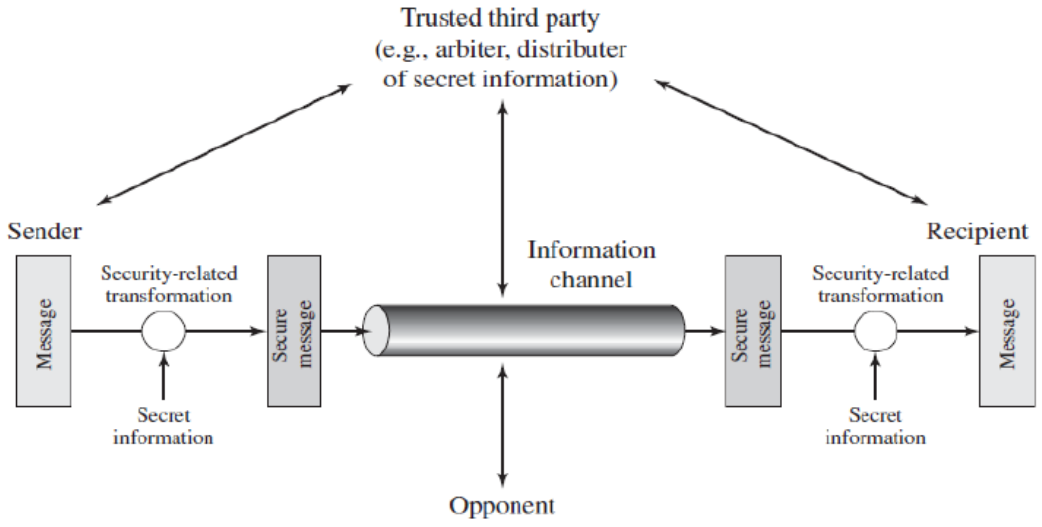
network, either by disabling the network or overloading it with messages so as to degrade performance.

It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

Symmetric and public key algorithms

- Encryption/Decryption methods fall into two categories.
  A. Symmetric key
  B. Public key
- In symmetric key algorithms, the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it.
- In many cases, the encryption and decryption keys are the same. In public key cryptography, encryption key is made public, but it is computationally infeasible to find the decryption key without the information known to the receiver.

A MODEL FOR NETWORK SECURITY



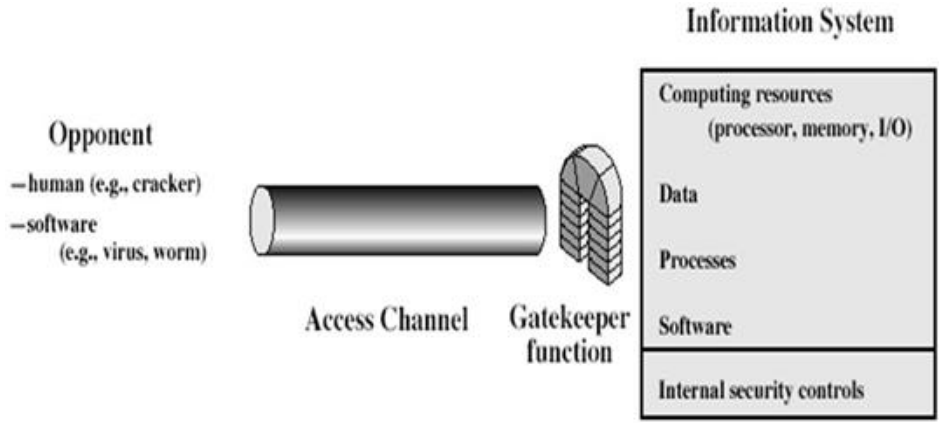
A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the

internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

Using this model requires us to:

- ☞ Design a suitable algorithm for the security transformation.
- ☞ Generate the secret information (keys) used by the algorithm.
- ☞ Develop methods to distribute and share the secret information.
- ☞ Specify a protocol enabling the principals to use the transformation and secret information for a security service.

Model for Network Access Security



Using this model requires us to:

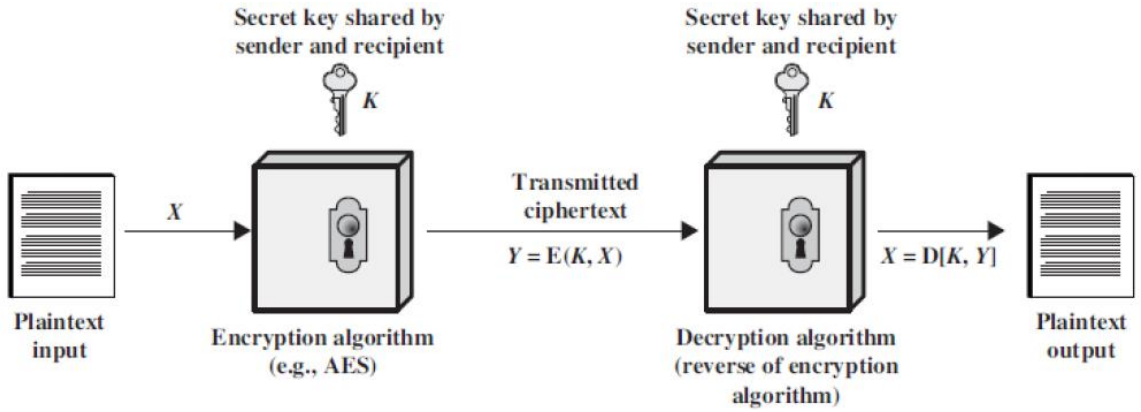
- ☞ Select appropriate gatekeeper functions to identify users.
- ☞ Implement security controls to ensure only authorized users access designated information or resources.

Trusted computer systems can be used to implement this model.

Conventional Encryption

- ☞ Referred conventional / private-key / single-key.
- ☞ Sender and recipient share a common key

All classical encryption algorithms are private-key was only type prior to invention of public key in 1970"**plaintext** - the original message.



Here the original message, referred to as plaintext, is converted into apparently random nonsense, referred to as cipher text. The encryption process consists of an algorithm and a key.

The key is a value independent of the plaintext. Changing the key changes the output of the algorithm. Once the cipher text is produced, it may be transmitted. Upon reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption. The security depends on several factors. First, the encryption algorithm must be powerful enough that it is impractical to decrypt a message on the basis of cipher text alone. Beyond that, the security depends on the secrecy of the key, not the secrecy of the algorithm.

Two requirements for secure use of symmetric encryption:

1. A strong encryption algorithm
2. A secret key known only to sender / receiver

$$Y = EK(X)$$

$$X = DK(Y)$$

- ☞ ***assume encryption algorithm is known***
- ☞ ***implies a secure channel to distribute key***

A source produces a message in plaintext, X = [X1, X2… XM] where M, are the number of letters in the message. A key of the form K = [K1, K2… KJ] is generated. If the key is generated at the source, then it must be provided to the destination by means of some secure channel.

With the message X and the encryption key K as input, the encryption algorithm forms the cipher text Y = [Y1, Y2, YN]. This can be expressed as Y = EK(X).

The intended receiver, in possession of the key, is able to invert the transformation: X = DK(Y)

An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both. It is assumed that the opponent knows the encryption and decryption algorithms.

If the opponent is interested in only this particular message, then the focus of effort is to recover X by generating a plaintext estimate. Often if the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover K by generating an estimate.

Classical Encryption Techniques

There are two basic building blocks of all encryption techniques: **substitution** and **transposition**.

Substitution Techniques

- **A substitution technique** is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

Caesar cipher (or) shift cipher

- The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

e.g., plain text: pay more money

Cipher text: SDB PRUH PRQHB

Note that the alphabet is wrapped around, so that letter following „z" is „a". For each plaintext letter p, substitute the cipher text letter c such that

$$C = E(p) = (p+3) \bmod 26$$

A shift may be any amount, so that general Caesar algorithm is

$$C = E(p) = (p+k) \bmod 26$$

Where k, takes on a value in the range 1 to 25. The decryption algorithm is simply

$$P = D(C) = (C-k) \bmod 26$$

Playfair cipher

The best known multiple letter encryption cipher is the **playfair**, which treats digrams in the plaintext as single units and translates these units into cipher text digrams. The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be „monarchy". The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order.

The letter "I" and "j" count as one letter. Plaintext is encrypted two letters at a time According to the following rules:

Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as „x". Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row following the last. Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last.

Otherwise, each plaintext letter is replaced by the letter that lies in its own row And the column occupied by the other plaintext letter.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

What is Enterprise Security?

- Security mechanism dealing with providing **confidentiality, integrity, authentication, authorization** and **non-repudiation** related to the entire organization's computing resources.

Why is Cyber security Important?

- **Cyber security** is important because it encompasses everything that pertains to **protecting our sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data**, and **governmental and industry information systems from theft and damage attempted by criminals and adversaries**.
- Cyber security risk is increasing, driven by global connectivity and usage of cloud services, like Amazon Web Services, to store sensitive data and personal information. Widespread poor configuration of cloud services paired with increasingly sophisticated cyber criminals means the risk that your organization suffers from a successful cyber-attack or data breach is on the rise.
- Gone are the days of simple firewalls and antivirus software being your sole security measures. Business leaders can no longer leave information security to cyber security professionals.
- **Cyber threats** can come from any level of your organization. You must educate your staff about simple ***social engineering scams*** like **phishing** and more sophisticated cyber security attacks like ransom ware (think WannaCry) or other malware designed to steal intellectual property or personal data.
- GDPR and other laws mean that cyber security is no longer something businesses of any size can ignore. Security incidents regularly affect businesses of all sizes and often make the front page causing irreversible reputational damage to the companies involved.

The importance of cyber security

- Our society is more technologically reliant than ever before and there is no sign that this trend will slow. Personal data that could result in identity theft is now posted to the public on our social media accounts. Sensitive information like social security

numbers, credit card information and bank account details are now stored in cloud storage services like **Dropbox** or **Google Drive**.

- The fact of the matter is whether you are an individual, small business or large multinational, you rely on computer systems every day. Pair this with the rise in cloud services, poor cloud service security, smartphones and the Internet of Things (IoT) and we have a many of cyber security threats that didn't exist a few decades ago. We need to understand the difference between cyber security and information security, even though the skillsets are becoming more similar.
- Governments around the world are bringing more attention to cybercrimes. GDPR is a great example. It has increased the reputational damage of data breaches by forcing all organizations that operate in the EU to:
  - *Communicate data breaches*
  - *Appoint a data-protection officer*
  - *Require user consent to process information*
  - *Anonymize data for privacy*
- The trend towards public disclosure is not limited to Europe. While there are no national laws overseeing data breach disclosure in the United States, there are data breach laws in all 50 states. Commonalities include:
  - *The requirement to notify those affect as soon as possible*
  - *Let the government know as soon as possible*
  - *Pay some sort of fine*
- California was the first state to regulate data breach disclosures in 2003, requiring persons or businesses to notify those affected "without reasonable delay" and "immediately following discovery". Victims can sue for up to $750 and companies can be fined up to $7,500 per victim.
- This has driven standards boards like the National Institute of Standards and Technology (NIST) to release frameworks to help organizations understand their security risks, improve cyber security measures and prevent cyber-attacks.

Why is cybercrime increasing?

- Information theft is the most expensive and fastest growing segment of cybercrime. Largely driven by the increasing exposure of identity information to the web via cloud services. But it is not the only target. Industrial controls that manage power grids and other infrastructure can be disrupted or destroyed. And identity theft isn't the only goal, cyber-attacks may aim to compromise data integrity (destroy or change data) to breed distrust in an organization or government.
- **Cybercriminal**s are becoming more ***sophisticated, changing what they target, how they affect organizations and their methods of attack for different security systems***.
- **Social engineering** remains the easiest form of cyber-attack with ransom ware and phishing being the easiest form of entry. Third-party and fourth-party vendors who process your data and have poor cyber security practices are another common attack vector, making vendor risk management and third-party risk management all the more important.
- According to the Ninth Annual Cost of Cybercrime Study from Accenture and the Ponemon Institute, the average cost of cybercrime for an organization has increased by **$1.4 million** over the last year to **$13.0 million** and the average number of data breaches rose by 11 percent to 145. Information risk management has never been more important.
- Data breaches can involve financial information like ***credit card numbers or bank account details, protected health information (PHI), personally identifiable information (PII), trade secrets, intellectual property and other targets of industrial espionage.*** Other terms for data breaches include unintentional information disclosure, data leak, cloud leak, information leakage or a data spill.
- Other factors driving the growth in cybercrime include:
  - *The distributed nature of the Internet*
  - *The ability for cybercriminals to attack targets outside their jurisdiction making policing extremely difficult*
  - *Increasing profitability and ease of commerce on the dark web*

What is the impact of cybercrime?

- A lack of focus on cyber security can damage your business in range of ways including:
  - ***Economic costs:*** *Theft of intellectual property, corporate information, disruption in trading and the cost of repairing damaged systems*
  - ***Reputational costs:*** *Loss of consumer trust, loss of current and future customers to competitors and poor media coverage*
  - ***Regulatory costs:*** *GDPR and other data breach laws mean that your organization could suffer from regulatory fines or sanctions as a result of cybercrimes*
- All businesses, regardless of the size, must ensure all staff understands cyber security threats and how to mitigate them. This should include regular training and a framework to work with to that aims to reduce the risk of data leaks or data breaches.
- Given the nature of cybercrime and how difficult it can be to detect, it is difficult to understand the direct and indirect costs of many security breaches. This doesn't mean the reputational damage of even a small data breach or other security event is not large. If anything, consumers expect increasingly sophisticated cyber security measures as time goes on.

