IdAM (Identity & Access Management)

FTVETI

ICT @ FTVETI

Objectives

After completing this unit, you should be able to:

- Understand fundamentals around Identity, Authentication, Authorization & Access Control
- Appreciate the basics of IdAM & its importance to business and security perspective
- Know various types of Access Controls and Access Administration at high level
- Get a view of various elements of an enterprise IdAM strategy and implementation challenges
- Explain the concept of zero trust
- Delve into perspectives around Password Protection
- Get an overview of Identity theft & methods

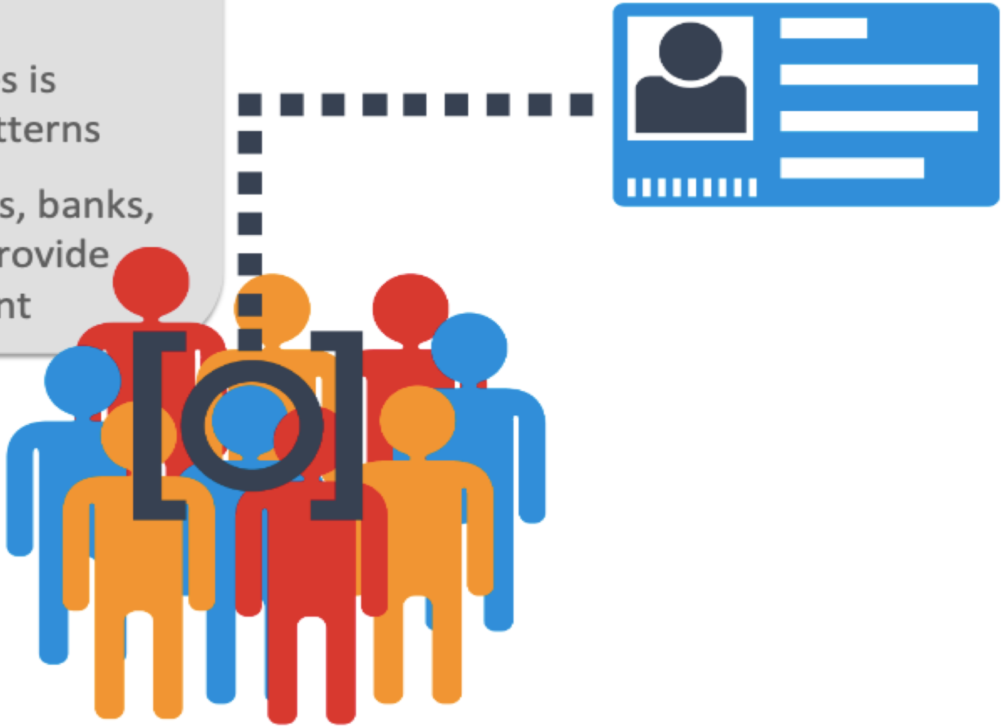
Before exploring about Authentication and Authorization we need to know few terminologies. Let us discuss the same

Identity (Recognition)

Tom	Jack
Jill	Tim
Computer	Telephone
Burger	Pizza

Identity In The Digital World

- Identity in the digital space, is a collection of data points about an entity, individual, organization or electronic device that helps in it's unique recognition
- Identification or Recognition of individuals or their devices is possible by associating unique & reliable identifiers or patterns
- Such an information is often used by websites, advertisers, banks, computers and so on to uniquely identify users so as to provide personalized experience and targeted promotional content



Digital Identity Artefacts

Below are few Digital Identity Artefacts:

- User-ID, Username & Passphrase, Password
- Date of birth
- Phone number
- Purchasing or Medical history
- Aadhaar or SSN
- Electronic transaction records

Authentication & Authorization

FTVETI

What Is Authentication?

- Authentication is a process where a user proves his identity to gain access to a resource such as application, system, device and so on
- During authentication the user needs to provide some pre-registered credentials in order to establish their identity

- **For ex:** On a typical LOGIN screen of a website, a user needs to enter his current (pre-registered) User-ID & Password combination for gaining an access to his account. Once the user is authenticated, typically a session gets created and referred for all the further interaction between the user and the application until the user logs off or the session gets terminated by other means (e.g. error, timeout, network loss)

What Do You Mean By Authorization?

- Authorization refers to the process responsible to determine user permissions to access a particular resource
- Authorization is usually performed by checking the resource access request, against a set of authorization policies typically stored in the backend
- Usually process of Authentication verifies a user's identity and it then enables Authorization. An authorization policy then decides what the given identity is allowed to do in the context of a particular system in concern

Authorization Access Control

- The Authorization model could also provide complex access controls based on:
  - Data, information, policies including user attributes
  - User roles, groups as allocated
  - Access channel (IP, Geolocation and so on)
  - Time of access
  - Resources requested by the user (Dynamic Behavioural Analysis)
  - Externally associated data (Threat Intelligence)
  - Business rules

Authentication & Authorization Principles

FTVETI

Authentication Processes

- Single Factor
- Multi Factor
- Identity Management
- Authenticator Management

Single Factor Authentication

Authenticators

- Single Challenge
- One Authenticator (password or key)

Implementation

- Inexpensive
- Simple

Usability

- Easy to use

Risk

- Easier to break
- Guessable passwords
- Leaked passwords

Risk Mitigation

- Password Complexity
- Periodic password change
- Different passwords per application

Multi Factor Authentication

Authenticators

- Multiple
- 2 or more
- Ex: Password & Mobile based OTP

Implementation

- Expensive
- Complex w.r.t Single Factor Authentication

Usability

- Not very difficult in cases of OTP and many more
- Biometrics may become a bit tedious

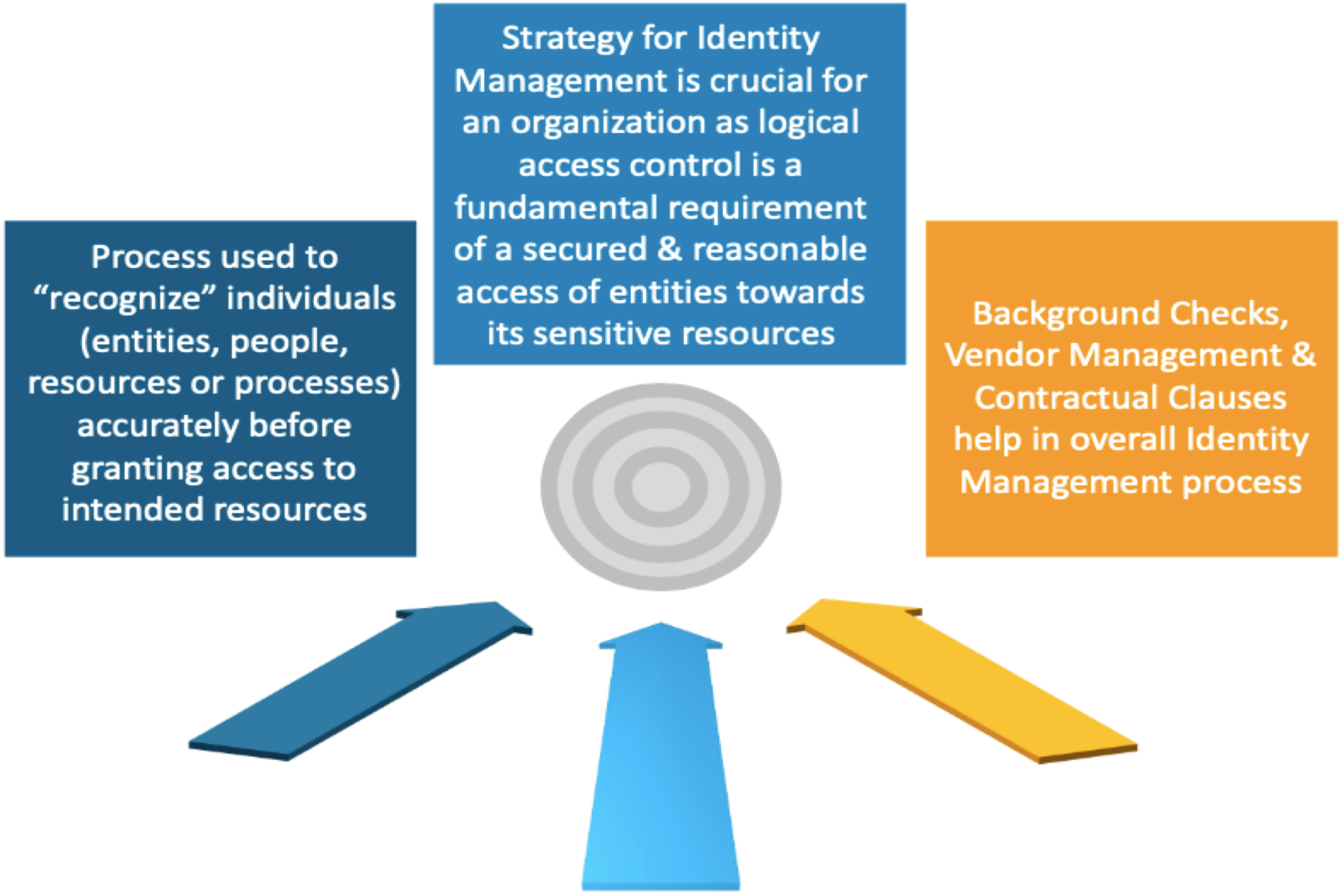
Risk

- Difficult to break
- One guessable authenticator may not allow access breach while another authenticator is still a secret
- Extreme cases – where all the authenticators are leaked, guessed, bypassed - Rare

Risk Mitigation

- Password Complexity
- Keeping authenticators such as mobile phones secure
- Different passwords per application

Identity Management



Process used to "recognize" individuals (entities, people, resources or processes) accurately before granting access to intended resources

Strategy for Identity Management is crucial for an organization as logical access control is a fundamental requirement of a secured & reasonable access of entities towards its sensitive resources

