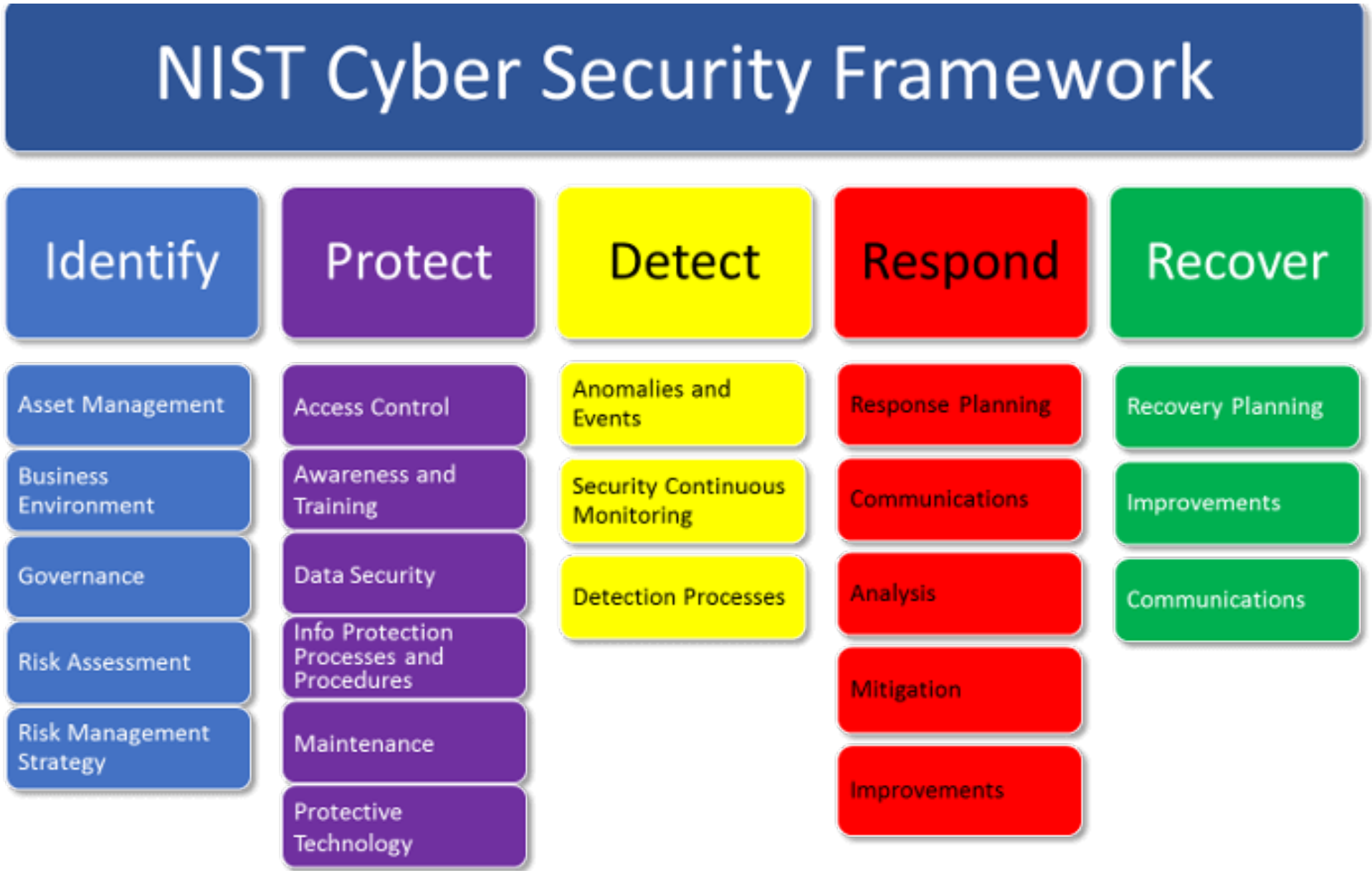
Access Control
&
Identity Management

Introduction & Overview

NIST CSF


NIST Cyber Security Framework
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Protect
Access Control
Awareness and Training
Data Security
Info Protection Processes and Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Communications
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communications

Why Access Control

- Protecting what needs to be done with available resources

- Access Control is the heart of Information Security

Access Control

- Access Control is the part of security that constrains the actions that are performed in a system based on access control rules.

- It consists of two main types:
  - Physical access control - fencing, hardware door locks, and mantraps that limit contact with devices
  - Technical access control - technology restrictions that limit users on computers from accessing data

Benefits of Access Control

A security practitioner must understand the concepts of controlling physical and logical access to assets.

A few benefits of access control are as follows:

Information Systems

Multiple layers of access controls are used to protect against compromise and damage to the systems, along with the information they contain.

Facilities

Various access controls protect and prevent entry and movement around the organization's physical locations to protect personnel, information, equipment, and other assets of the organization.

Personnel

Access controls ensure that only legitimate people with certain privileges and associated with the organization can interact with others in the organization.

Ref. #cissptrainingvideos2017 #cissp #cissptraining

Benefits of Access Control

A few other benefits of access control are as follows:

Support Systems

Access control avoids compromise of the support systems such as power, fire suppression controls, water, and Heating, Ventilation and Air Conditioning (HVAC systems) by any malicious entity, which may hamper the ability to support critical systems and can cause harm to the organization's personnel.

Logical Access Controls

Logical access controls are protection mechanisms that limit users' access to information. They are generally built into the operating system.

Some of the common access control modes include the following:

- Read Only
- Read and Write
- Execute

Insights

What is Access?

The right

What is access mechanism?

Flow of information between subject and object

What is access control?

Mechanism to protect the assets!

Terminologies in Access Control

The terms access, subject, object, and access controls are defined below:

Access is the transfer of data between subjects and objects.

Subject is an active component that needs access to an object or the data within it.

Object is a passive component that contains data or information.

Access control is the security feature which controls how a user and/or system interact and communicate with other systems and resources.

Access Control – First Element

The first element of an effective access control program in an organization is to establish identity and access management policy, and related standards and procedures.

The identity and access management policy:

- specifies the way users and programs are granted access through proper identification and authentication;
- specifies the guidelines of granting privileges to various resources;
- improves the governance process; and
- prevents inconsistencies in provisioning, administration, and access control management.