How to protect your organization against cybercrime

- There are three simple steps you can take you increase security and reduce risk of cybercrime:
  1. *Educate all levels of your organization about the risks of social engineering and common social engineering scams like phishing emails and typo squatting*
  2. *Invest in tools that limit information loss, monitor your third-party risk and fourth-party vendor risk and continuously scan for data exposure and leak credentials*
  3. *Use technology to reduce costs like automatically sending out vendor assessment questionnaires as part of an overall cyber security risk assessment strategy*

Examples of damages to companies affected by cyber-attacks and data breaches

- The amount of cyber-attacks and data breaches in the recent years is staggering and it's easy to produce a laundry list of companies who are household names that have been affected. Here's a few examples:

1. ***Equifax:*** *The Equifax cybercrime identity theft event affected approximately 145.5 million U.S. consumers along with 400,000-44 million British residents and 19,000 Canadian residents. Equifax shares dropped 13% in early trading the day after the breach and numerous lawsuits were filed against Equifax as a result of the breach. Not to mention the reputational damage that Equifax suffered. On July 22 2019, Equifax agreed to a settlement with the FTC which included a $300 million fund for victim compensation, $175m for states and territories in the agreement and $100 million in fines.*
2. ***eBay:*** *Between February and March 2014, eBay was the victim of a breach of encrypted passwords, which resulted in asking all of its 145 million users to reset their password. Attackers used a small set of employee credentials to access this trove of user data. The stolen information included encrypted passwords and other personal information, including names, e-mail addresses, physical addresses, phone numbers and dates of birth. The breach was disclosed in May 2014, after a month-long investigation by eBay.*
3. ***Adult Friend Finder:*** *In October 2016, hackers collected 20 years of data on six databases that included names, email addresses and passwords for The Friend Finder Network. The Friend Finder Network includes websites like Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com. Most of the passwords were protected only by the weak SHA-1 hashing algorithm, which meant that 99% of them had been cracked by the time LeakedSource.com published its analysis of the entire data set on November 14.*
4. ***Yahoo:*** *Yahoo disclosed that a breach in August 2013 by a group of hackers had compromised 1 billion accounts. In this instance, security questions and answers were also compromised, increasing the risk of identity theft. The breach was first reported by Yahoo on December 14, 2016, and forced all affected users to change passwords, and to reenter any unencrypted security questions and answers to make them encrypted in the future. However, by October of 2017, Yahoo changed the estimate to 3 billion user accounts. An investigation revealed that users' passwords in clear text, payment card data and bank information were not stolen. Nonetheless, this remains one of the largest data breaches of this type in history.*

What is cyber defense?

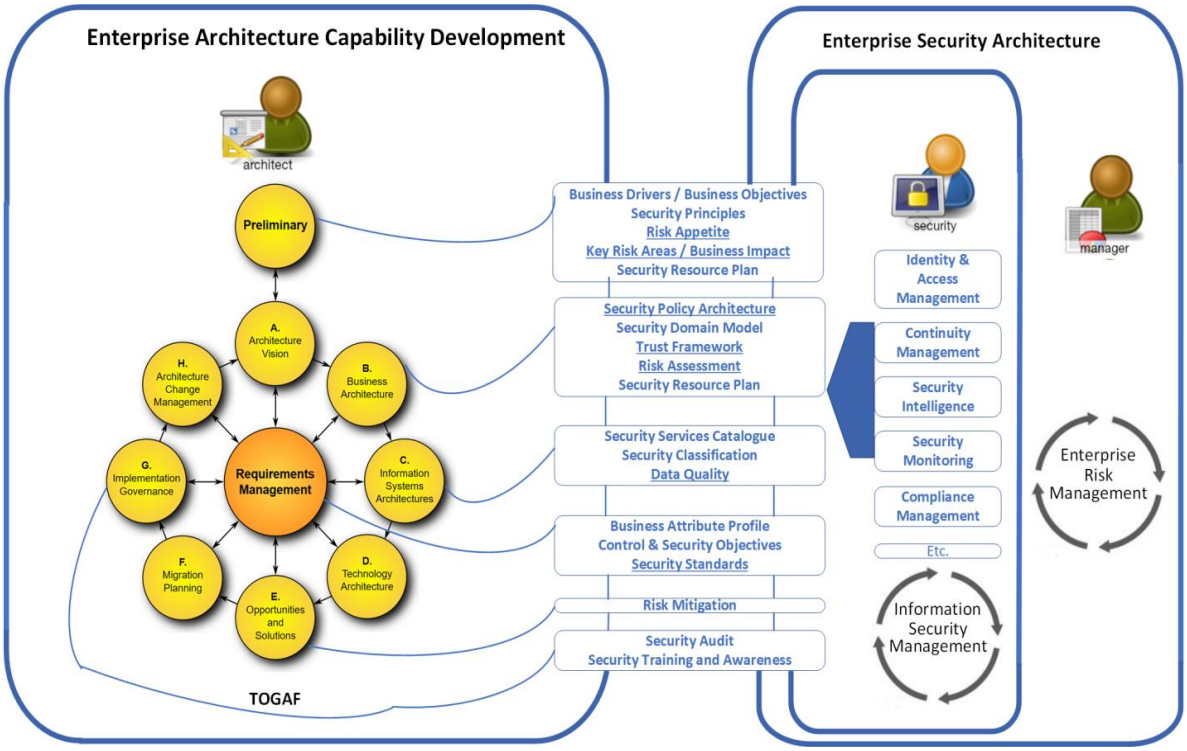
- **Cyber defense** is a computer network defense mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks.
- Cyber defense focuses on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with.
- With the growth in volume as well as complexity of cyber-attacks**, cyber defense** is essential for most entities in order to protect sensitive information as well as to safeguard assets.
- **Cyber defense** protects your most important business assets against attack. By aligning the knowledge of the threats you face with an understanding of your environment, you're able to maximize the effectiveness of your security spend and target your resources at the critical locations. All this is driven from your business strategy, by identifying where it may be at risk from a range of threats - from a malicious insider right through to **Advanced Persistent Threats (APT)**.
- Cyber defense covers a wide range of activities that are essential in enabling your business to protect itself against attack and respond to a rapidly evolving threat landscape. This will include:
  - *Cyber preventions to reduce your appeal to the attackers*
  - *Preventative controls that require their attacks to be more costly*
  - *Attack detection capability to spot when they are targeting you*
  - *Reaction and response capabilities to repel them*
- Typically a cyber-defense engagement will include a range of services aimed at long term assurance of your business - from the understanding of how security impacts your business strategy and priorities, through to training and guidance that helps your employees establish the right security culture.
- At the same time, the engagement will include specialist technical analysis and investigation to make sure you can map out and protect the paths attackers will use to compromise your most sensitive assets. These activities also enable you to obtain

evidence of any previous threats that have breached your defenses and providing the capability to manage or remove them as needed.

- Using this blend of services, cyber defense provides the assurances you need to run your business without worrying about the threats it faces, and makes sure your security strategy utilizes your resources in the most effective manner.

Enterprise Security within an Enterprise Architecture Context

- An **Enterprise Security Architecture** is a structure of organizational, conceptual, logical, and physical components that interact to achieve and maintain a state of managed risk and security.
- **Enterprise Security Architecture** is also a driver and enabler of secure, resilient, and reliable behavior that addresses and mitigates security risks throughout the enterprise.
- That's essentially what security architecture is all about except it never exists in isolation - it needs enterprise architecture to reside in. Lastly, security architecture is a process - it's something you do - not something you can buy.
- One of the biggest learning's is that security architecture and information security are not just technology problems - security is not a technical problem to be solved - it's a risk to be managed.
- Let's take a look at these aspects in a little more detail. "It doesn't exist in isolation", "it's a process - something you do", and "security is a risk to be managed not a problem to be solved"
- In the diagram below I'm showing how the phases in TOGAF EA artifact's produced from TOGAF relate to security architecture highlighting the core security and risk concepts that are used in Information Security Management (ISM) and Enterprise Risk Management (ERM).



- Security architecture flows from enterprise architecture. So regardless of whether you use TOGAF, Zachman or another framework the artifact's (outputs) produced from EA become the inputs and the starting point for defining your security architecture.
- Enterprise Security Architecture is also the design artifacts that describe how the security controls are positioned (security posture), and how they relate to the overall IT Architecture. These controls serve the purpose to maintain quality attributes, among them confidentiality, integrity, availability, non-repudiation, accountability and assurance.

Chapter 2

Brief overview of Commercial Issues on Security

Introduction

- Human being from ages had two inherent needs:
    1. To communicate and share information and
    2. To communicate selectively.
- These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information.
- Unauthorized people could not extract any information, even if the scrambled messages fell in their hand.
    - *The art and science of concealing the messages to introduce secrecy in information security is recognized as **cryptography**.*
- The word '**cryptography**' was coined by combining two Greek words, '**Krypto**' meaning **hidden** and '**graphene**' meaning **writing**.

What is Cryptography?

- **Cryptography** is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as **data confidentiality, data integrity, authentication, and non-repudiation** are central to modern cryptography.
- Modern **cryptography** exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics.
- Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.
- **Cryptography** is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

- Earlier cryptography was effectively synonymous with encryption but nowadays cryptography is mainly based on mathematical theory and computer science practice.

Modern cryptography concerns with:

1. ***Confidentiality*** *- Information cannot be understood by anyone.*
2. ***Integrity*** *- Information cannot be altered.*
3. ***Non-repudiation*** *- Sender cannot deny his/her intentions in the transmission of the information at a later stage.*
4. ***Authentication*** *- Sender and receiver can confirm each.*

- Cryptography is used in many applications like banking transactions cards, computer passwords, and e- commerce transactions.

Three types of cryptographic techniques used in general.

1. *Symmetric-key cryptography*
2. *Hash functions.*
3. *Public-key cryptography*

- **Symmetric-key Cryptography**: Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.
- **Public-Key Cryptography**: This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.
- **Hash Functions**: No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

Web Services Security

- **Web security** is also known as "**Cyber security**". It basically means protecting a website or web application by **detecting, preventing and responding to cyber threats**.

- Websites and web applications are just as prone to security breaches as physical homes, stores, and government locations. Unfortunately, cybercrime happens every day, and great web security measures are needed to protect websites and web applications from becoming compromised.
- That's exactly **what web security does** – it is a system of protection measures and protocols that can protect your website or web application from being hacked or entered by unauthorized personnel. This integral division of Information Security is vital to the protection of websites, web applications, and web services. Anything that is applied over the Internet should have some form of web security to protect it.

Details of Web Security

- There are a lot of factors that go into web security and web protection. Any website or application that is secure is surely backed by different types of checkpoints and techniques for keeping it safe.
- There are a variety of security standards that must be followed at all times, and these standards are implemented and highlighted by the OWASP. Most experienced web developers from top cyber security companies will follow the standards of the OWASP as well as keep a close eye on the Web Hacking Incident Database to see when, how, and why different people are hacking different websites and services.
- Essential steps in protecting web apps from attacks include applying up-to-date encryption, setting proper authentication, continuously patching discovered vulnerabilities, avoiding data theft by having secure software development practices. The reality is that clever attackers may be competent enough to find flaws even in a fairly robust secured environment, and so a holistic security strategy is advised.

Available Technology

- There are different types of technologies available for maintaining the best security standards. Some popular technical solutions for testing, building, and preventing threats include:
  - *Black box testing tools*
  - *Fuzzing tools*
  - *White box testing tools*
  - *Web application firewalls (WAF)*
  - *Security or vulnerability scanners*
  - *Password cracking tools*

Likelihood of Threat

- Your website or web application's security depends on the level of protection tools that have been equipped and tested on it. There are a few major threats to security which are the most common ways in which a website or web application becomes hacked. Some of the top vulnerabilities for all web-based services include:
  - *SQL injection*
  - *Password breach*
  - *Cross-site scripting*
  - *Data breach*
  - *Remote file inclusion*
  - *Code injection*
- Preventing these common threats is the key to making sure that your web-based service is practicing the best methods of security.

The Best Strategies

- There are two big defense strategies that a developer can use to protect their website or web application. The two main methods are as follows:
  1. **Resource assignment** – By assigning all necessary resources to causes that are dedicated to alerting the developer about new web security issues and threats, the developer can receive a constant and updated alert system that will help them detect and eradicate any threats before security is officially breached.

2. **Web scanning** – There are several web scanning solutions already in existence that are available for purchase or download. These solutions, however, are only good for known vulnerability threats – seeking unknown threats can be much more complicated. This method can protect against many breaches, however, and is proven to keep websites safe in the long run.

Web Security also protects the visitors from the below-mentioned points –

- **Stolen Data:** Cyber-criminals frequently hacks visitor's data that is stored on a website like email addresses, payment information, and a few other details.
- **Phishing schemes**: This is not just related to email, but through phishing, hackers design a layout that looks exactly like the website to trick the user by compelling them to give their sensitive details.
- **Session hijacking**: Certain cyber attackers can take over a user's session and compel them to take undesired actions on a site.
- **Malicious redirects**. Sometimes the attacks can redirect visitors from the site they visited to a malicious website.
- **SEO Spam**. Unusual links, pages, and comments can be displayed on a site by the hackers to distract your visitors and drive traffic to malicious websites.

- Thus, web security is easy to install and it also helps the business people to make their website safe and secure. A web application firewall prevents automated attacks that usually target small or lesser-known websites. These attacks are borne out by malicious bots or malware that automatically scan for vulnerabilities they can misuse, or cause DDoS attacks that slow down or crash your website.
- Thus, Web security is extremely important, especially for websites or web applications that deal with confidential, private, or protected information. Security methods are evolving to match the different types of vulnerabilities that come into existence.