Background Checks, Vendor Management & Contractual Clauses help in overall Identity Management process

Authenticator Management

Authentication

01

Authenticators include passwords, tokens, keys, biometrics, PKI certificates, access cards and so on which helps a user, entity to prove his pre-verified entity and ask for access

02

Authenticator management is a key process which involves issuing, revoking and servicing of authenticators

03

Ensuring that authenticators are created, distributed, serviced, handled and terminated securely is very important from security point of view

04

Usage of 'Default' valued authenticators is a risk & should be avoided as they are easily known, discoverable and guessed by attackers

Tenets Of Authorization

- SOD – Segregation of Duties
- Need to Know Basis
- Principle of Least Privilege
- Unsuccessful Logons
- Session Concurrency/ Last Login Notification
- Notification of System Usage

SOD – Segregation Of Duties

- SOD primarily separates the responsibilities associated with an action of process to decrease the opportunity for misbehaviour or policy violations
- One Developer & another Tester concept

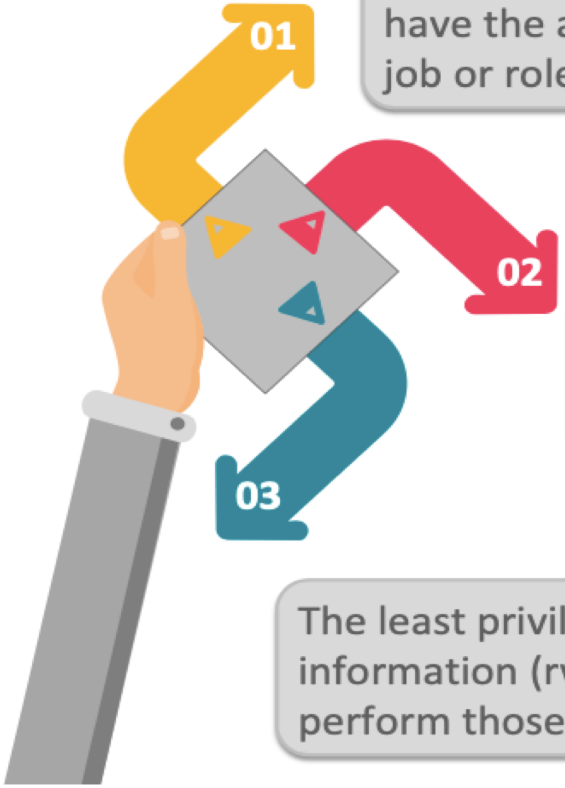
Developer

Tester

Need To Know Basis

- Access to Systems should only be granted to entities with a legitimate need to know the information contained within those systems
- This principle prevents over exposure of sensitive information which then becomes likely to be misused
- **Example 1:** An employee using an allotted virtual machine may need the credentials of the local user for login however may never need the credentials of the hypervisor or even the root/ admin
- **Example 2:** A manager in an organization may need to know some personal information including salary information about this direct reports but may never require information about other employees in the organization

Principle Of Least Privilege



The least privilege principle states that individuals or systems should only have the access necessary to perform specific activities required of their job or role

When entities or individuals are not performing work on these types of activities, they should use the privileged access accounts

The least privilege principle ensures that what can be done with the information (rwx) is limited to the least amount of access necessary to perform those actions

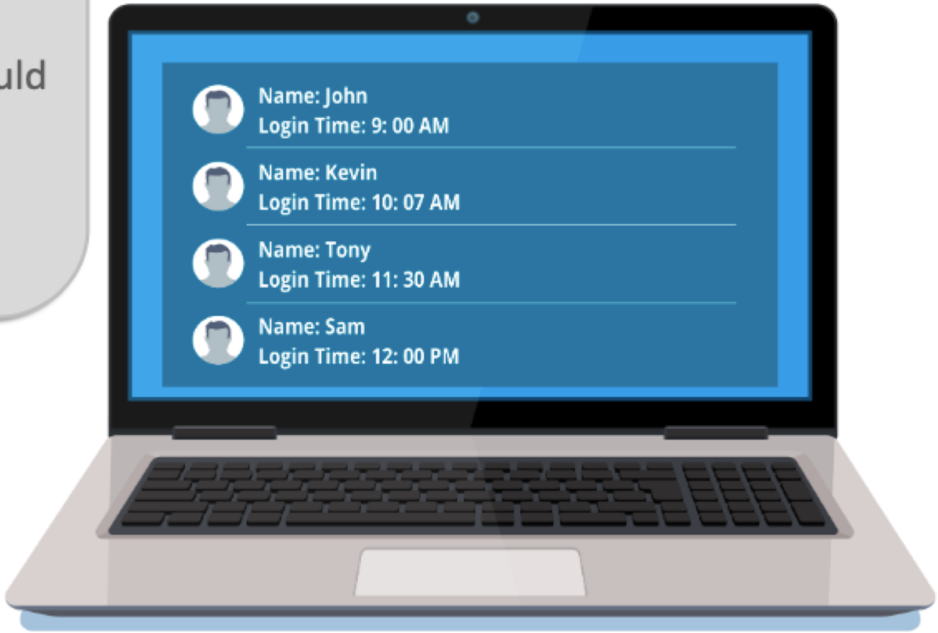
Unsuccessful Logons

- Limiting the number of unsuccessful logon attempts by a user during a specific period can reduce the potential for guessing credentials
- Procedures may include locking accounts after a certain number of attempts, requiring an end user to contact the help desk, or simply unlocking the account after a specific period
- A common mobile device control is to erase information if a certain number of logins have been attempted

Unsuccessful Login
Successful Login
Successful Login
Unsuccessful Login
Unsuccessful Login

Session Concurrency/ Last Login Notification

- Notifying the end user of the last login can provide information to the end user in order to determine if unauthorized access was obtained using their account
- Concurrent sessions occur when two or more sessions exist at the same time. This may be prohibited because most users would only create a single session for system access
- Additional sessions using the same credentials might be an indication of malicious behaviour or a compromised account



Name: John
Login Time: 9: 00 AM

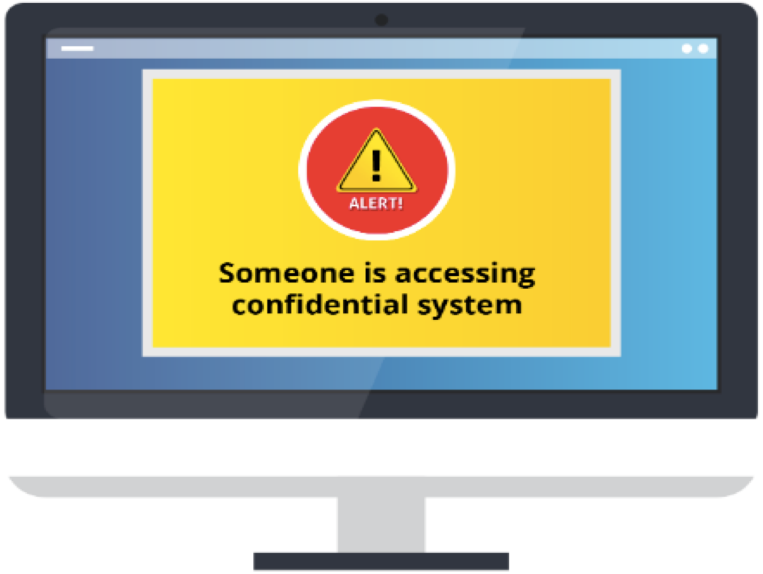
Name: Kevin
Login Time: 10: 07 AM

Name: Tony
Login Time: 11: 30 AM

Name: Sam
Login Time: 12: 00 PM

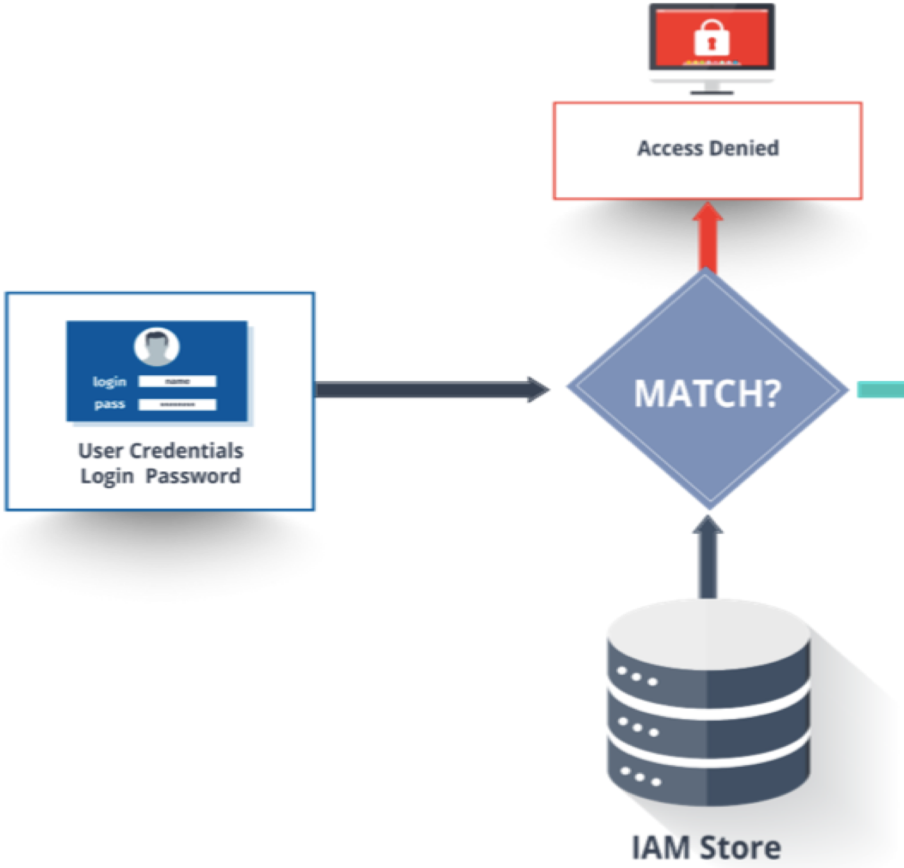
Notification Of System Usage

Banners & Login displays notify the user who are accessing a confidential system & If they access this system, they may be subject to monitoring, audits, & jurisdiction of the system



