Department of
Software Engineering
BAHRIA UNIVERSITY
Discovering Knowledge

BAHRIA UNIVERSITY
Discovering Knowledge

Access Control

Information Security (CSC-407)

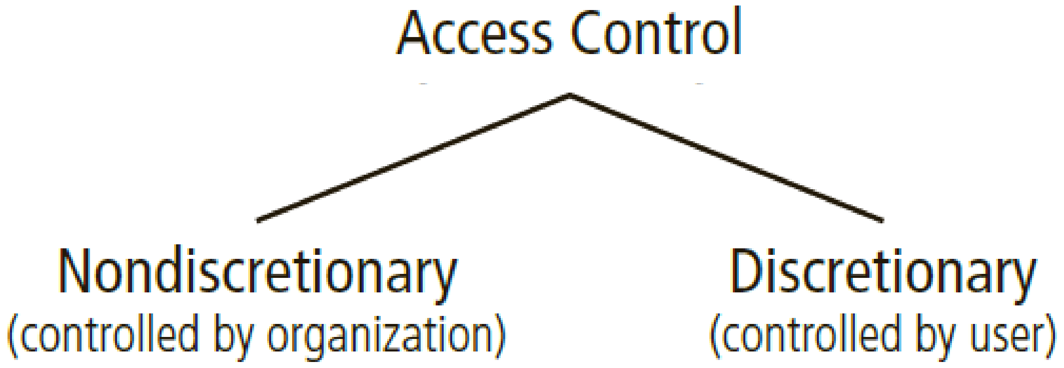
Fall 2024 (BSE-7A & 7B)

Introduction

- Technology based **controlling** is essential to a well-planned **information security program**, especially in many IT functions that are not **under direct human control**.
- E.g. ***network and computer systems*** make ***"millions of decisions every second"***, and operate in ways and at speeds that people cannot control in real time.
- ***Note:*** expertise on configuration / maintenance of technology-based control require **specialized training**.

Access Control Approaches

- **Access control:** the methods by which systems specify **who** may use a particular resource and **how** they may use it.
- Access control is achieved through a combination of ***policies*** and ***technologies***.



Access Control

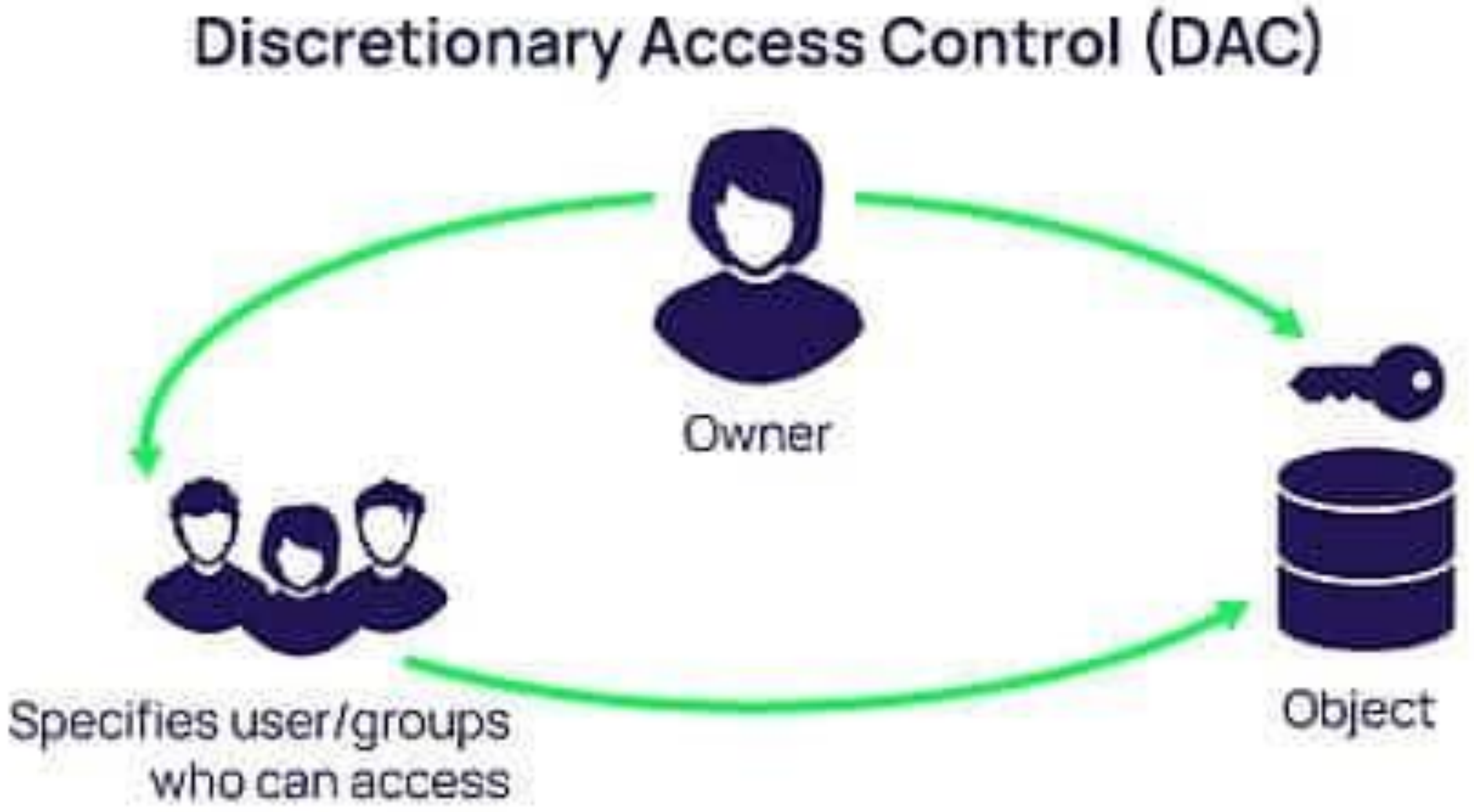
Nondiscretionary
(controlled by organization)