What is public key infrastructure (PKI)?

- A **public key infrastructure (PKI)** is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

- Public Key Infrastructure (PKI) is a technology for authenticating users and devices in the digital world. The basic idea is to have one or more trusted parties digitally sign documents certifying that a particular cryptographic key belongs to a particular user or device. The key can then be used as an identity for the user in digital networks.
- The users and devices that have keys are often just called entities. In general, anything can be associated with a key that it can use as its identity. Besides a user or device, it could be a program, process, manufacturer, component, or something else. The purpose of a PKI is to securely associate a key with an entity.
- The trusted party signing the document associating the key with the device is called a certificate authority (CA). The certificate authority also has a cryptographic key that it uses for signing these documents. These documents are called certificates.
- In the real world, there are many certificate authorities, and most computers and web browsers trust a hundred or so certificate authorities by default.
- A public key infrastructure relies on digital signature technology, which uses public key cryptography. The basic idea is that the secret key of each entity is only known by that entity and is used for signing. This key is called the private key. There is another key derived from it, called the public key, which is used for verifying signatures but cannot be used to sign. This public key is made available to anyone, and is typically included in the certificate document.
- The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.
- In cryptography, a PKI is an arrangement that binds public keys with respective identities of entities (like people and organizations). The binding is established through a process of registration and issuance of certificates at and by a certificate

authority (CA). Depending on the assurance level of the binding, this may be carried out by an automated process or under human supervision.

- The PKI role that assures valid and correct registration is called a registration authority (RA). An RA is responsible for accepting requests for digital certificates and authenticating the entity making the request. In a Microsoft PKI, a registration authority is usually called a subordinate CA.
- An entity must be uniquely identifiable within each CA domain on the basis of information about that entity. A third-party validation authority (VA) can provide this entity information on behalf of the CA.
- The X.509 standard defines the most commonly used format for public key certificates.

Chapter 3

Network Firewall Security

Securing Private Networks

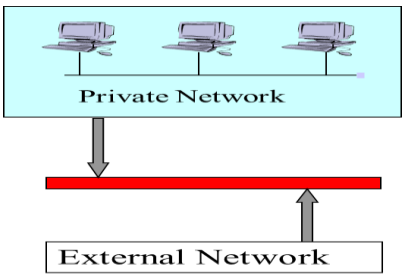
- Minimize external access to LAN
- Done by means of firewalls and proxy servers
- Firewalls provide a secure interface between an "inner" trusted network and "outer" untrusted network.
- every packet to and from inner and outer network is "processed"
- Firewalls require hardware and software to implement
- Software that is used are proxies and filters that allow or deny network traffic access to either network

Overview of Firewall

- Firewall is a router or other communications device which filters access to a protected network.
- Firewall is also a program that screens all incoming traffic and protects the network from unwelcome intruders.
- It is a means of protection a local system or network of systems from network-based security threats,
    - while affording access to the outside world via WANs or the Internet

Firewall Objectives

- Keep intruders, malicious code and unwanted traffic or information out
- Keep private and sensitive information in
- security wall between private (protected) network and outside word



Firewall features

- General Firewall Features
  - Port Control
  - Network Address Translation
  - Application Monitoring
  - Packet Filtering
  - Access control
- Additional features
  - Data encryption
  - Authentication
  - Connection relay (hide internal network)
  - reporting/logging
  - e-mail virus protection
  - spy ware protection
- Use one or both methods
  - Packet filtering
  - Proxy service
- It protects from
  - Remote logins
  - IP spoofing
  - Source addressing
  - SMTP session hijacking
  - Spam
  - Denial of service
  - E-mail bombs…

Firewall design principles

- Internet connectivity is no longer an option for most organizations. However, while internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets. This creates the threat to the organization.
- While it is possible to equip each workstation and server on the premises network with strong security features, such as **intrusion protection**, this is not a practical approach. The alternative, increasingly accepted, is the ***firewall***.
- The **firewall** is inserted between the **premise network** and **internet** to establish a controlled link and to create an outer security wall or perimeter.
    - The aim of this perimeter is to protect the premises network from internet based attacks and to provide a single choke point where security and audit can be imposed.
- The firewall can be a single computer system or a set of two or more systems that cooperate to perform the firewall function.

Firewall characteristics

- All traffic from inside to outside, and vice versa, must pass through the firewall.
    - This is achieved by physically blocking all access to the local network except via the firewall.
- Various configurations are possible. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.
- The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

Four techniques that firewall use to control access and enforce the site's security policy is as follows:

1. ***Service control*** *– determines the type of internet services that can be accessed, inbound or outbound. The firewall may filter traffic on this basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as web or mail service.*

2. *Direction control – determines the direction in which particular service request may be initiated and allowed to flow through the firewall.*
3. *User control – controls access to a service according to which user is attempting to access it.*
4. *Behavior control – controls how particular services are used.*

Capabilities of firewall

- A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.
- A firewall provides a location for monitoring security related events. Audits and alarms can be implemented on the firewall system.
- A firewall is a convenient platform for several internet functions that are not security related. A firewall can serve as the platform for IPsec.

Limitations of firewall

- The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.
- The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
- The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

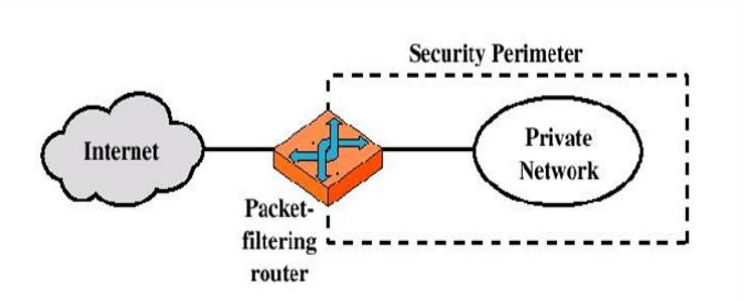
Types of firewalls

There are 3 common types of firewalls.

1. *Packet Filtering Firewalls*
2. *Application-level gateways/ Proxy Server Firewalls*
3. *Circuit-level gateways*

Packet filtering router

- A packet filtering router applies a set of rules to each incoming IP packet and then forwards or discards the packet. The router is typically configured to filter packets going in both directions.
- Filtering rules are based on the information contained in a network packet:
  - ***Source IP address:*** *The IP address of the system that originated the IP packet (e.g., 192.178.1.1)*
  - ***Destination IP address:*** *The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2)*
  - ***Source and destination port address:*** *The transport level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELNET*
  - ***IP protocol field*** *– defines the transport protocol.*
  - ***Interface*** *– for a router with three or more ports, which interface of the router the packet come from or which interface of the router the packet is destined for.*



IP source	IP dest	Port source	Port dest	Action
any	192.54.113.10	any	25	allow
93.54.84.35	any	any	23	allow
any	any	any	23	deny

- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
  - *If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet.*
  - *If there is no match to any rule, then a default action is taken.*
    Two default policies are possible:
    Default = discard: *That which is not expressly permitted is prohibited.*

Default = forward: That which is not expressly prohibited is permitted.

- Packet filtering is generally accomplished using ***Access Control Lists (ACL)*** on routers
- The **default discard policy** is the more conservative. Initially everything is blocked, and services must be added on a case-by-case basis. This policy is more visible to users, who are most likely to see the firewall as a hindrance.
- The default forward policy increases ease of use for end users but provides reduced security.

Advantages of packet filter router

- *Simple Transparent to users*
- *Very fast*

Weakness of packet filter firewalls

- *Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application specific vulnerabilities or functions.*
- *Because of the limited information available to the firewall, the logging functionality present in packet filter firewall is limited.*
- *It does not support advanced user authentication schemes.*
- *They are generally vulnerable to attacks such as layer address spoofing.*

Some of the attacks that can be made on packet filtering routers and the appropriate counter measures are the following:

A. **IP address spoofing** – the intruders transmit packets from the outside with a source IP address field containing an address of an internal host. Countermeasure: to discard packet with an inside source address if the packet arrives on an external interface.

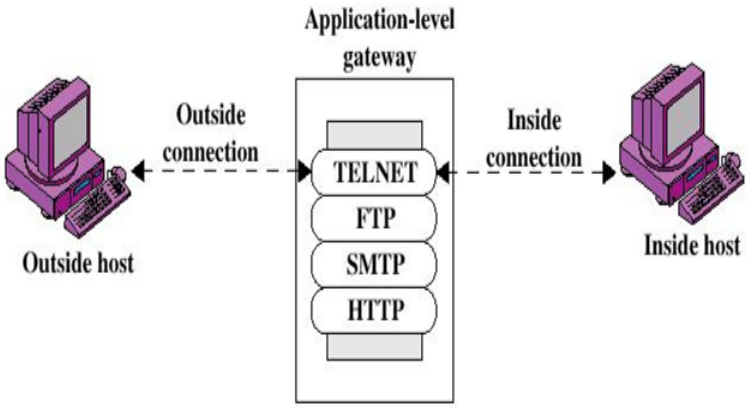
B. **Source routing attacks** – the source station specifies the route that a packet should take as it crosses the internet; i.e., it will bypass the firewall. Countermeasure: to discard all packets that uses this option.

C. **Tiny fragment attacks** – the intruder create extremely small fragments and force the TCP header information into a separate packet fragment. The attacker hopes that only the first fragment is examined and the remaining fragments are passed through.

Countermeasure: to discard all packets where the protocol type is TCP and the IP Fragment offset is equal to 1.

Application level gateway

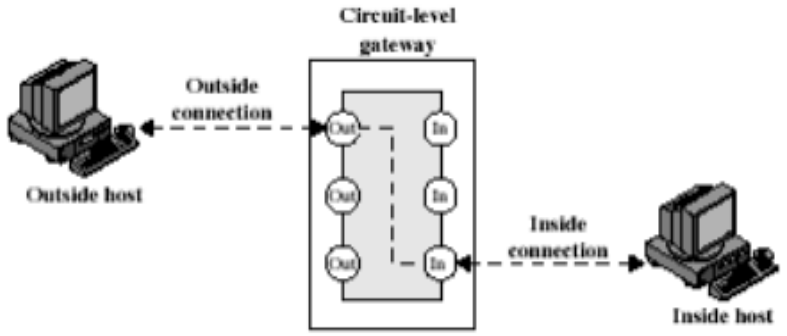
- An ***Application level gateway***, also called a ***proxy server***, acts as a relay of application level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.
- When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.
- **Advantages of application level gateways**
  - *Tend to be **more secure than packet filters**.*
  - *It is **easy to log and audit** all incoming traffic at the application level.*
- A prime disadvantage is the ***additional processing overhead on each connection***.



Circuit level gateway

- Circuit level gateway can be a ***stand-alone system or it can be a specified function performed by an application level gateway*** for certain applications.
- A Circuit level gateway does not permit an ***end to-end TCP connection***; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outer host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

- A typical use of Circuit level gateways is a situation in which the system administrator trusts the internal users.
- The gateway can be configured to support application level or proxy service on inbound connections and circuit level functions for outbound connections.



(c) Circuit-level gateway

Bastion host

- Is a special purpose computer on a network specifically designed and configured to withstand attacks.
- It is a system identified by the firewall administrator as a critical strong point in the network's security.
- The Bastion host ***serves as a platform for an application level and circuit level gateway***.
- Common characteristics of a Bastion host are as follows:
  - The Bastion host hardware platform executes a secure version of its operating system, making it a trusted system.
  - Only the services that the network administrator considers essential are installed on the Bastion host. These include proxy applications such as Telnet, DNS, FTP, SMTP, and user authentication.
  - It may require additional authentication before a user is allowed access to the proxy services.
  - Each proxy is configured to support only a subset of standard application's command set.
  - Each proxy is configured to allow access only to specific host systems.

- Each proxy maintains detailed audit information by logging all traffic, each connection and the duration of each connection.
- Each proxy is independent of other proxies on the Bastion host.
- A proxy generally performs no disk access other than to read its initial configuration file.
- Each proxy runs on a non-privileged user in a private and secured directory on the Bastion host.

Firewall configurations

There are 3 common firewall configurations.

1. *Screened host firewall, single-homed Bastion configuration*

- In this configuration, the firewall consists of two systems: a ***packet filtering router*** *and* ***a bastion host***.
- Typically, the router is configured so that
  - *For traffic from the internet, only IP packets destined for the Bastion host are allowed in.*
  - *For traffic from the internal network, only IP packets from the Bastion host are allowed out.*
- The **Bastion host** performs ***authentication and proxy functions***.
- This configuration has greater security than simply a packet filtering router or an application level gateway alone, for two reasons:
  1. *This configuration implements both packet level and application level filtering, allowing for considerable flexibility in defining security policy.*
  2. *An intruder must generally penetrate two separate systems before the security of the internal network is compromised.*
- This configuration also affords flexibility in providing direct Internet access.
  - *For example, the internal network may include a public information server, such as a Web server, for which a high level of security is not required.*
  - *In that case, the router can be configured to allow direct traffic between the information server and the Internet.*

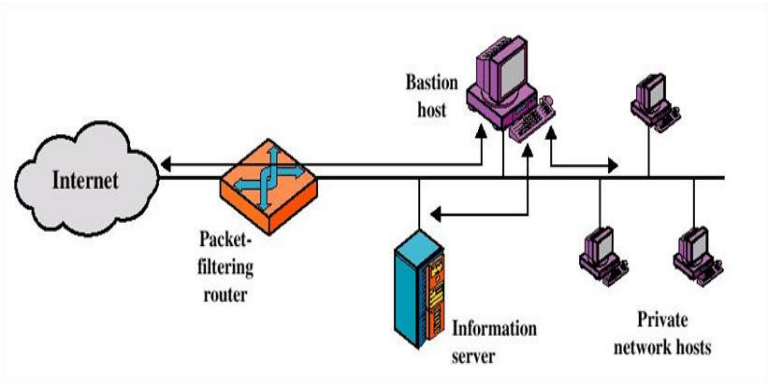


Figure 1: Screened host firewall, single-homed Bastion configuration

2. Screened host firewall, dual homed Bastion configuration

- In the previous configuration, if the packet filtering router is compromised, traffic could flow directly through the router between the internet and the other hosts on the private network. This configuration physically prevents such a security break.
- Traffic between the Internet and other hosts on the private network has to flow through the bastion host
- Uses two NICs for greater security.