Regulation Of Access

Access


Access Denied
login
name
pass
User Credentials
Login Password
MATCH?
Access Granted to the resource Permissions : as per the granted Access Level
IAM Store

Access Control

Access Control

Access control is referred to as a security method used to control who or what can access (Read, Use, Modify and so on) resources in the digital environment

Forms of Access Control:

Physical access control limits access to physical resources (buildings, offices, devices and so on)

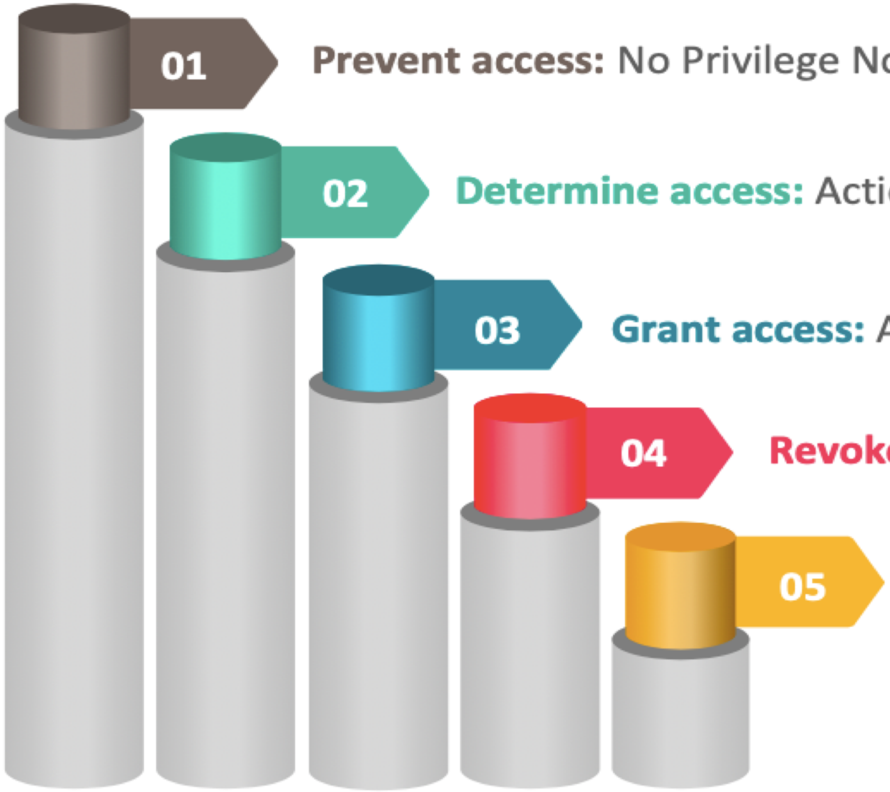
Logical access control regulates access to data, computing resources & networks

Types of Access Control:

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role – Based Access Control (RBAC)
- Rule – Based Access Control (RuBAC)

Key Considerations

- Key concerns of an access control scheme are:



01 **Prevent access:** No Privilege No Access concept

02 **Determine access:** Action with an object is taken after the access decision

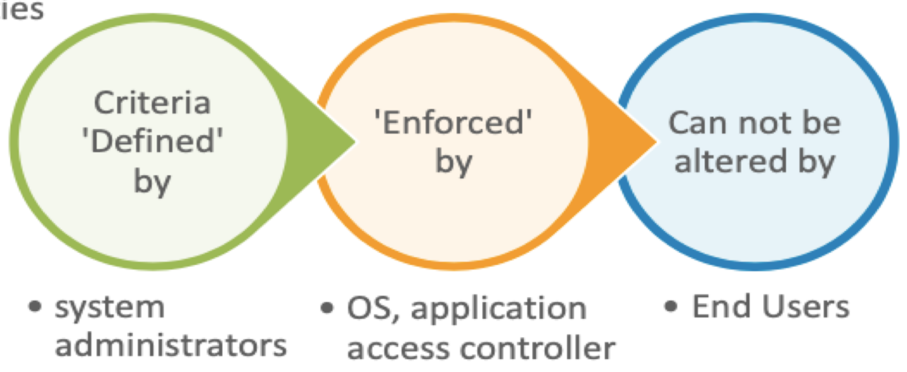
03 **Grant access:** Access provision

04 **Revoke access:** Removal of access

05 **Audit access:** Determine access trails

Mandatory Access Control (MAC)

- Primarily MAC is a way of assignment of access rights, based on policies/restrictions enforced by a designated central authority
- MAC usually restricts the power of individual resource owners (of granting / denying access to other users) to objects in a systems
- Usually employed in military or government domain
- MAC typically uses assignment of classification label to each file system object ; such as "confidential", "secret" and "top secret"
- Each system user or device is allotted a corresponding classification level and a clearance level
- MAC is a very secure type of access control
- Key consideration : In MAC pattern, individual resource owners are not allowed to make their own assignments of access permissions to other users and entities



Criteria 'Defined' by

- system administrators

'Enforced' by

- OS, application access controller

Can not be altered by

- End Users

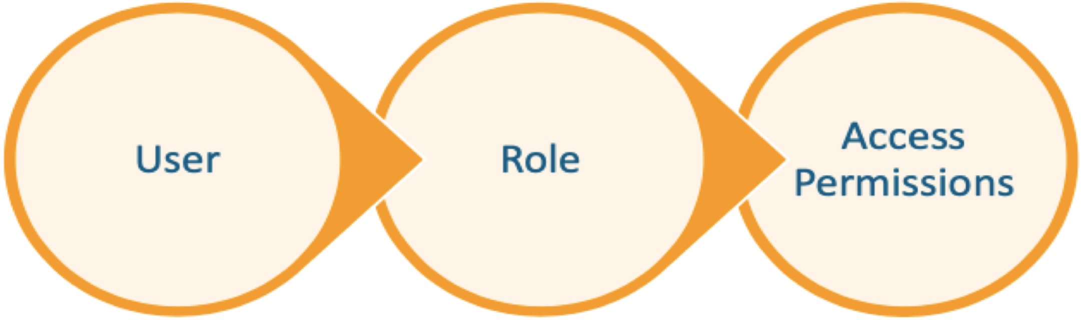
Discretionary Access Control (DAC)

- A **Discretionary Access Control (DAC)** policy is a way to allocate access rights on the basis of rules specified by users (typically the information owners)
- The fundamental concept behind DAC is, typically the information that the owners can govern access to files and objects

User	File: A.txt	File: B.txt
Jack	rwx	r--
Jill	r--	rwx

Role – Based Access Control (RBAC)

- **Role – based access control (RBAC)** works on the basis of a "Role" of a user within an enterprise
- RBAC is a strong security control, because it enables users(employees) to access only the relevant information that pertains to their "current" role in the organization
- User Permissions are mapped to specific enterprise roles and whenever an employee changes the role - the corresponding access permissions change



- Granted by Admin

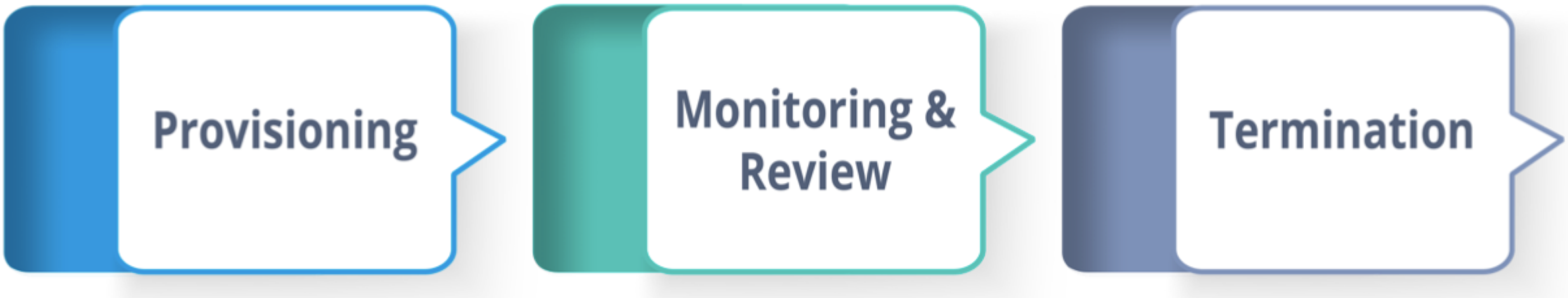
Rule – Based Access Control (RuBAC)

- **Rules Based Access Control** is a strategy to manage user access on multiple systems, based on dynamically triggered rules
- RuBAC is also referred to as Automated Provisioning
- With RuBAC, once a request is sent for accessing a network resource, some security control, for ex: firewall - would verify the properties of the request against a set of pre-defined rules. **Example:** A corresponding rule might be for blocking an IP address, or specific ports and so on

Access Administration

FTVETI

Access Administration Process



Provisioning

Monitoring & Review

Termination

FTVETI

Access Provisioning

- **User provisioning**
  - Deals with maintaining access provisioning lifecycle
  - Critical aspect of organizational security
  - Helps in creating a standard enterprise-wide set of practices around creation, servicing, management & deletion of user accounts
  - Helps ease IT burdens once the process streamlines
- Usually the complexity of user provisioning is a function of the risk impact associated with the requested resources for access
- **High level categories of User Provisioning:**
  - **Discretionary Account Provisioning:** Access decisions are typically taken by an administrator & permissions are accordingly granted to the requesting user
  - **Self-service Account Provisioning:** Users have a mean to request for accounts and also manage their own passwords via given tools & interfaces
  - **Workflow-based Account Provisioning:** Accounts are granted access permissions based on a chain of approvals within organizational structure
  - **Automated Account Provisioning:** Usually a centralized User management application is used to uniformly add manage all the accounts being requested. This is the most streamlined & systematic approach and promotes swift monitoring, analytics and effective policy enforcement

