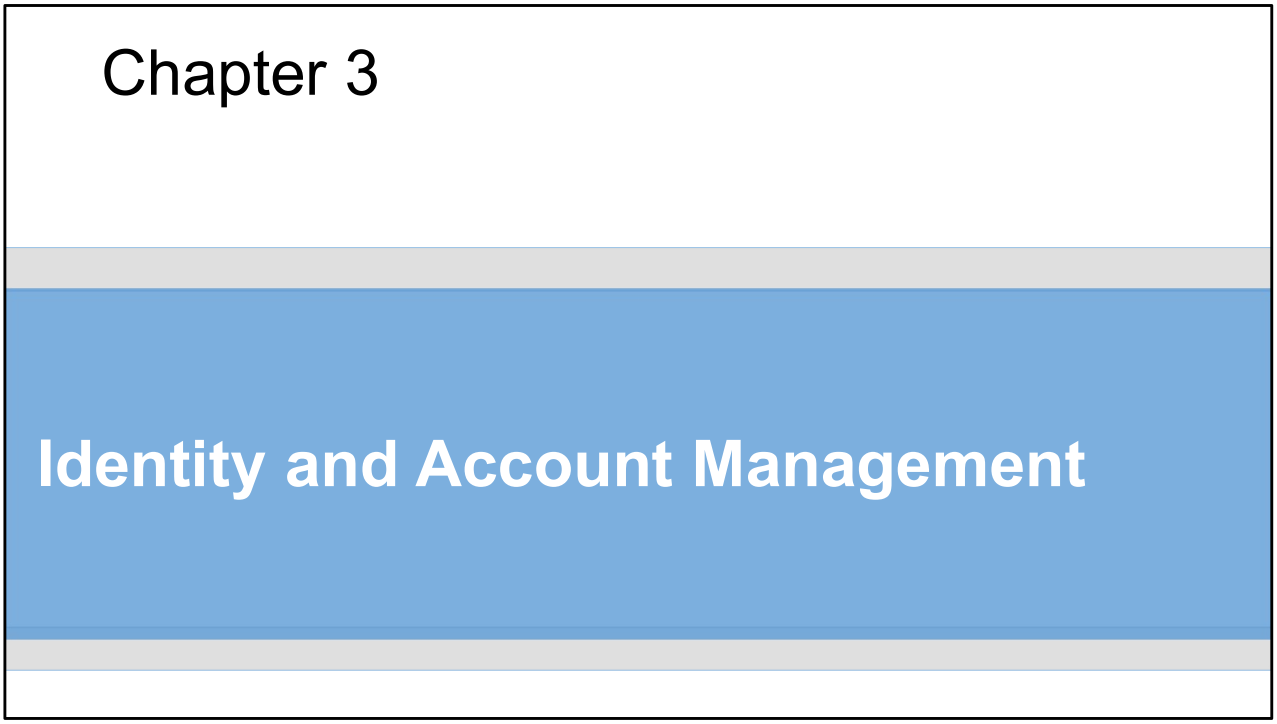
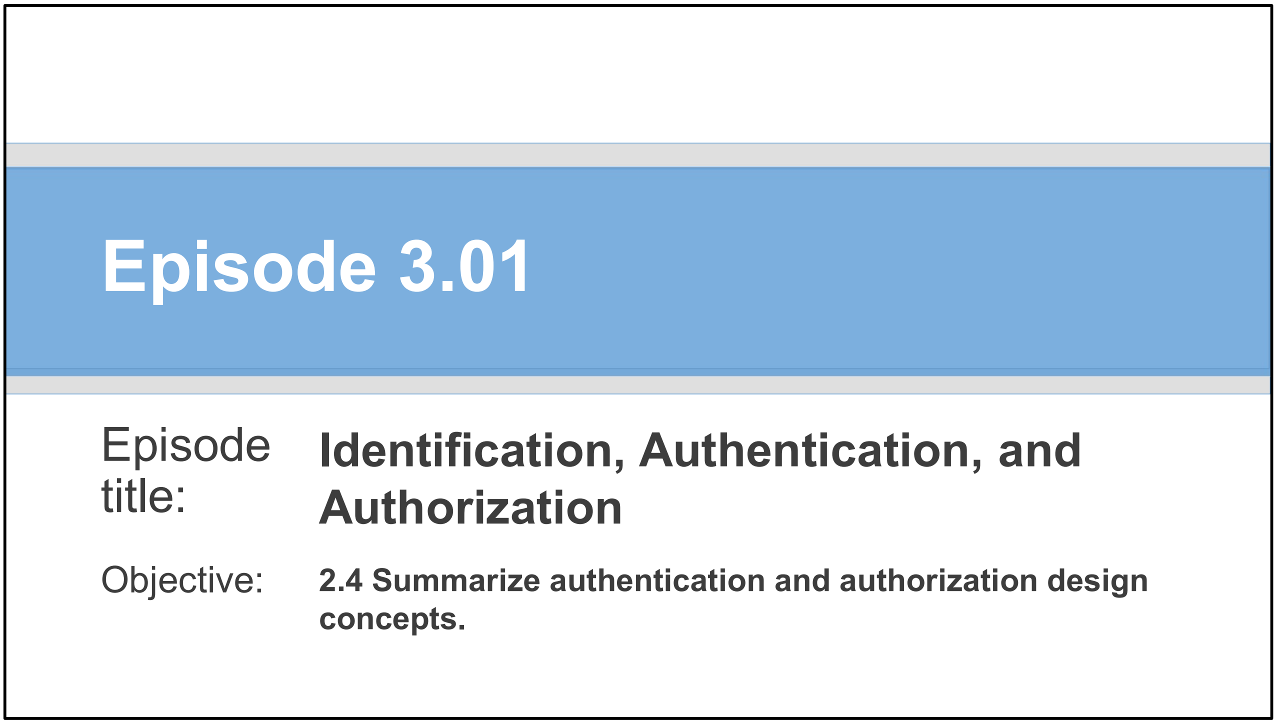