Discretionary
(controlled by user)

Discretionary Access Controls (DACs)

- Provide the ability to **share resources** in a **peer-to-peer** configuration that allows **users to control** and **provide access** to information or resources **at their disposal**.
- Users can allow ***unrestricted access*** or allow ***specific people*** or ***groups*** to access these resources.
- **E.g.**, user might have a hard drive that contains information to be shared with office coworkers.

Discretionary Access Controls (DACs)


Discretionary Access Control (DAC)
Owner
Object
Specifies user/groups who can access

Nondiscretionary Access Controls (NDACs)

- Managed by a ***central authority in the organization***.
- NDACs are tied to a person's position ***(role-based access controls)*** and responsibilities ***(task-based access controls)***.

a. ***Role-based access controls (RBACs)*** are associated with the user's position in an organization ***(e.g. project manager)***.

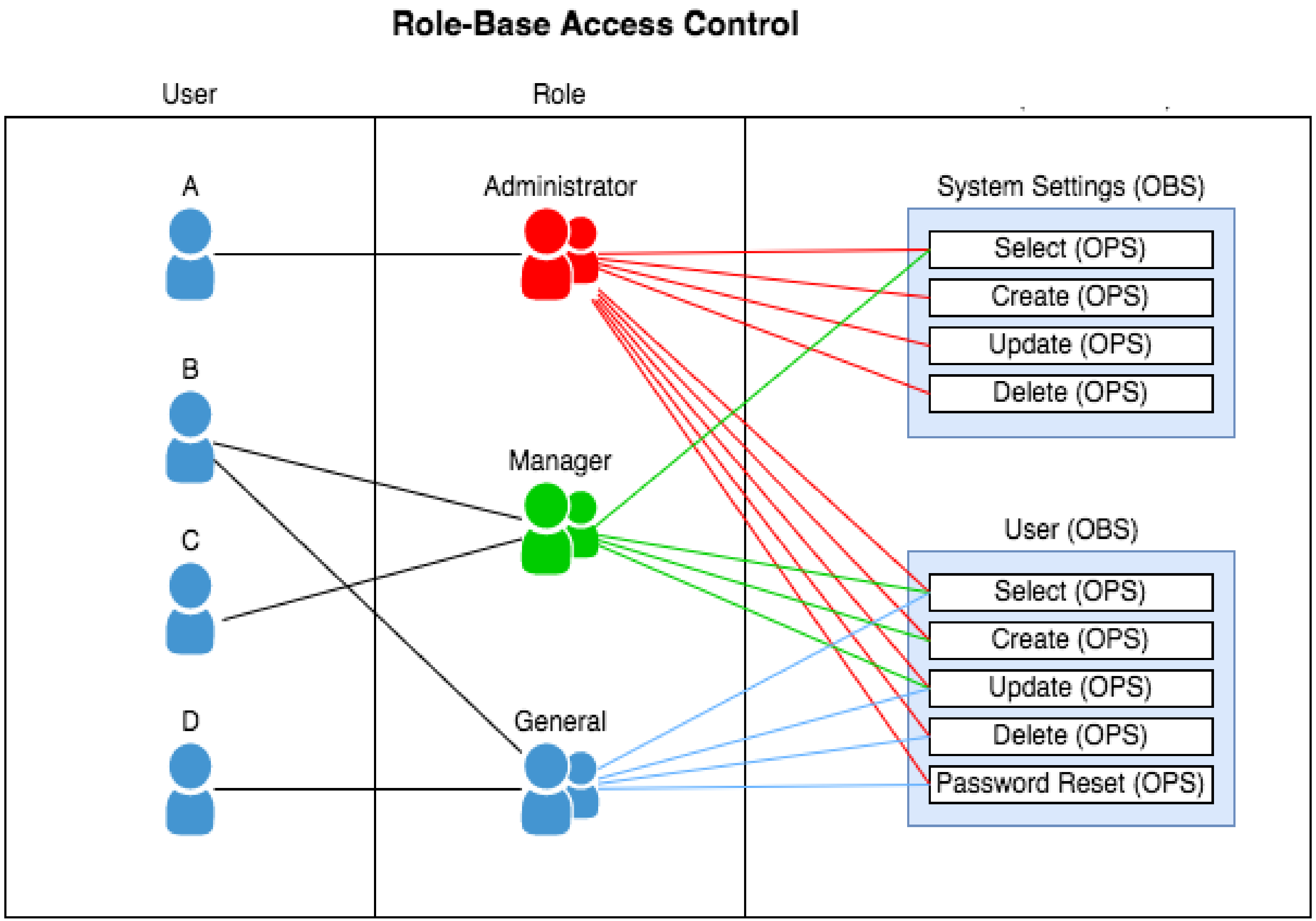
b. ***Task-based access controls (TBACs)*** are tied to a particular chore or responsibility, ***(e.g. a department's temporary printer administrator)***.

