CYBER SECURITY

USER AUTHENTICATION
&
ACCESS CONTROL

Identification

- In cyber security, identification is the process of declaring who you are, often by providing a username or other identifier.

Authentication

- Authentication in cybersecurity is the process of verifying the identity of a user, device, or system before granting access to resources or systems.

- Identification is the act of identifying a particular user, often through a username. Authentication is the proof of this user's identity, which is commonly managed by entering a password.

- Identification is the first step in most online transactions and requires a user to “identify” themselves, usually by providing a name, email address, phone number, or username. This is the process of someone saying that they are a certain person.
- The authentication process is a way for a user to prove that they are still the person they claimed to be during the identification phase.
- Authentication requires one of the following:

  Something a person knows: a password or security question

  Something a person has: a token, smartcard, ID card, or cryptographic key

  Something a person is: biometric data, such as a fingerprint or facial scan

- The safest authentication methods involve multi-factor authentication (MFA)opens in a new tab, which requires the use of more than one form of authentication.

Authentication Factors

Knowledge

Something only the user knows

- Passwords
- PIN
- Security questions
- ...

Possession

Something only the user has

- SMS OTP
- Magic links
- Security keys
- ...

Inherence

Something only the user is

- Fingerprint
- Face recognition
- Iris / retina scans
- ...

descope

Password security starts with creating a strong password. A strong password is:

- At least 12 characters long but 14 or more is better.
- A combination of uppercase letters, lowercase letters, numbers, and symbols.
- Not a word that can be found in a dictionary or the name of a person, character, product, or organization.
- Significantly different from your previous passwords.
- It should not contain your personal information.
- It should not contain your family information

Secure your passwords

- Don’t share a password with anyone. Not even a friend or family member.
- Never send a password by email, instant message, or any other means of communication that is not reliably secure.
- Use a unique password for each website
- Change password periodically.

Password Guessing

- Password Guessing is a type of cyberattack where an attacker tries to gain access to an account by manually or automatically trying different passwords—usually based on personal info or common passwords.
- A form of cyber intrusion, involve attackers systematically attempting various passwords to gain unauthorized access to systems. These attacks exploit weak or predictable passwords, making it crucial to understand and defend against them.

How It Works:

Personal Information (like name, birthdate, pet's name)

Common Passwords (like 123456, password, admin)

Automated Tools (to try thousands of passwords quickly)

Types of Password Guessing Attacks:

Brute-force attacks:

This involves trying all possible combinations of characters until the correct password is found.

Dictionary attacks:

Attackers use lists of common words, phrases, and password permutations to try and guess passwords.