Chapter 3

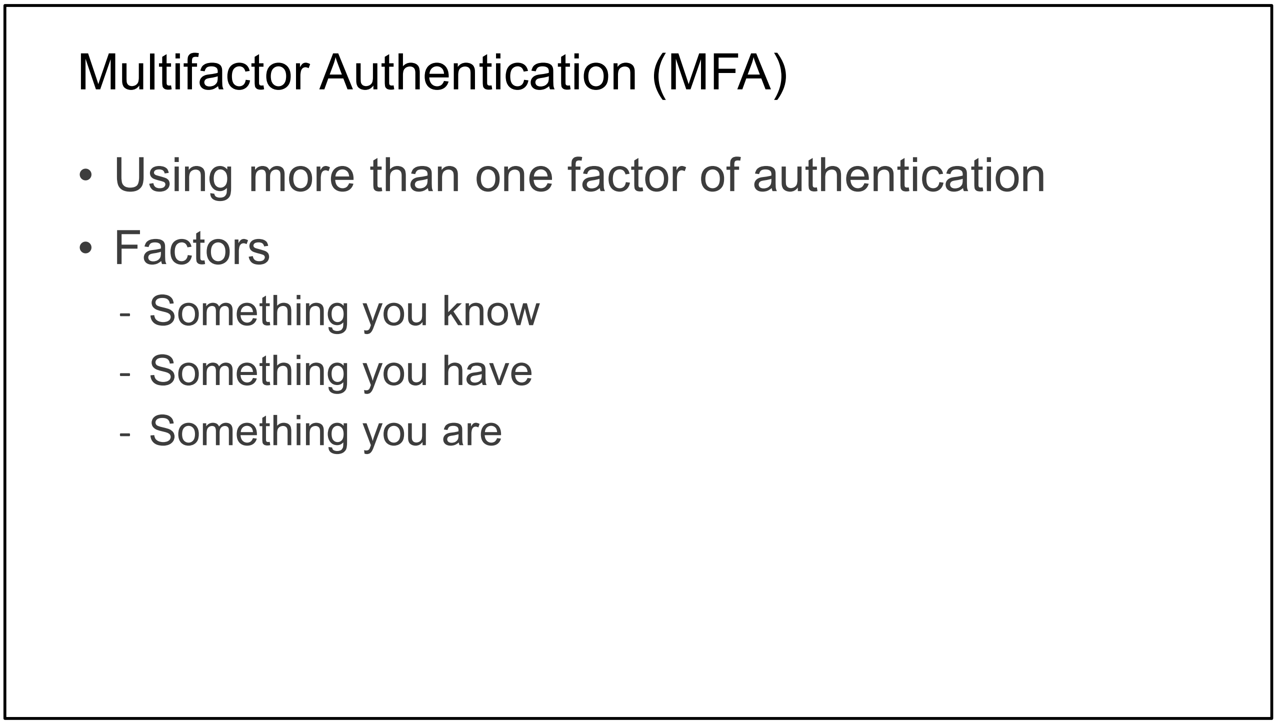
Identity and Account Management



Episode 3.01

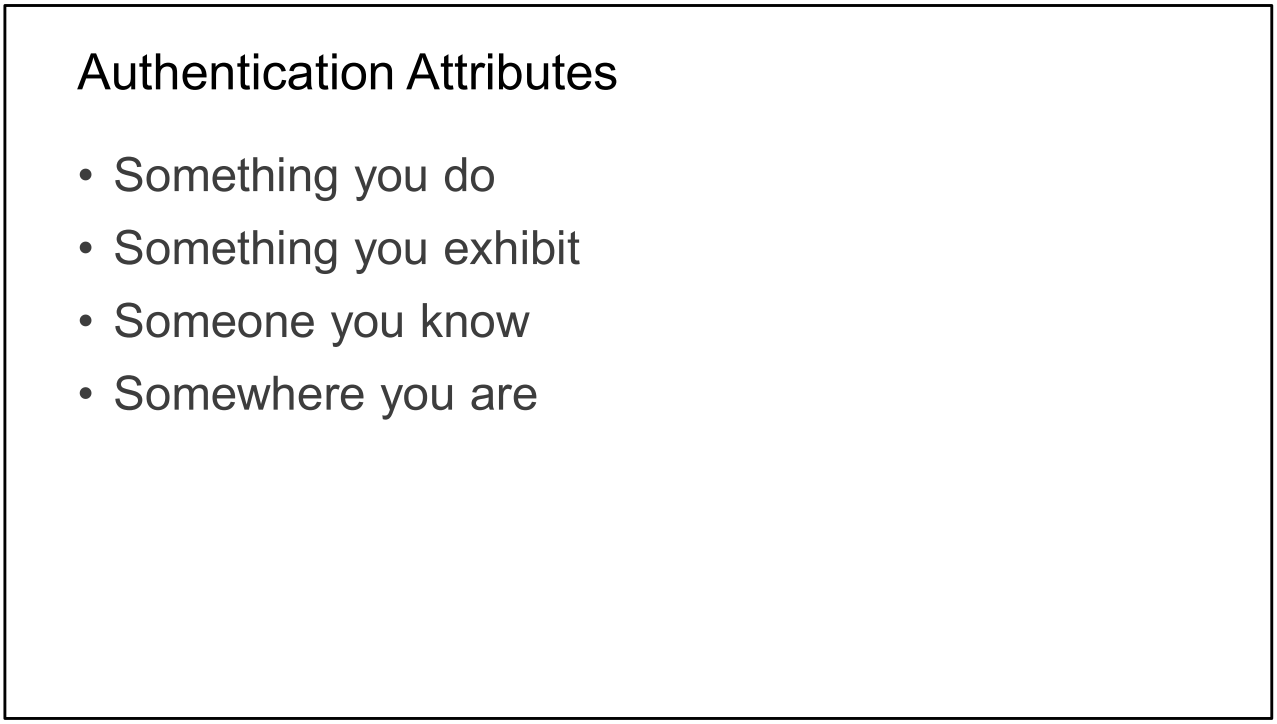
Episode title: **Identification, Authentication, and Authorization**

Objective: **2.4 Summarize authentication and authorization design concepts.**



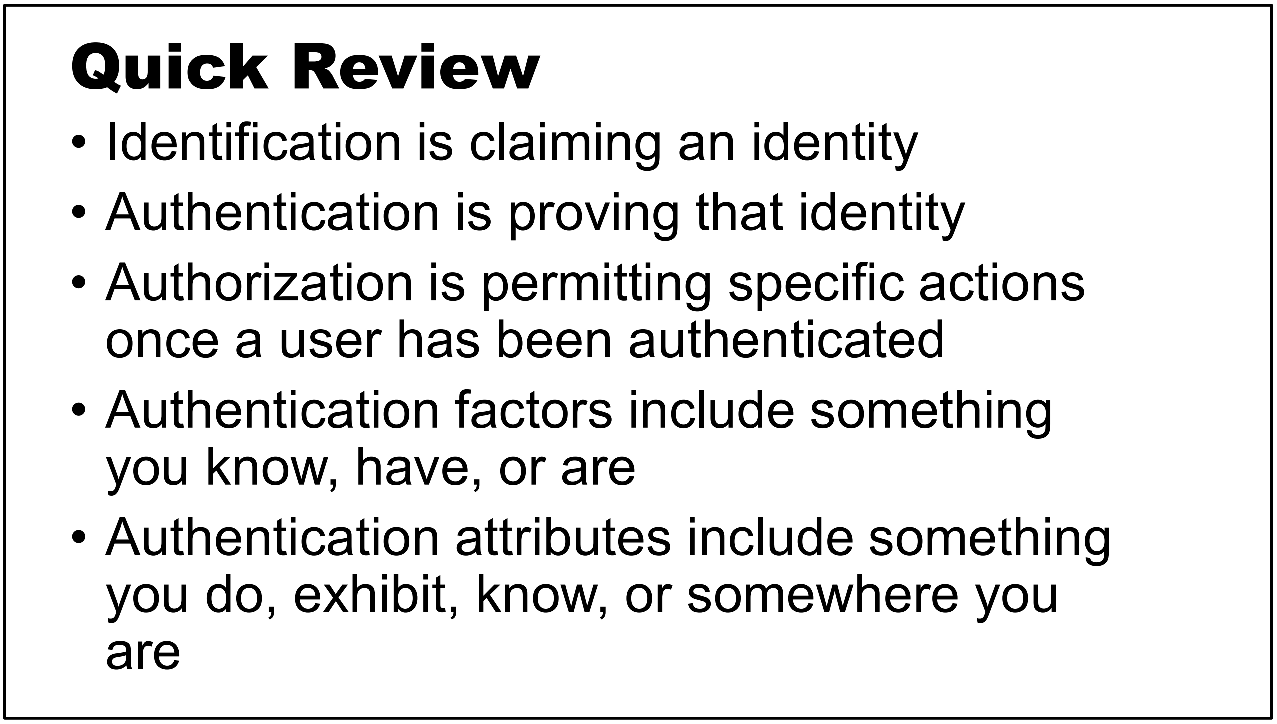
Multifactor Authentication (MFA)

- Using more than one factor of authentication
- Factors
  - Something you know
  - Something you have
  - Something you are



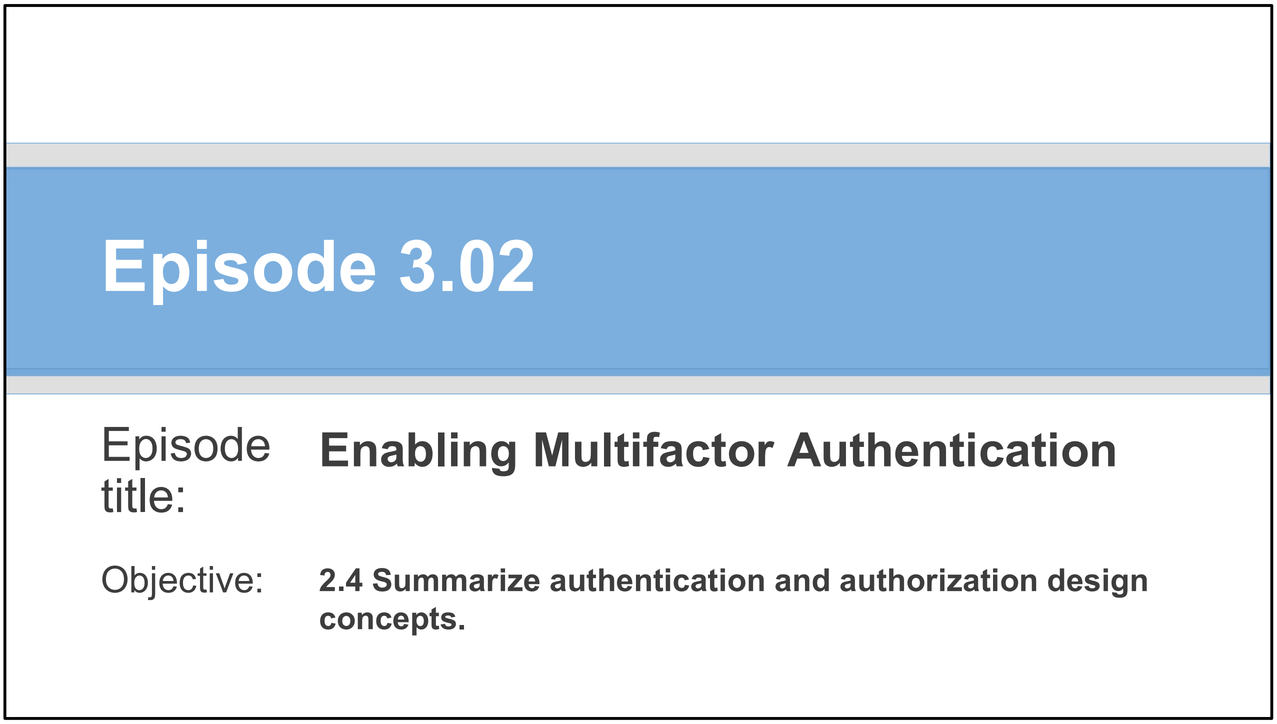
Authentication Attributes

- Something you do
- Something you exhibit
- Someone you know
- Somewhere you are



Quick Review

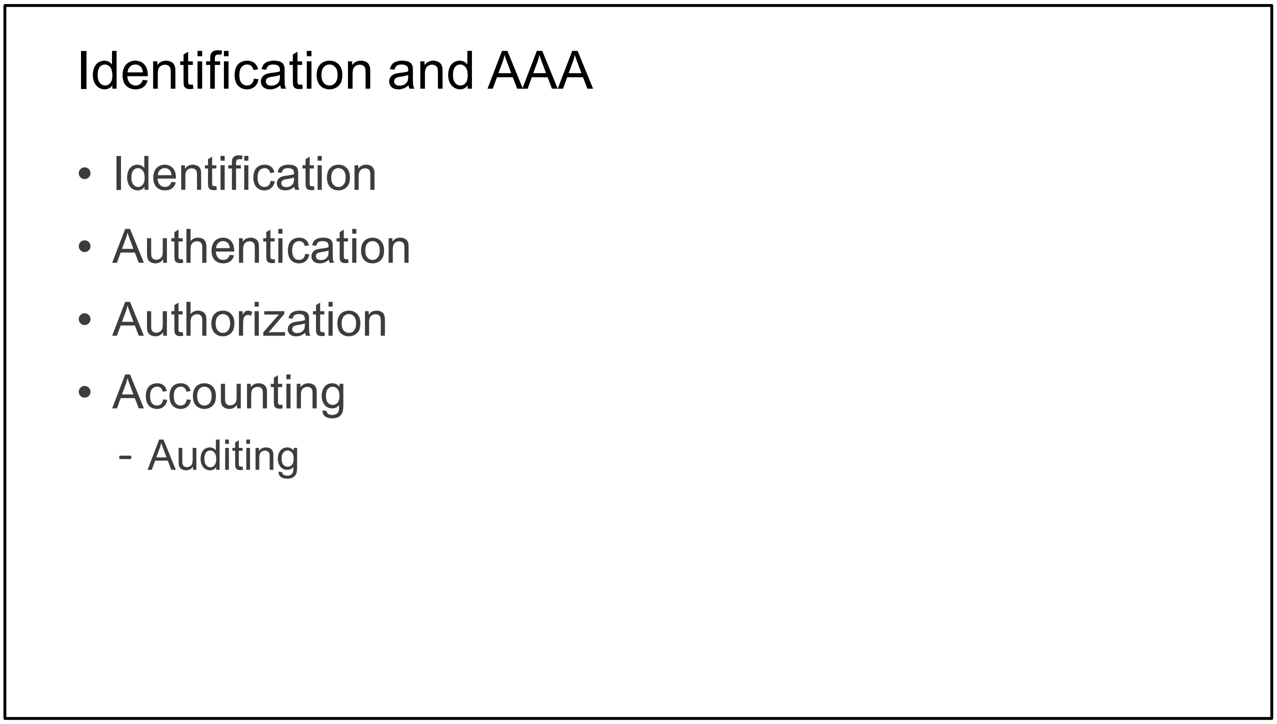
- Identification is claiming an identity
- Authentication is proving that identity
- Authorization is permitting specific actions once a user has been authenticated
- Authentication factors include something you know, have, or are
- Authentication attributes include something you do, exhibit, know, or somewhere you are