NDACs (Cont.)

- **RBACs** and **TBACs** make it easier to maintain restrictions associated with a particular **role** or **task**, especially if different people perform the same **role** or **task**.
- Instead of assigning and revoking privileges of employees *(who come and go)*, administrator assigns **access rights** to role or task.
- When users are associated with that role or task, they automatically receive the corresponding **access rights**.
- When users’ turns are over, they are removed from the role or task and access rights is revoked.

NDACs (Cont.)

- **RBACs** tend to last long, whereas **TBACs** are much more short.



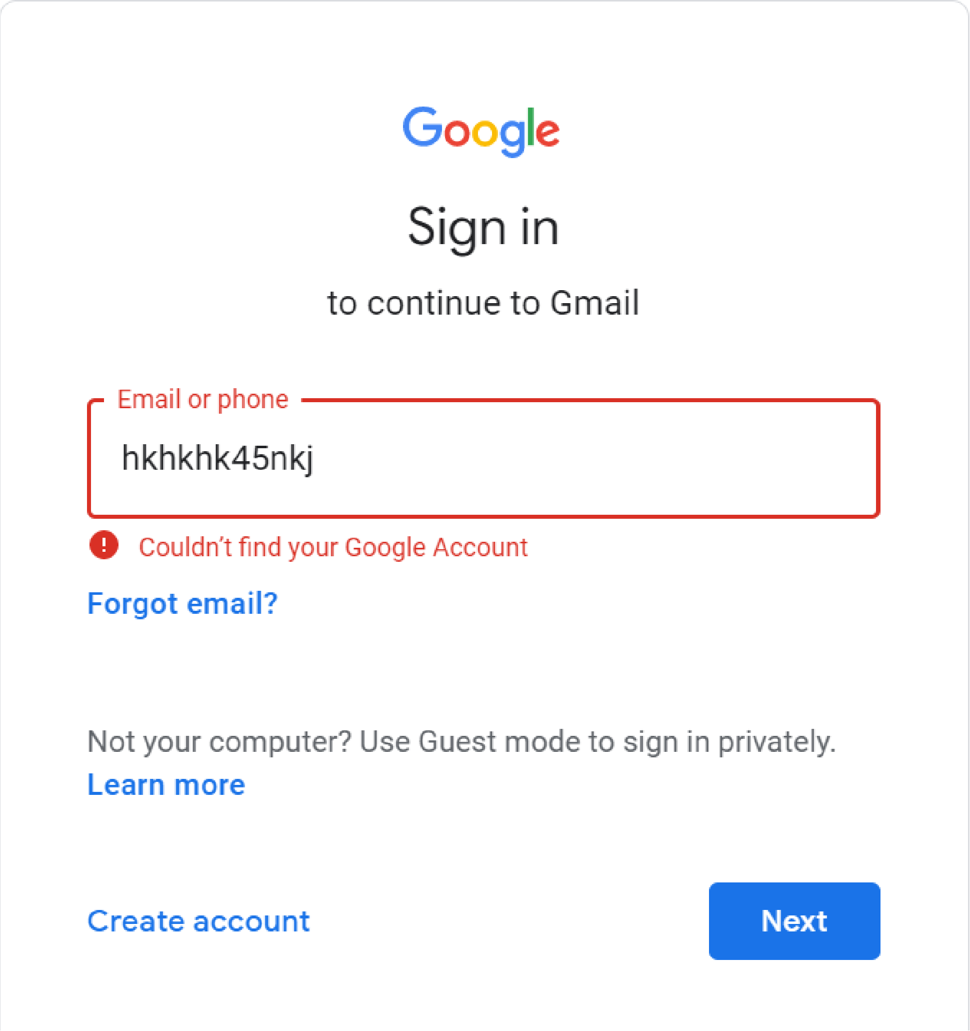
Access Control Mechanisms

- All access control rely on four mechanisms (*represent the four fundamental functions of access control systems*):
  - Identification: *I am a user of the system*.
  - Authentication: *I can prove I'm a user of the system*.
  - Authorization: *Here's what I can do with the system*.
  - Accountability: *You can track and monitor my use of system*.

Identification

- It is a label by which they are **“known to the system”**, usually called an **identifier (ID)**,
- The label must be mapped to only a **single entity** within the security domain.
- Some organizations use **composite identifiers**, such as concatenation of ***(department name, random numbers and special characters)***. While others generate **random IDs**.
- **Identification example,** username in login credentials & ATM card identifier.

Identification (Cont.)



Google

Sign in

to continue to Gmail

Email or phone

hkhkhk45nkj

Couldn’t find your Google Account

Forgot email?