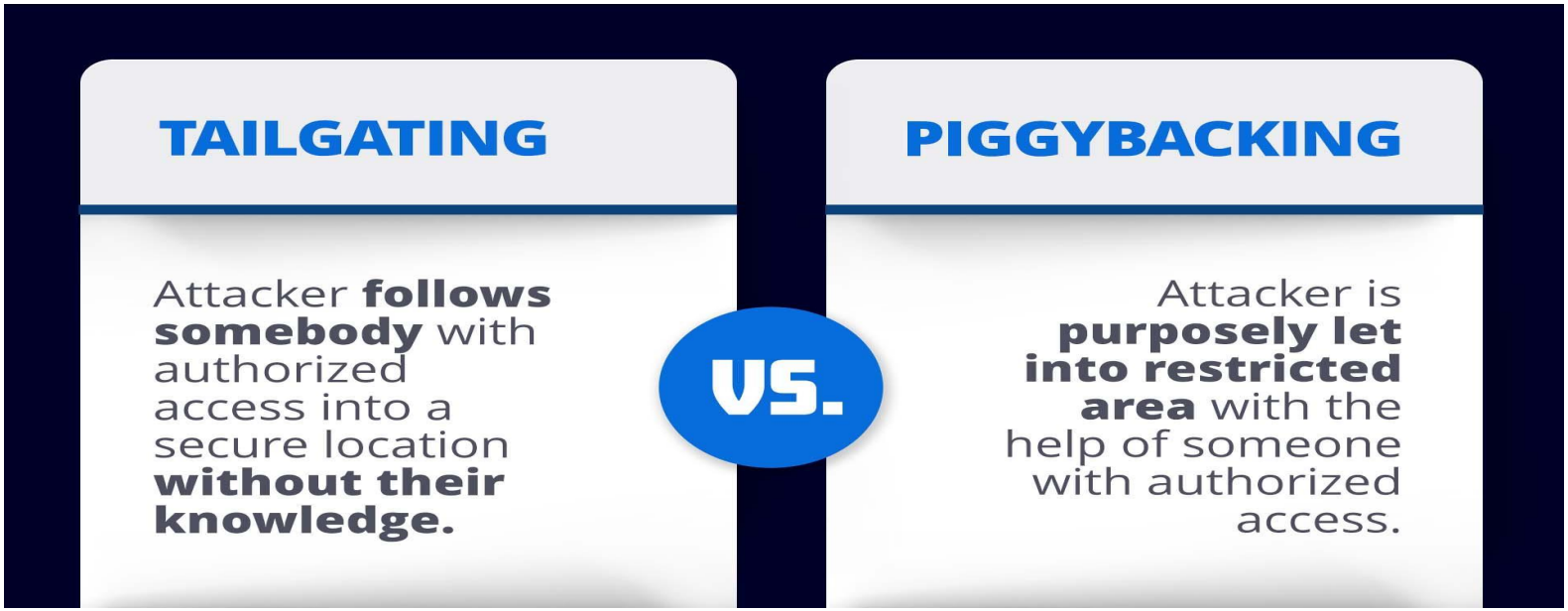
Hybrid Attack

Definition: Combines dictionary and brute-force by adding variations to dictionary words.

Password Attacks

- Piggybacking

Piggybacking in cybersecurity refers to a type of unauthorized access where someone follows an authorized person into a restricted area or system without permission. It's often a social engineering tactic used to bypass physical or digital security controls.




WHAT IS TAILGATING IN CYBER SECURITY?
it.networks

How Piggybacking Happens

- An attacker waits for an employee to enter a secure door and quickly slips in behind them.
- Someone uses a logged-in computer without proper permission.
- Exploiting unattended devices or unlocked terminals.
- Taking advantage of shared credentials or sessions.

How to Prevent Piggybacking

- **Physical Security:**
  - Enforce strict access control policies.
  - Use security badges and turnstiles.
  - Train employees to challenge unknown individuals.
  - Install surveillance cameras.
- **Digital Security:**
  - Require users to log off or lock their computers when away.
  - Use session timeouts.
  - Implement multi-factor authentication.
  - Monitor active sessions.

Shoulder surfing

- Shoulder surfing is a type of social engineering attack where an attacker watches over someone's shoulder (or in some cases, uses a camera or binoculars) to steal sensitive information such as passwords, PINs, or other personal data. This is a physical security threat, but can also extend to digital security if done remotely (e.g., through public webcams).

How Shoulder Surfing Happens

- **Public Spaces:**
  - An attacker looks over someone's shoulder while they're typing sensitive information in a public space (e.g., coffee shops, airports, or buses).
  - Common targets include PIN numbers at ATMs, passwords on login screens, and credit card information on online shopping sites.
- **Over-the-Shoulder Observation:**
  - The attacker may casually position themselves near a person working on their computer, smartphone, or tablet.
  - Can also happen in offices or places where people have private conversations in front of screens.
- **Use of Cameras or Devices:**
  - In some cases, the attacker might use a camera or smartphone to record what's on someone's screen.
  - A more sophisticated form of shoulder surfing, but still relies on the same principle.