Terminologies

Identification – Presenting credentials

- Method of establishing the subject's identity
- Use of username and other public information

Authentication – Checking credentials

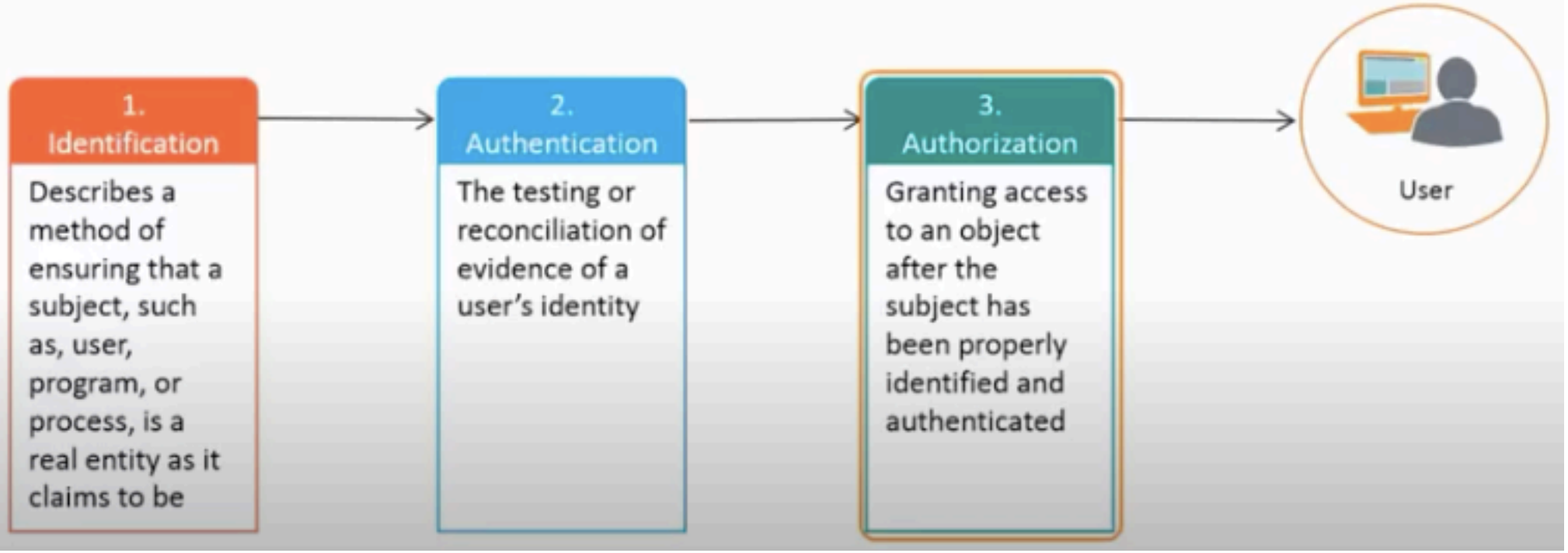
- Method of proving identity
- Strong authentication

Authorization – Granting permission

- Approval based on authenticity

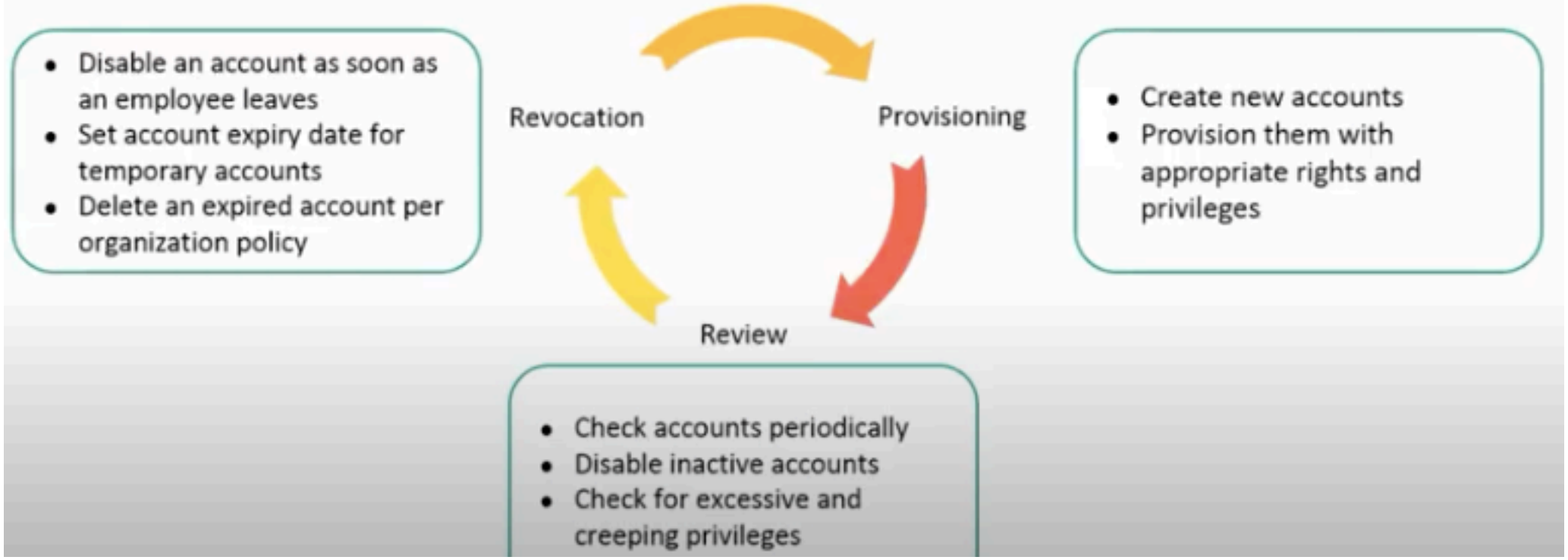
Access Control – Basic Steps

To be able to access a set of data or a resource, a subject has to be identified, authenticated, and authorized. The process is shown below.



Identity and Access Life Cycle

The identity and access provisioning lifecycle must be maintained and secured.



Digital Identification

To ensure an application is authorized to make requests to potentially sensitive resources, the system can use digital identification, such as a certificate or one-time session.