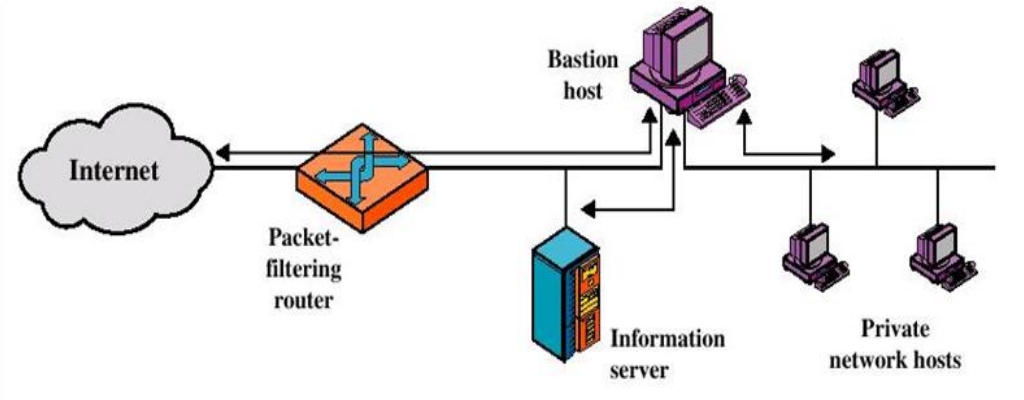


Figure 2: Screened host firewall system (dual-homed bastion host)

3. Screened subnet firewall configuration

- In this configuration, two packet filtering routers are used,
  - *One between the Bastion host and internet and*
  - *One between the Bastion host and the internal network.*

- This configuration creates an isolated sub network, which may consist of simply the Bastion host but may also include one or more information servers and modems for dial-in capability.
- Typically both the internet and the internal network have access to hosts on the screened subnet, but traffic across the screened subnet is blocked.
- This configuration offers several advantages:
  - *There are now three levels of defense to prevent intruders.*
  - *The outside router advertises only the existence of the screened subnet to the internet; therefore* ***the internal network is invisible to the internet.***
  - *Similarly, the inside router advertises only the existence of the screened subnet to the internal network; therefore* ***the systems on the internal network cannot construct direct routes to the internet.***

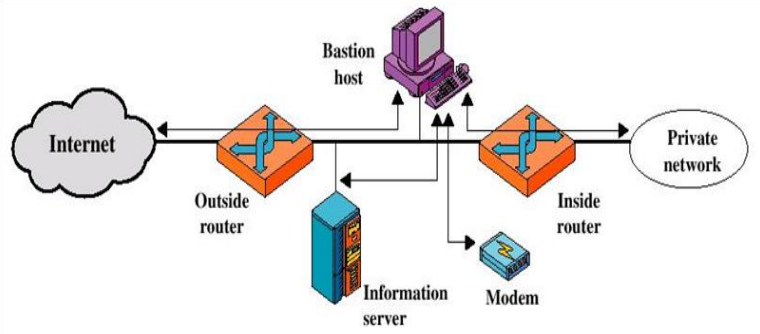


Figure 3: Screened-subnet firewall system

Trusted systems

- One way to enhance the ability of a system to defend against intruders and malicious programs is to ***implement trusted system technology***.

Data access control

- Following successful logon, the user has been granted access to one or set of hosts and applications.
- This is generally not sufficient for a system that includes sensitive data in its database.
- Through the user access control procedure, a user can be identified to the system.
- Associated with each user, there can be a profile that specifies permissible operations and file accesses. The operating system can then enforce rules based on the user profile. The

database management system, however, must control access to specific records or even portions of records.

- The operating system may grant a user permission to access a file or use an application, following which there are no further security checks, the database management system must make a decision on each individual access attempt. That decision will depend not only on the user's identity but also on the specific parts of the data being accessed and even on the information already divulged to the user.
- A general model of access control as exercised by file or database management system is that of an access matrix. The basic elements of the model are as follows:
  - ***Subject:*** *An entity capable of accessing objects. Generally, the concept of subject equates with that of process.*
  - ***Object****: Anything to which access is controlled. Examples include files, portion of files, programs, and segments of memory.*
  - ***Access right****: The way in which the object is accessed by a subject. Examples are read, write and execute.*
- One axis of the matrix consists of identified subjects that may attempt data access. Typically, this list will consist of individual users or user groups.
- The other axis lists the objects that may be accessed. Objects may be individual data fields.
- Each entry in the matrix indicates the access rights of that subject for that object. The matrix may be decomposed by columns, yielding access control lists. Thus, for each object, an access control list lists users and their permitted access rights.
- The access control list may contain a default, or public, entry.

a. Access matrix Access control list for Program1:

   1. *Process1 (Read, Execute) Access control list for Segment A:*
   2. *Process1 (Read, Write) Access control list for Segment B: Process2 (Read)*

b. Access control list Capability list for Process1: Program1 (Read, Execute) Segment A (Read) Capability list for Process2: Segment B (Read)

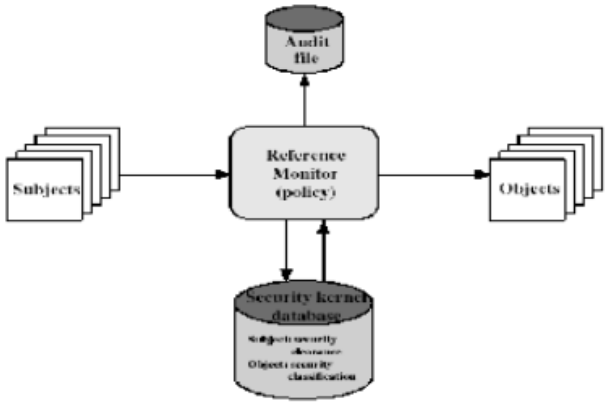
c. Capability list Decomposition by rows yields capability tickets. A capability ticket specifies authorized objects and operations for a user.

- Each user has a number of tickets and may be authorized to loan or give them to others. Because tickets may be dispersed around the system, they present a greater security problem than access control lists.
- In particular, the ticket must be un-forgeable. One way to accomplish this is to have the operating system hold all tickets on behalf of users. These tickets would have to be held in a region of memory inaccessible to users.
- The concept of Trusted Systems When multiple categories or levels of data are defined, the requirement is referred to as multilevel security.
- The general statement of the requirement for multilevel security is that a subject at a high level may not convey information to a subject at a lower or non-comparable level unless that flow accurately reflects the will of an authorized user. For implementation purposes, this requirement is in two parts and is simply stated.
- A multilevel secure system must enforce:
  - ***No read up:*** *A subject can only read an object of less or equal security level. This is referred to as simple security property.*
  - ***No write down:*** *A subject can only write into an object of greater or equal security level. This is referred to as *-property (star property).*
- These two rules, if properly enforced, provide multilevel security.

Reference Monitor concept

- The reference monitor is a controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on the basis of security parameters of the subject and object.
- The reference monitor has access to a file, known as the ***security kernel database*** that lists the access privileges (security clearance) of each subject and the protection attributes (classification level) of each object.
- The reference monitor enforces the security rules and has the following properties:
  - ***Complete mediation***: The security rules are enforced on every access, not just, fr example, when a file is opened.
  - ***Isolation***: The reference monitor and database are protected from unauthorized modification.

- ***Verifiability:*** The reference monitor's correctness must be provable. That is, it must be possible to demonstrate mathematically that the reference monitor enforces the security rules and provides complete mediation and isolation. Important security events, such as detected security violations and authorized changes to the security kernel database, are stored in the audit file.



Host Security

- Host Security refers to securing the operating system, file system and the resources of the Host from unauthorized access or modification or destruction.
- This is in contrast to things like: firewalls and VPNs (network security) or Apache or Oracle penetration testing (application security).
- Doing a good job at Host Security on all of your hosts is one of the most important ways to prevent break-ins.

Chapter 4

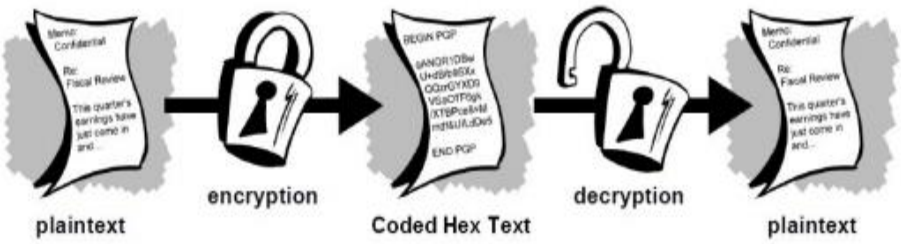
Review of Shared Key Cryptography and Hash Functions

What is Cryptography?

- Cryptography is the science of using mathematics to encrypt and decrypt data.
- Cryptography is the art and science of keeping messages secure.
- The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.

Terminologies

- A message is **plaintext** (sometimes called **cleartext**). The process of disguising a message in such a way as to hide its substance is **encryption**. An encrypted message is **ciphertext**. The process of turning ciphertext back into plaintext is **decryption**.
- A **cipher** (or **cypher**) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure.



- A **cryptosystem** is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a **cipher system**. The various components of a basic cryptosystem are as follows –
  - Plaintext
  - Encryption Algorithm
  - Ciphertext
- Decryption Algorithm
- Encryption Key
- Decryption Key

- While **cryptography** is the science of securing data, **cryptanalysis** is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. **Cryptanalysts** are also called attackers. **Cryptology** embraces both cryptography and cryptanalysis.

History of Cryptography

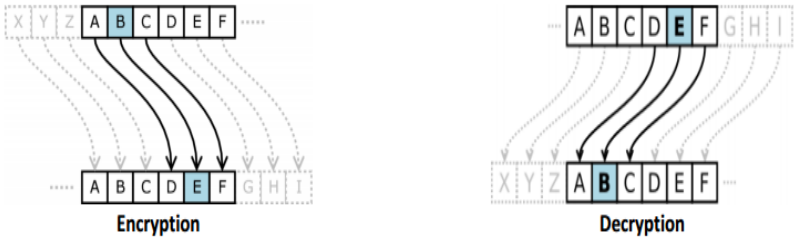
- As civilizations evolved, human beings got organized in **tribes, groups, and kingdoms**. This led to the emergence of ideas such as power, battles, supremacy, and politics.
- These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography.
- The roots of cryptography are found in Roman and Egyptian civilizations.

Hieroglyph

- The first known evidence of cryptography can be traced to the use of 'hieroglyph'. Some 4000 years ago, the Egyptians used to communicate by messages written in hieroglyph.

Caesar Shift Cipher

- Caesar Shift Cipher, relies on shifting the letters of a message by an agreed number (three was a common choice); the recipient of this message would then shift the letters back by the same number and obtain the original message.
- The Caesar cipher is named after Julius Caesar, who used it with a shift of three to protect messages of military significance.



PLAINTEXT: internet society Ghana chapter

CYPHERTEXT: lqwhuqhw vrflhwb jkdqd fkdswhu

Kamasutra Cipher

- The Kamasutra cipher is one of the earliest known substitution methods.
- It is described in the Kamasutra around 400 BC. The purpose was to teach women how to hide secret messages from prying eyes.
- The technique involves randomly pairing letters of the alphabet, and then substituting each letter in the original message with its partner.

UPPER HALF	W	Z	V	P	O	F	D	E	A	B	R	M	Y
LOWER HALF	N	H	G	X	K	S	I	C	J	U	T	Q	L

- The key is the permutation of the alphabet.