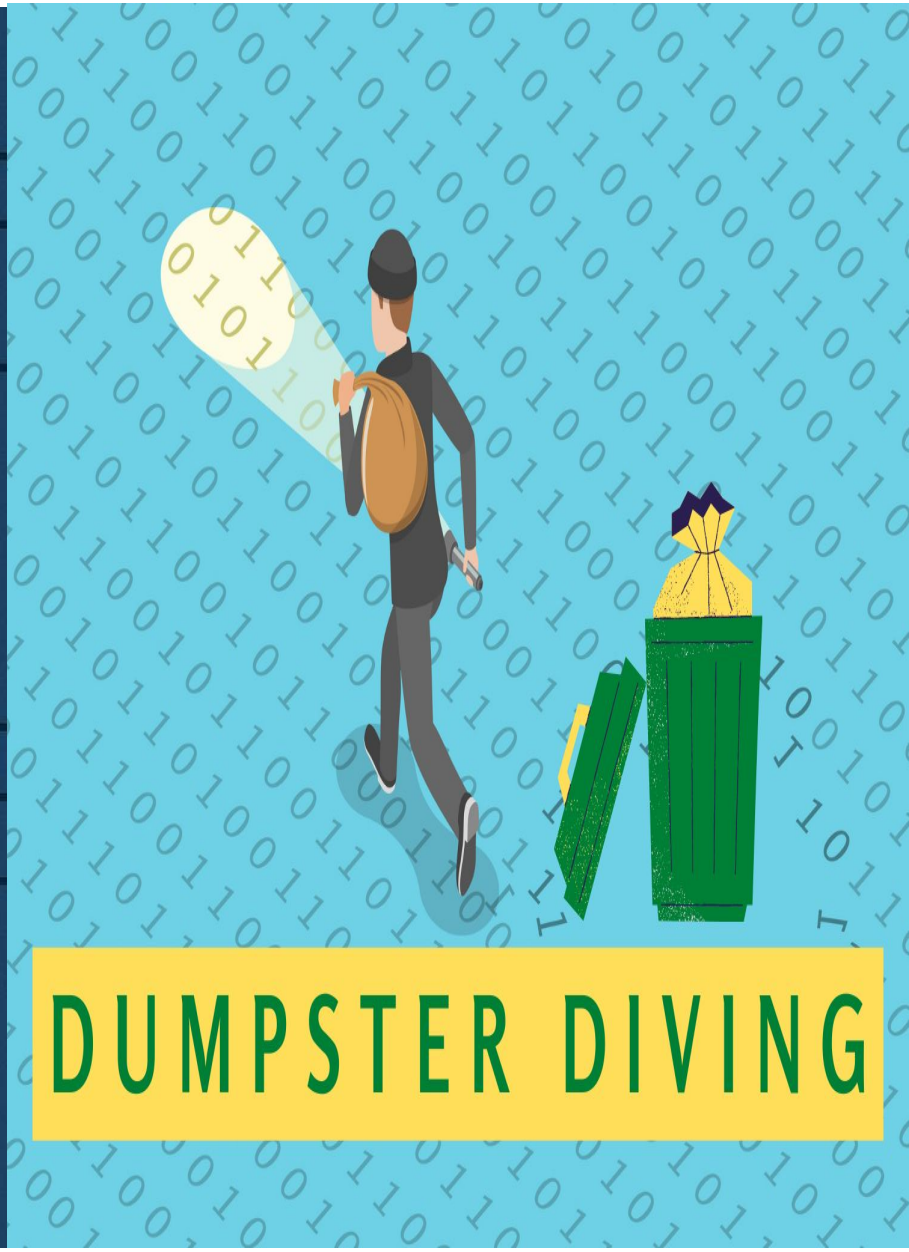
How to Protect Against Shoulder Surfing

- **Be Aware of Your Surroundings:**
  - Always be cautious about who's around when you're entering sensitive information.
  - Try to sit in places where you can limit the number of people who can easily see your screen.
- **Use Privacy Screens:**
  - Install a privacy screen filter on your phone, tablet, or laptop. It narrows the viewing angle of your screen so that only the person directly in front of it can see the display.
- **Shield Your Keypad:**
  - When typing in passwords, PINs, or other sensitive data, use your hand or body to shield the screen or keypad.
  - This is especially important in public areas like ATMs, payment kiosks, or during phone calls.
- **Turn Off Autocomplete/Auto-Fill:**
  - Disable features that automatically fill in passwords, credit card information, or addresses. This reduces the chances of an attacker using the data they might see.
- **Public Wi-Fi Caution:**
  - When using public Wi-Fi networks, ensure your device is encrypted, and avoid entering sensitive information unless you're using a VPN.
- **Secure Your Device:**
  - Lock your devices with strong authentication, and ensure that only authorized users can access them.

Dumpster diving

- Dumpster diving involves searching through trash, recycling bins, or discarded paper (e.g., in dumpsters or waste bins) to find items that may contain valuable information—whether it's personal, financial, or organizational.
- It’s not just limited to trash bins outside businesses or homes; it can include digital information like hard drives or storage devices that were improperly disposed of.


DUMPSTER DIVING


DUMPSTER DIVING

How Does Dumpster Diving Work?

Physical Search:

- Attackers may sift through paper documents or cardboard boxes looking for documents that contain private details.
- They may focus on documents from banks, insurance companies, government agencies, or companies.

Digital Dumpster Diving:

- Finding discarded computers, phones, or storage devices and retrieving data from them, even if it has been deleted.
- This can involve technical skills, such as recovering deleted files from hard drives, USBs, or CDs.

How to Protect Against Dumpster Diving

- **Shred Documents:**
  - Shred paper documents that contain sensitive information (e.g., old credit card statements, tax returns, or contracts) before discarding them. Use a cross-cut shredder for maximum security.
- **Destroy Old Devices:**
  - Wipe hard drives, USB sticks, or old smartphones before disposal to prevent data recovery.
  - Use software tools that overwrite data several times to make recovery impossible (e.g., DBAN or Eraser).
- **Use a Professional Document Disposal Service:**
  - For businesses or offices, consider using a professional shredding service to dispose of sensitive documents securely.
- **Be Mindful of Digital Trash:**
  - Don’t just delete files—erase them securely. Ensure that any device, disk, or storage media is wiped clean before throwing it away or recycling it.
- **Dispose of Electronic Devices Properly:**
  - When disposing of computers, phones, or old equipment, make sure the hard drives are physically destroyed or wiped using secure methods.
- **Secure Internal Documents:**
  - Implement internal policies to ensure that employees discard or destroy sensitive business data properly (e.g., using shredding bins for paper and encryption for digital files).