Some of the most common types of identification methods are as follows:

- Username
- User ID
- Account number
- Personal Identification Number (PIN)
- Identification Badges
- MAC Address
- IP Address
- Email Address
- Radio Frequency Identification (RFID)

Digital Identification - Characteristics

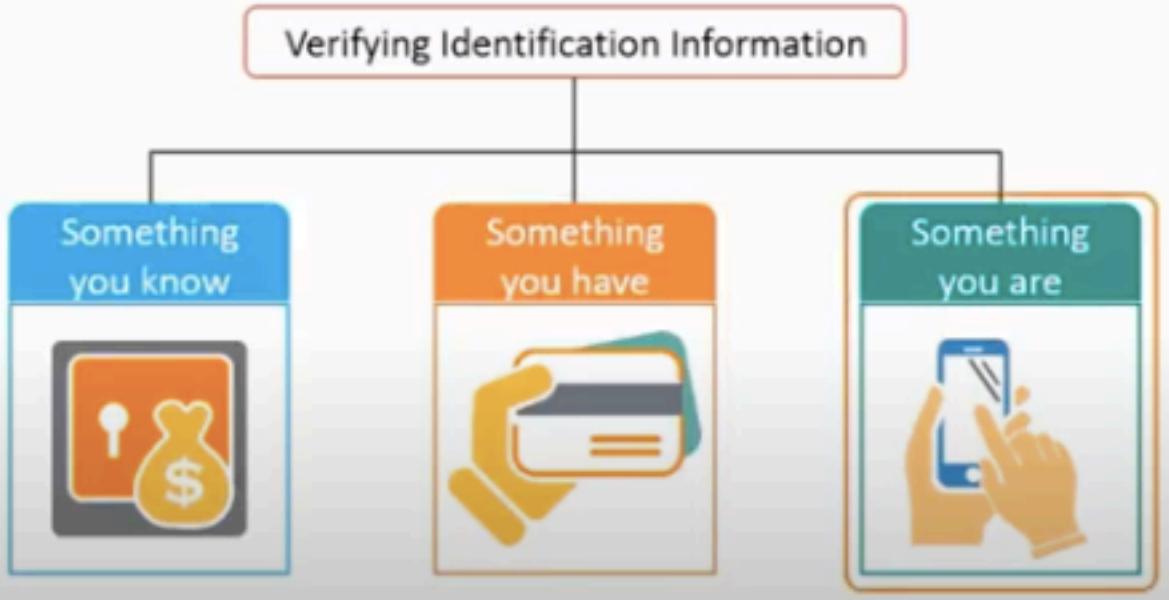
Following are the three important security characteristics of identity:

Uniqueness	Non-descriptiveness	Secure assurance
The user identification must be unique	The user's role or job function should not be exposed by Identity (ID)	ID issuing process must be well documented and secure

Digital Identification -Verification

The function of Identification is to map a known quantity to an unknown entity to make it known.

There are three general factors that can be used for verifying identification:



Digital Authentication

Depending on the number of factors used, there are two ways of strengthening authentication.

Two-Factor Authentication

A secure method of authentication in which the user is required to provide at least two out of the three identification factors.

Three-Factor Authentication

For highest level of security, the user is asked to provide all the three identification factors.

Digital Authentication - Biometrics

Biometrics, based on individuals' physiological and behavioral characteristics, is one of the most effective and accurate methods of verifying identification.

Acceptance

- Refers to user acceptance of biometric system
- Depends on privacy intrusiveness, and psychological or physical discomfort

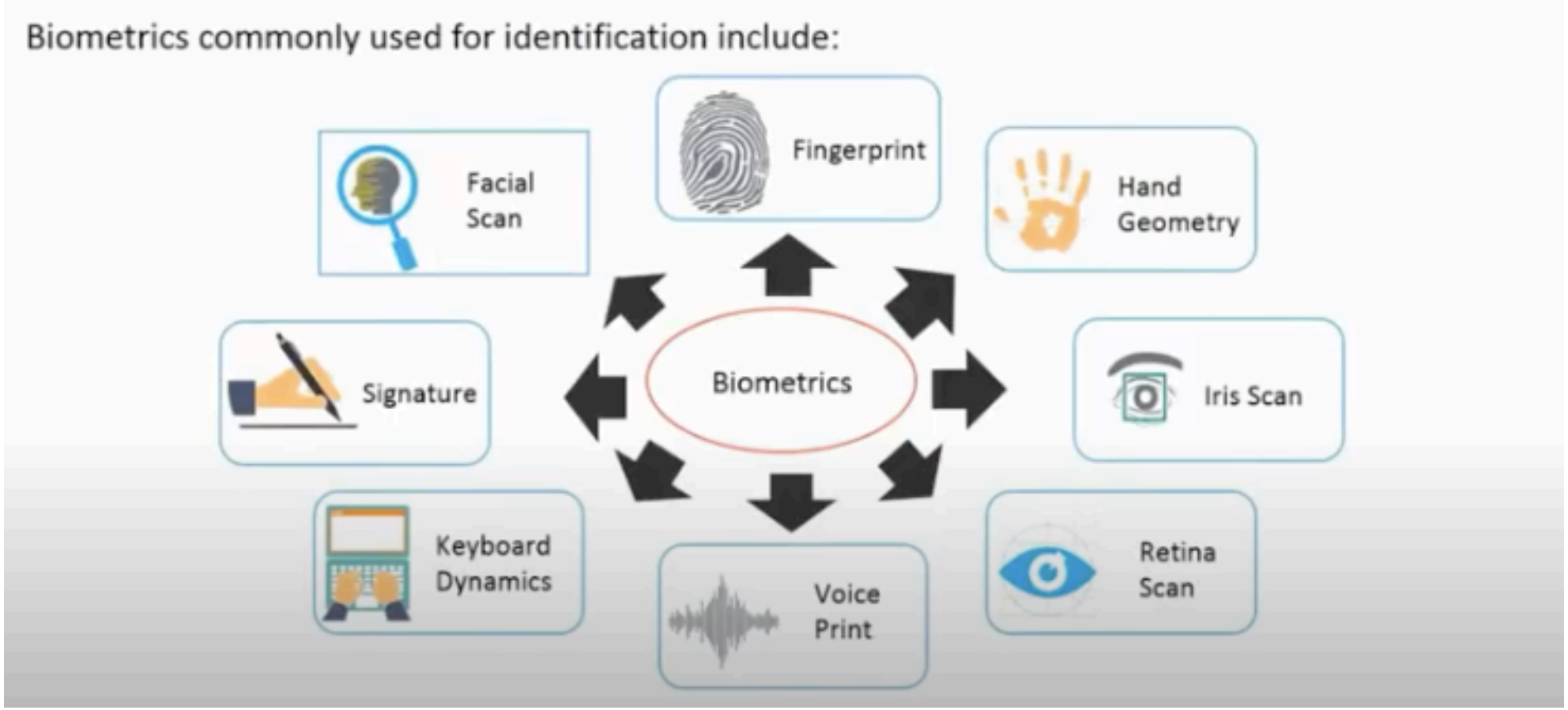
Throughput Rate

- Also called biometric system response time
- Refers to the time taken to process the authentication request

Enrollment Time

- Refers to the time taken by the biometric system to register and create an account for the first time

Digital Authentication - Biometrics



Digital Authentication - Passwords

The combination of username and password is the most common identification and authentication scheme.