Internet society Ghana chapter

Dwrctwcr fkedcrl vzjwj ezjxrct

Goal and Services

- **Goal:** The primary goal of cryptography is to secure important data on the hard disk or as it passes through a medium that may not be secure itself. Usually, that medium is a computer network.
- **Services**: Cryptography can provide the following services:
  - ***Confidentiality (secrecy)***
    - ✓ *Ensuring that no one can read the message except the intended receiver*
    - ✓ *Data is kept secret from those without the proper credentials, even if that data travels through an insecure medium*
  - ***Integrity (anti-tampering)***
    - ✓ *Assuring the receiver that the received message has not been altered in any way from the original.*
  - ***Authentication***

- ✓ *Cryptography can help establish identity for authentication purposes*
- ✓ *The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)*

☞ ***Non-repudiation.***

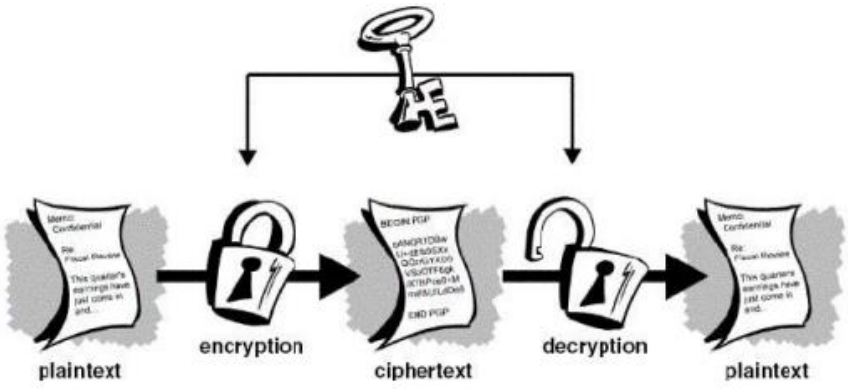
- ✓ *A mechanism to prove that the sender really sent this message*

Types of Cryptography

1. Symmetric Key Cryptography
2. Asymmetric Key Cryptography
3. Hash Functions

Symmetric Key Cryptography

- Also known as **Secret Key Cryptography** or **Conventional Cryptography.**
- Symmetric Key Cryptography is an encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.
- The Algorithm use is also known as a secret key algorithm or sometimes called a symmetric algorithm
- A key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher.
- The key for encrypting and decrypting the file had to be known to all the recipients. Else, the message could not be decrypted by conventional means.



Symmetric Key Cryptography – Examples

1. **Data Encryption Standard (DES):** The Data Encryption Standard was published in 1977 by the US National Bureau of Standards. DES uses a 56 bit key and maps a 64 bit

input block of plaintext onto a 64 bit output block of ciphertext. 56 bits is a rather small key for today's computing power.

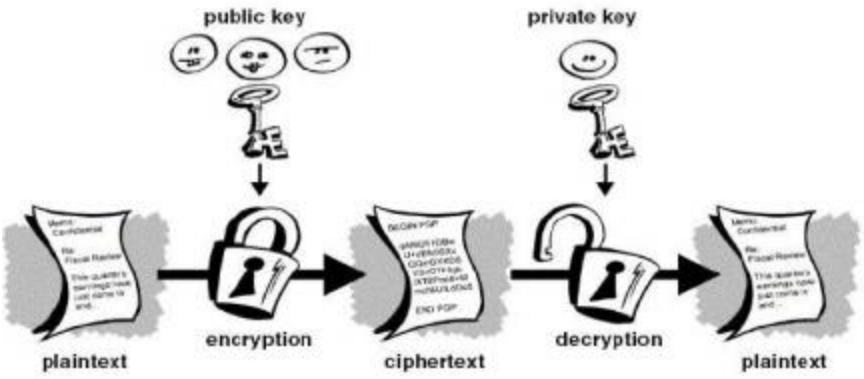
2. **Triple DES:** Triple DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES.
3. **Advanced Encryption Standard (AES)** (RFC3602): Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES).

Problems with Conventional Cryptography

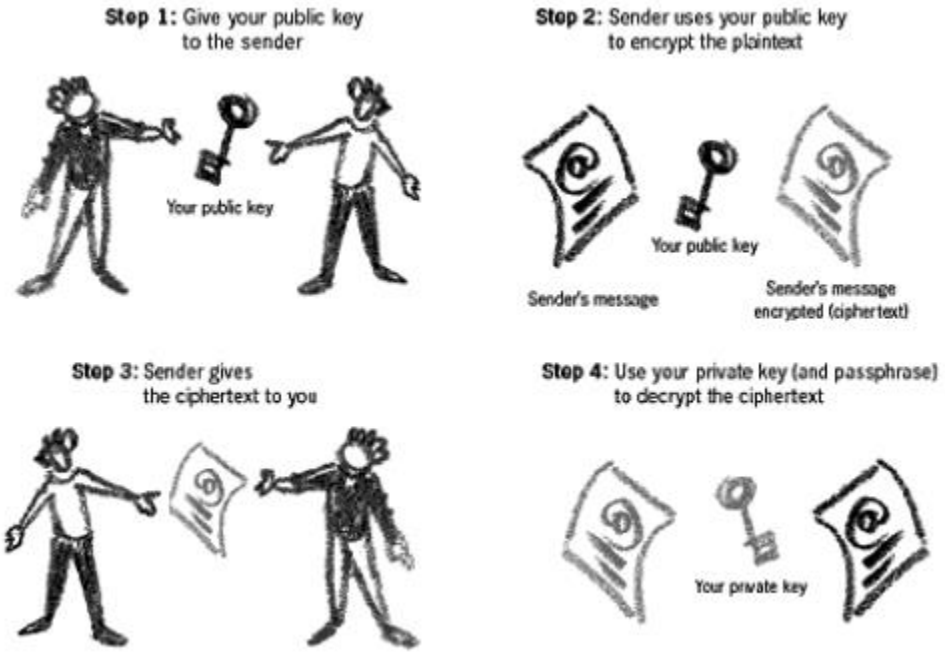
1. **Key Management:** Symmetric-key systems are simpler and faster; their main drawback is that the two parties must somehow exchange the key in a secure way and keep it secure after that. Key Management caused nightmare for the parties using the symmetric key cryptography. They were worried about how to get the keys safely and securely across to all users so that the decryption of the message would be possible. This gave the chance for third parties to intercept the keys in transit to decode the top-secret messages. Thus, if the key was compromised, the entire coding system was compromised and a “Secret” would no longer remain a “Secret”. This is why the “Public Key Cryptography” came into existence.

Asymmetric Key Cryptography

- **Asymmetric cryptography**, also known as **Public-key cryptography**, refers to a cryptographic algorithm which requires two separate keys, one of which is private and one of which is public. The public key is used to encrypt the message and the private one is used to decrypt the message.



Steps of Asymmetric cryptosystem



- Public Key Cryptography is a very advanced form of cryptography. Officially, it was invented by Whitfield Diffie and Martin Hellman in 1975. The basic technique of public key cryptography was first discovered in 1973 by the British Clifford Cocks of Communications-Electronics Security Group (CESG) of (Government Communications Headquarters - GCHQ) but this was a secret until 1997.

Asymmetric Key Cryptography – Examples

1. **Digital Signature Standard (DSS):** Digital Signature Standard (DSS) is the digital signature algorithm (DSA) developed by the U.S. National Security Agency (NSA) to generate a digital signature for the authentication of electronic documents. DSS was put

forth by the National Institute of Standards and Technology (NIST) in 1994, and has become the United States government standard for authentication of electronic documents. DSS is specified in Federal Information Processing Standard (FIPS) 186.

2. **Algorithm – RSA:** - RSA (**Rivest, Shamir** and **Adleman** who first publicly described it in 1977) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

RSA Cryptanalysis

- Rivest, Shamir, and Adelman placed a challenge in Martin Gardner's column in Scientific American (journal) in which the readers were invited to crack.
  C=114,381,625,757,888,867,669,235,779,976,146,612,010,218,296,721,242,362,562,561,842,935,706,935,245,733,897,830,597,123,563,958,705,058,989,075,147,599,290,026,879,543,541
- This was solved in April 26, 1994, cracked by an international effort via the internet with the use of **1600 workstations, mainframes, and supercomputers attacked the number for eight months before finding its Public key and its private key**.

  Encryption key = **9007**

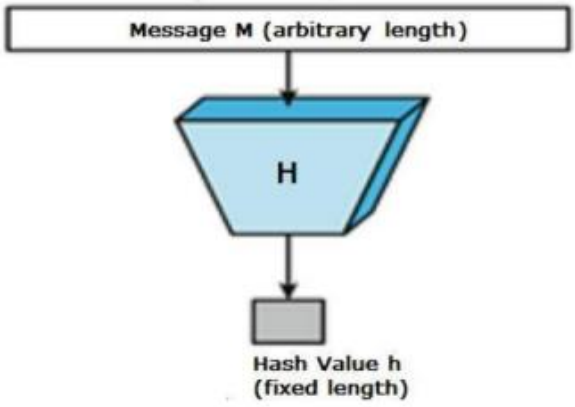
  The message "**first solver wins one hundred dollars**".
- Of course, the **RSA** algorithm is safe, as it would be incredibly difficult to gather up such international participation to commit malicious acts.

3. *ElGamal*
   - ElGamal is a public key method that is used in both encryption and digital signing.
   - The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol.
   - It is used in many applications and uses discrete logarithms.
   - ElGamal encryption is used in the free GNU Privacy Guard software

Hash Functions

- A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value, such that any (accidental or

intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digests.



- The ideal cryptographic hash function has four main properties:
  - It is easy to compute the hash value for any given message.
  - It is infeasible to generate a message that has a given hash.
  - It is infeasible to modify a message without changing the hash.
  - It is infeasible to find two different messages with the same hash.

Features of Hash Functions

- The typical features of hash functions are –

A. Fixed Length Output *HashValue*

- Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as **hashing the data**. In general, the hash is much smaller than the input data; hence hash functions are sometimes called **compression functions**.
- Since a hash is a smaller representation of a larger data, it is also referred to as a **digest**.
- Hash function with n bit output is referred to as an **n-bit hash function**. Popular hash functions generate values between 160 and 512 bits.

B. Efficiency of Operation

- Generally for any hash function h with input x, computation of h*x* is a fast operation. Computationally hash functions are much faster than a symmetric encryption.

Properties of Hash Functions

- In order to be an effective cryptographic tool, the hash function is desired to possess following properties −

A. Pre-Image Resistance

- This property means that it should be computationally hard to reverse a hash function. In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
- This property protects against an attacker who only has a hash value and is trying to find the input.

B. Second Pre-Image Resistance

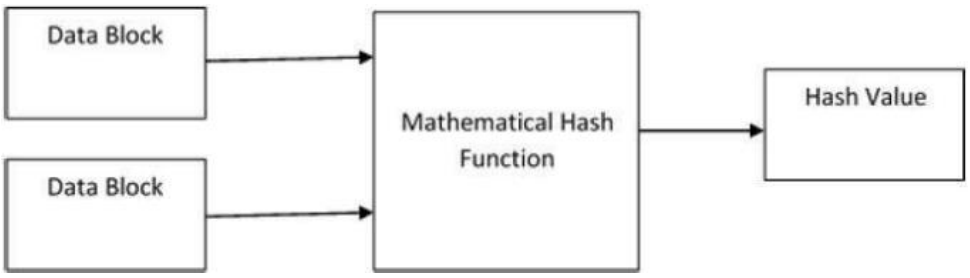
- This property means given an input and its hash, it should be hard to find a different input with the same hash.
- In other words, if a hash function h for an input x produces hash value h*x*, then it should be difficult to find any other input value y such that h*y* = h*x*. This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.

C. Collision Resistance

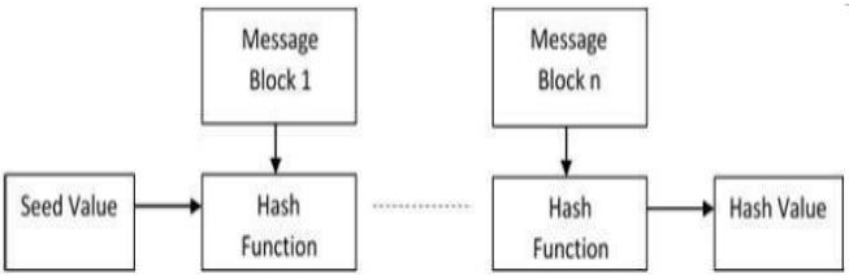
- This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.
- In other words, for a hash function h, it is hard to find any two different inputs x and y such that h*x* = h*y*. Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions. This property of collision free only confirms that these collisions should be hard to find. This property makes it very difficult for an attacker to find two input values with the same hash.
- Also, if a hash function is collision-resistant **then it is second pre-image resistant.**

Design of Hashing Algorithms

- At the heart of a hashing is a mathematical function that operates on two fixed-size blocks of data to create a hash code. This hash function forms the part of the hashing algorithm.
- The size of each data block varies depending on the algorithm. Typically the block sizes are from 128 bits to 512 bits. The following illustration demonstrates hash function −



- Hashing algorithm involves rounds of above hash function like a block cipher. Each round takes an input of a fixed size, typically a combination of the most recent message block and the output of the last round.
- This process is repeated for as many rounds as are required to hash the entire message. Schematic of hashing algorithm is depicted in the following illustration −



- Since, the hash value of first message block becomes an input to the second hash operation, output of which alters the result of the third operation, and so on. This effect, known as an **avalanche** effect of hashing.
- Avalanche effect results in substantially different hash values for two messages that differ by even a single bit of data. Understand the difference between hash function and algorithm correctly. The hash function generates a hash code by operating on two blocks of fixed-length binary data.
- Hashing algorithm is a process for using the hash function, specifying how the message will be broken up and how the results from previous message blocks are chained together.

Popular Hash Functions

- Let us briefly see some popular hash functions –

A. Message Digest *MD*

- MD5 was most popular and widely used hash function for quite some years. The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It was

adopted as Internet Standard RFC 1321. It is a 128-bit hash function. MD5 digests have been widely used in the software world to provide assurance about integrity of transferred file. For example, file servers often provide a pre-computed MD5 checksum for the files, so that a user can compare the checksum of the downloaded file to it.

- In 2004, collisions were found in MD5. An analytical attack was reported to be successful only in an hour by using computer cluster. This collision attack resulted in compromised MD5 and hence it is no longer recommended for use.