Episode 3.02

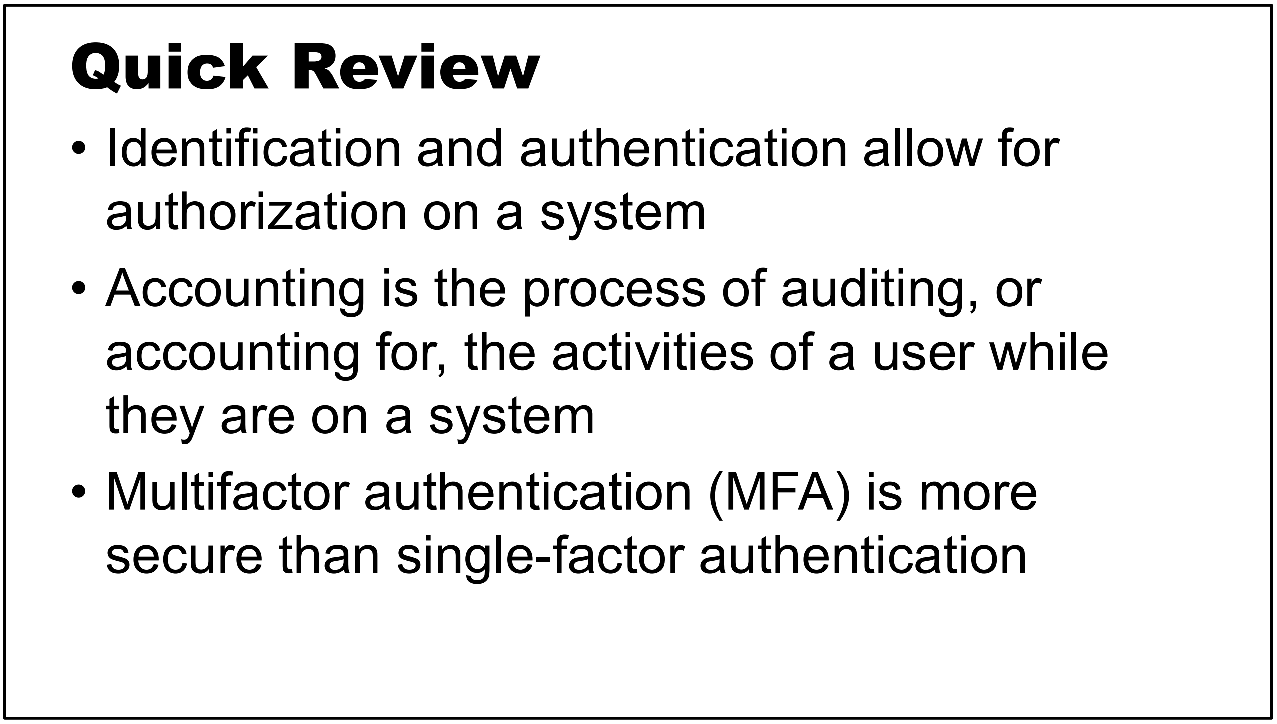
Episode title: **Enabling Multifactor Authentication**

Objective: **2.4 Summarize authentication and authorization design concepts.**



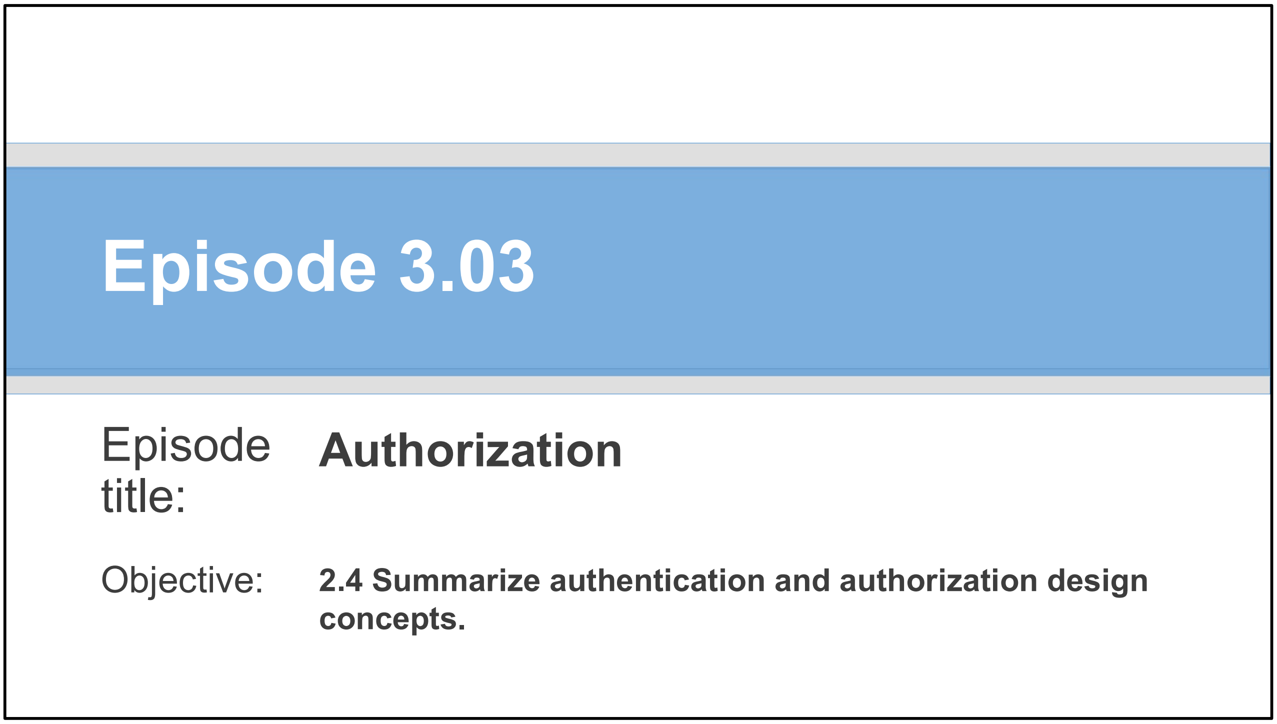
Identification and AAA

- Identification
- Authentication
- Authorization
- Accounting
  - Auditing



Quick Review

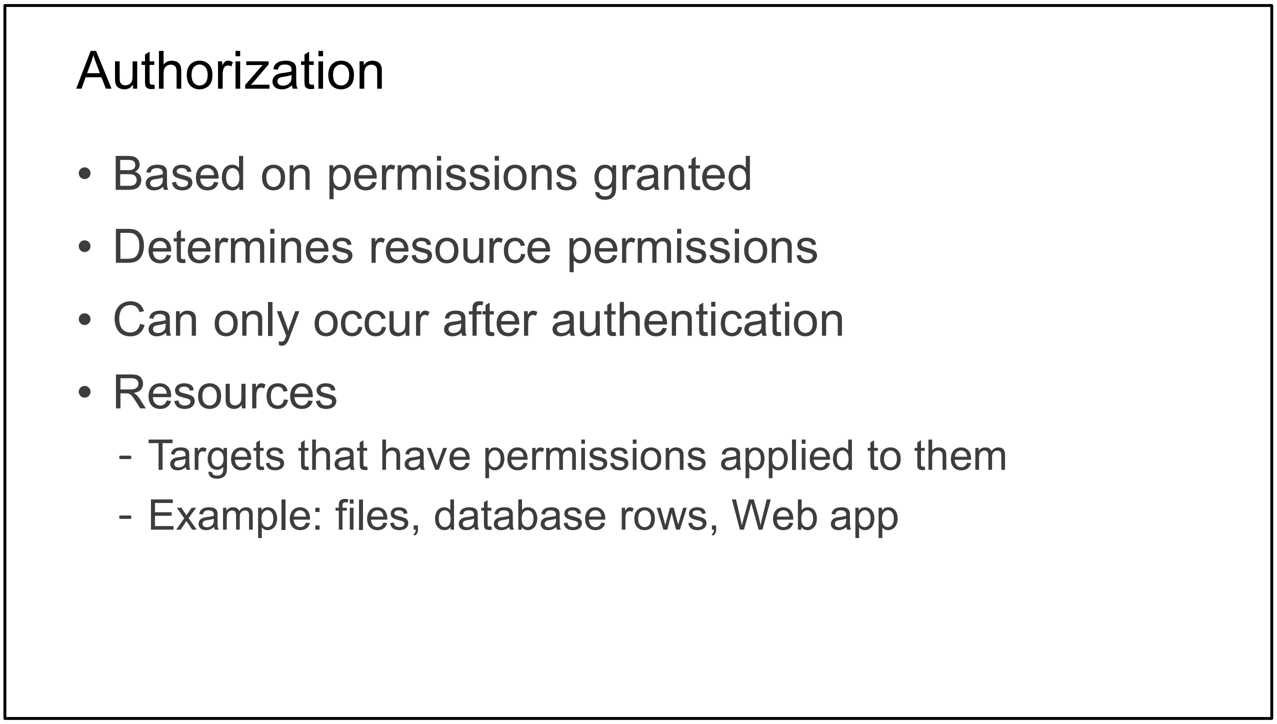
- Identification and authentication allow for authorization on a system
- Accounting is the process of auditing, or accounting for, the activities of a user while they are on a system
- Multifactor authentication (MFA) is more secure than single-factor authentication