Problems with Passwords

- Insecure
- Easily broken
- Inconvenient
- Repudiable

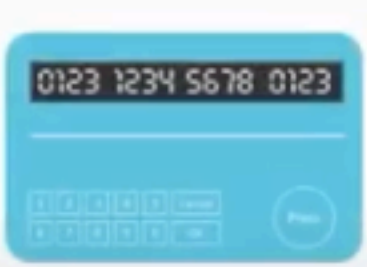
Common Password Attacks

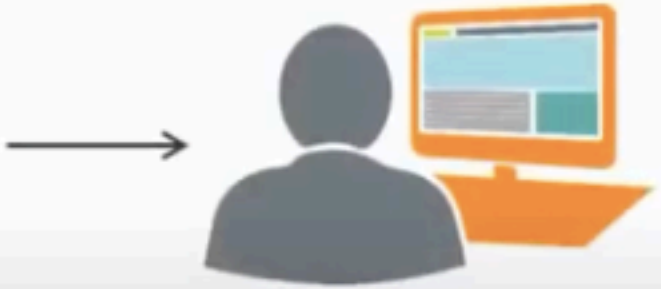
- Dictionary (Crack, John the Ripper)
- Brute force (I0phtcrack)
- Hybrid attack (Dictionary and Brute Force)
- Trojan horse login program (Password sending Trojans)
- Social engineering

Digital Authentication – Token device

Time based:

- Requires synchronized internal clocks between the token device and the authentication server.