Not your computer? Use Guest mode to sign in privately.
Learn more

Authentication

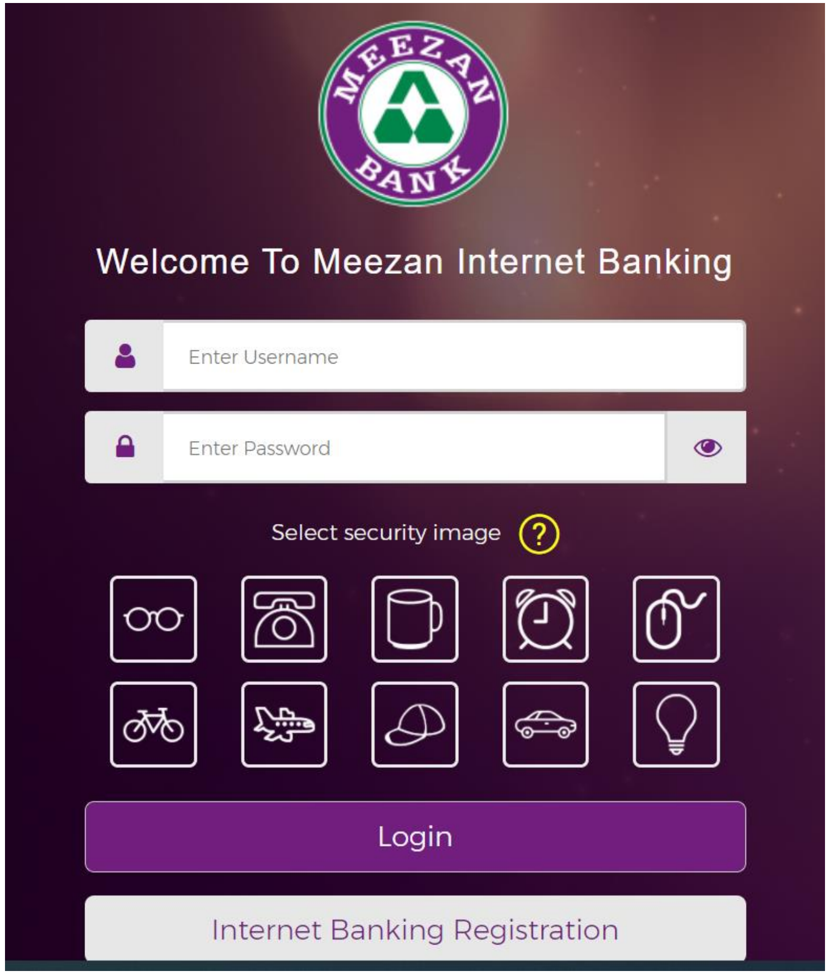
- It is the process of validating an entity's **claimed** identity, which includes ***password, PIN, tokens***.
- Password is a private word or combination of several characters that only the user should know.
- It is reported that the average user has **26 online accounts**, but uses only **5 different passwords**.
- Hence, password must be easy to remember, where it should be associated with something the a user can remember.
- One solution is use of automated ***password-tracking software***.

Authentication (Cont.)

- **ATM cards** with **magnetic stripes** that contain the digital user PIN *(often encrypted)*.
- A **token**, which is a computer-generated number used to support remote login authentication.
- Authentications relying on **individual characteristics**, such as **fingerprints, palm prints, hand geometry, retina scans** ***(collectively known as biometrics)***.

Strong Authentication

- Certain **critical areas** may require the use of **strong authentication** (i.e. ***at-least two authentication*** mechanisms drawn from two different factors of authentication).
- **E.g.** password and token combination in **Online Banking Login**.