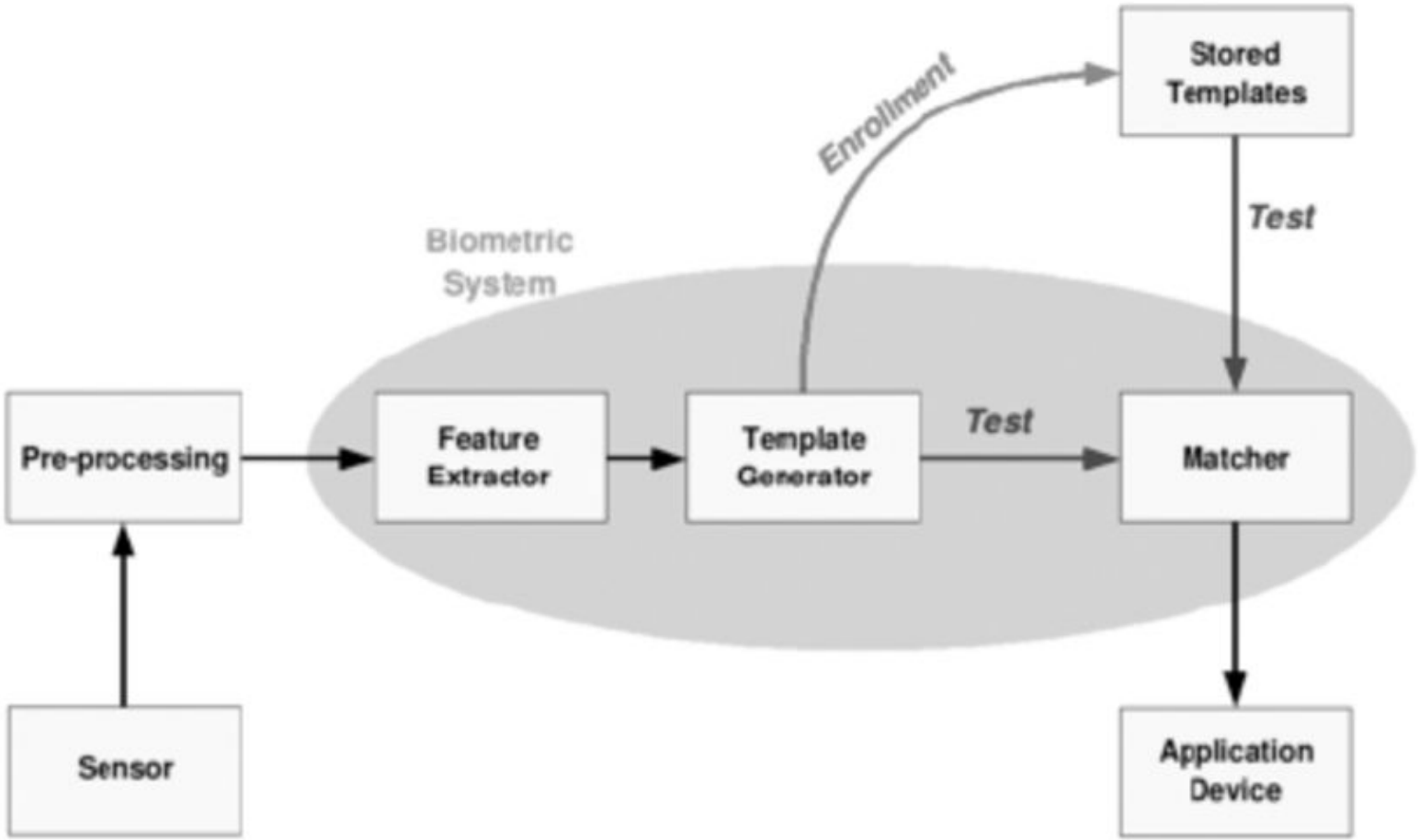
Biometrics

- Biometrics refers to the use of unique biological or behavioral characteristics to identify or authenticate individuals.

Phases of Biometric System

- **1. Enrollment phase:**
  In the enrollment phase, biometric information of the user or person is recorded in a database. It is a one-time process. Generally, in this phase, measurement of the appropriate information is done very precisely.
- **2. Recognition phase:**
  This is the second phase of the biometric system. This occurs when the detection part begins based on the first phase of the authentication of the user. This phase must be quick, accurate, and able to determine the authentication problem easily.