Episode 3.03

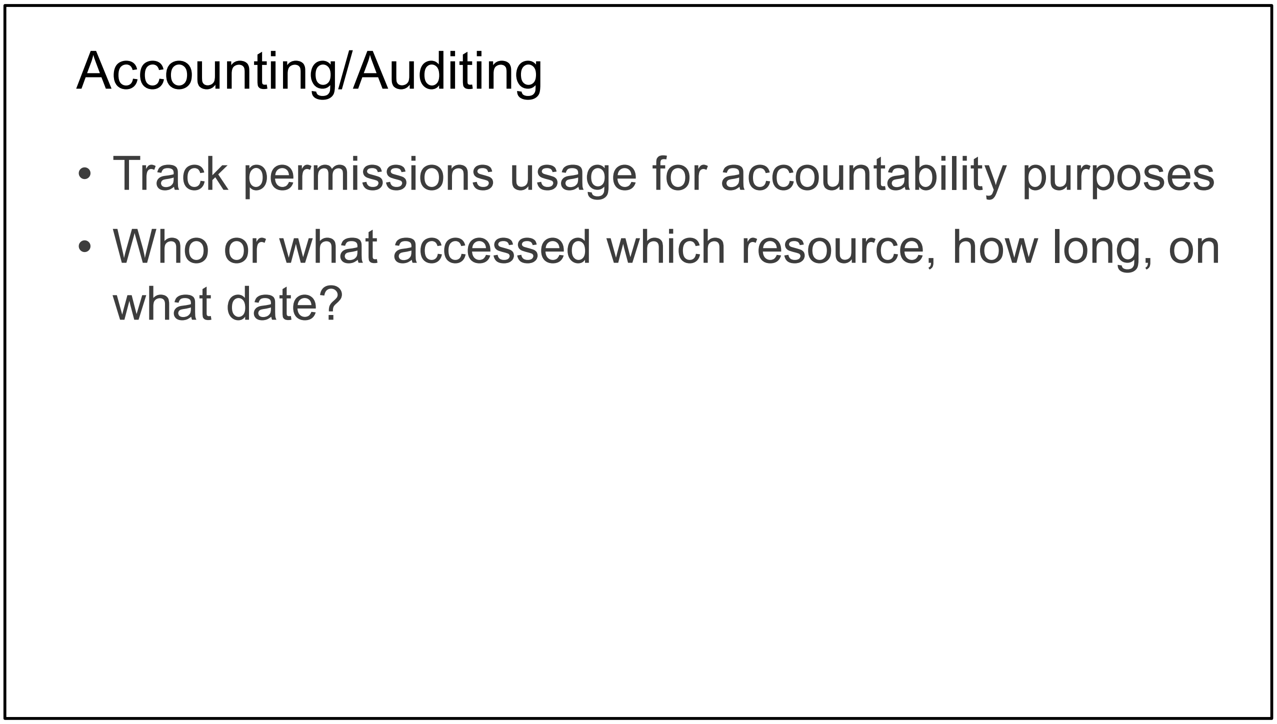
Episode title: **Authorization**

Objective: **2.4 Summarize authentication and authorization design concepts.**



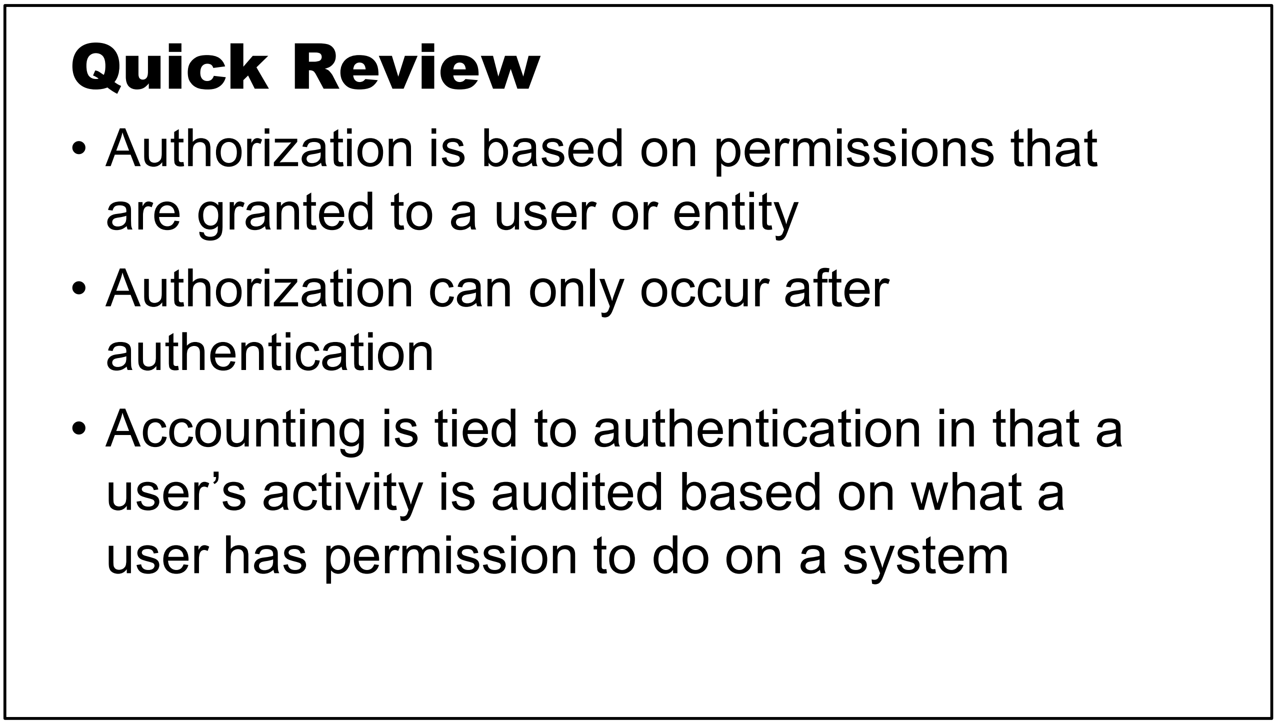
Authorization

- Based on permissions granted
- Determines resource permissions
- Can only occur after authentication
- Resources
  - Targets that have permissions applied to them
  - Example: files, database rows, Web app



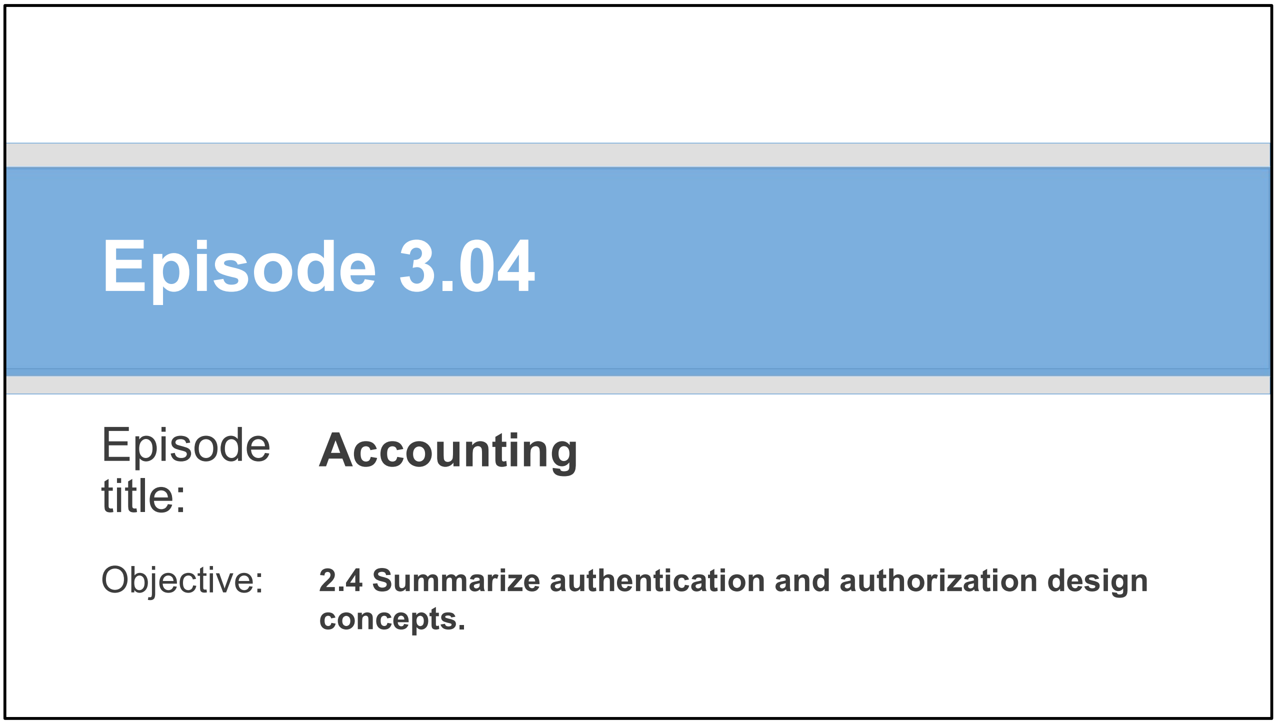
Accounting/Auditing

- Track permissions usage for accountability purposes
- Who or what accessed which resource, how long, on what date?