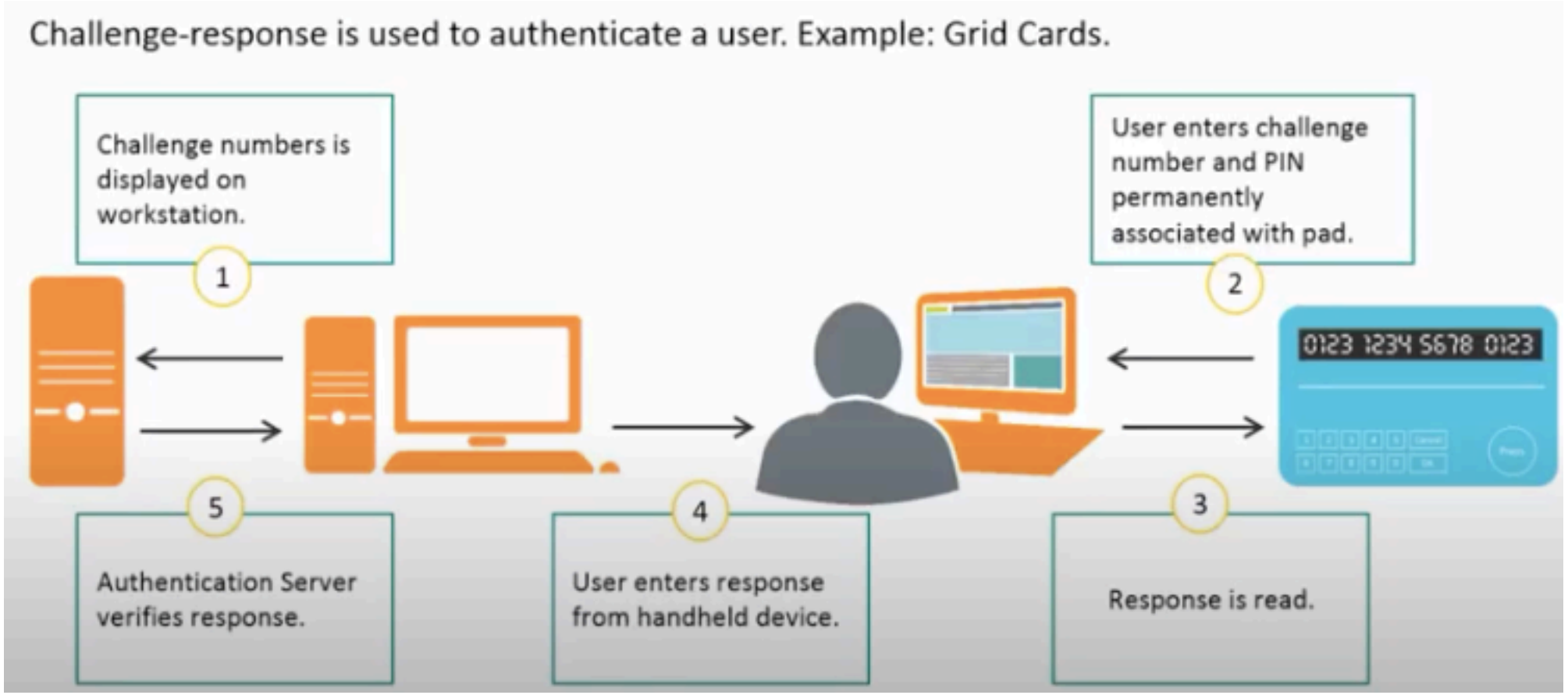


1. Every minute clock reading is enciphered with secret key and displayed. This is one-time password.

2. User reads secret key and along with the PIN enters the data into workstation.

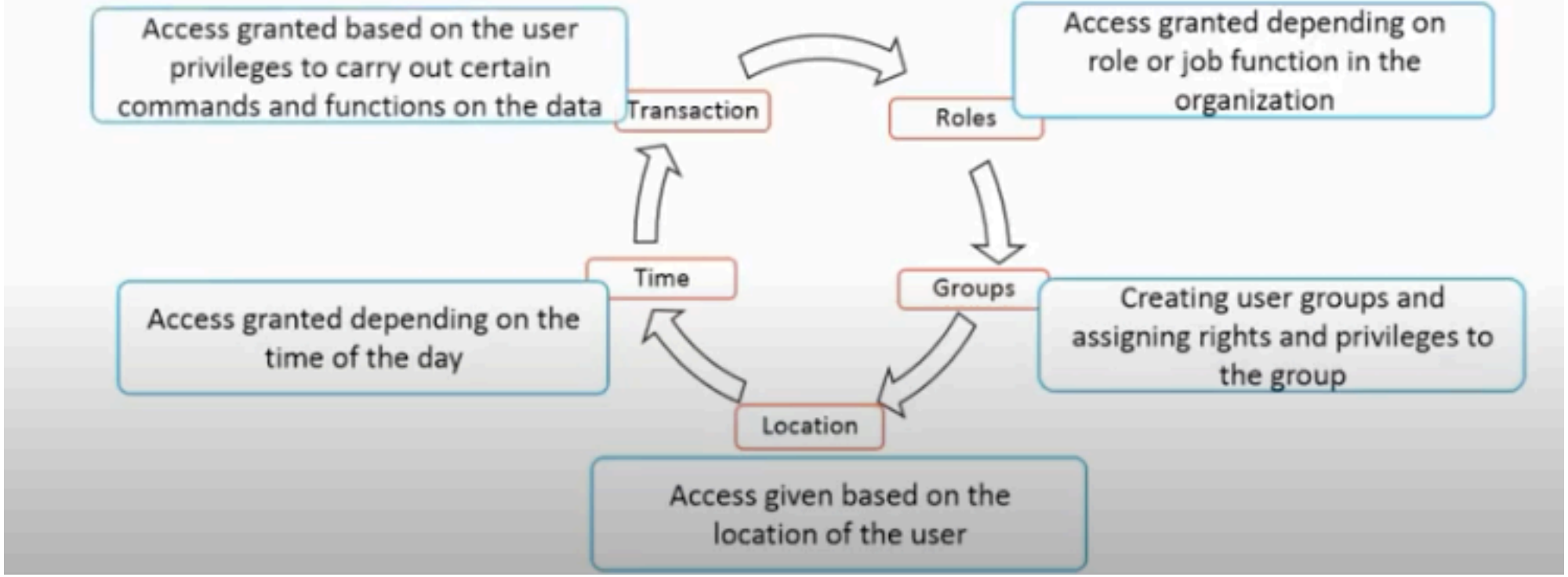
3. Authentication Server knows secret keys to all cards by clock synchronization with the cards. It verifies the entered data.

Digital Authentication – Challenge-Response



Access Control Model

An organization should grant access privilege to subjects based on its level of trust and need to know.
Access criteria are based on:



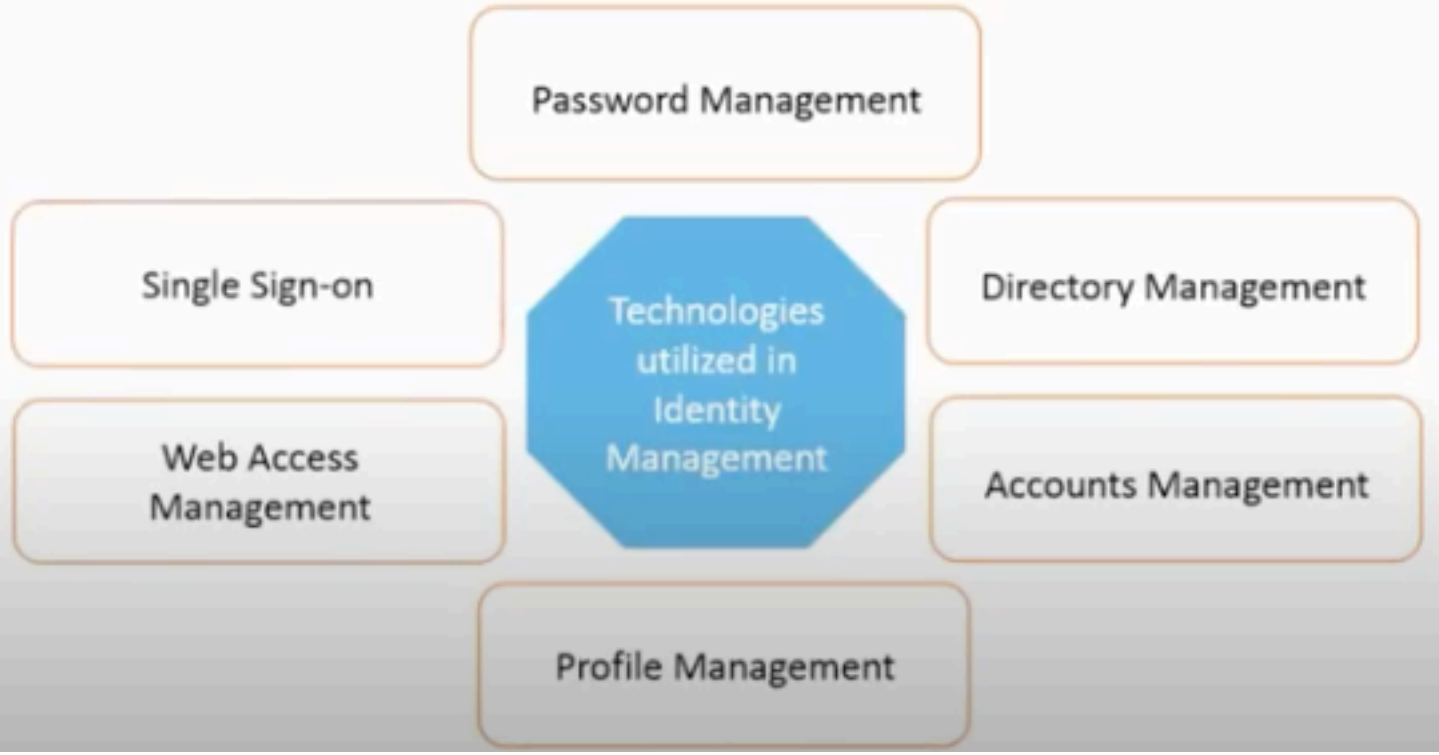
Access Control Model - Authorization

Authorization is based mainly on the following concepts.