Block diagram of Biometric



Types of Biometric System

1. Physiological Biometrics

- Fingerprint Recognition :- Unique pattern of ridges and valleys on fingers. Most common and widely used.
- Facial Recognition:- Uses features like eyes, nose, jawline, etc., for identity verification.
- Iris or Retina Scanning:- Pattern of blood vessels in the eye's retina. Requires scanning with infrared light.
- Hand Geometry:- Measures size and shape of the hand and fingers. Less unique, used in access control.
- DNA Matching:- The most unique identifier, but expensive and slow for everyday use.
- Palm Vein Recognition:- Infrared scan of unique vein pattern inside the palm. Highly secure.

Behavioral Biometrics

- Voice Recognition :- Uses pitch, tone, accent, and speech rhythm to recognize a person.
- Keystroke Dynamics (typing rhythm):- How a person types — speed, rhythm, pressure, hold and release times of keys.
- Signature Recognition:- Measures how a person signs (speed, angle, pressure), not just the shape.
- Mouse Recognition:- The way someone moves, clicks, or drags a mouse (speed, curve, hesitation).
- Touchscreen Recognition:- How a person interacts with a touchscreen — pressure, speed, swipe angles.

PHYSIOLOGICAL BIOMETRICS

Fingerprint
The unique pattern on your finger is commonly used to unlock smartphones and authorise mobile payments.

Hand geometry
Your hand's shape and dimensions can be used for access control and clocking in-and-out at work

Finger vein pattern
Finger vein recognition looks for unique pattern of veins beneath the skin to combat fingerprint fraud

The eye
The eye's unique and complex characteristics are increasingly used for automated passport controls and national ID programmes

Face shape
Cameras are now able to analyse your face's shape and features to identify you

BEHAVIOURAL BIOMETRICS

Voice
The unique patterns in your voice can be analysed and compared to an example voiceprint to confirm your ID

Signature dynamics
You can be verified by the direction and pressure of your pen stroke, as well as the shape of your signature

Keystrokes
Biometric data can also come from the manner and rhythm in which you type on a keyboard

Gait
The way you walk has certain unique identifiers that suggest who you are based on age, height and weight

Gestures
Smartphones and laptops can use facial, smile and movement recognition to control and unlock your device

Access controls

- Access control is a security measure that regulates who or what can view or use resources in a system.

Types of Access Control Models

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

Discretionary Access Control (DAC)

Discretionary Access Control (DAC) is a security model where the owner of a resource (like a file or folder) decides who can access it and what actions they can perform

Key Characteristics of DAC

- **Decentralized Control:**
  Access control is managed by the resource owner, not a central authority.

- **Flexibility:**
  Owners can easily grant or revoke access as needed, making it adaptable to changing needs.

- **Ease of Use:**
  DAC is generally more intuitive and user-friendly than other access control models like Mandatory Access Control (MAC).