Quick Review

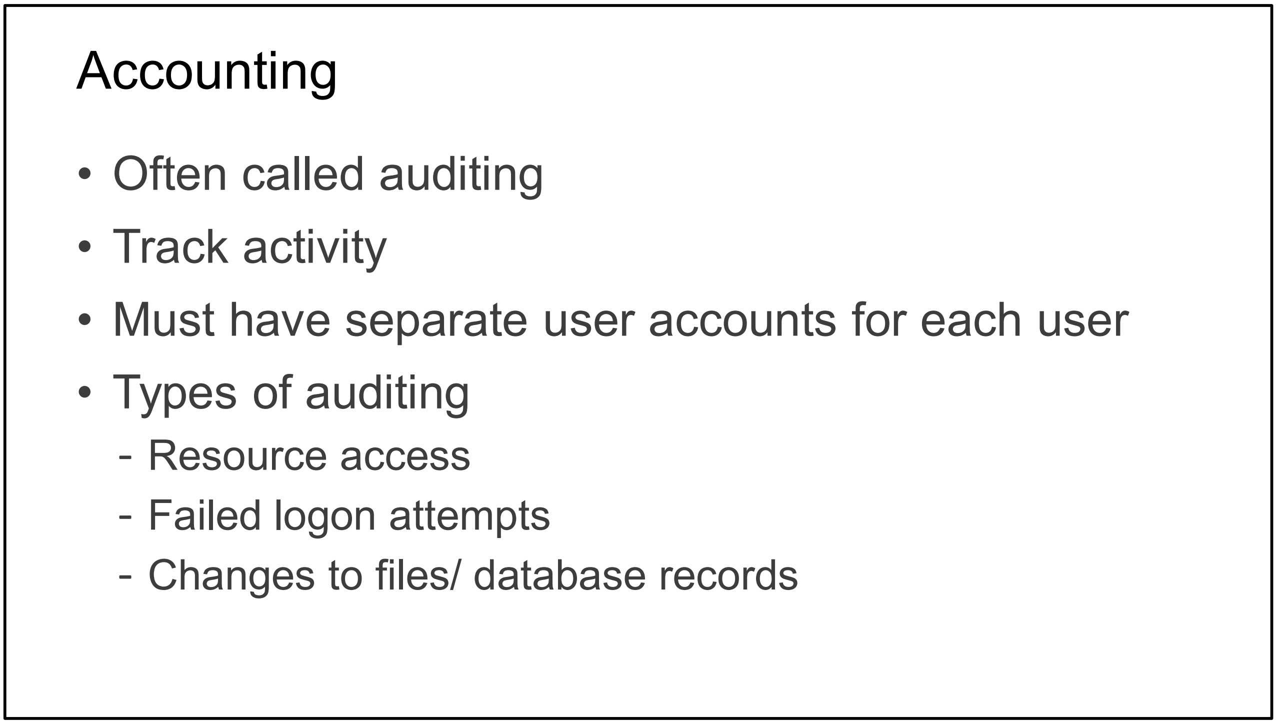
- Authorization is based on permissions that are granted to a user or entity
- Authorization can only occur after authentication
- Accounting is tied to authentication in that a user's activity is audited based on what a user has permission to do on a system



Episode 3.04

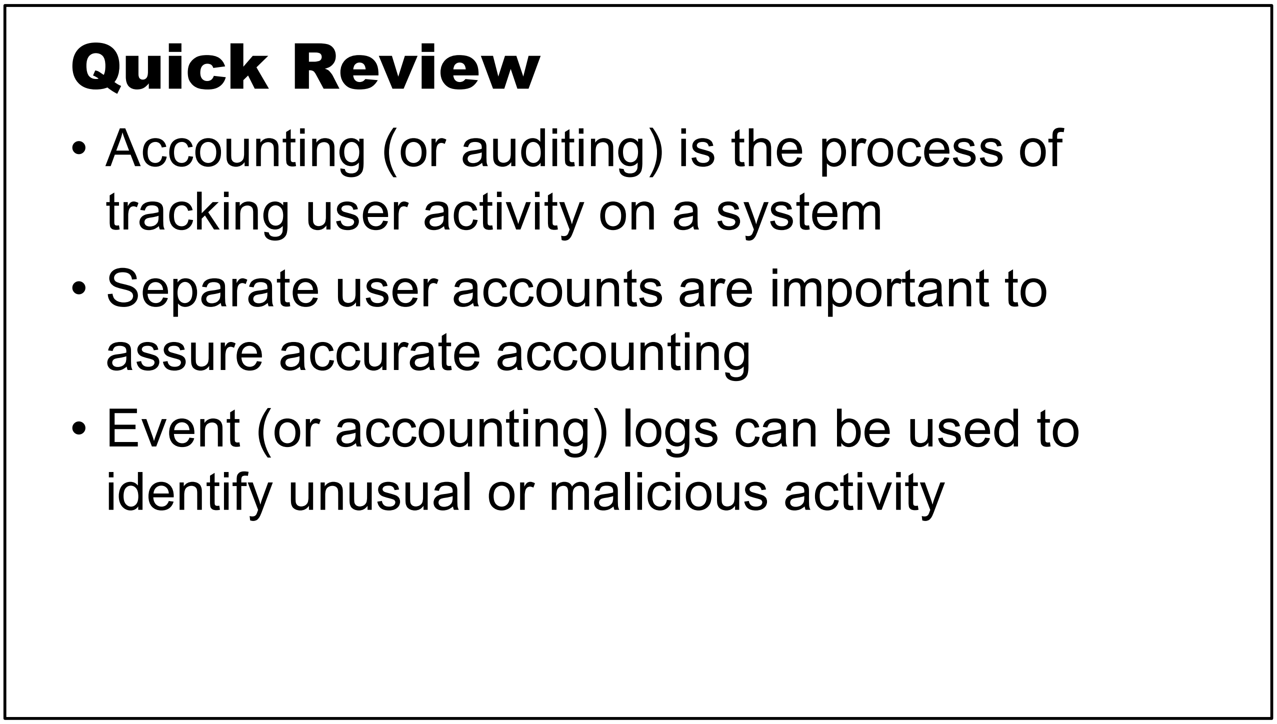
Episode title: **Accounting**

Objective: **2.4 Summarize authentication and authorization design concepts.**



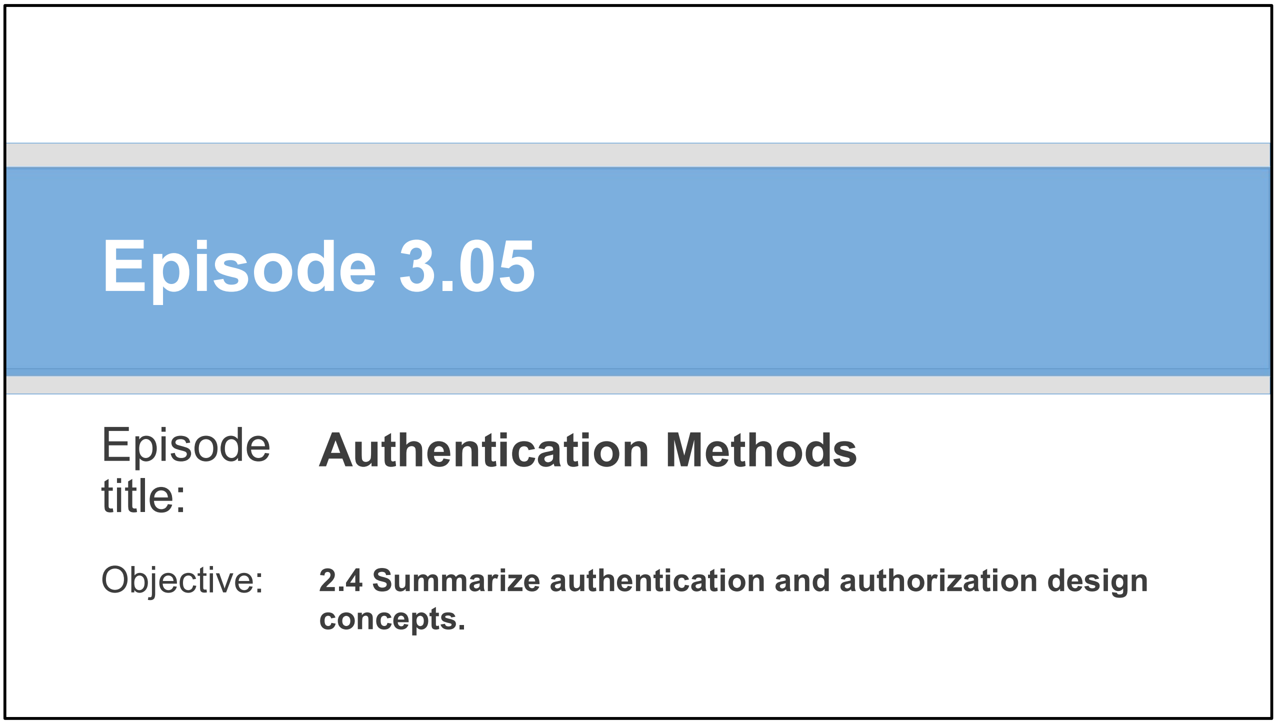
Accounting

- Often called auditing
- Track activity
- Must have separate user accounts for each user
- Types of auditing
  - Resource access
  - Failed logon attempts
  - Changes to files/ database records