Access Monitoring & Review

- Monitoring access changes provides the ability to determine if users still need access
- It is especially important to monitor the access of administrators having elevated access to databases, security technologies, & networking infrastructure because of potential damage that could result from abuse of these privileges. Reviews of these accounts & associated privileges should occur regularly
- During transfer of employees to other roles, physical & logical access should be reviewed to ensure that the access is provided as needed by the individual
- Keys, badges to buildings, offices or access to a different section of the organization may no longer be needed

ADMIN
LOGIN
I have access to database, Security technologies and other datas

Access Termination

- Access administration process should define procedures to remove access as part of the termination process for personnel
- This should be integrated with the change management or disposition process for system access
- Employee termination require prompt removal of logical & physical access
- Terminations correctly handled by the manager, HR representative, & physical security reduces the risk of security violations

As we have learnt about the concept of Authorization, Authentication and Access Control, we need to know about Management of Identity and Access

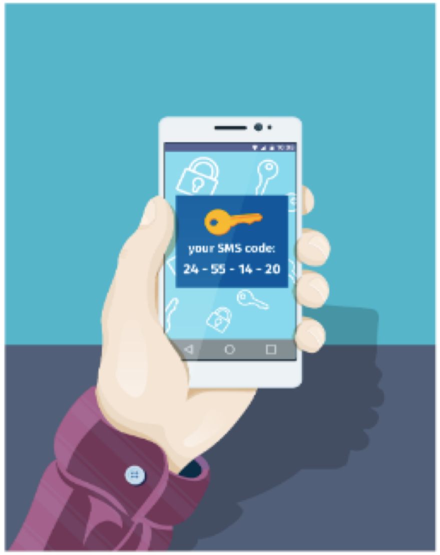
IdAM – Identity & Access Management

FTVETI

ICT @ FTVETI

Managing Digital Identities

- Effective Management of Digital Identities:
  - Needed for Security, Accountability & Trust
  - Helps in Definition, Creation, Management of digital identity & associated metadata



IdAM

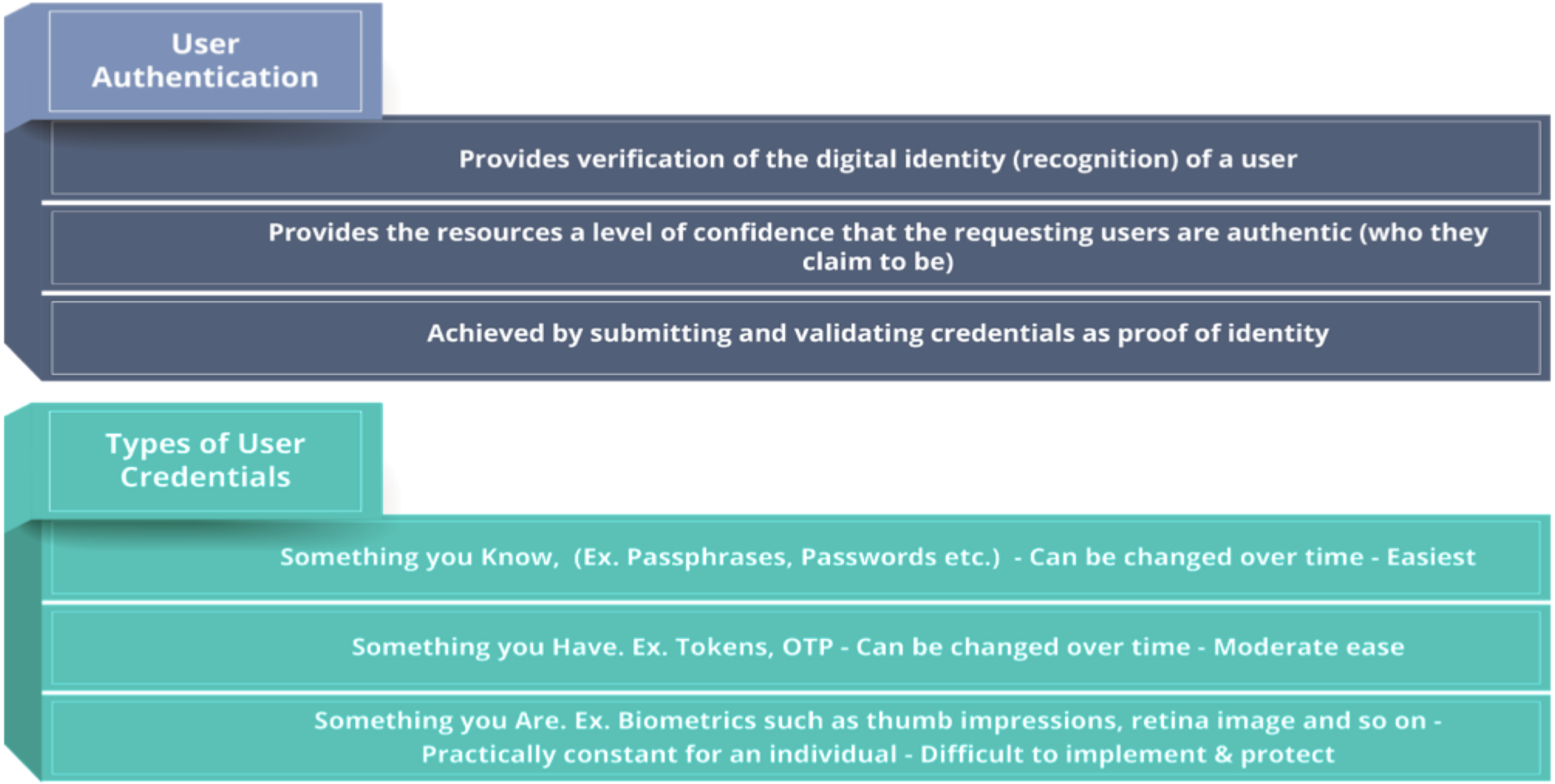
Identity and Access Management (IdAM)

- It is a Harmonious group of policies, processes & systems
- It helps an organization to Define, Create, Govern the utilization, Secure identity information and Manage access permissions of various resources to users

Idam Key Capabilities

- Management of Digital Identities
- Management of User Authentication
- Management of Resource Access Authorization

IdAM – Authentication Of Users



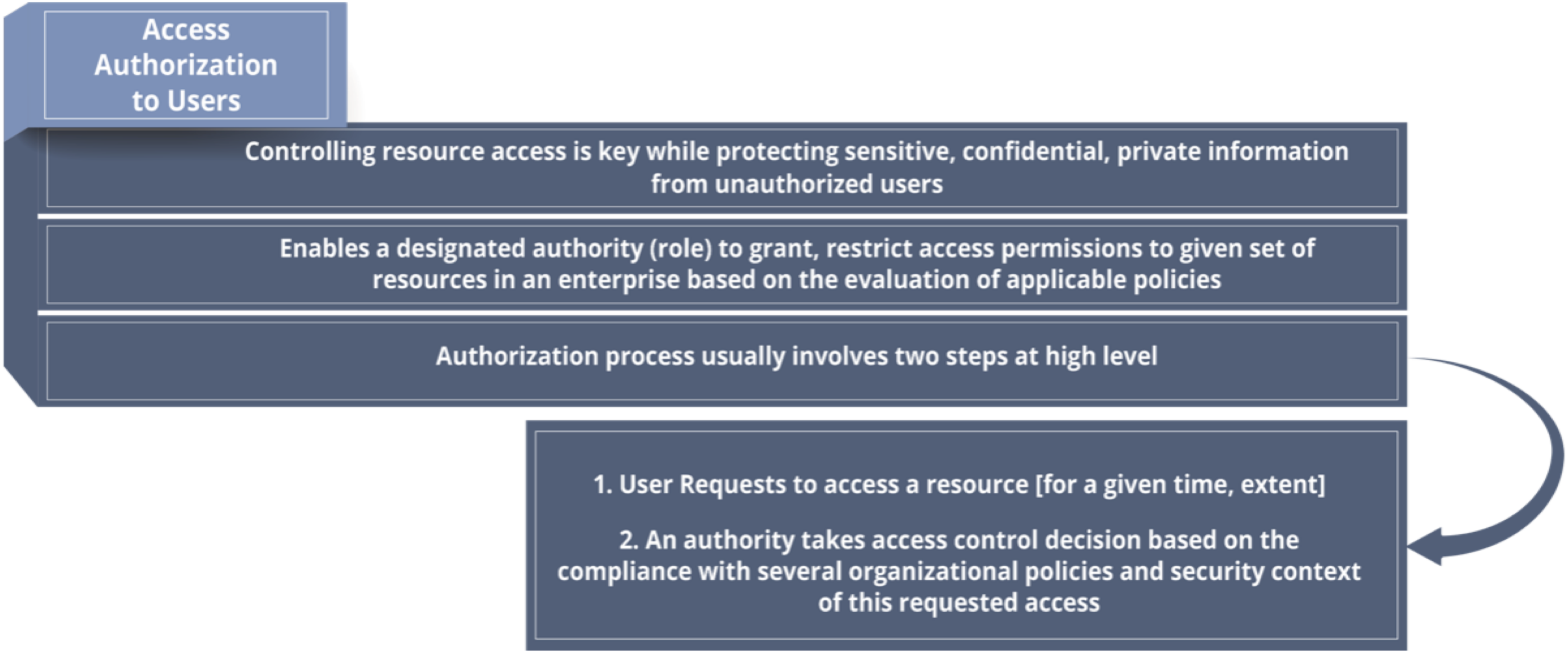
User Authentication

- Provides verification of the digital identity (recognition) of a user
- Provides the resources a level of confidence that the requesting users are authentic (who they claim to be)
- Achieved by submitting and validating credentials as proof of identity