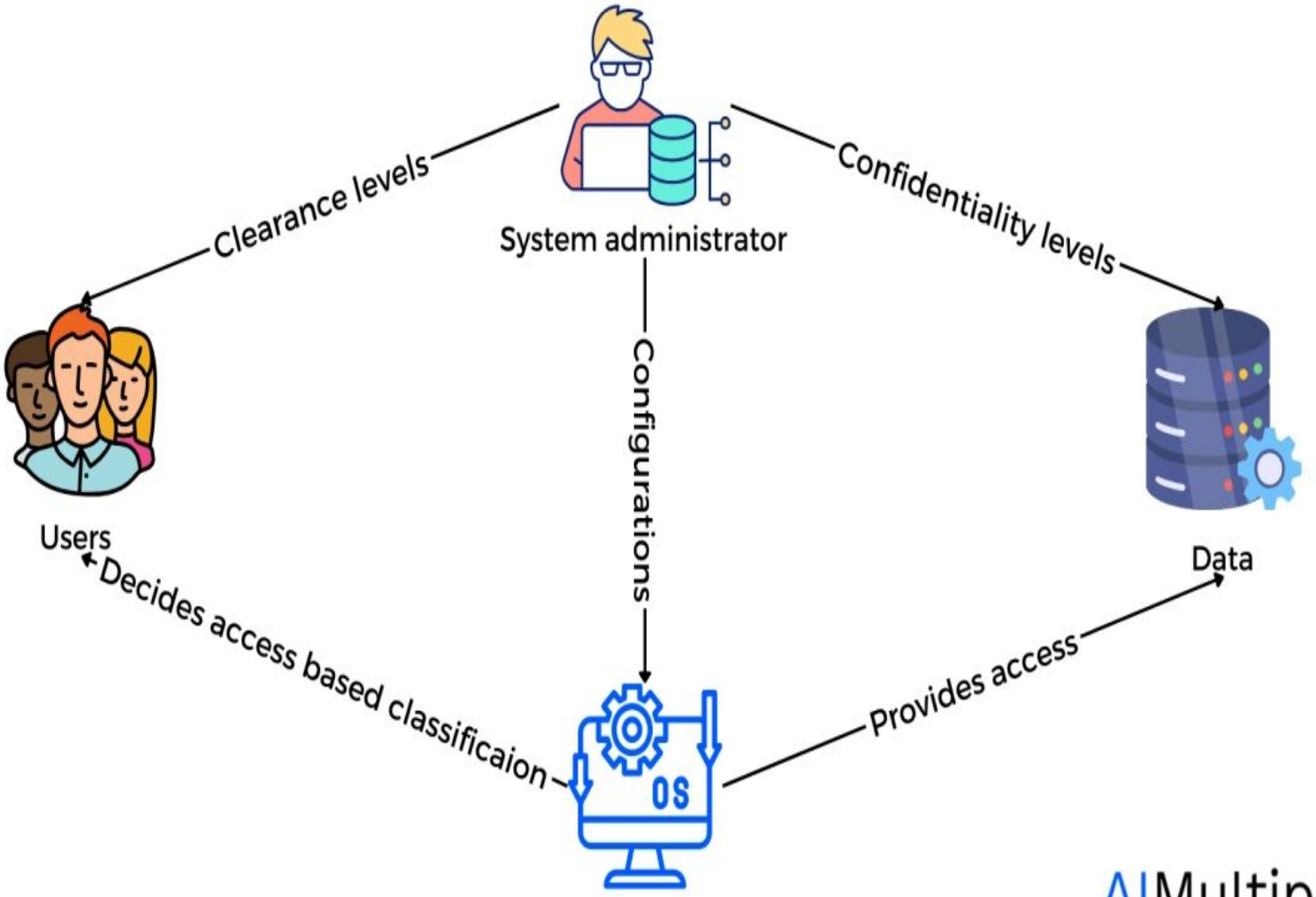
Examples of DAC

- File Permissions in Operating Systems:
- Sharing Documents in Google Docs:
- Smartphone App Permissions

Mandatory Access Control (MAC)

- Mandatory Access Control (MAC) is a cyber security mechanism that enforces strict, centralized control over access to resources.
- Access decisions are based on predefined security policies and user clearances, rather than the discretion of individual users or resource owners

Mandatory access control (MAC)