- **Need-to-know Principle**: According to this principle, depending on the subject's job duties and requirements, the subject is given access to specific information.
- **Authorization Creep:** This occurs when an employee working for an organization moves from one department to another, and is assigned new access rights and permissions without reviewing or removing the old permissions.
- **Access Control List (ACL):** It specifies the subjects which are granted access and the operations allowed on objects.
- **Default to Zero:** Access controls should always start with zero access. Administrator can then allow various accesses based on the organization's security policy.

Identity Management Solutions

Some of the technologies utilized in Identity Management solutions include the following:



Identity Management Solutions - Directory

Centralized directory service for the enterprise supports many directory technologies. The most common directory standards are as follows:

X.500	X.500 is a series of computer networking standards covering electronic directory services.
Lightweight Directory Access Protocol (LDAP)	It is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
Active Directory (AD)	It is a directory service that Microsoft developed for Windows domain networks, and is included in most Windows Server operating systems as a set of processes and services.
X.400	It defines standards for Data Communication Networks for Message Handling Systems (MHS), which is commonly known as email.

Identity Management Solutions - WAM

Web Access Management (WAM) makes use of software controls to control what users can access from web-based enterprise assets using their web browser.

- Password, digital certificate, token, and others can be used to authenticate users
- WAM acts as a gateway between users and corporate web-based resources
- WAM also provides Single Sign-On capability

Identity Management Solutions - SSO

In Single Sign-On (SSO), the user needs to enter credentials only once to get access to all the corporate resources which are entitled to the user.

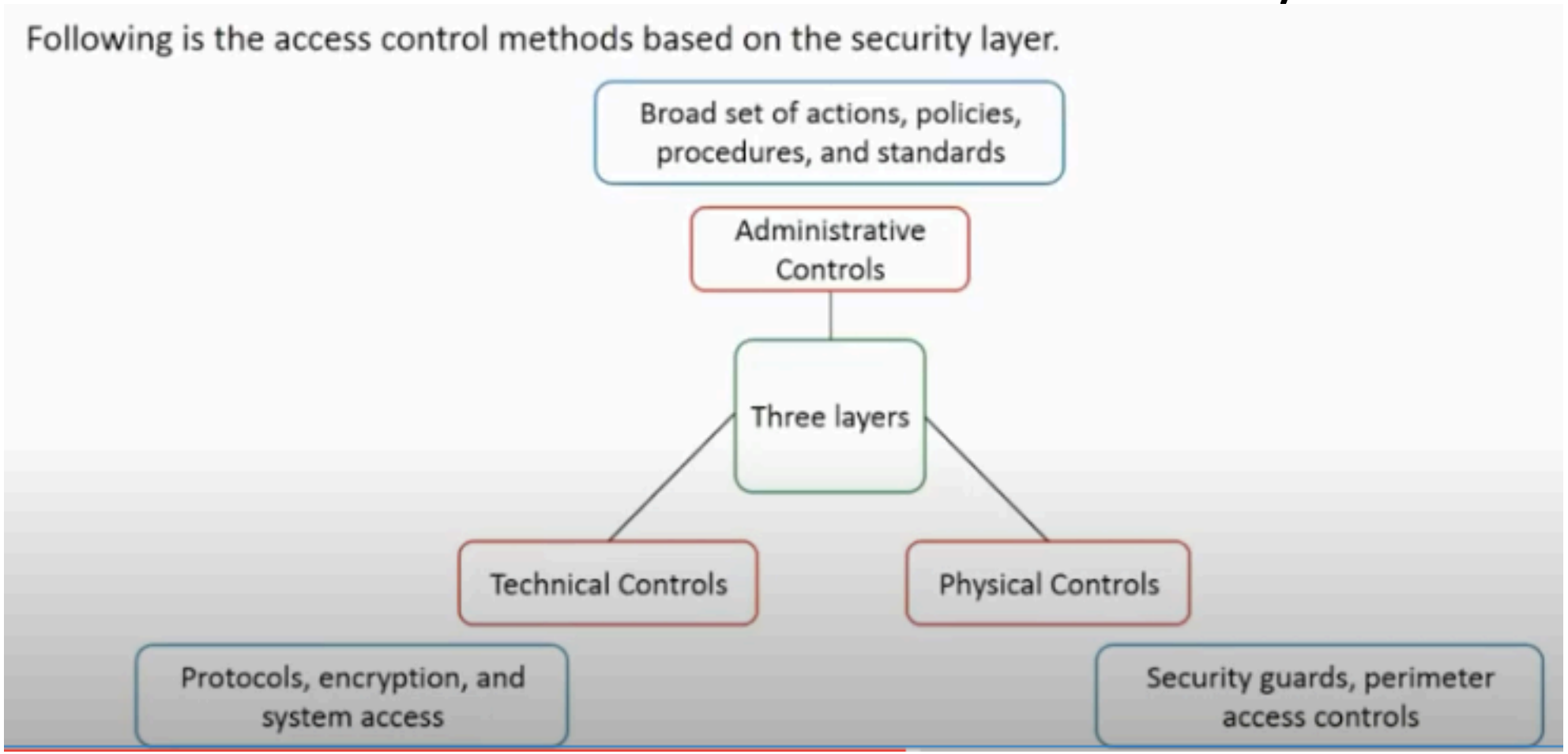
Pros	Cons
For all enterprise systems and applications the user has one password	Difficult to implement
Only one strong password needs to be remembered and used	Centralized point of failure
The user accounts can be easily created on hiring, modified, and deleted on dismissal	Compromise of data

Identity Management – SSO Examples

Some examples of SSO technologies are listed below.

Kerberos	Kerberos authentication protocol uses key distribution center, tokens or tickets, and symmetric key cryptography.
SESAME	Secure European System for Applications in a Multivendor Environment (SESAME) authentication protocol uses symmetric and asymmetric cryptography.
Security Domain	All the resources working under the same security policy are managed by the same group.
Domain Service	It is a network service which identifies resources such as printers and file servers on a network, and makes them available to users and programs.
Dumb Terminal	Thin Clients or Dumb Terminal's access control, processing, and storage depends on a central server.
Script-based Single Sign-on	Organization can implement its SSO solution by developing a script.

Access Control Methods – 3 layers



Access Control Methods based on functionality

Following is the access control methods based on the functionality:

- Preventive: Avoid problems before they occur
- Detective: Detect a problem that has occurred
- Corrective: Correct the problem that has occurred
- Deterrent: Discourages someone from doing an act
- Recovery: Restore a resource from an event that has occurred
- Compensative: Provides alternative controls to other controls

Access Control Model

Access Control Model (ACM) are used for defining the access control mechanism and policy definition for any access to be defined.