Types of User Credentials

- Something you Know, (Ex. Passphrases, Passwords etc.) - Can be changed over time - Easiest
- Something you Have. Ex. Tokens, OTP - Can be changed over time - Moderate ease
- Something you Are. Ex. Biometrics such as thumb impressions, retina image and so on - Practically constant for an individual - Difficult to implement & protect

IdAM – Authorization Of Access To Resources



Access Authorization to Users

Controlling resource access is key while protecting sensitive, confidential, private information from unauthorized users

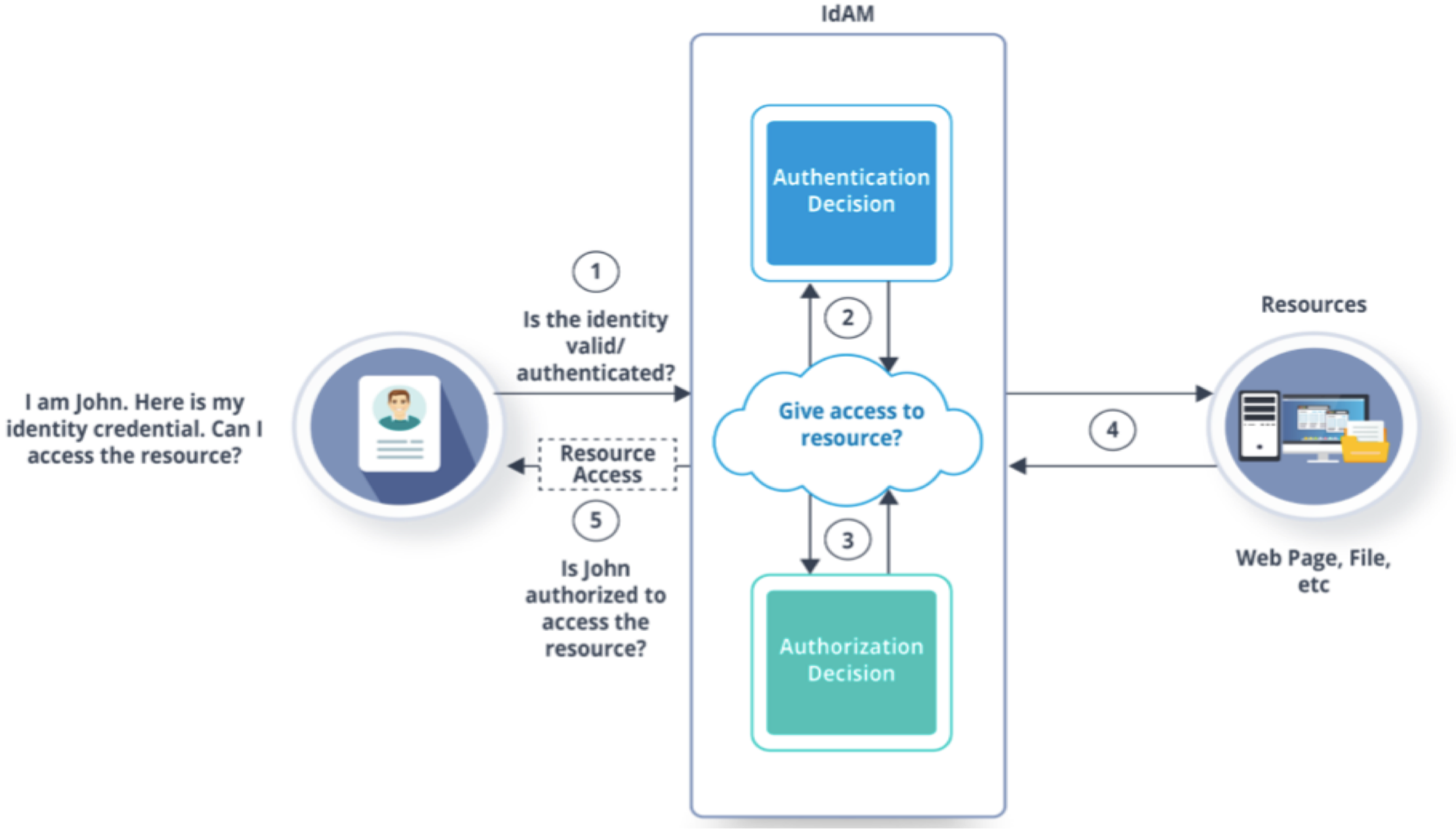
Enables a designated authority (role) to grant, restrict access permissions to given set of resources in an enterprise based on the evaluation of applicable policies

Authorization process usually involves two steps at high level

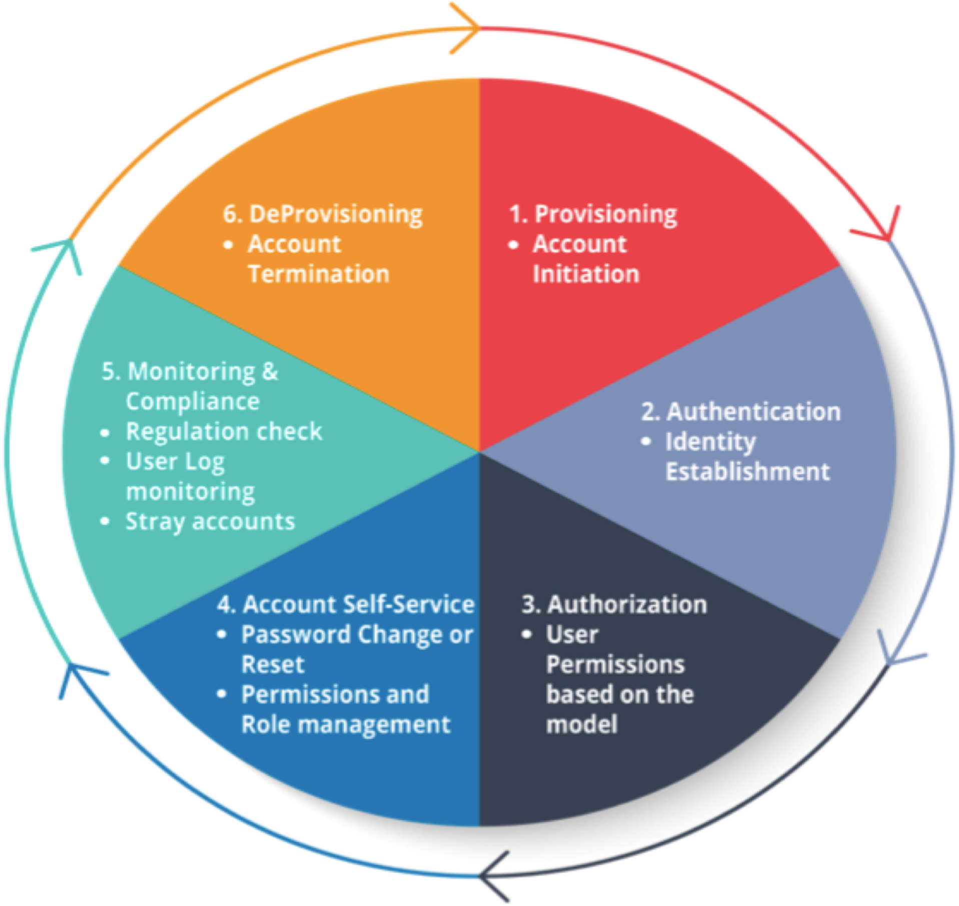
1. User Requests to access a resource [for a given time, extent]

2. An authority takes access control decision based on the compliance with several organizational policies and security context of this requested access

IdAM


IdAM
Authentication Decision
Authorization Decision
Give access to resource?
I am John. Here is my identity credential. Can I access the resource?
1
Is the identity valid/ authenticated?
2
3
Resource Access
5
Is John authorized to access the resource?
4
Resources
Web Page, File, etc

IdAM Life Cycle



1. Provisioning
   - Account Initiation

2. Authentication
   - Identity Establishment

3. Authorization
   - User Permissions based on the model

4. Account Self-Service
   - Password Change or Reset
   - Permissions and Role management

5. Monitoring & Compliance
   - Regulation check
   - User Log monitoring
   - Stray accounts

6. DeProvisioning
   - Account Termination

Benefits Of IdAM To Business

Minimization of Data Breach Risk

- SSO (Single Sign – On), MFA (Multi-factor Authentication), Protection of Identity data via encryption

Centralized access control

- Centralized policies for access permissions - enables a smooth workflow, less confusion, & better traceability

Facilitate compliance

- Data access governance & Privacy Management – helps meeting the requirements of various industrial/ global regulations & standards

Improvement of end-user experience

- Balances Security & end-user convenience & helps in boosting employee productivity

Reduction of IT/ Support costs

- Smooth workflows & handling of various use cases helps in reduced needs of IT support & manual intervention, this in turn helps in optimization of IT resources & costs

IdAM Implementation Perspectives

Employees

- IdAM Solutions help an organization's IT landscape cross beyond the traditional castle based setup into an open & flexible environment
- It ensures that every user (employee) can simultaneously be productive & secure at any time, anywhere & using any device thereby supporting concepts like Globally remote working, BYOD, 24x7 working possibilities
- SSO (Single sign-on) provides easy & one-click access to all internal (scoped) applications for increased productivity

Customers

- IdAM systems typically enable plethora of customers securely accessing mobile, cloud & external applications globally