AIMultiple

Key Characteristics of MAC

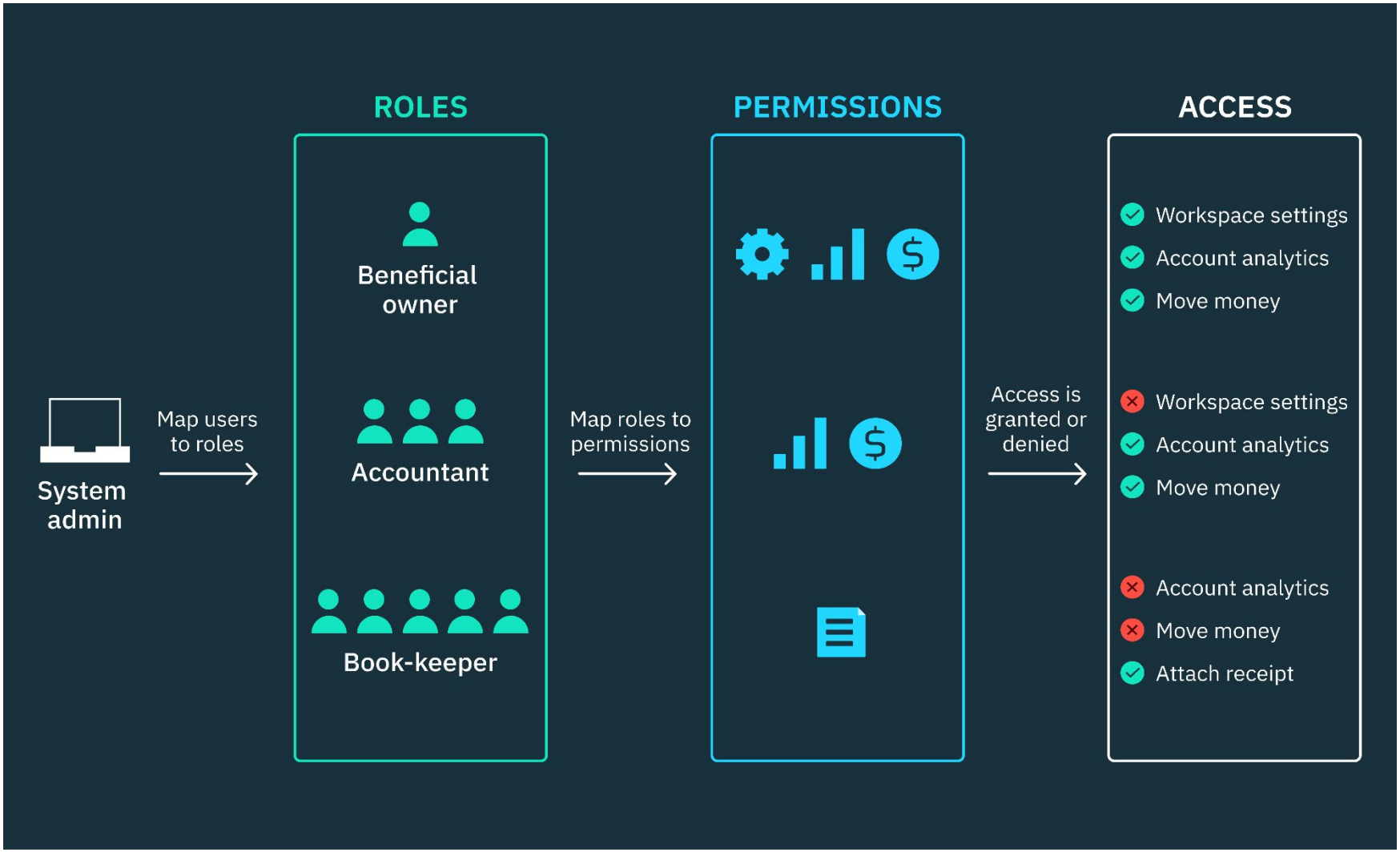
- **Centralized Control:**
  Access policies are defined and managed by a central authority, not individual users.
- **Security Labels:**
  Resources and users are assigned security labels (e.g., "Top Secret," "Confidential") and
  compartments (e.g., "Department M").
- **Clearance Levels:**
  Users have clearance levels that determine what security labels they are authorized to access.
- **Need-to-Know Basis:**
  Access is granted only if a user's clearance level matches or exceeds the resource's security level and if they belong to the appropriate compartment.
- **Non-Discretionary:**
  Access is not determined by the resource owner or user, but by the system's security policy.

Example

- Network Administrator
- Institute Principal

Role-Based Access Control (RBAC)

- Role-Based Access Control (RBAC) is a cybersecurity method that restricts system access based on a user's role within an organization, granting permissions based on job functions rather than individual identities
- This approach enhances security by limiting access to sensitive data and resources, minimizing the risk of breaches and data leakage.


ROLES
PERMISSIONS
ACCESS
System admin
Map users to roles
Beneficial owner
Accountant
Book-keeper
Map roles to permissions
Access is granted or denied
Workspace settings
Account analytics
Move money
Workspace settings
Account analytics
Move money
Account analytics
Move money
Attach receipt

