سبر 1213

Network Defense

Lecture #2 Part 2

Understanding Identity and Access Management

Something You Are

- **Biometrics Methods**
  - Vein matching
  - Voice recognition
  - Facial recognition
  - Gait analysis

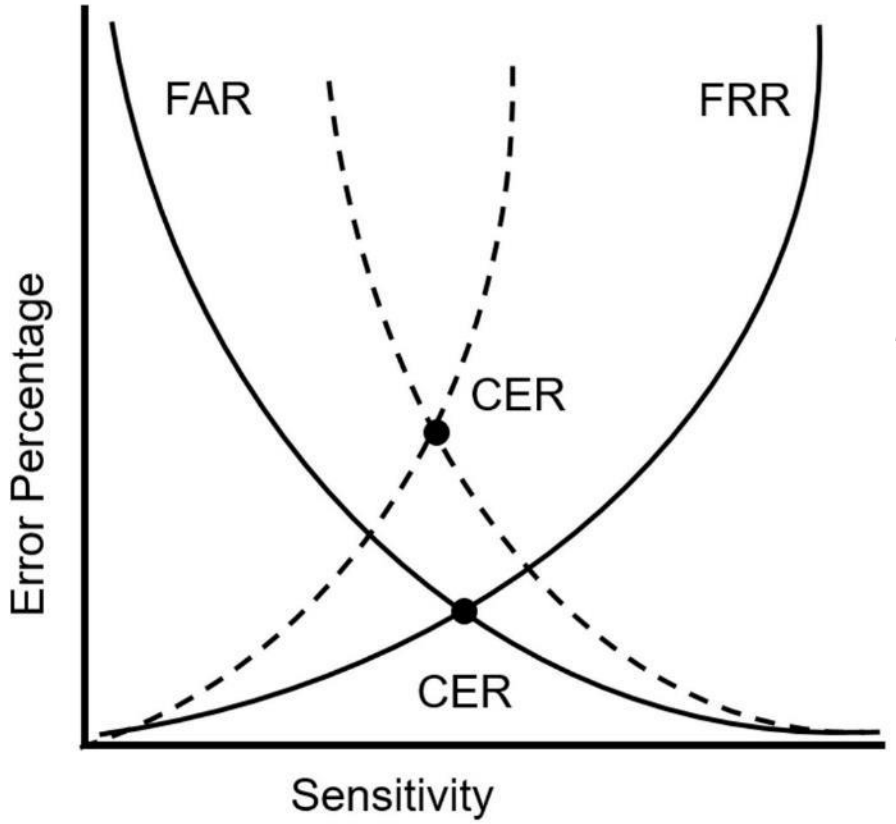
Biometrics

- **False acceptance**
- **False rejection**
- **True acceptance**
- **True rejection**

	Biometric System Not Accurate	Biometric System Accurate
Registered User	**False Acceptance**	True Acceptance
Unknown User	**False Rejection**	True Rejection

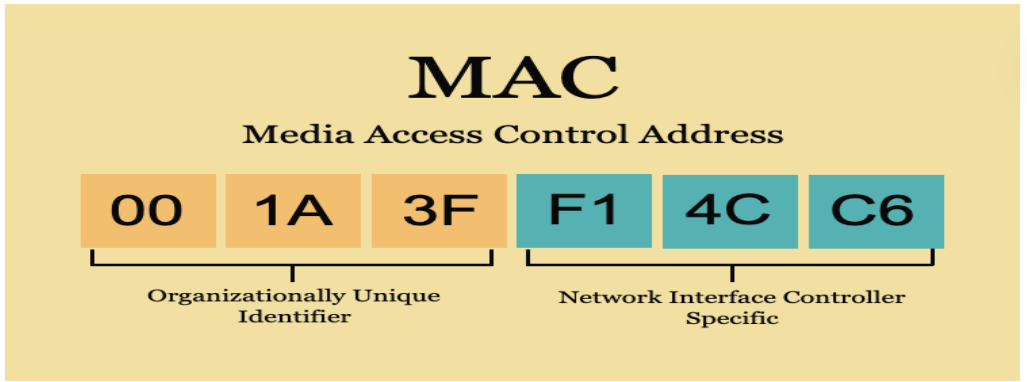
Biometrics

- **Crossover error rate**
  - False acceptance rate
  - False rejection rate
  - Lower CER indicates better accuracy



Somewhere You are

- **Often uses geolocation**
  - IP address
  - MAC address



Authentication Attributes

- Something You Exhibit
- Someone You Know

Two-factor/Multifactor Authentication

- **Multifactor authentication**
  - Combines authentication from two or more factors
- **Examples**:
  - PIN and CAC
  - PIV and password
  - Fingerprint and smart card