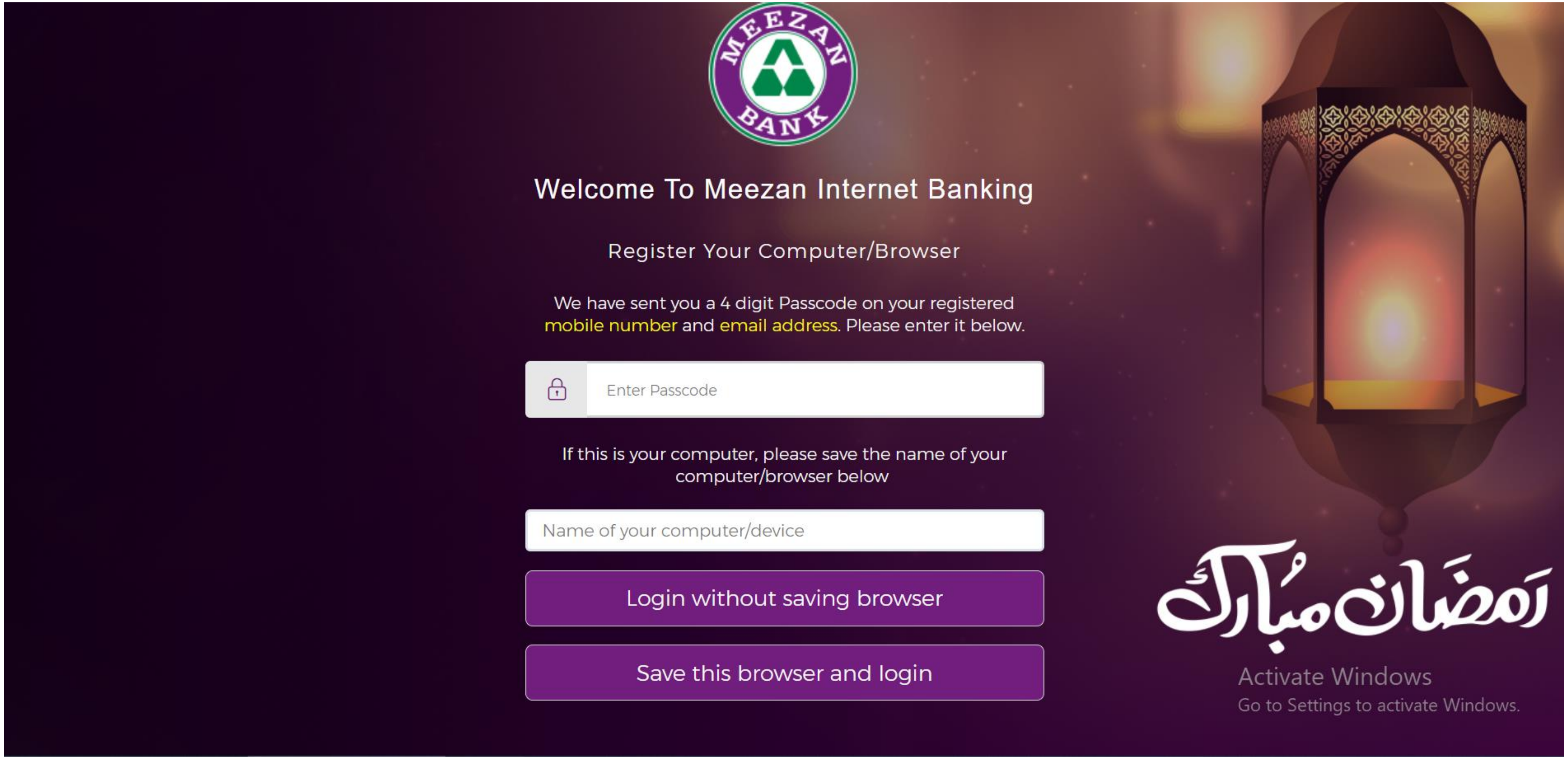
Welcome To Meezan Internet Banking

Enter Username

Enter Password

Select security image

Strong Authentication (Cont.)



Welcome To Meezan Internet Banking

Register Your Computer/Browser

We have sent you a 4 digit Passcode on your registered mobile number and email address. Please enter it below.

Enter Passcode

If this is your computer, please save the name of your computer/browser below

Name of your computer/device

MEEZAN BANK
Login without saving browser
Save this browser and login
رمضان مبارک
Activate Windows
Go to Settings to activate Windows.

Biometrics Authentication

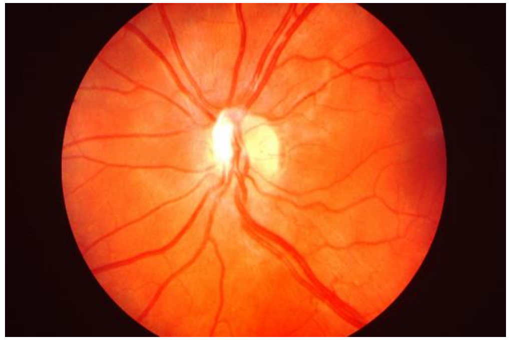
- **Biometric access control:** the use of ***physiological characteristics*** to provide authentication.
- Biometric means **“life measurement”** in Greek.
- Use of biometric-based authentication is expected to have a significant impact in the future.
- ***Technical*** and ***ethical*** issues are expected to be resolved with the biometric based technology.

Biometrics Authentication (Cont.)

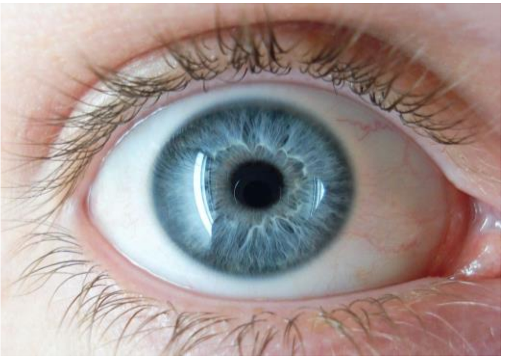
- Biometric authentication technologies include the following:
  - **Fingerprint** comparison of the person's **actual fingerprint** to a **stored fingerprint**.
  - **Palm print** comparison of person's **actual palm** print to a **stored palm** print.
  - **Hand geometry** comparison of person's **actual hand** to a **stored measurement**.
  - **Facial recognition** using a digital camera, in which **person's face** is compared to a **stored image**.

Biometrics Authentication (Cont.)

- Biometric authentication technologies (Cont.):
  - **Retinal print** comparison of the **person's actual retina** to a **stored retina image**.



  - **Iris** *(i.e. the colored part of your eye)* **pattern** comparison of the **person's actual iris** to a **stored iris image**.
  - Iris pattern is unique to you, and nobody else in the world has the exact same pattern.