B. Secure Hash Function *SHA*

- Family of SHA comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. Though from same family, there are structurally different.
- The original version is SHA-0, a 160-bit hash function, was published by the National Institute of Standards and Technology *NIST* in 1993. It had few weaknesses and did not become very popular.
- Later in 1995, SHA-1 was designed to correct alleged weaknesses of SHA-0. SHA-1 is the most widely used of the existing SHA hash functions. It is employed in several widely used applications and protocols including Secure Socket Layer *SSL* security.
- In 2005, a method was found for uncovering collisions for SHA-1 within practical time frame making long-term employability of SHA-1 doubtful. SHA-2 family has four further SHA variants, SHA-224, SHA-256, SHA-384, and SHA-512 depending up on number of bits in their hash value. No successful attacks have yet been reported on SHA-2 hash function. Though SHA-2 is a strong hash function. Though significantly different, its basic design is still follows design of SHA-1. Hence, NIST called for new competitive hash function designs.
- In October 2012, the NIST chose the Keccak algorithm as the new SHA-3 standard. Keccak offers many benefits, such as efficient performance and good resistance for attacks.

C. RIPEMD

- The RIPEND is an acronym for RACE Integrity Primitives Evaluation Message Digest.

- This set of hash functions was designed by open research community and generally known as a family of European hash functions.
- The set includes RIPEND, RIPEMD-128, and RIPEMD-160. There also exist 256, and 320-bit versions of this algorithm.
- Original RIPEMD 128*bit* is based upon the design principles used in MD4 and found to provide questionable security. RIPEMD 128-bit version came as a quick fix replacement to overcome vulnerabilities on the original RIPEMD.
- RIPEMD-160 is an improved version and the most widely used version in the family. The 256 and 320-bit versions reduce the chance of accidental collision, but do not have higher levels of security as compared to RIPEMD-128 and RIPEMD-160 respectively.

D. Whirlpool

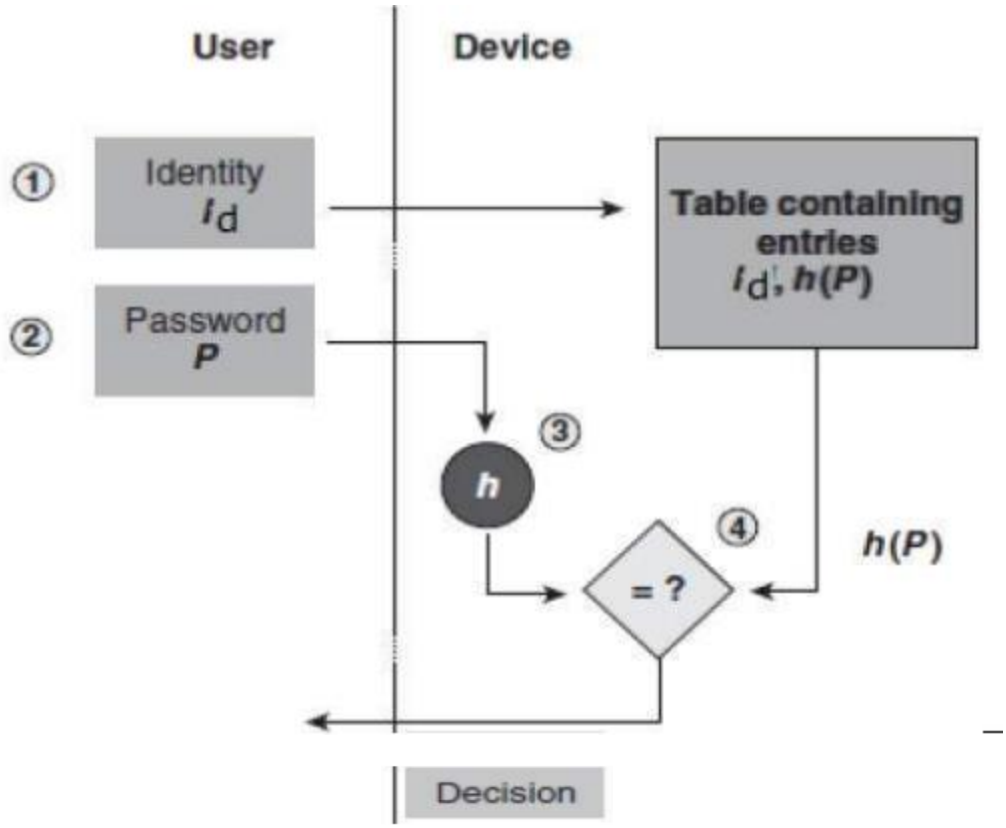
- This is a 512-bit hash function.
- It is derived from the modified version of Advanced Encryption Standard *AES*.
- One of the designers was Vincent Rijmen, a co-creator of the AES.
- Three versions of Whirlpool have been released; namely WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL.

Applications of Hash Functions

There are two direct applications of hash function based on its cryptographic properties.

1. Password Storage

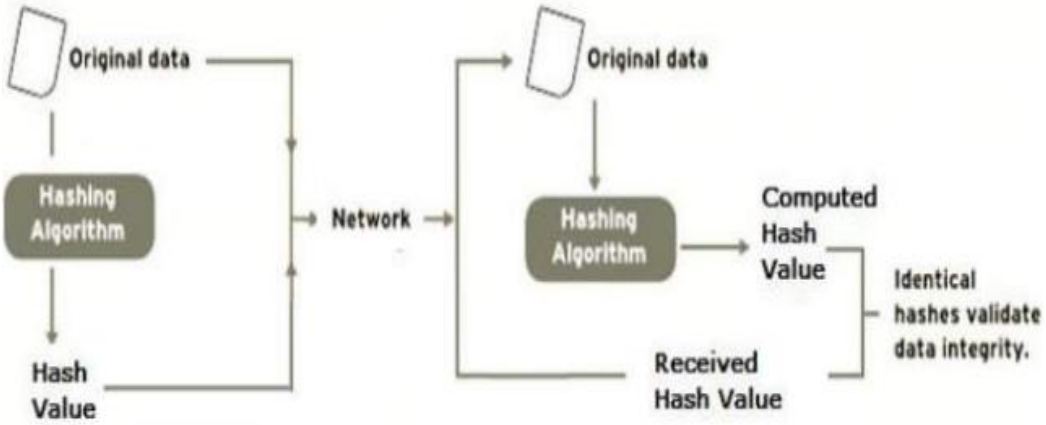
- Hash functions provide protection to password storage. Instead of storing password in clear, mostly all logon processes store the hash values of passwords in the file. The Password file consists of a table of pairs which are in the form *userid*, *h*(*P*). The process of logon is depicted in the following illustration −



- An intruder can only see the hashes of passwords, even if he accessed the password. He can neither logon using hash nor can he derive the password from hash value since hash function possesses the property of pre-image resistance.

2. Data Integrity Check

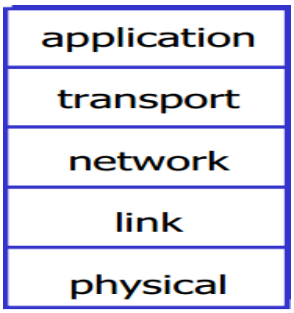
- Data integrity check is a most common application of the hash functions. It is used to generate the checksums on data files. This application provides assurance to the user about correctness of the data. The process is depicted in the following illustration –



- The integrity check helps the user to detect any changes made to original file. It however, does not provide any assurance about originality. The attacker, instead of modifying file data, can change the entire file and compute all together new hash and send to the receiver. This integrity check application is useful only if the user is sure about the originality of file.

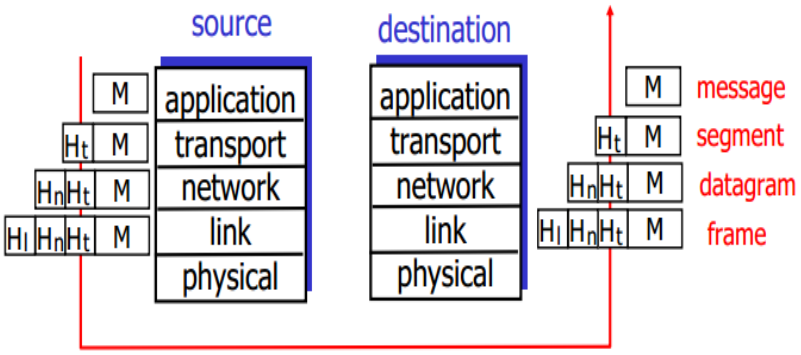
Introduction to the TCP/IP Stack

1. Application: supports network applications
   - ftp, smtp, http, ssh, telnet, DHCP (Dynamic Host Configuration Protocol)…
2. Transport: data transfer from end system to end system.
   - TCP, UDP, SPX…
3. Network: finding the way through the network from machine to machine.
   - IP (IPv4, IPv6), ICMP, IPX
4. (data) link: data transfer between two neighbors in the network
   - ppp, ethernet, ATM, ISDN, 802.11 (WLAN).
5. physical: bits "on the wire"



Protocol layer and data

- Each layer takes data from next higher layer.
  - *Adds header information to create a new data unit (message, segment, frame, packet …)*
  - *Send the new data unit to next lower layer*



Physical layer

- Provides services to the link layer.
- Transmitting raw bits
- No packet headers or tails
- Simplex – Only one direction (Television broadcast, radio)
- Half duplex - One direction at a time (walkie talkie)
- Full duplex (Telephone)

Data Link layer

- Provides services to the network layer.
- Uses MAC addressing.
- Hubs, bridges, switches work on this layer
- Some possible services:
  - Error detection and correction
  - Flow control

Network layer

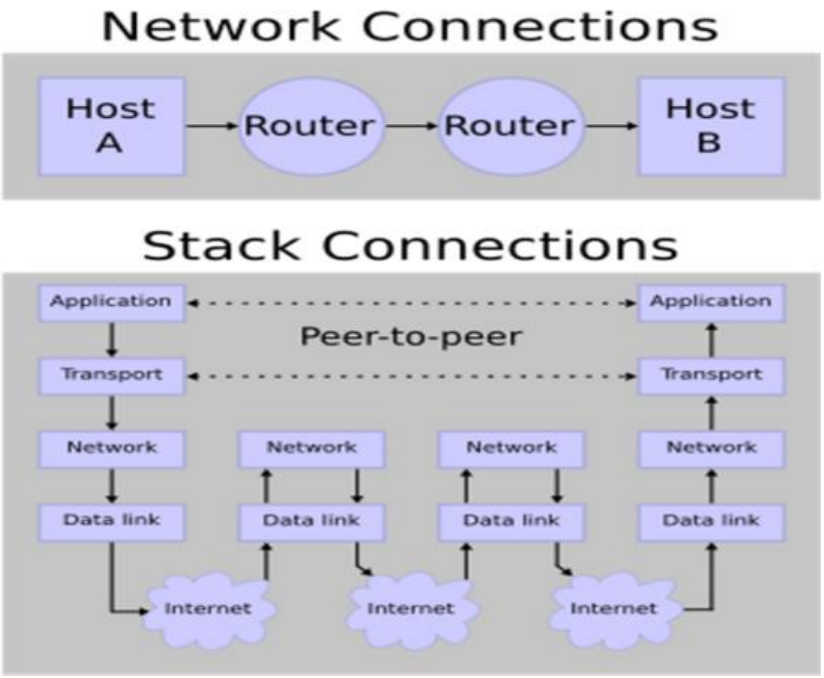
- Provides services to the transport layer.
- Uses IP addressing
- Some switches work on this layer.
- Getting data (packets of data) all the way from the source to the destination.
- Congestion control
- Routing
- Fairness

Transport layer

- Provides services to the application layer.
- TCP and UDP work on this layer.
- Source and destination port numbers in the header of each transport layer data packet.
- Some possible services:
  - *Virtual circuits (TCP).*
  - *Flow Control*

Application layer

- Provides a way for the user application to gain access to OSI.
- Makes sure that necessary communication resources exist (for example, is there a modem in the sender's computer?)
- The application layer is concerned with the user's view of the network.
- Domain Name System (DNS): -Converts an Internet domain into an IP address
- As the "top of the stack" layer, the application layer is the only one that does not provide any services to the layer above it in the stack—there isn't one! Instead, it provides services to programs that want to use the network, and to you, the user.
- IRC (Internet Relay Chat)



Network Security (ports and protocols)

- Protocol is a set of rules outlining the format to be used for communication between systems.
- TCP/IP (Transmission Control Protocol/Internet Protocol), the suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP.
- TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols, such as Netware, also support TCP/IP.
- UDP (User Datagram Protocol) a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network.
- In TCP/IP and UDP networks, a port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network. Some ports have numbers that are pre-assigned to them by the IANA, and these are known as ***well-known ports (specified in RFC 1700)***. This list of well-known port numbers specifies the port used by the server process as its contact port.

Port Number	Description
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP Data. File Transfer Protocol is a protocol used on the Internet for sending files.
21	FTP – Control.
22	SSH Remote Login Protocol. Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.

	It is a replacement for rlogin, rsh, rcp, and rdist. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled. When using ssh's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted; therefore it is almost impossible for an outsider to collect passwords. SSH is available for Windows, Unix, Macintosh, and OS/2, and it also works with RSA authentication.
23	Telnet. A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.
25	Simple Mail Transfer Protocol (SMTP). Short for Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.
53	Domain Name System (DNS). Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to

	translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.
80	HTTP. Short for HyperText Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed. HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies, including ActiveX, Java, JavaScript and cookies.
109	POP2
110	POP3

Chapter 5

Application Security

Application Security (vulnerabilities of programming/scripting languages)

Introduction

Application either through Mobile, web, PCs, tablets provides array of services which contains user personal information. With new applications, new security vulnerabilities are also discovered every day in commonly used applications. This vulnerability can put personal data of user at risk.