Quick Review

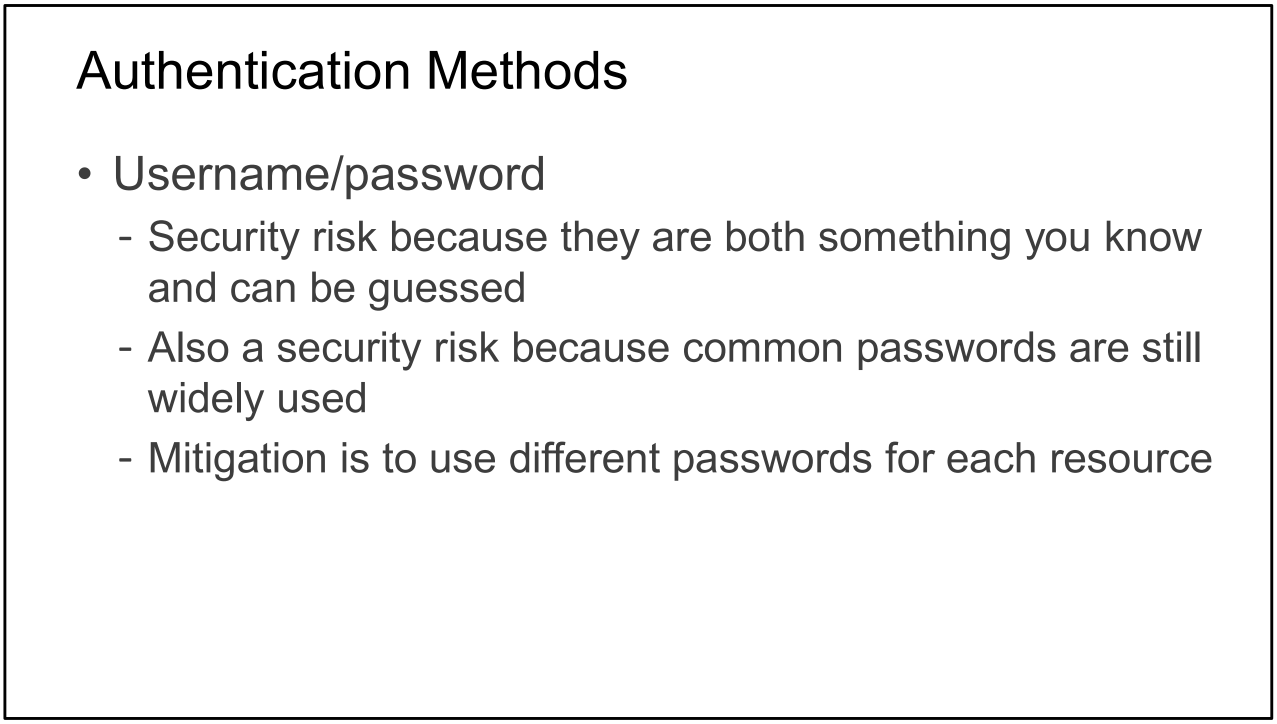
- Accounting (or auditing) is the process of tracking user activity on a system
- Separate user accounts are important to assure accurate accounting
- Event (or accounting) logs can be used to identify unusual or malicious activity



Episode 3.05

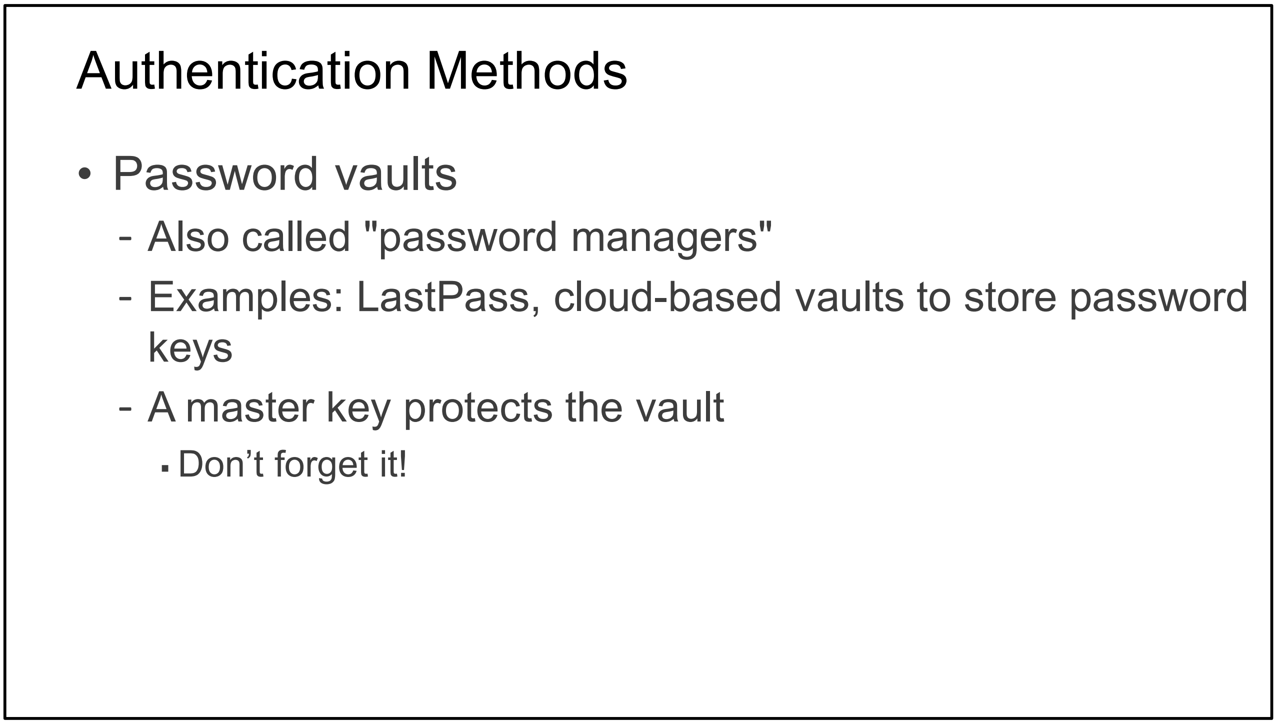
Episode title: **Authentication Methods**

Objective: **2.4 Summarize authentication and authorization design concepts.**



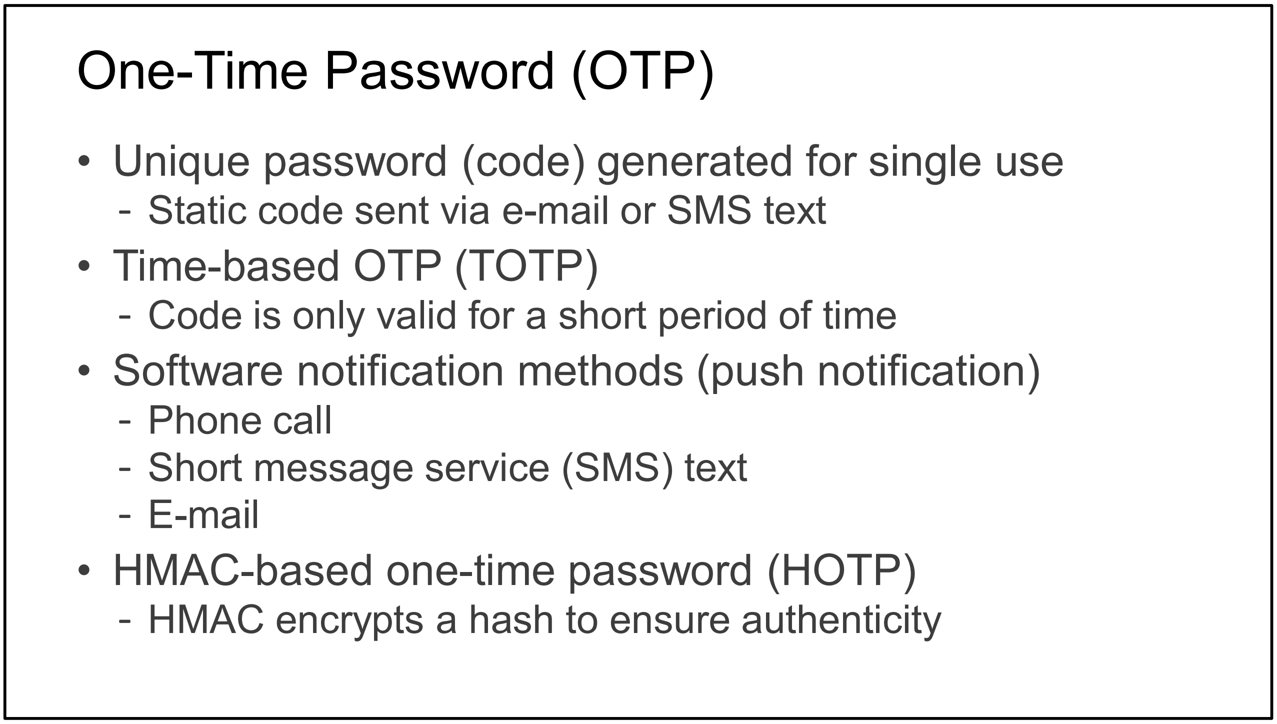
Authentication Methods

- Username/password
  - Security risk because they are both something you know and can be guessed
  - Also a security risk because common passwords are still widely used
  - Mitigation is to use different passwords for each resource



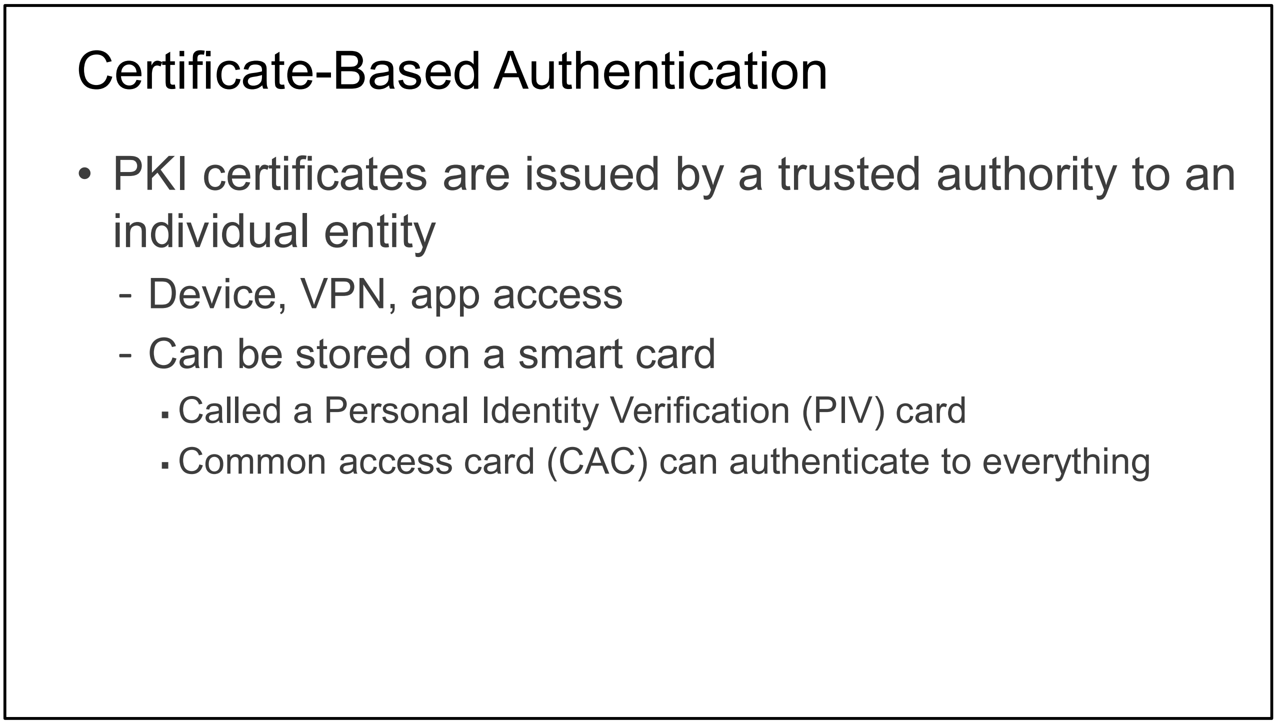
Authentication Methods

- Password vaults
  - Also called "password managers"
  - Examples: LastPass, cloud-based vaults to store password keys
  - A master key protects the vault
    - Don’t forget it!