Models

DAC (Discretionary Access Control)- Restrictive model as set by data owners

Subject has total control over objects which is determined by Data owner

MAC – (Mandatory Access Control) Most Restrictive Access Control Model – which is controlled by Operating system

End-User cannot set controls

RBAC (Role Based Access Control) - based on a user's role and implements key security principles

Assigns permissions to particular roles in the organization and then users are assigned to roles

ABAC (Attribute Based Access Control)

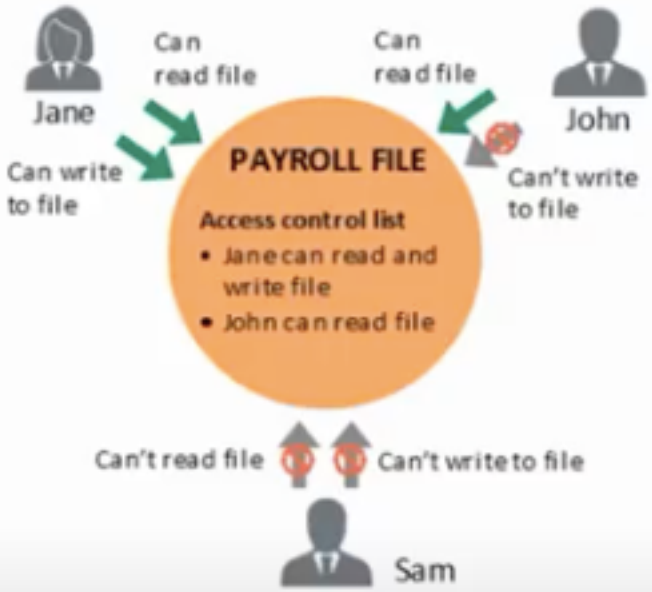
Dynamically assign roles to subjects based on a set of rules defined by a custodian / owner

Access Control Model- DAC (Discretionary)

The way in which a subject will access an object is guided by access control model. A model must be chosen to fulfill the directives of the security policy.

DAC Model:

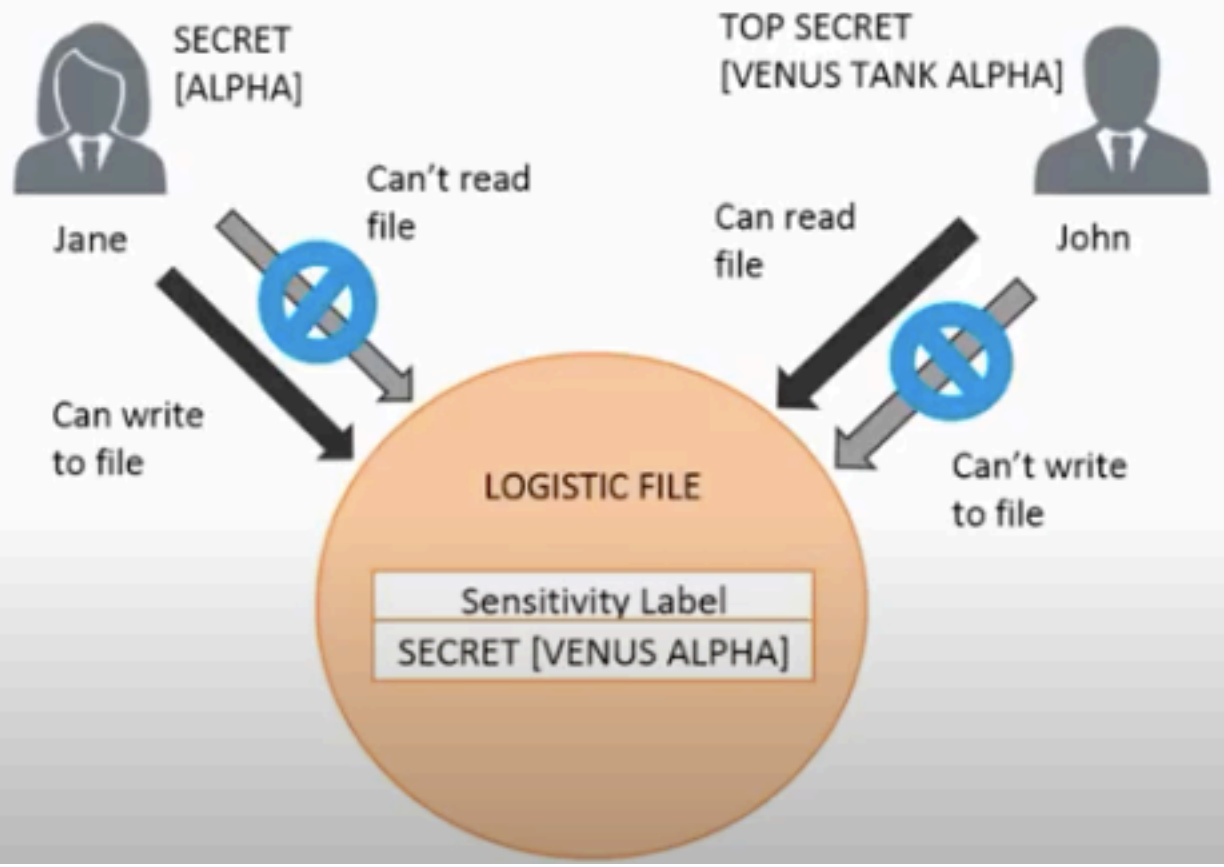
- Access to resources will be decided by data owners
- The access control depends on the owner's discretion and authorization granted to the users
- For enforcing the security policy, Access Control Lists (ACLs) are used



Access Control Model- MAC (Mandatory)

MAC Model:

- System's security policy is enforced by the operating system with the use of security labels
- The resources have security labels that contain data classifications and the users have security clearances
- When information classification and confidentiality is important, this model is used



Access Control Model- RBAC (Role Based)

A Role-Based Access Control (RBAC) model is also known as Non-discretionary Access Control.

Access is granted depending on subject's role and/or designation.

Following are the four commonly used RBAC architectures:

- Non-RBAC
- Limited RBAC
- Hybrid RBAC
- Full RBAC

Access Control Model- ABAC (Attributes Based)

The following factors support different Access Control Models.