Example

- Administrator
- Student

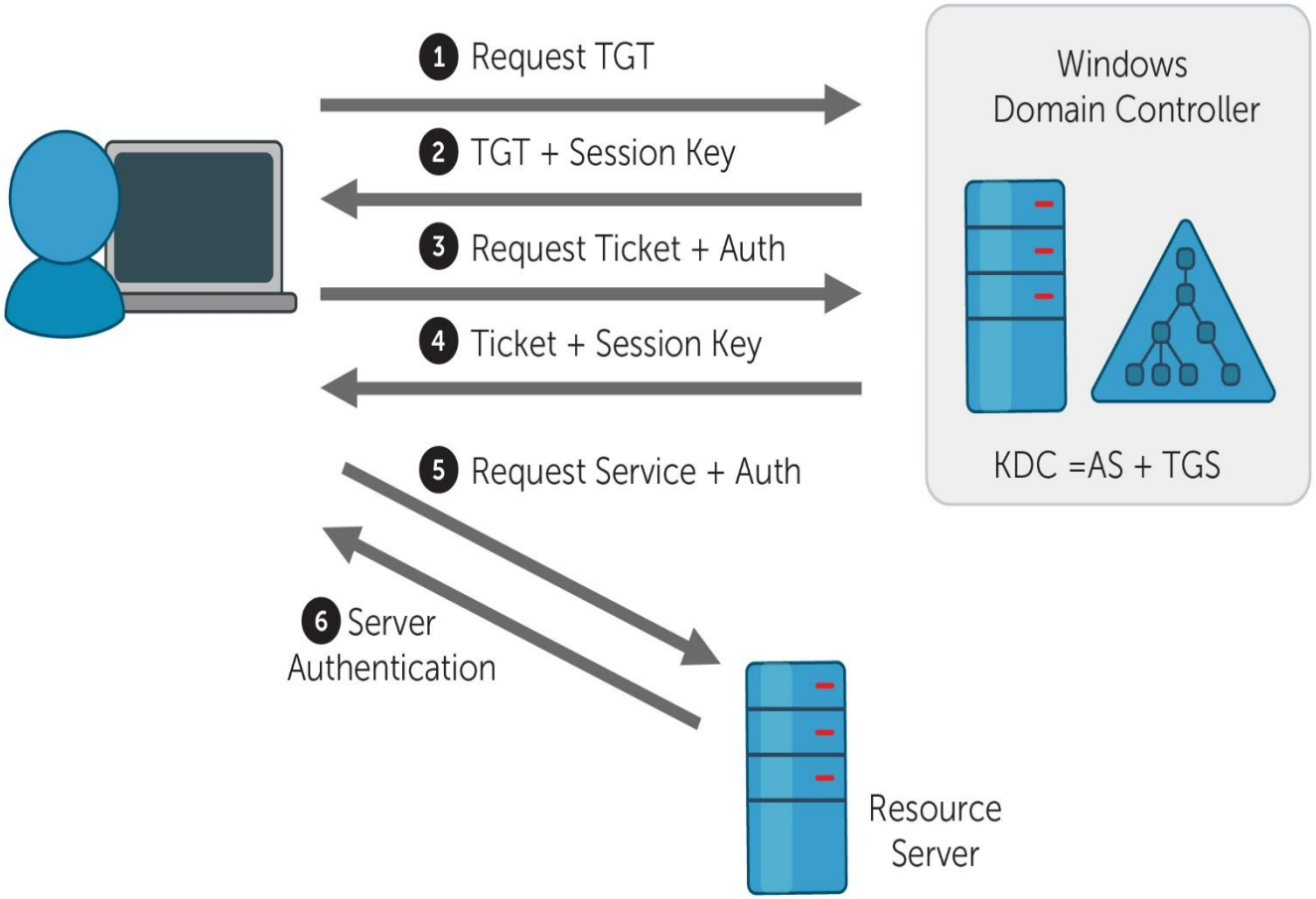
Feature	Discretionary Access Control (DAC)	Mandatory Access Control (MAC)	Role-Based Access Control (RBAC)
Control Authority	Resource owner (user) controls access	Central authority or system-enforced	Access based on roles assigned by an administrator
Flexibility	High — users can grant/revoke access	Low — users cannot change permissions	Medium — roles must be predefined but allow user grouping
Security Level	Lower — users can make mistakes	Very high — strict policy enforcement	High — if roles are well-designed
Ease of Management	Simple for small environments	Complex — needs classification and policy setup	Scalable — efficient in large organizations
User Involvement	Users control access to their own data	Users have no control over access	Users are assigned roles; cannot manage permissions directly
Best For	Small systems, personal use	Government, military, high-security environments	Corporate or enterprise systems
Permission Assignment	Individually to users	Based on security labels and clearance levels	Based on job roles and responsibilities
Example	File sharing on personal computers	Classified government documents	Hospital: Doctors, nurses, and admins have different roles
Risk of Misuse	Higher — users might grant access wrongly	Very low — strict access rules	Moderate — depends on role design
Policy Changes	Handled by users individually	Handled by central authority	Handled by admin through role updates

Authentication Protocol: Kerberos

- Kerberos is a computer network authentication protocol that allows secure communication between users and services on a network by verifying identities using tickets

The main components of Kerberos are:

- **Authentication Server (AS):** The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.
- **Database:** The Authentication Server verifies the access rights of users in the database.
- **Ticket Granting Server (TGS):** The Ticket Granting Server issues the ticket for the Server


1 Request TGT
2 TGT + Session Key
3 Request Ticket + Auth
4 Ticket + Session Key
5 Request Service + Auth
6 Server Authentication
Windows Domain Controller
KDC =AS + TGS
Resource Server

Working of Kerberos

Step-1: User login and request services on the host. Thus user requests for ticket-granting service.
Step-2: Authentication Server verifies user's access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using the Password of the user.
Step-3: The decryption of the message is done using the password then send the ticket to Ticket Granting Server. The Ticket contains authenticators like user names and network addresses.
Step-4: Ticket Granting Server decrypts the ticket sent by User and authenticator verifies the request then creates the ticket for requesting services from the Server.
Step-5: The user sends the Ticket and Authenticator to the Server.
Step-6: The server verifies the Ticket and authenticators then generate access to the service. After this User can access the services.