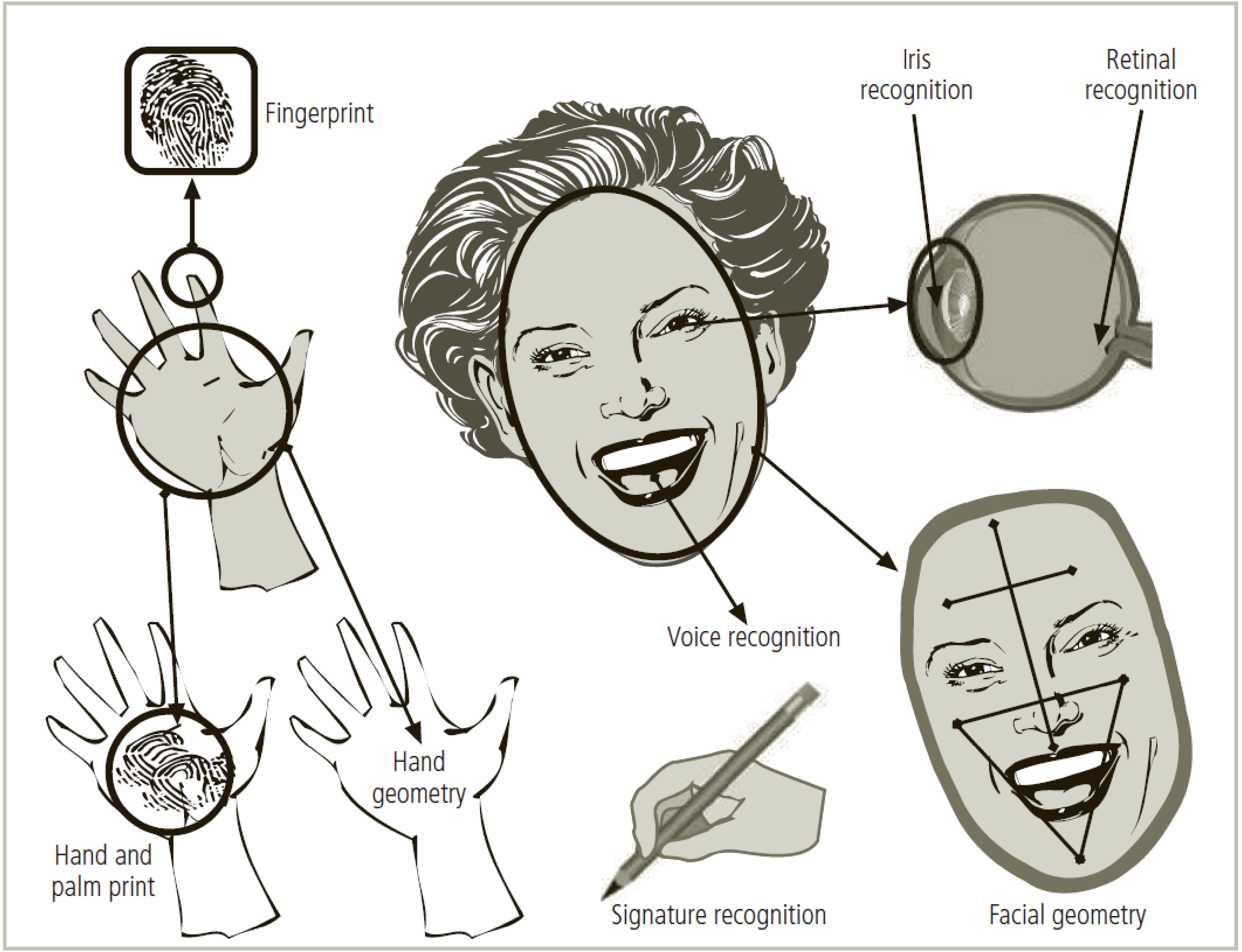
Biometrics Authentication (Cont.)

- Among all possible biometrics, **only three** human characteristics are usually considered **truly unique**:

  a. Fingerprints.

  b. Retina of eye ***(blood vessel pattern).***

  c. Iris of eye ***(random pattern of features found in iris, including freckles, pits, striations, vasculature, coronas and crypts)***.


Fingerprint
Iris recognition
Retinal recognition
Voice recognition
Hand and palm print
Hand geometry
Signature recognition
Facial geometry

Effectiveness of Biometrics

- Some human characteristics can change **over time** due to **normal development**, **injury** or **illness**.

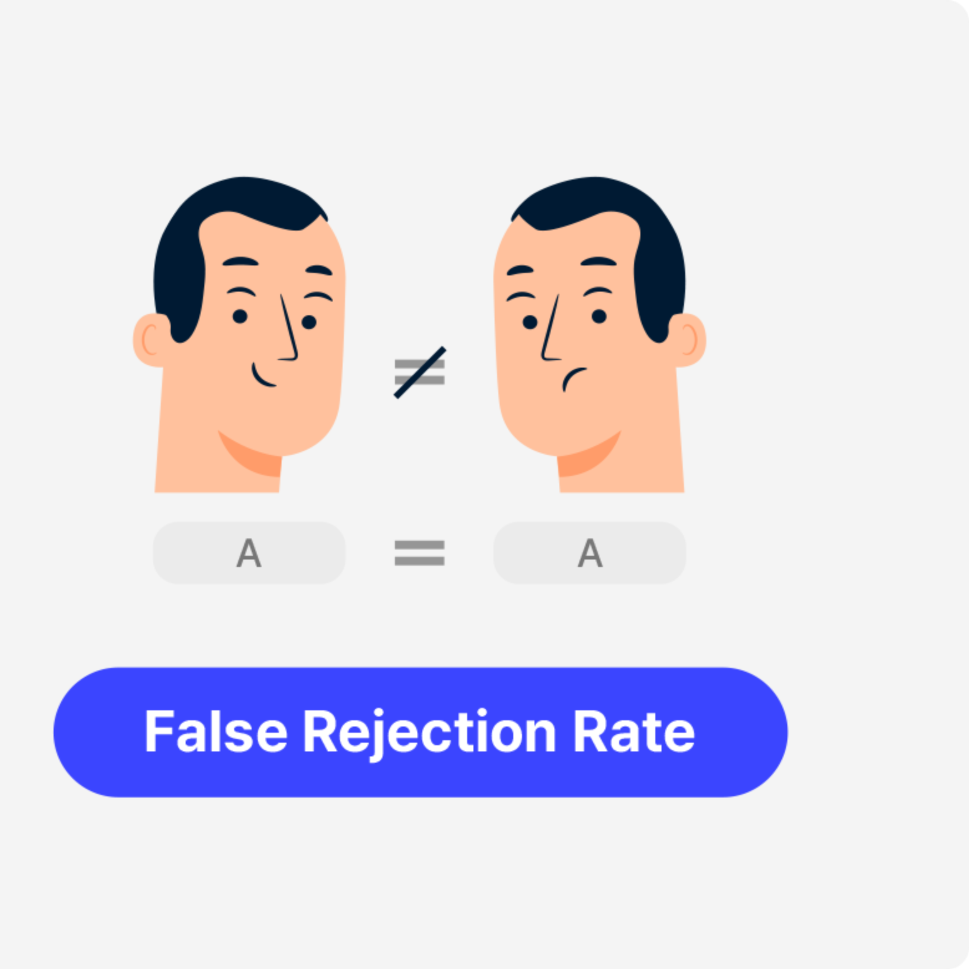
- Biometric technologies are evaluated on three basic criteria:
  - **False reject rate**
  - **False accept rate**
  - **Crossover error rate**