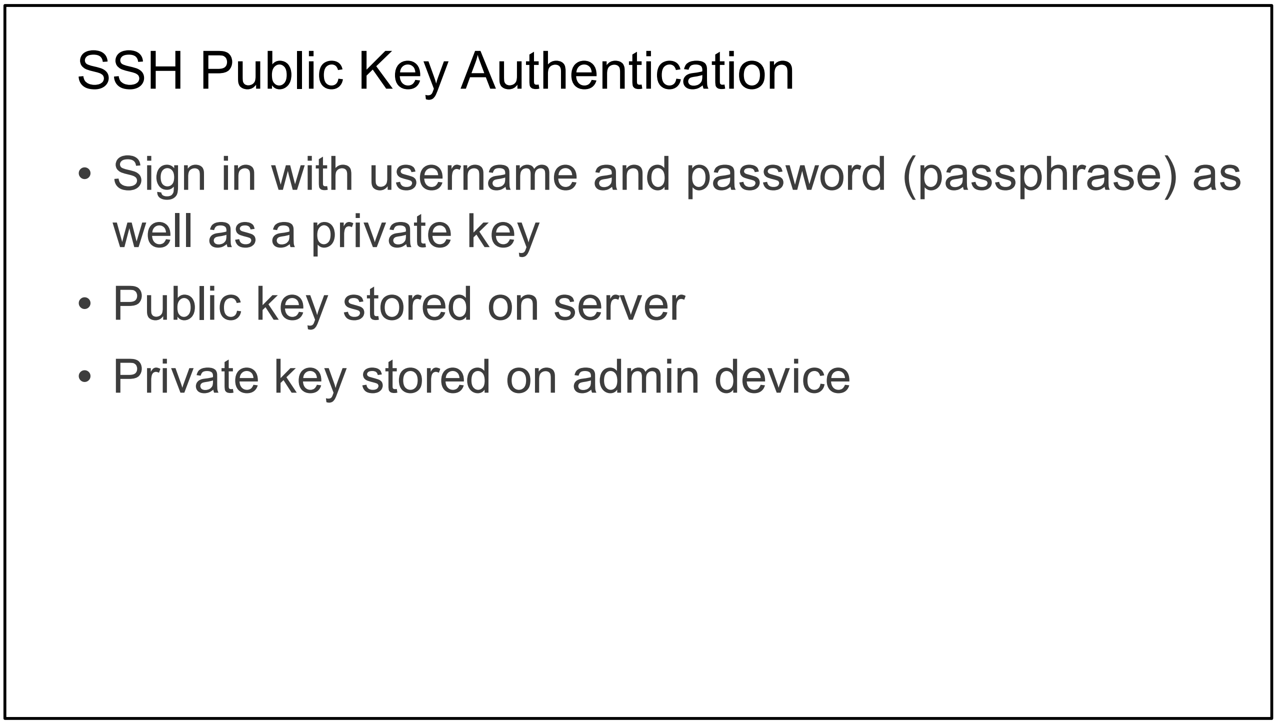
One-Time Password (OTP)

- Unique password (code) generated for single use
  - Static code sent via e-mail or SMS text
- Time-based OTP (TOTP)
  - Code is only valid for a short period of time
- Software notification methods (push notification)
  - Phone call
  - Short message service (SMS) text
  - E-mail
- HMAC-based one-time password (HOTP)
  - HMAC encrypts a hash to ensure authenticity



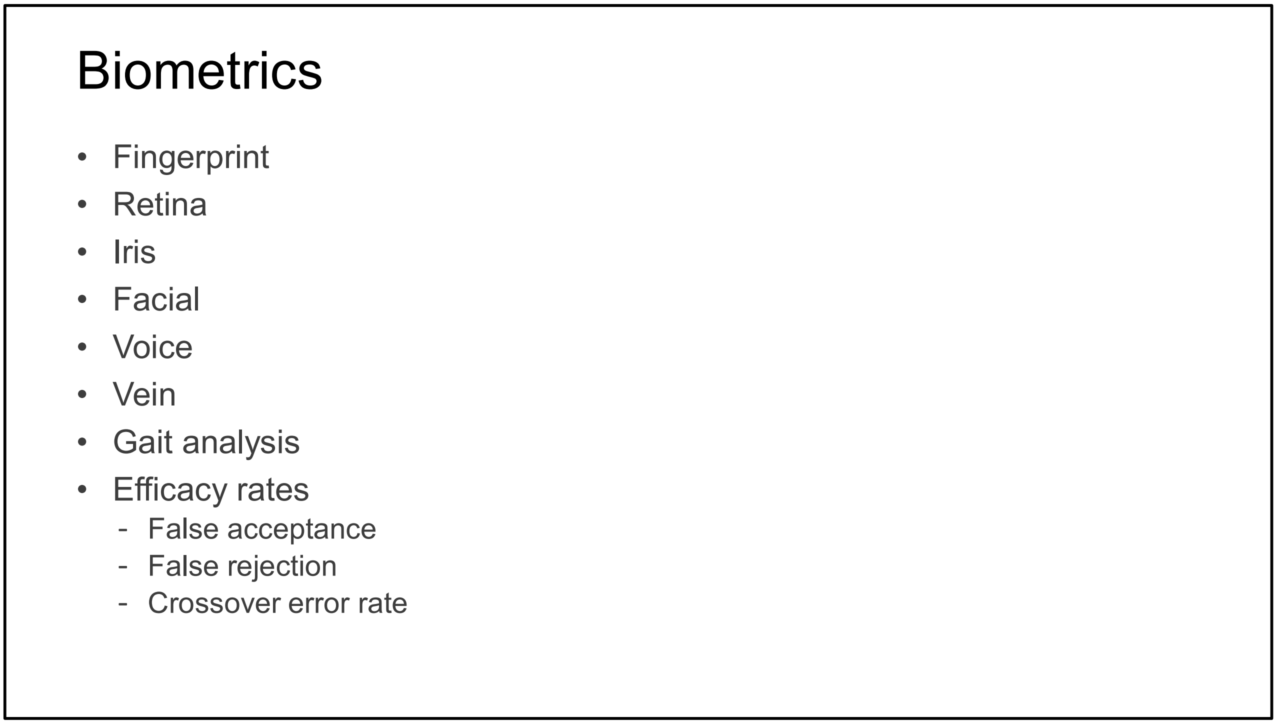
Certificate-Based Authentication

- PKI certificates are issued by a trusted authority to an individual entity
  - Device, VPN, app access
  - Can be stored on a smart card
    - Called a Personal Identity Verification (PIV) card
    - Common access card (CAC) can authenticate to everything



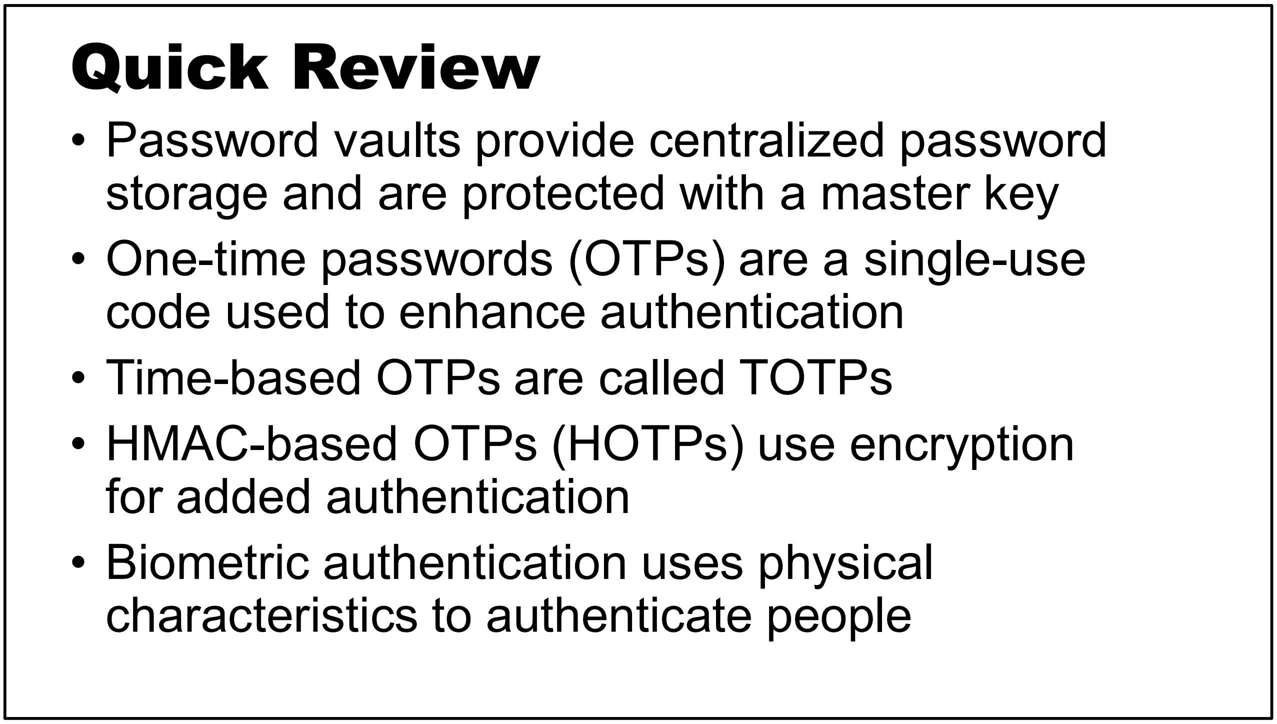
SSH Public Key Authentication

- Sign in with username and password (passphrase) as well as a private key
- Public key stored on server
- Private key stored on admin device