Application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application. Once an attacker has found a flaw, or application vulnerability, and determined how to access it, it can exploit the application vulnerability to facilitate a cyber-crime. These crimes target the confidentiality, integrity, or availability (known as the "CIA") of resources possessed by an application, its creators, and its users.

Application security, or "**AppSec**," is what an organization does to protect its critical data from external threats by ensuring the security of all of the software used to run the business, whether built internally, bought or downloaded. Application security helps identify, fix and prevent security vulnerabilities in any kind of software application.

Mainly there are two types of applications:

1. Mobile Applications
2. Web Based applications

Need for Application Security:

Security of applications is critical due to the following reasons:

1. **Storage and Processing of Sensitive Data:**

   Mobile devices are being used to access a range of services, from social networking, banking, ticketing, and shopping to corporate applications such as email, enterprise resource planning (ERP), customer relationship management (CRM), and calendar and address book applications. The applications store and transmit a lot of sensitive personal and corporate information, such as login credentials, credit card details, private contact entries, invoices, and purchase orders. If developed insecurely, these applications could potentially disclose sensitive information.

2. **Non transparent Use of Mobile Devices:**

Using personal phones for corporate purposes makes it difficult to enforce corporate policies and restrictions on these devices. Also, an attacker can more easily compromise personal devices than corporate- issued devices, which are locked down using far more draconian measures. Sensitive corporate applications and data on unmanaged personal devices open up security risks, such as exposure of confidential corporate information through lost or stolen phones, data interception and manipulation through Wi-Fi sniffing, and man-in-the-middle attacks at public Wi-Fi hotspots.

3. **Regulatory requirements:**

Around the world, countries have their own regulatory requirements for enterprises that manage sensitive and confidential customer data such as personally identifiable information, personal health information, cardholder information, and financial information. Hence organizations dealing with such information must mandate use of minimum security requirements.

Malicious Code (virus worms, malware)

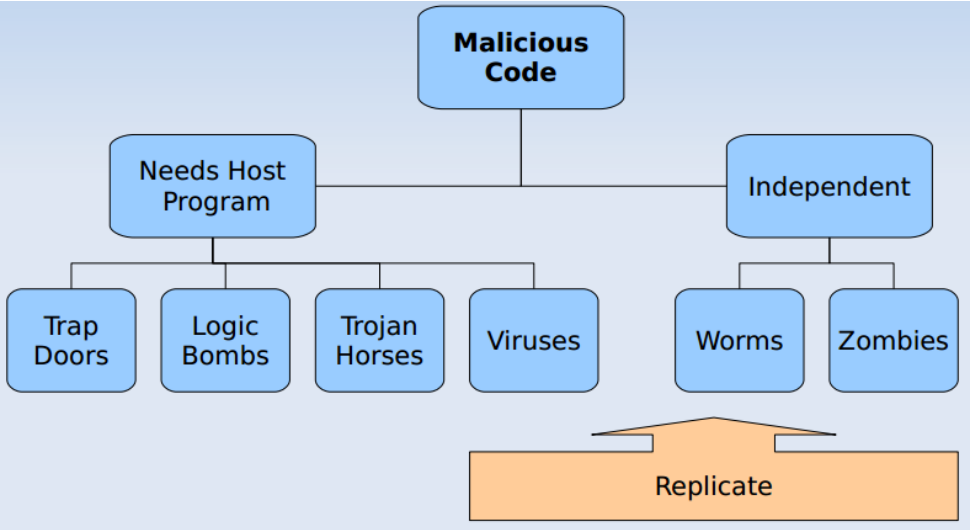
- **Malicious code** is software that performs unauthorized functions causing the normal operation of an information system to be abnormal.
- According to **SPECTRIA InfoSec Services**, malicious code is defined as "software which interferes with the normal operation of a computer system" or "software, which executes without the express consent of the user."

There are several types of malicious code such as viruses, worms, Trojan horses, and programming flaws. The programming flaws can be included with malicious intent or just be bad programming practices.

- **Malicious code** refers to a broad category of software threats to your network and systems. Perhaps the most sophisticated types of threats to computer systems are presented by malicious codes that exploit vulnerabilities in computer systems.
- Any code which **modifies or destroys data, steals data, allows unauthorized access Exploits or damage a system**, and does something that user did not intend to do, is called **malicious code**.

Types of Malicious Code

There are many types of malicious code of which the most well known types are viruses, worms, and Trojan Horses. Other types are intentional and accidental coding flaws, logic bomb, and trapdoor/backdoor.



A. **Independents:** are self-contained program that can be scheduled and run by the operating system.
B. **Needs host program:** are essentially fragments of programs that cannot exist independently of some actual application program, utility or system program.

Trap doors:

A trap door is a secret entry point into a program that allows someone that is aware at the trap door to gain access without going through the usual security access procedure. In many cases attacks using trap doors can give a great degree of access to the application, important data, or given the hosting system. Trap doors have been used legitimately by programmers to debug and test programs, some of the legitimate reasons for trap doors are:

1. *Intentionally leaves them for testing, and make testing easier.*
2. *Intentionally leaves them for covert means of access. In the other words, allows access in event of errors.*
3. *Intentionally leaves them for fixing bugs.*

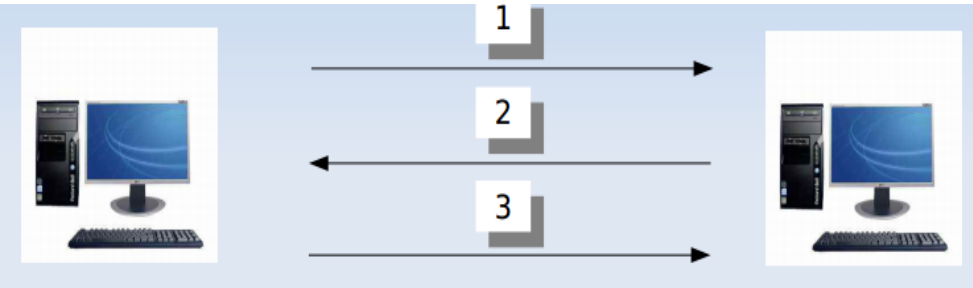
But they may use illegitimately, to provide future, illegal access. Trap doors become threats when they are used by unscrupulous programmers to gain unauthorized access.

Back door

- is another name for a trap door, back doors provide immediate access to a system by passing employed authentication and security protocols, Attackers can use back doors to bypass security control and gain control at a system without time consuming hacking.

Logic Bombs

- The logic bomb is code embedded in some legitimate program that execute when a certain predefined events occurs, these codes surreptitiously inserted into an application or operating system that causes it to perform some destructive or security – compromising activity whenever specified conditions are met.
- A bomb may sent a note to an attacker when a user is logged on to the internet and is using an specific program such as a word processor, this message informs the attacker that the user is ready for an attack, figure 2 shows a logic bomb in operation .Notice that this bomb dose not actually begin the attack but tells the attacker that the victim has met needed state for an attack to begin



Logic Bombs

1. Attacker implants logic bomb
2. Victim reports installation
3. Attacker sends attack message
4. Victim dose as logic bomb installation

Trojan Horses:

- A malicious, security–breaking program that is disguised as something benign, such as directory lister, archiver, game, or (in one notorious 1990 case on Mac) a program to find and destroy viruses!"
- A Trojan horse is a useful, or apparently useful program or command procedure containing hidden code that when invoked performs some unwanted or harmful function.

Trojan Horses can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly. for example, to gain access to the files of another user on a shared system, a user could create a Trojan Horse program that when executed, changed the invoking user's file permissions so that the file are readable by any user. The program appears to be performing a useful function but it may also be quietly deleting the victim's files.

Zombie:

- A zombie is a program that secretly takes over another internet attached computer and then uses that computer to launch attacks that are difficult to trace to the zombie's creator. Zombies are used in Denial of service attacks, typically against targeted web sites. The zombie is planted on hundreds of computers belonging to unsuspecting third parties and then used to overwhelm the target website by launching on overwhelming onslaught of internet traffic.

Viruses:

Cracker program that searches out other programs and infects them by embedding a copy of itself in them so that they become Trojan horses. When these programs are executed, the embedded virus is executed too, thus propagating the ' infection ' this normally happens invisibly to the user. Unlike a worm, a virus cannot infect other computers without assistance. It is propagated by vectors such as humans trading programs with their friends the virus may do nothing but propagate itself and then allow the program to run normally. Usually, however, after propagating silently for a while, it starts doing things like writing cute messages on the terminal or playing strange tricks with the display. Many nasty viruses, written by particularly perversely minded crackers, do irreversible. Damage, like nuking the entire user's files...

Biological Virus	Computer Virus
Consist of DNA or RNA strand surrounded by protein shell to bond to host cell	Consist of set of instructions stored in host program
No life outside of host cell	Active only when host program is executed
Replicates by taking over host's metabolic machinery with it's own DNA/RNA	Replicates when host program is executed or host file is opened
Copies infect other cells	Copies infect (attach to) other host program

A virus can do anything that other programs do. The only difference is that it attaches itself to another program and executes secretly when the host program is run. Once a virus is executing, it can perform any function such as erasing files and programs.

During its lifetime a typical virus goes through the following four phases:

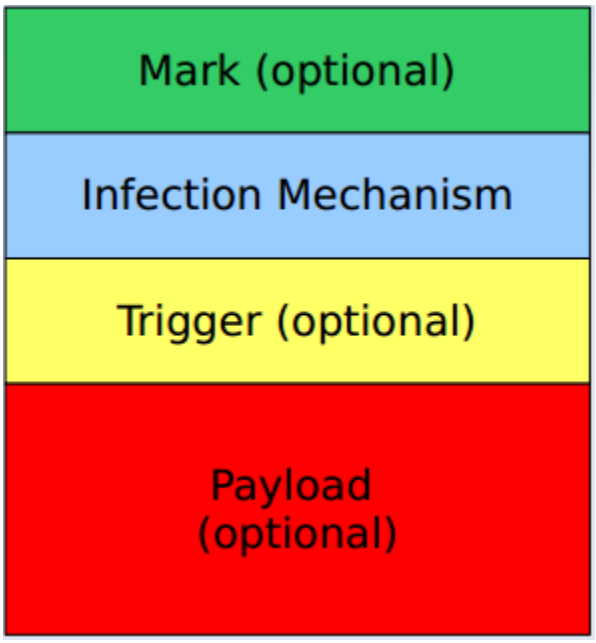
1. **Dormant phase**: The virus is idle the virus will eventually be activated by some event, such as a date. The presence of another program or file, or the capacity of the disk exceeding some limit, not all viruses have this stage.
2. **Propagation phase:** The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
3. **Triggering phase:** The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.
4. **Execution phase:** The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

Virus Anatomy,

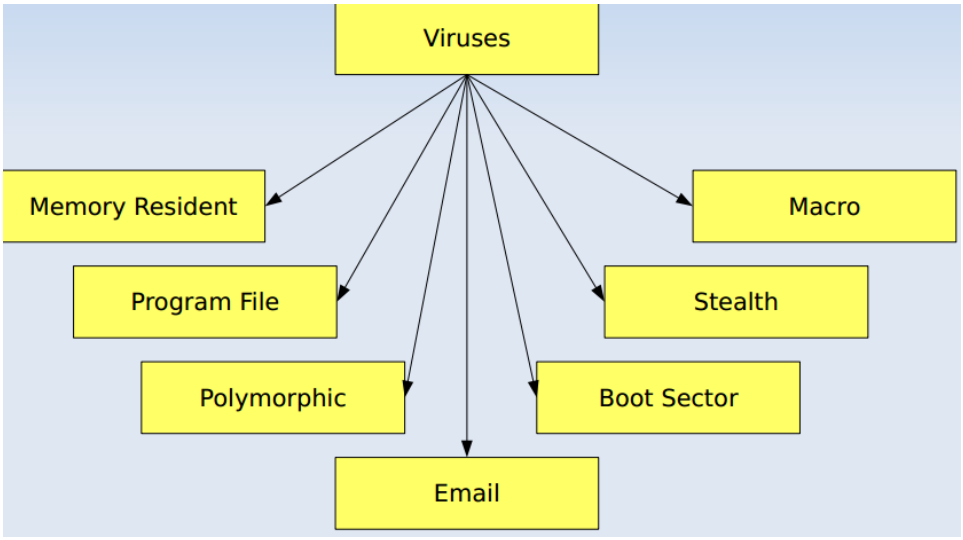
Virus Structure has four ports

1. Mark can prevent re-infection attempt.
2. Infection Mechanism causes spread to other files
3. Trigger are conditions for delivering payload

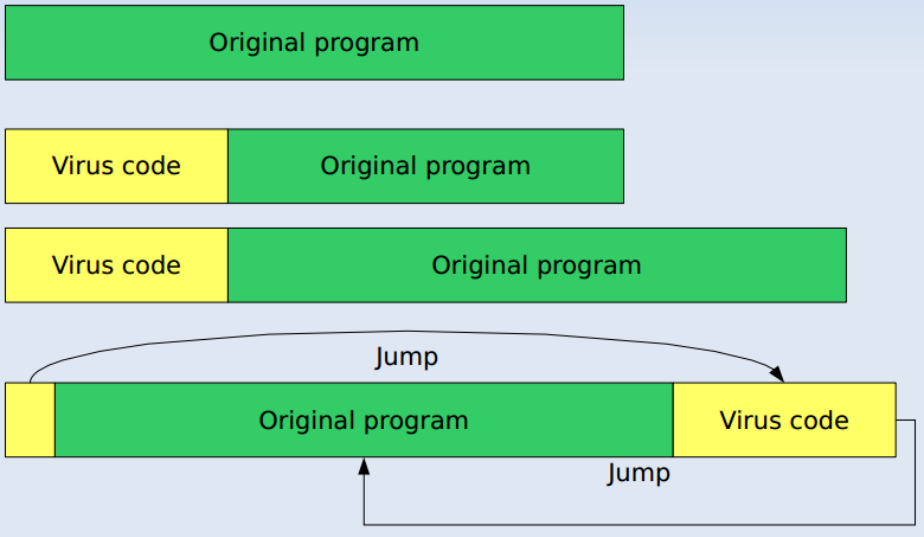
4. Payload is the possible damage to infected computer



Types of virus,



Program File Viruses



Memory – resident virus:

- lodges in main memory as part of a resident system program. From that point on, virus infects every program that executes.