False Reject Rate

- **False Reject Rate (FRR):** percentage of **legitimate / authorized** users who are **denied access** because of a failure in the biometric device.
- Occurs when a biometric device is ***too sensitive*** and a ***valid user*** is not authenticated.
- This error rate is of **little concern** to security professionals since rejection of an authorized user represents **no threat to security**.

False Reject Rate (Cont.)

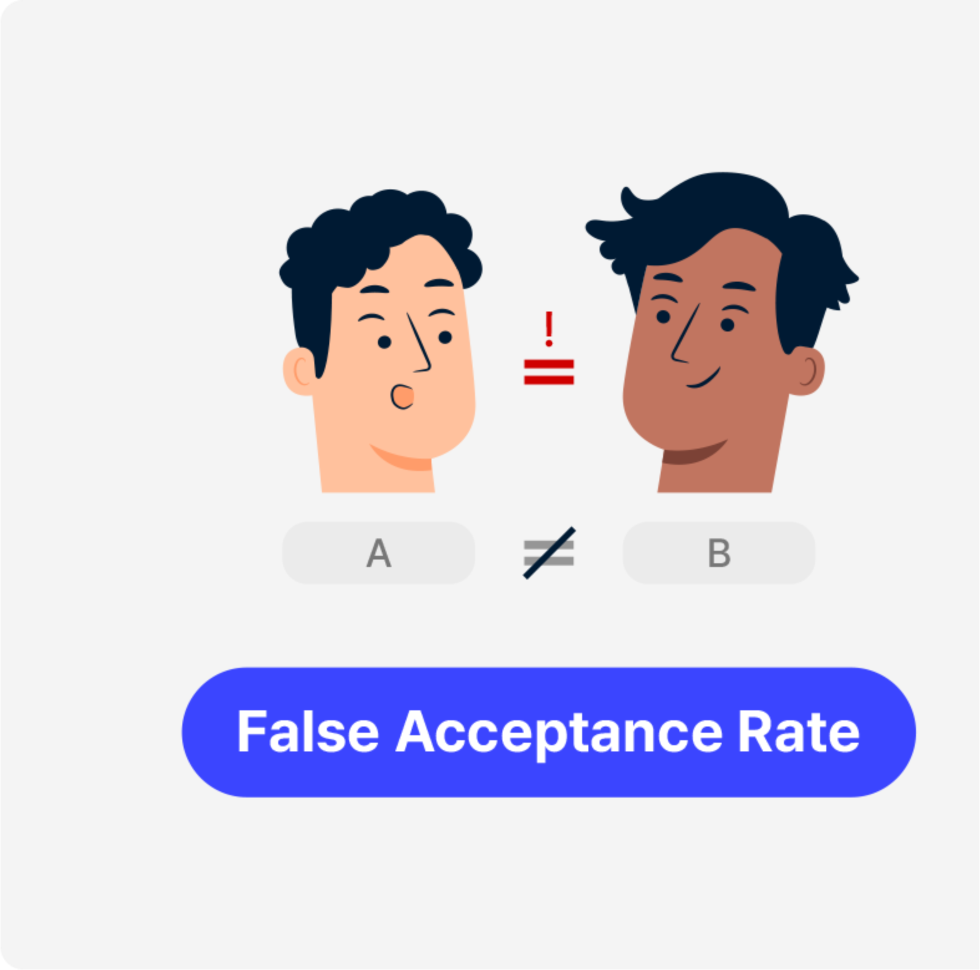
- False reject rate is *often ignored* unless it reaches a level high enough to generate *complaints* from unauthenticated people.



False Accept Rate

- **False Accept Rate (FAR):** percentage of **unauthorized users** who are **granted access** to a restricted system or area because of a failure in the biometric device.
- This failure is unacceptable to security professionals.
- Occurs when a biometric device is ***not sensitive enough*** and an ***invalid user*** is authenticated.

False Accept Rate (Cont.)