Partners

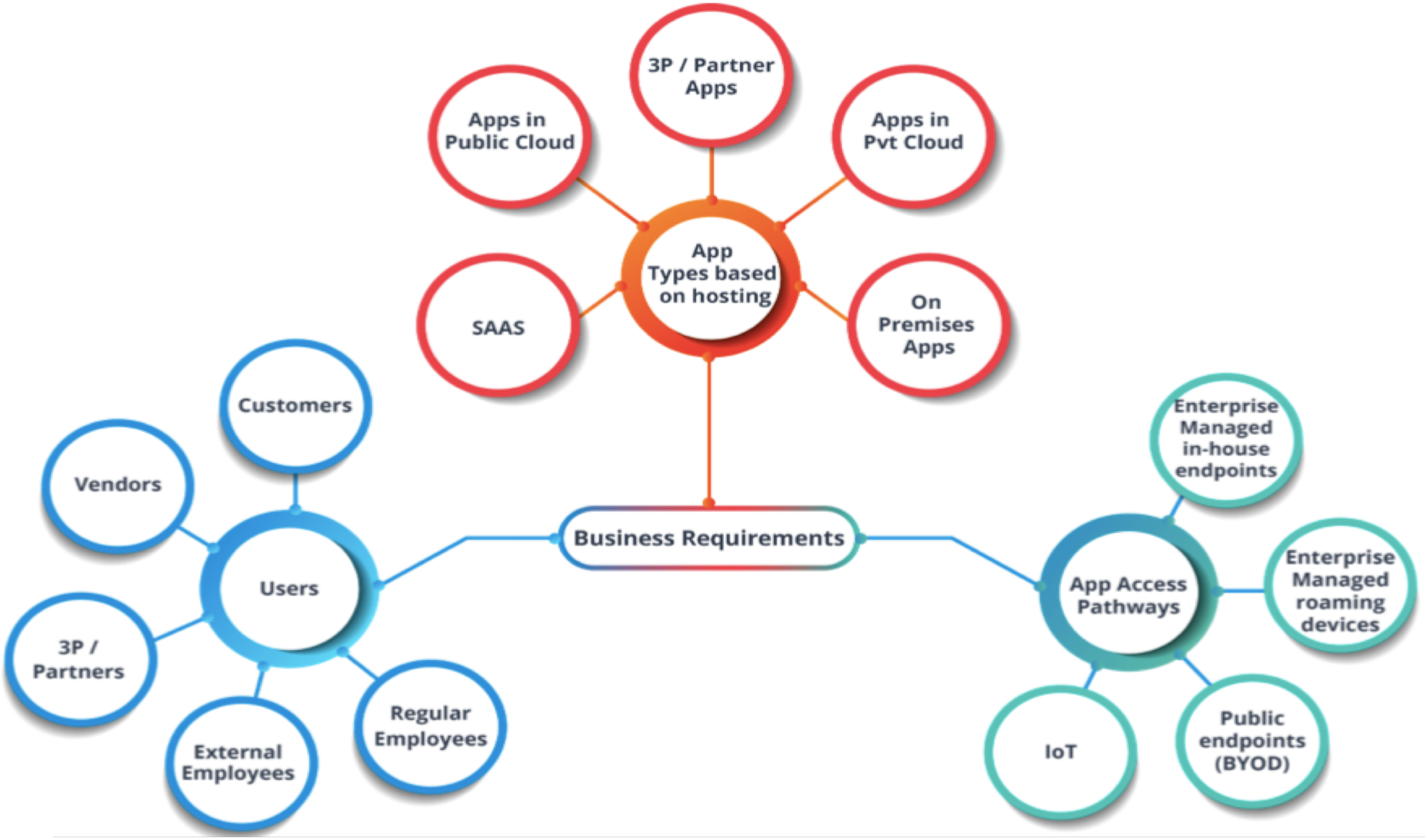
- It is a routine practice to have a collaboration with multitude of partner (third party) organizations for accomplishment of business objectives in optimal cost
- IdAM typically facilitates a secure yet compliant & efficient access for such partner agencies to various resources or business application that they may need to fulfil the statement of work (performing the work they are designated to do)

Organization

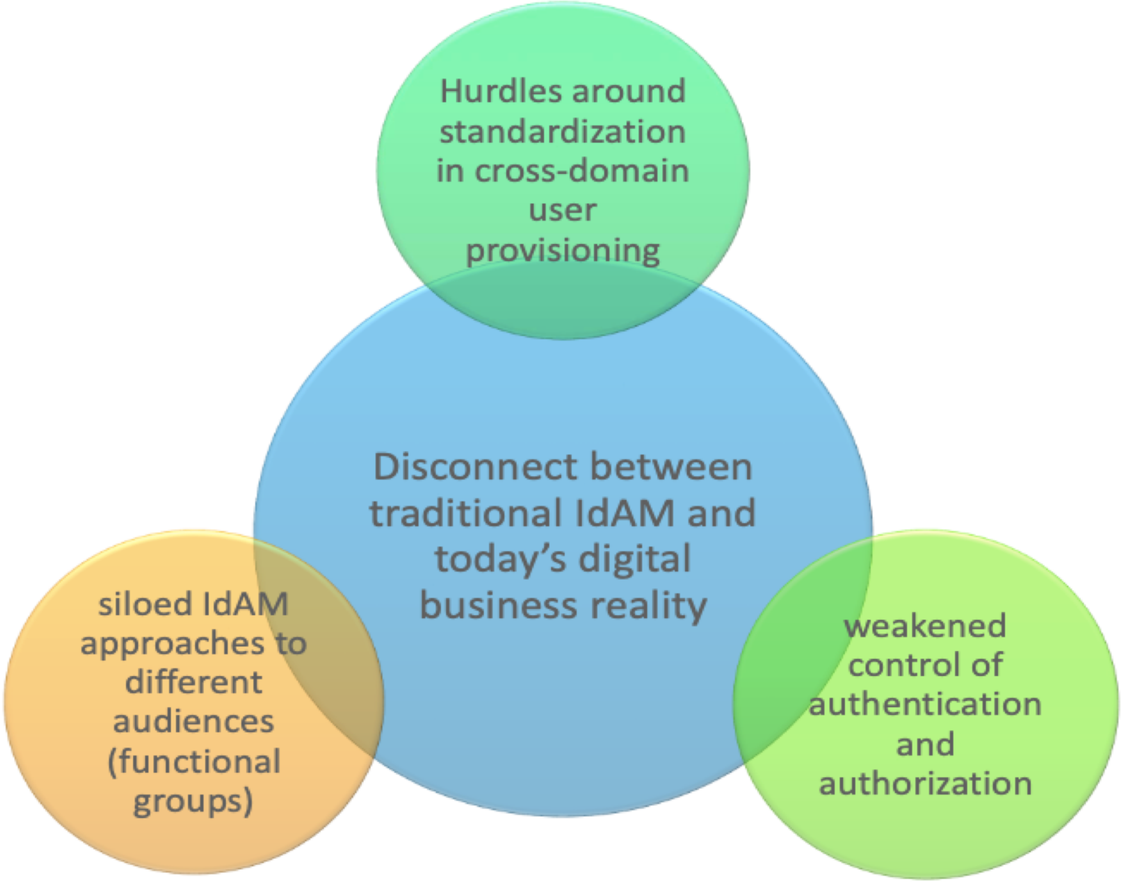
- IdAM provides a balance between Security (for authentication, authorization and user management) and great user experience along with a flexibility towards futuristic integration possibilities with upcoming technology trends

IdAM Strategy

IAM Challenges By Digital Business Requirements



Business Reality Vs Traditional IdAM



Hurdles around standardization in cross-domain user provisioning

Disconnect between traditional IdAM and today's digital business reality

siloed IdAM approaches to different audiences (functional groups)

weakened control of authentication and authorization

Disconnect

Issue: Standardized Cross-Domain User Provisioning

- Close connection with enterprise user database
- Reduced security due to delay in removing authorizations
- Reduced business dexterity due to delay in adding or creating authorizations

Issue: Scenarios That Allow Less Secure Authentication And Authorization

- Diminishing traditional perimeter
  - Usage of Mobile device, Cloud (SaaS , IaaS) and so on, disregards traditional OS based authentication options
  - External applications' local authentication options may not be as effective or in tandem with requirements

Issue : Idam Silos For Each Function

- A change in employee status usually is a gradual process than a single identifiable event
- Heterogeneous federation in business environment Vs. consumer environments.
- SaaS applications serve organizations, businesses and individuals in the same way

Concept Of Zero Trust

Zero Trust is a security concept according to which, organizations should never spontaneously trust any request for access irrespective of its location w.r.t. to the boundaries of it's perimeters. Each & every connection request must be thoroughly verified before permitting the access

Operate on the principle of least privilege — in the right context

Based on sensitivity of applications and data

Uniformly handle access channels, hosting models & business functions

Integrate Cyber – security & log aggregation solutions with IdAM tools

Zero Trust Model

The Zero Trust model of information security primarily helps organizations to transcend beyond the traditional castle based approach of security which considered everything inside as secure

With the advancements in technology, as the boundaries of organization's perimeter is diminishing - the old castle based approach no longer works well and if not altered , paves the way to complex & severe data breaches. For Ex: As per the old approach if an attacker gets inside a perimeter firewall he is then practically free to move anywhere within the org network without any major hurdles

Approach To An Effective IdAM Strategy

Maintain or improve customer experience across channels

Identify interdependencies and other risks

Ensure executive attention and buy – in

Avoid disrupting existing employee services

IdAM Implementation Challenges

IdAM Requires Cooperation From Several Technology Management Teams

- IT operations performs essential identity administration
- App developers adhere to secure IdAM practices in code development
- Compliance managers drive audit requirements
- CIOs and CISOs provide budget and support

IdAM Requires Business Leaders To Define Requirements And Promote IdAM

- Marketing and line-of-business owners guard customer experience
- Business leaders define usability and process requirements
- HR provides quality identity data
- Call center professionals provide customer-facing identity support

IdAM Prospects

FTVETI

Futuristic IdAM

Ever Increasing "Digital Business" necessities a superior approach to Identity

- Authenticate customers without hurting the customer experience
- Support workforce enablement without impacting employee experience
- Support rapid adoption of cloud-based services
- Provide secure integration and data exchange across multiple users in diverse business functions