Polymorphic virus:

- creates copies during replication that are functionally equivalents but have distinctly different bit patterns. In this case the "signature "of the virus will vary with each copy. To achieve this variation, the virus may randomly insert superfluous instructions or interchange the order of independent in-generally called a mutation engine, creates a random encryption key to encrypt the reminder of the virus. The key is stored with the virus, and the mutation engine itself is altered.
- When an infected program is invoked, the virus uses the stored random key to decrypt the virus, when the virus replicates, a different random key is selected.

Boot Sector Virus:

- Boot sector viruses infect the system area of the disk that is read when the disk is initially accessed or booted. This area can include the master boot record the operation system's boot sector or both. A virus infecting these areas typically takes the system instructions it finds and moves them to some other area on the disk. The virus is then free to place its own code in the boot record. When the system initializes, the virus loads into memory and simply points to the new location for the system instructions. The system then boots in a normal fashion except the virus is now resident in memory. A boot sector virus can replicate without your executing any programs from an infected disk. Simply accessing

the disk is sufficient. For example , most PCs do a systems check on boot up that verifies the operation of the floppy drive even this verification process is sufficient to activate a boot sector virus if one exist on a floppy left in the machine and the hard drive can also become infected .

Stealth Virus:

- A format virus explicitly designed to hide itself from detection by antivirus software. When the virus is loaded into memory, it monitors system calls to files and disk sectors, when a call is trapped the, virus modifies the information returned to the process making the call so that it sees the original uninfected information. This aids the virus in avoiding detection. For example many boot sector viruses contain stealth ability. If the infected disk is booted, programs such as FDISK report a normal boot record. The virus is intercepting sector calls from FDISK and returning the original boot sector information. If you boot the system from a clean floppy disk however, the drive is inaccessible. If you run FDISK again, the program reports a corrupted boot sector on the drive. To use stealth, however, the virus must be actively running in memory, which means that the stealth portion of the virus is vulnerable to detect by antivirus.

Macro Virus:

- Macro Virus is set of macro commands, specific to an application, which automatically executes in an unsolicited manner and spread to that application's documents. According to the national computer security agency (www.ncsa.com), macro viruses now make up two – thirds of all computer viruses. Macro viruses are particularly threatening for a number of reasons:

1- A macro virus is platform independent. Virtually all of the macro viruses infect Microsoft word documents. Any hardware platform and operating system that supports word can be infected.

2- Macro viruses infect documents, not executable portions of code. Most of the information introduced on to a computer system is in the form of a document rather than a program.

3- Macro viruses are easily spread. A very common method is by electronic mail.

Email Virus:

- A more recent development in malicious software is the e-mail virus. The first rapidly spreading e-mail viruses, such as Melissa, made use of a Microsoft word macro embedded in an attachment. If the recipient opens the e-mail attachment, the word macro is activated then:

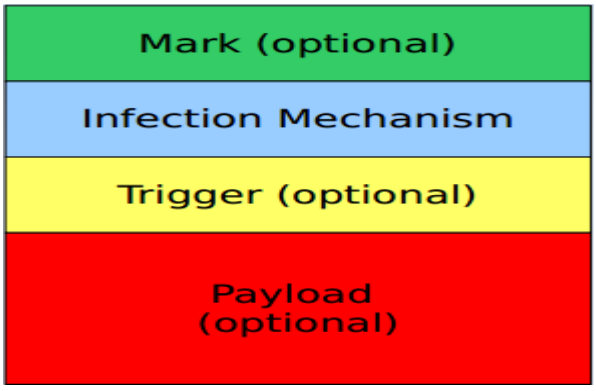
1- The e-mail virus sends itself to everyone on the mailing list in the user's e-mail package
2- The virus does local damage

Worms:

- A program that propagates itself over a network, reproducing itself as it goes ... Worm is also self-replicating but a stand-alone program that exploits security holes to compromise other computers and spread copies of itself through the network. Unlike viruses, worms do not need to parasitically attach to other programs. Because of the recursive structure of this propagation, the spread rate of worms is very fast and poses a big threat on the Internet infrastructure as a whole.

Worms Anatomy

- Mark structurally similar to viruses, except a stand-alone program instead of program fragment
- Infection Mechanism searches for weakly protected computers through a network (i.e., worms are network based)
- Triggers are Conditions for delivering payload
- Payload might drop a Trojan horse or parasitically infect files, so worms can have Trojan horse or virus characteristics



Blaster (a.k.a. Lovesan) worm (August 11th, 2003)

The worm exploits the buffer overflow vulnerability in the Distributed Component Object Model (DCOM) Remote Procedure Calls (RPC) interface that allows arbitrary code to be executed on most of the Windows NT, Windows 2000, and Windows XP platforms. Fortunately, the worm is designed very poorly. Firstly, its scanning rate is very small and the worm itself is latency-limited. Therefore, every machine was probed only once in a half an hour on average during the peak of the epidemics. Secondly, the worm has a bug that forced many of the machines to endlessly reboot thus reducing the number of the scanning hosts.

The worm has a payload to create a SYN DDoS attack against Windows update sites. The Blaster worm showed that the auto update functionality provided by Microsoft is quite successful. Despite the fact that at the time the bug was discovered almost all of the PCs were vulnerable just three weeks later when the worm started to spread only half a million of the machines were subverted. Another important lesson from the Blaster worm epidemics is that even the machines that are not patched by the worm outbreak time are soon patched and only one or at most two worms that share the same vulnerability have a chance for widespread.

E-mail Security

> *Not everyone in the organization needs to know how to secure the e-mail service, but anyone who handles patient information must understand e-mail's vulnerabilities and recognize when a system is secure enough to transmit sensitive information.*

- E-mail messages are generally sent over **untrusted networks**—**external networks** that are outside the organization's security boundary. When these messages lack appropriate security safeguards, they are like **postcards** that can be **read, copied,** and **modified** at any point along these paths.
- Securing an e-mail system is the responsibility of an organization's IT department and e-mail administrator. However, anyone responsible for the confidentiality, integrity, and availability of the information sent via e-mail should be aware of the threats facing e-mail systems and understand the basic techniques for securing these systems.

The E-mail System in a Nutshell

- An **e-mail system** is made up of two primary components that reside in an organization's IT infrastructure: **mail clients** and **mail servers**.
- Users read, compose, send, and store their e-mail using mail clients. Mail is formatted and sent from the mail client via the network infrastructure to a mail server. The mail

server is the computer that delivers, forwards, and stores e-mail messages. All components such as the mail servers, the mail clients, and the infrastructure that connects and supports them must be protected.

- Voluntary industry standards (e.g., SMTP, ESMTP, POP, IMAP) for formatting, processing, transmitting, delivering, and displaying e-mail ensure interoperability among the many different mail client and server solutions.
- E-mail security relies on principles of good planning and management that provide for the security of both the e-mail system and the IT infrastructure. With proper planning, system management, and continuous monitoring, organizations can implement and maintain effective security.

Common Threats

- Because **e-mail** is widely deployed, well understood, and used to communicate with untrusted, external organizations, it is frequently the target of attacks. Attackers can exploit e-mail to gain control over an organization, access confidential information, or disrupt IT access to resources.
- Common threats to e-mail systems include the following:

A. **Malware**. Increasingly, attackers are taking advantage of e-mail to deliver a variety of attacks to organizations through the use of malware, or "malicious software," that include ***viruses, worms, Trojan horses, and spyware***. These attacks, if successful, may give the malicious entity control over workstations and servers, which can then be exploited to change privileges, gain access to sensitive information, monitor users' activities, and perform other malicious actions.

B. **Spam and phishing**. Unsolicited commercial e-mail, commonly referred to as spam, is the sending of unwanted bulk commercial e-mail messages. Such messages can disrupt user productivity, utilize IT resources excessively, and be used as a distribution mechanism for malware. Related to spam is phishing, which refers to the use of deceptive computer-based means to trick individuals into responding to the e-mail and disclosing sensitive information. Compromised e-mail systems are often used to deliver spam messages and conduct phishing attacks using an otherwise trusted e-mail address.

C. **Social engineering**. Rather than hack into a system, an attacker can use e-mail to gather sensitive information from an organization's users or get users to perform actions that further an attack. A common social engineering attack is e-mail spoofing, in which one person or program successfully masquerades as another by falsifying the sender information shown in e-mails to hide the true origin.

D. **Entities with malicious intent**. Malicious entities may gain unauthorized access to resources elsewhere in the organization's network via a successful attack on a mail server. For example, once the mail server is compromised, an attacker could retrieve users' passwords, which may grant the attacker access to other hosts on the organization's network.

E. **Unintentional acts by authorized users**. Not all security threats are intentional. Authorized users may inadvertently send proprietary or other sensitive information via e-mail, exposing the organization to embarrassment or legal action.

E-mail Security Safeguards

- Management, operational, and technical safeguards are necessary to ensure that the confidentiality, integrity, and availability needs of the mail system, its supporting environment, and the data handled by it are addressed.
- The National Institute of Standards and Technology is a non-regulatory agency within the Department of Commerce. Its Information Technology Laboratory recommends that organizations employ the following guidelines in planning, implementing, and maintaining secure e-mail systems.

Implement Management Controls

- Management security controls—such as organization-wide information security policies and procedures, risk assessments, configuration management and change control, and contingency planning—are essential to the effective operation and maintenance of a secure e-mail system and the supporting network infrastructure. Additionally, organizations should implement and deliver security awareness and training, because many attacks rely either partially or wholly on social engineering techniques to manipulate users.

Carefully Plan the System Implementation

- The most critical aspect of deploying a secure e-mail system is careful planning before installation, configuration, and deployment. As is often said, security should be considered from the initial planning stage, at the beginning of the system development life cycle, to maximize security and minimize costs.

Secure the Mail Server Application

- Organizations should install the minimal mail server services required and eliminate any known vulnerabilities through patches, configurations, or upgrades. If the installation program installs unnecessary applications, services, or scripts, these should be removed immediately after the installation process is complete.
- Securing the mail server application generally includes patching and upgrading the mail server; configuring the mail server user authentication and access and resource controls; configuring, protecting, and analyzing log files; and periodically testing the security of the mail server application.

Secure the Mail Client

- In many respects, the client side of e-mail represents a greater risk to security than the mail server. Providing an appropriate level of security for the mail client requires carefully considering and addressing numerous issues.
- Securely installing, configuring, and using mail client applications generally includes patching and upgrading the mail client applications; configuring the mail client security features (e.g., disable automatic opening of messages); enabling antivirus, ant-spam, and ant-phishing features; configuring mailbox authentication and access; and securing the client's host operating system.

Secure the Transmission

- Most standard e-mail protocols send, by default, user authentication data and e-mail content in the clear; that is, unencrypted. Sending data in the clear may allow an attacker to easily compromise a user account or intercept and alter unencrypted e-mails. At a minimum, most organizations should encrypt the user authentication session even if they do not encrypt the actual e-mail data.
- A related control to protect the confidentiality and integrity of the message is to deploy a secure e-mail solution such as leveraging PKI technology to encrypt and sign the

message. Digital rights management and data leakage prevention systems can be used to prevent the accidental leakage and exfiltration of sensitive information.

Secure the Supporting Operating Environment

- While the mail server and mail clients are the two primary components of an e-mail system, the supporting network infrastructure is essential to its secure operations. Many times, the network infrastructure, including such components as firewalls, routers, and intrusion detection and prevention systems, will provide the first layer of defense between untrusted networks and a mail server.

Maintaining a Secure Mail System

- Maintaining the security of a mail system is an ongoing process, requiring constant effort, resources, and vigilance, and usually involves the following actions:

A. Configure, Protect, and Analyze Log Files

- Log files are often an organization's only record of suspicious behavior. Enabling logging mechanisms allows the organization to use collected data to detect both failed and successful intrusions, initiate alert notifications when further investigation is needed, and assist in system recovery and post-event investigations.
- Organizations require both procedures and tools to process and analyze the log files and review alert notifications.

B. Back up Data Frequently

- One of the most important functions of a mail server administrator is maintaining the integrity of the data on the mail server. This is important because mail servers are often one of the most vital and exposed servers on an organization's network.
- The mail administrator should back up the mail server on a regular basis to reduce downtime in the event of a mail service outage and support compliance with regulations on the backup and archiving of data and information, including those found in e-mail.

C. Protect against Malware

- Organizations require malware scanning and spam filtering capabilities at the mail client and the mail system levels. Organizations should also conduct awareness and training activities for users, including telecommuters, so that users are better prepared to recognize malicious mail messages and attachments and handle them appropriately.

D. Perform Periodic Security Testing

- Periodic security testing of the mail system confirms that protective measures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the operational mail system. Organizations should consider using a combination of techniques, including vulnerability scanning, to assess the mail system and its supporting environment.