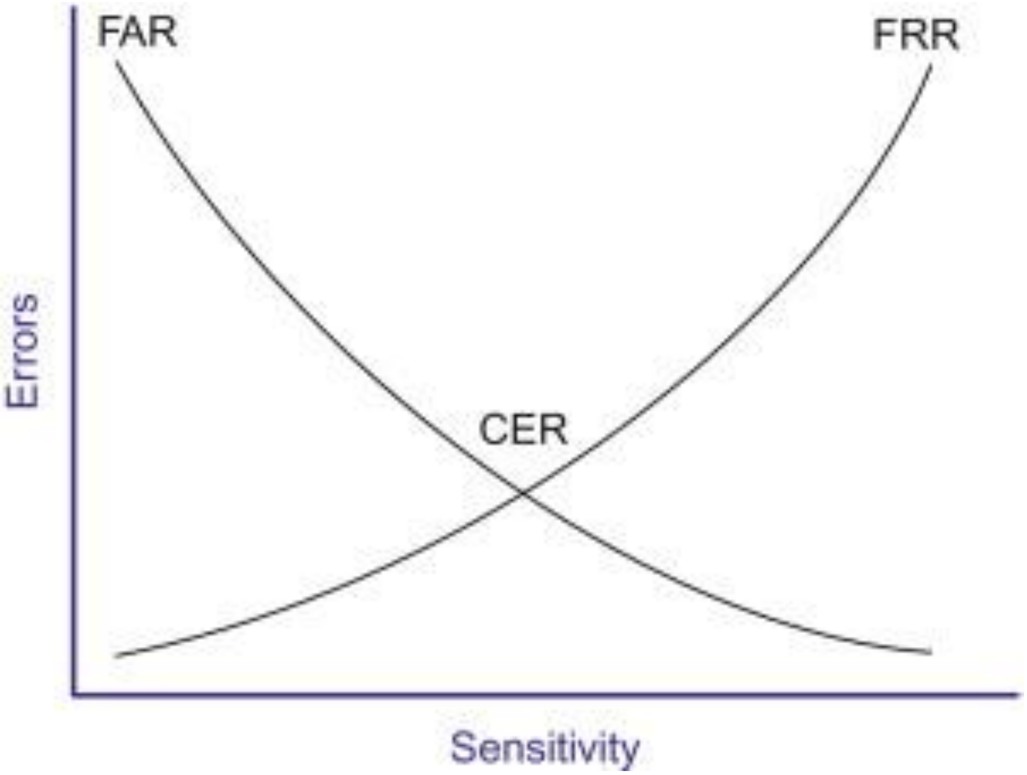


Crossover Error Rate

- **Crossover Error Rate (CER):** the level at which number of false rejections **equals** the false acceptances, identified by a point at which false reject and false accept rates **intersect**.
- Most biometric systems can be adjusted to compensate both for **FRR** and **FAR**.
- The trick is to find **balance** between the necessary level of security and minimizing the frustrations of authentic users.
- The optimal setting is somewhere near a point at which the two error rates are equal ***(i.e. CER)***.

Crossover Error Rate (Cont.)

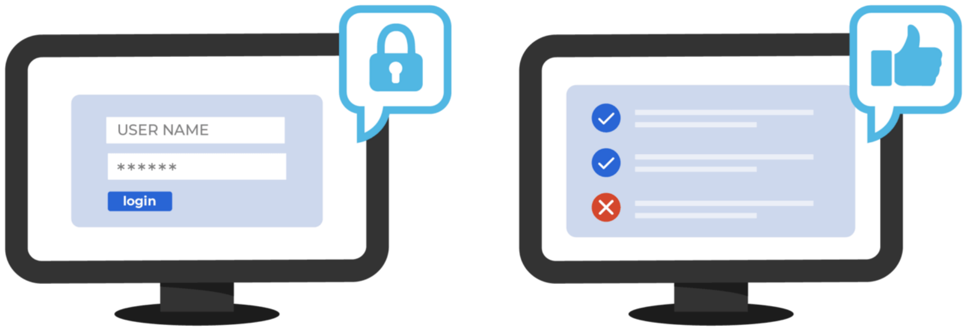
- CERs are used to compare various biometric solutions and ***may vary by manufacturer***.
- If a biometric device provides a CER of 1%, its **FRR** and **FAR** are both 1%.
- A device with a CER of 1% is considered superior to a device with a CER of 5%.



Authorization

- **Authorization:** the process of giving an **authenticated entity** permission to access a specific resource or function (i.e. list of **information assets** and **access levels**).
- Authorization generally works with authentication, where it is generally preceded by authentication.

Authentication **Authorization**



Confirms users are who they say they are.

Gives users permission to access a resource.

Authorization (Cont.)

- Authorization can be handled in one of three ways:

1. Authorization for **each authenticated user**, where system performs an authentication process to verify **each entity** and grants access to resources for only that entity.
2. Authorization for **members of a group**, where system matches authenticated entities to a list of **group memberships** and grants access based on group's **access rights**.
3. Authorization **across multiple systems**, where a **central** authentication and authorization system verifies an entity's and grants it credentials across multiple systems.

Accountability

- Also known as **auditability**, which ensures that all actions on a system ***(i.e. authorized or unauthorized)*** can be tracked.
- Accountability is most often accomplished by means of **system logs** and **auditing** of records.
- Systems logs record specific information, such as **failed access attempts** and **systems modifications**.
- System logs have many uses such as, ***intrusion detection, determining root cause of system failure or tracking the use of a particular resource***.

Thank You!