- **Rules for Access:** Rules decides how the subject can access the object
- **Constrained User Interface:** Constrained user interfaces restrict users' access to a system of application by disallowing them to view or use certain information or functions
- **Access Control Matrix:** It has subjects and objects in a table and indicates the actions a specific subject can take on an object
- **Content:** Based on the content within an object the access is granted
- **Context:** Decisions are made by "reviewing the situation"

Types of Access Control Administration

There are two types of Access Control Administration:

Centralized Access Control Administration	Decentralized Access Control Administration
• Access to all the organization's resources is managed by a single entity (department or individual) • User's access privileges can be controlled in a uniform and consistent way • Example: The security administrator (entity) configures the mechanisms that enforce access control, processes any changes needed to a user's access control profile, disables access when necessary, and completely removes these rights when a user is terminated, leaves the company, or moves to a different position.	• Resource owners are responsible for access control • Access control for users is managed independently at each location as they know the user's need for the access to certain data, files, and resources better • Example: A computer system that has software and hardware controls for ensuring data integrity
Advantage—Strict control and access uniformity	Advantage—Flexible access control
Disadvantage—Can overload the central administration	Disadvantage—Controls may not be consistent throughout the organization

Accountability

Accountability helps in holding user responsible for their own action; verification of proper enforcement of security policies; and investigation. The following gives a broad overview of the items and actions that can be audited and logged:

System-level events

- System/computer performance
- Successful and unsuccessful log on attempts
- Log on attempt's timestamp

Application-level events

- Error messages
- File modifications

User-level events

- Identification and authentication attempts
- Commands used

Accountability

Non-repudiation plays an important role in accountability to ensure users, processes, and actions are responsible for impacts.

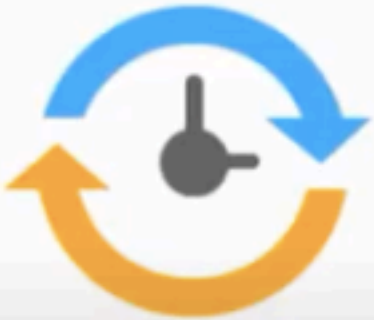
Following are the vital requirements to ensure accountability of actions :

Session Management

Session is the term used to describe a single entity communicating with another for a specified period of time. The way a single instance of identification, authentication, and authorization is applied to the entities is termed as 'Session Management.'

Control and protection of desktop sessions can be achieved through:

- Screensavers
- Session/Login limitation
- Timeouts
- Automatic Logouts
- Schedule Limitations



Emerging Trends – Federated ID

Federated ID management systems use the following models:

Cross-certification model:

- In this model, every organization must individually certify every other participating organization.
- Managing the trust relationships become difficult as the number of participating organizations increases.

Trusted third party or Bridge model:

- In this model, every organization subscribes to the standards and practices of a trusted third party, which manages the verification and due diligence process for all the participating organizations.
- After the verification by the third party, the participating organizations are considered trustworthy by all the other participants.
- For the participating organizations identity verification purposes, the third party acts as a trusted party or bridge between them.

Emerging Trends –ID as a Service (IDaaS)

Identity as a Service (IDaaS):

In this model, a third-party service provider builds, hosts, and manages an authentication infrastructure.

- IDaaS can be considered as Single Sign-On (SSO) for the cloud.
- The service is provided as third party management of identity and access control functions, including user life cycle management and Single Sign-On.
- An IDaaS is provided as a subscription-based managed service.
- A cloud service provider may provide subscribers through a secure portal, a role-based access to specific applications, and entire virtualized desktops.

Emerging Trends – SAML 2.0

Security Assertion Markup Language (SAML) 2.0:

It is a standard for exchanging authentication and authorization data between different security domains. It is an XML-based protocol that enables web-based authentication and authorization scenarios, which includes Single Sign-On (SSO).

The SAML specification defines three roles:

- the principal (typically a user)
- the identity provider (IdP)
- the service provider (SP)

Emerging Trends – OIULA

Once In-Unlimited Access:

This model is used where the organizations do not need to restrict resources in

- a very granular manner, or
- manage user access

An organization may employ a Once in-Unlimited Access (OIUA) model by having a separate area of their intranet that is available to all the employees without the need to identify or authenticate each individual application.

Access Control Threats

Common threats to access control are listed below.

- DoS/DDos
- Backdoor attacks
- Spoofing
- Man-in-the middle: Replay attack and TCP hijacking
- Social Engineering
- Dumpster Diving
- Password Guessing
- Brute-Force Attack
- Dictionary attack
- Trojan horse
- Phishing
- Pharming
- Software Exploitation

Access Control Protection Methods

Some of the common protection methods against the access control attacks are listed below.

- Physical security of system
- Controlling electronic access to password files
- Strong password policy
- Using multifactor authentication
- Last login notification
- Password file encryption
- Masking passwords
- Account lockout
- User awareness about security

Access Control - Best Practices

Some of the best practices include:

- Deny access to systems by undefined users or anonymous accounts.
- Limit and monitor the usage of administrator and other powerful accounts.
- Suspend/delay access capability after a specific number of unsuccessful logon attempts.
- Remove obsolete user accounts as soon as the user leaves the company.
- Suspend inactive accounts after 30 to 60 days.
- Enforce strict access criteria.
- Enforce the need-to-know and least-privilege practices.
- Disable unnecessary system features, services, and ports.
- Replace default password settings on accounts.
- Limit and monitor global access rules.

Access Control - Best Practices (contd.)

Some of the best practices include:

- Ensure logon IDs are non-descriptive of job function.
- Remove redundant resource rules from accounts and group memberships.
- Remove redundant IDs, accounts, and role-based accounts from resource access lists.
- Enforce password rotation.
- Enforce strong password requirements.
- Audit system, user events, actions, and review reports periodically.
- Protect audit logs.

Execution

- Access Control policies are defined for work around
- Team efforts succeed the process of access control
- Identification of whereabouts during mis-match of authentication and authorization benefits the organisation
- Audits provide periodic updates while re-defining based on technological advancements

Best Processes

- Separation of duties - not to give one-person total control
- Job rotation - individuals periodically moved between job responsibilities
- Least privilege - limiting access to information based on what is needed to perform a job function
- Implicit deny - if condition is not explicitly met, access request is rejected
- Mandatory vacations - limits fraud, because perpetrator must be present daily to hide fraudulent actions