Evolve from Isolated IdAM approaches Towards "Zero Trust" Identity

- Improve business agility and competitiveness.
- Achieve compliance, enhance productivity, save spends, and drive revenue !
- Integrate Security at the very root level of IdAM strategy

Password Protection

FTVETI

Password Policies And Practices

- Having a strong & up to date password policy is a key security requirement for an organization
- A good password has primarily two attributes
  - Easy for users to remember
  - Difficult for anyone else to guess or discover
- Key attacks on unknown passwords:
  - **Dictionary attacks:** guessing commonly-used passwords
  - **Brute-force attacks:** guessing every possible password
- Known passwords
  - Leaked passwords are known & may be used unless they are changed
  - However, when the password gets leaked it also shows the pattern in which a user is prone to choose his/her passwords

Password Storage – Provider's View

01 Need secure mechanism to recognize users via Login credentials (UserID & Passwords)

02 Make sure that no plain text passwords are stored in the database (using cryptographic hashes)

03 Make sure that appropriate "salting" (method of additional obfuscation) of passwords is used to make passwords difficult to be used even after potential leakage

04 Ensure enough password complexity requirements are imposed so that user's password remains strong enough against brute-force and dictionary attacks

05 Balance password complexity & ease of use

Password Handling – User's View

Easy passwords can be set (not safe) & authentication remains quick

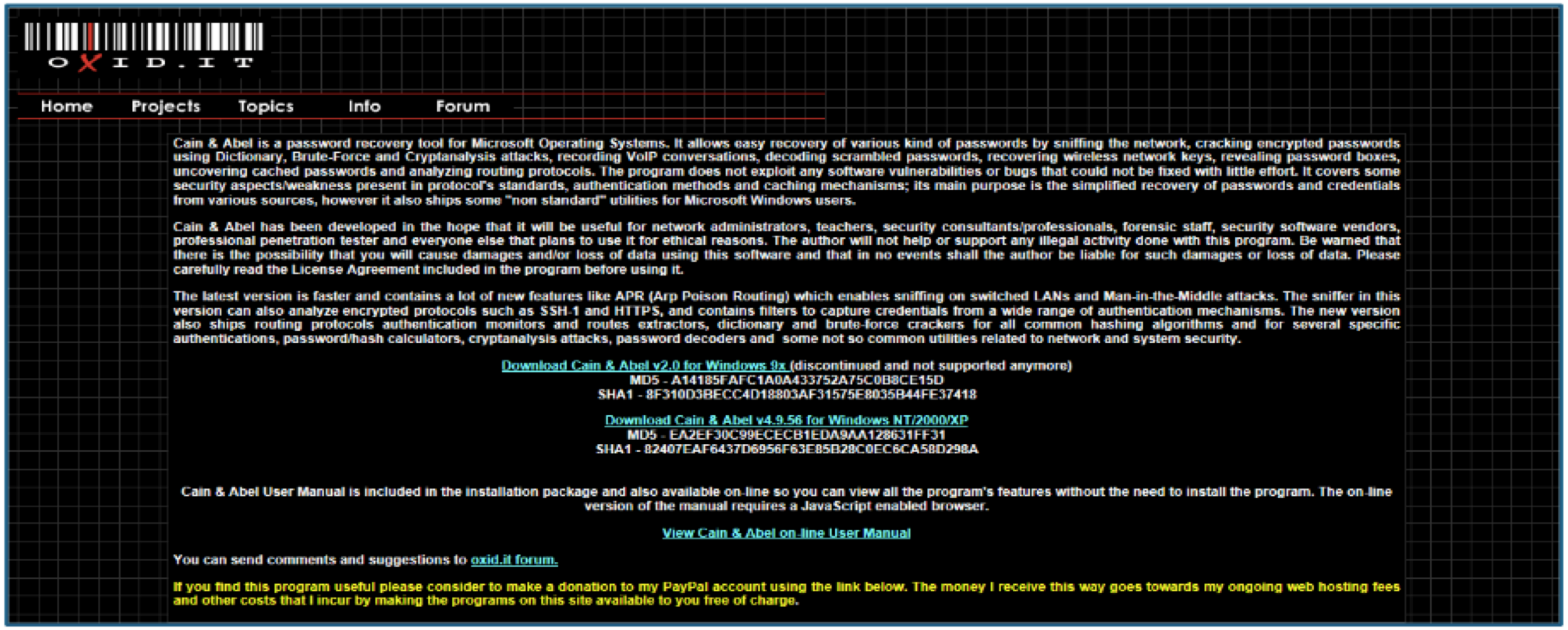
Expect the provider to be secure against typical application security attacks & password leakage

Ease password servicing (resets, change and so on)

Enablement of Copy Pasting passwords (not a safe way)

Demo 1: Password Management

- Check the strength of the Windows password by password cracking tool
- Install **Cain and Abel** tool from the following URL: http://www.oxid.it/cain.html
- Retrieve password from the local machine



Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols. The program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort. It covers some security aspects/weakness present in protocol's standards, authentication methods and caching mechanisms; its main purpose is the simplified recovery of passwords and credentials from various sources, however it also ships some "non standard" utilities for Microsoft Windows users.

Cain & Abel has been developed in the hope that it will be useful for network administrators, teachers, security consultants/professionals, forensic staff, security software vendors, professional penetration tester and everyone else that plans to use it for ethical reasons. The author will not help or support any illegal activity done with this program. Be warned that there is the possibility that you will cause damages and/or loss of data using this software and that in no events shall the author be liable for such damages or loss of data. Please carefully read the License Agreement included in the program before using it.

The latest version is faster and contains a lot of new features like APR (Arp Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks. The sniffer in this version can also analyze encrypted protocols such as SSH-1 and HTTPS, and contains filters to capture credentials from a wide range of authentication mechanisms. The new version also ships routing protocols authentication monitors and routes extractors, dictionary and brute-force crackers for all common hashing algorithms and for several specific authentications, password/hash calculators, cryptanalysis attacks, password decoders and some not so common utilities related to network and system security.

Download Cain & Abel v2.0 for Windows 9x (discontinued and not supported anymore)
MD5 - A14185FAFC1A0A433752A75C0B8CE15D
SHA1 - 8F310D3BECC4D18803AF31575E8035B44FE37418

Download Cain & Abel v4.9.56 for Windows NT/2000/XP
MD5 - EA2EF30C99ECECB1EDA9AA128631FF31
SHA1 - 82407EAF6437D6956F63E85B28C0EC6CA58D298A

Cain & Abel User Manual is included in the installation package and also available on-line so you can view all the program's features without the need to install the program. The on-line version of the manual requires a JavaScript enabled browser.

View Cain & Abel on-line User Manual

You can send comments and suggestions to oxid.it forum.

If you find this program useful please consider to make a donation to my PayPal account using the link below. The money I receive this way goes towards my ongoing web hosting fees and other costs that I incur by making the programs on this site available to you free of charge.

Identity Theft

Identity Theft

Identity Theft

- Identity theft or Identity fraud, is a type of cyber crime where an attacker obtains key chunks of PII (personally identifiable information), such as Social Security or driver's license numbers, with a goal of being able to impersonate the victim
- The information can then be easily misused against either the victim or to achieve unauthorized gains

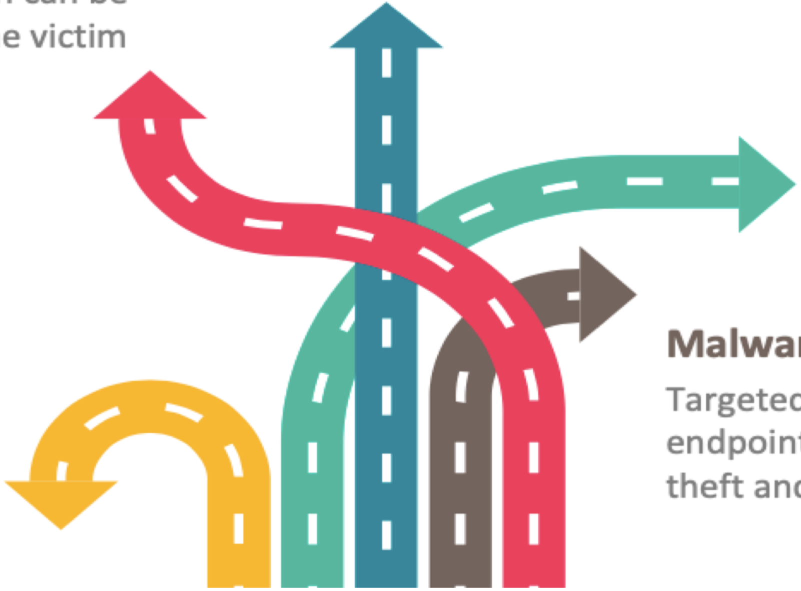
True-name identity theft

- The hacker uses PII to open fresh real accounts. He may connect several other services such as credit cards & mobile phones, to such accounts and then commit crime using them in the name of victim!