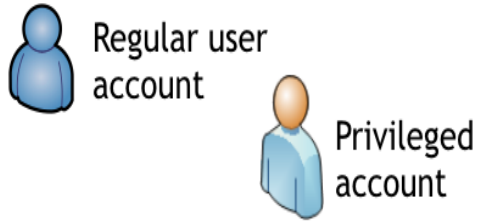
-

Managing Accounts

- **Credential Policies and Account Types**
  - Personnel or end-user accounts
  - Administrator and root accounts
  - Service accounts
  - Device accounts
  - Third-party accounts
  - Guest accounts
  - Shared and generic

Managing Accounts

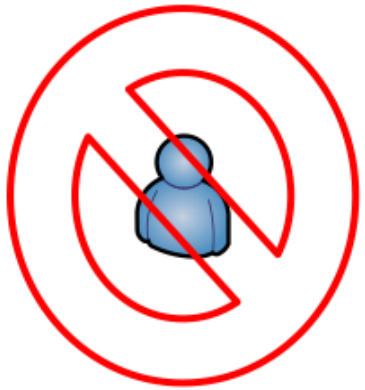
- **Privileged Access Management**
- **Using Two Accounts**



- **Prohibiting Shared and Generic Accounts**

Managing Accounts

- **Disablement Policies**
  - Terminated employee
  - Leave of absence
  - Delete account

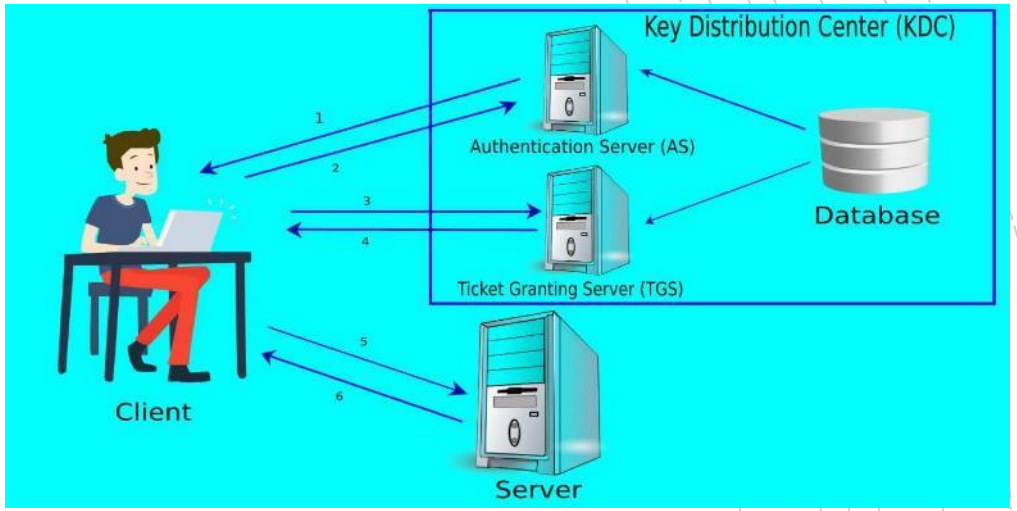


- **Time-Based Logins**

- **Account Audits**

Comparing Authentication Services

- Single Sign-On
- Kerberos
- SSO and a Federation



Comparing Authentication Services

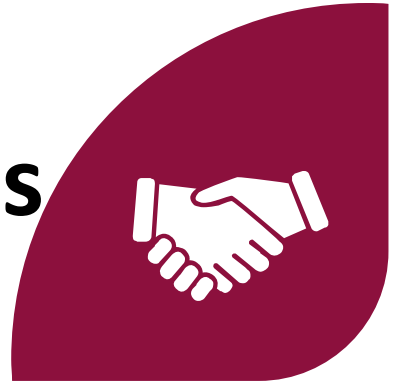
1 SAML

- Principle
- Identify provider
- Service provider
- Can also be used for authorization

2 SAML and Authorization

3 OAuth

4 OpenID and OpenID Connect



Comparing Access Control Models

- **Role-Based Access Control**
  - Uses roles (often implemented as groups)
  - Grant access by placing users into roles based on their assigned jobs, functions, or tasks
  - Often use a matrix

Role	Server Privileges	Project Privileges
Administrators	All	All
Executives	None	All
Project Managers	None	All on assigned projects No access on unassigned projects
Team Members	None	Access for assigned tasks Limited views within scope of their assigned tasks No views outside the scope of their assigned tasks

End of Part Two