Account-takeover identity theft

- The hacker uses victim's PII to gain access to his/her existing accounts. The communication details such as email addresses, phone and so on, are then changed to execute huge purchase transactions using the money contained in victim's accounts

Common Techniques For Identity Theft



Phishing

Phishing a type of social engineering attack, it is a deceitful endeavour to acquire sensitive information from a victim. Usually to phish a user or a group of users successfully the attacker pretends to be a trusted entity. The user becomes a victim if he/she gets allured enough to divulge the information asked. **Ex:** Fake login pages of reputed banks

Shoulder Surfing

Casual spying around by looking into the computer, mobile, ATM screens of others. Sometimes useful clues or information can be derived by a hacker and used against the victim

Spamming

Indiscriminate burst of emails containing malicious, phishing, misleading information. Victims fall prey to such attack easily by following the content of such Spam emails

Dumpster Driving

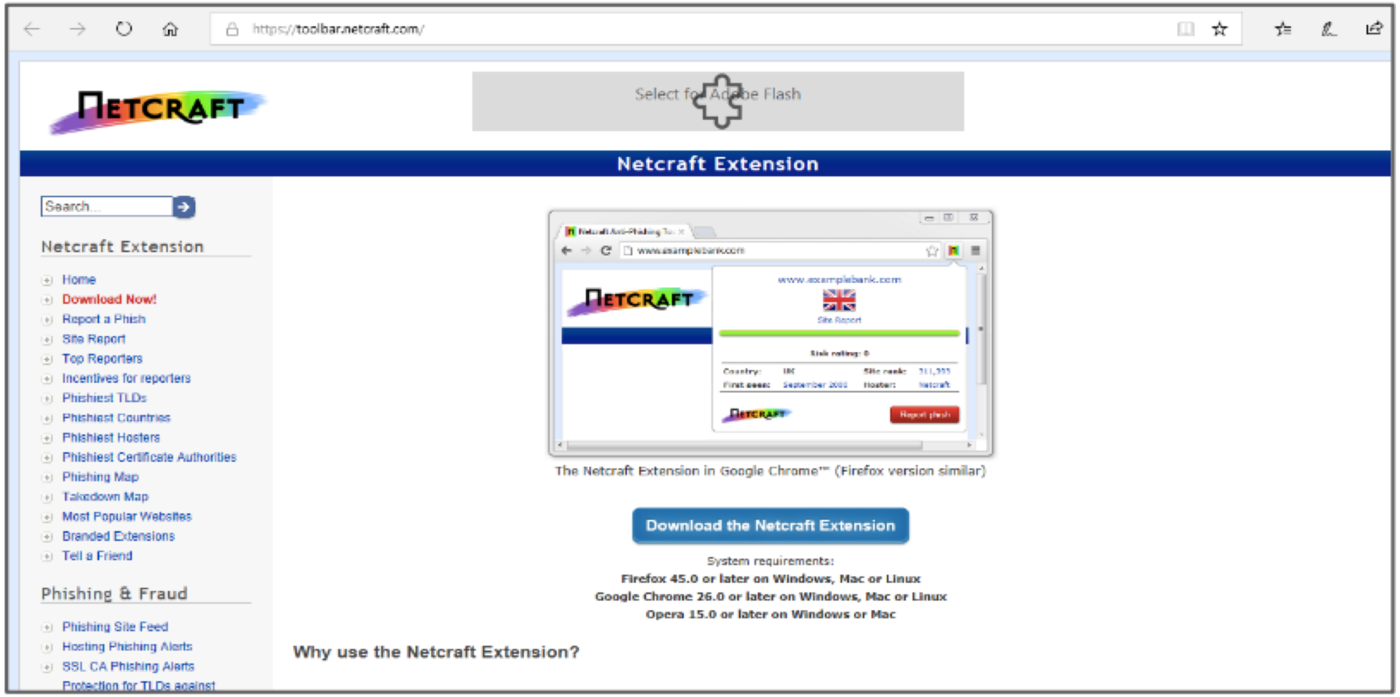
Digging through garbage - to search for traces of personally identifiable information. Such information can be later used for Identity Theft & related cyber crimes

Malware

Targeted malwares can be installed on a victim's endpoints which can then cause PII, sensitive data theft and in turn reveal identity of the victim

Demo 2: Phishing

- Protect yourself against phishing sites attempting to steal your user details
- Install and configure **Netcraft Anti Phishing** toolbar from the link: http://toolbar.netcraft.com



Netcraft Extension

The Netcraft Extension in Google Chrome™ (Firefox version similar)

System requirements:
Firefox 45.0 or later on Windows, Mac or Linux
Google Chrome 26.0 or later on Windows, Mac or Linux
Opera 15.0 or later on Windows or Mac

Why use the Netcraft Extension?

Quiz #1

- An Enterprise is concerned about recent unauthorized physical access attempts to the data centre. In order to mitigate the risk, the employees while entry to the data centre are mandated to swipe their access card & then enter a PIN sent to their registered mobiles. What type of authentication mechanism has been implemented?
  a. IdAM
  b. Pre Authentication
  c. Multi Factor Authentication
  d. Authorization

Answer #1

- An Enterprise is concerned about recent unauthorized physical access attempts to the data centre. In order to mitigate the risk, the employees while entry to the data centre are mandated to swipe their access card & then enter a PIN sent to their registered mobiles. What type of authentication mechanism has been implemented?

  a. IdAM

  b. Pre Authentication

  c. **Multi Factor Authentication**

  d. Authorization

Answer c:
Explanation: Multi-factor authentication is a method of verification of a user's identity, in which a user is permitted access only after successfully presenting 2 or more evidences/factors to an authentication mechanism

Quiz #2

- Within an R&D department of an enterprise, frequent file collaboration is required amongst teams. Hence to facilitate collaboration, the management has approved an access control scheme where each user can grant or deny access permissions for owned files, to other users based on the need and his/her own judgement. What kind of access control model does this scheme refer to?
  a. Mandatory Access Control (MAC)
  b. Discretionary Access Control (DAC)
  c. Attribute Based Access Control (ABAC)
  d. Rule Based Access Control (RuBAC)

Answer #2

- Within an R&D department of an enterprise, frequent file collaboration is required amongst teams. Hence to facilitate collaboration, the management has approved an access control scheme where each user can grant or deny access permissions for owned files, to other users based on the need and his/her own judgement. What kind of access control model does this scheme refer to?

  a. Mandatory Access Control (MAC)

  b. Discretionary Access Control (DAC)

  c. Attribute Based Access Control (ABAC)

  d. Rule Based Access Control (RuBAC)

Answer b:
Explanation: A discretionary access control (DAC) policy is a way to allocate access rights on the basis of rules specified by users (typically the information owners). The fundamental concept behind DAC is, typically the information owners can govern the access to the files, objects

Quiz #3

- An organization has installed biometric access control systems. However, management is concerned with high FRR. What could be the implications?
  a. Employees will effortlessly gain access
  b. There will be an alert for each denied user
  c. Employees can easily bypass the access control
  d. Most of the deserving users will be denied access

Answer #3

- An organization has installed biometric access control systems. However, management is concerned with high FRR. What could be the implications?

  a. Employees will effortlessly gain access

  b. There will be an alert for each denied user

  c. Employees can easily bypass the access control

  d. Most of the deserving users will be denied access

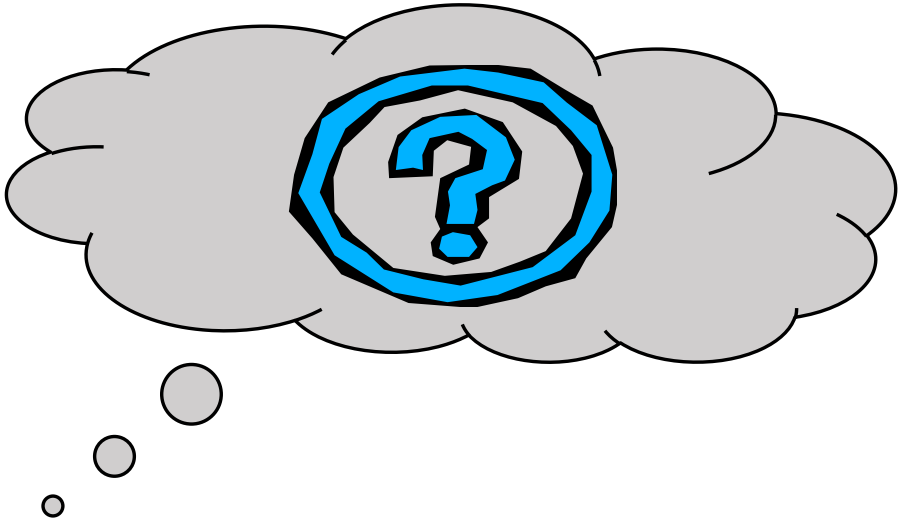
Answer d:
Explanation: FAR (False Acceptance Rate) is the likelihood that the biometric security system will incorrectly ACCEPT an access attempt, by an Unauthorized user. FRR (False Recognition Rate) is the likelihood that the biometric security system will incorrectly REJECT an access attempt, by an Authorized user. Hence high FRR means - more rejections in error, of deserving candidates!

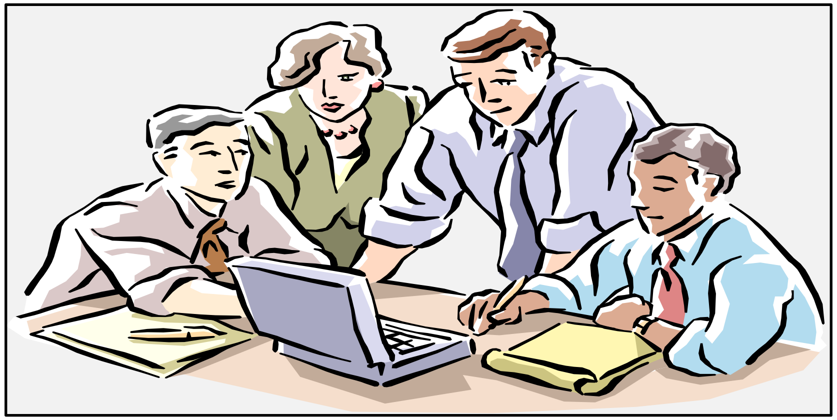
Summary

In this unit, you should have learnt:

- Fundamentals of Identity, Authentication, Authorization & Access Control
- Basics of IdAM & its importance to business and security perspective
- Various types of Access Controls and Access Administration at high level
- IdAM strategy and implementation challenges
- Concept of zero trust
- Password Protection
- Identity theft & methods

QUESTIONS PLEASE ☺





FTVETI

ICT @ FTVETI