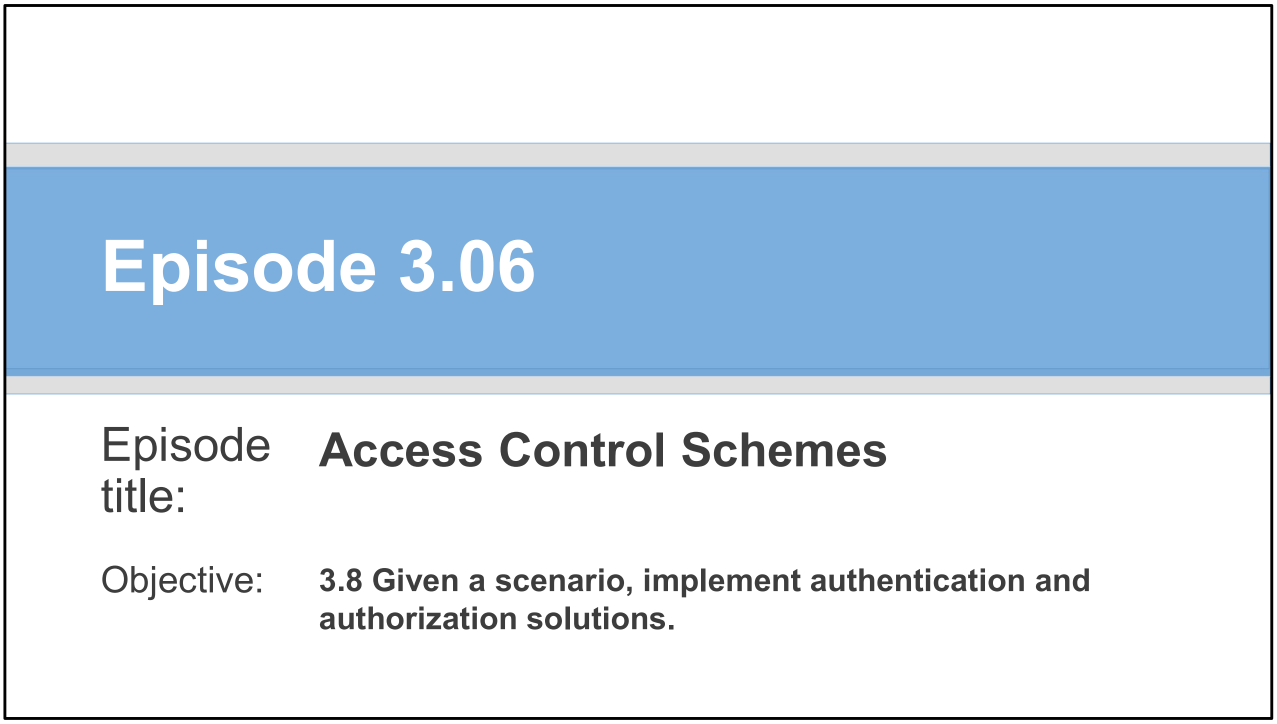
Biometrics

- Fingerprint
- Retina
- Iris
- Facial
- Voice
- Vein
- Gait analysis
- Efficacy rates
  - False acceptance
  - False rejection
  - Crossover error rate



Quick Review

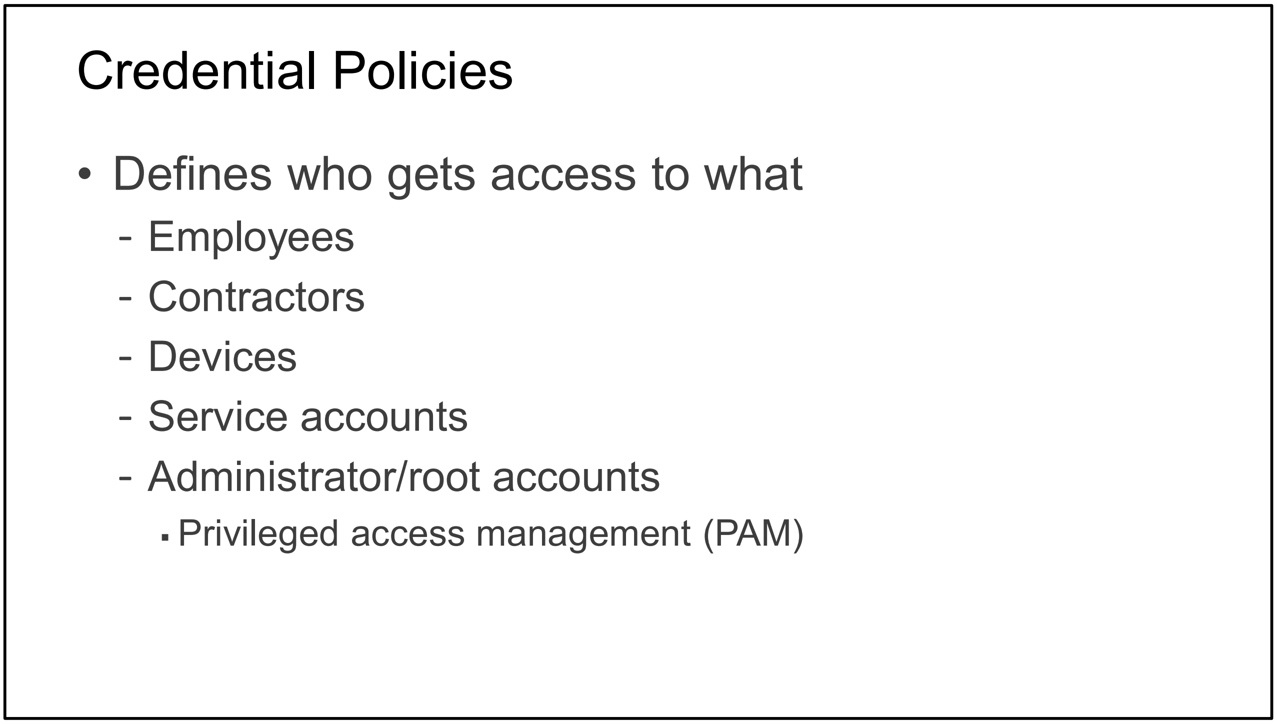
- Password vaults provide centralized password storage and are protected with a master key
- One-time passwords (OTPs) are a single-use code used to enhance authentication
- Time-based OTPs are called TOTPs
- HMAC-based OTPs (HOTPs) use encryption for added authentication
- Biometric authentication uses physical characteristics to authenticate people



Episode 3.06

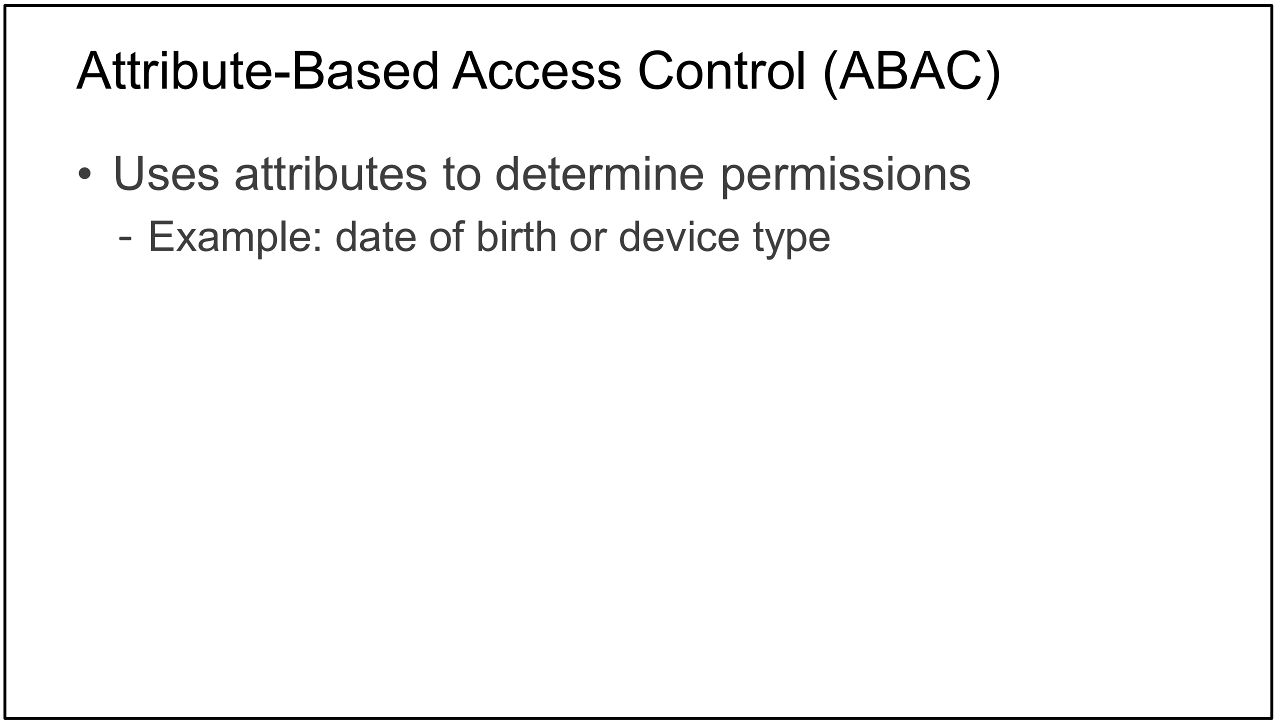
Episode title: **Access Control Schemes**

Objective: **3.8 Given a scenario, implement authentication and authorization solutions.**



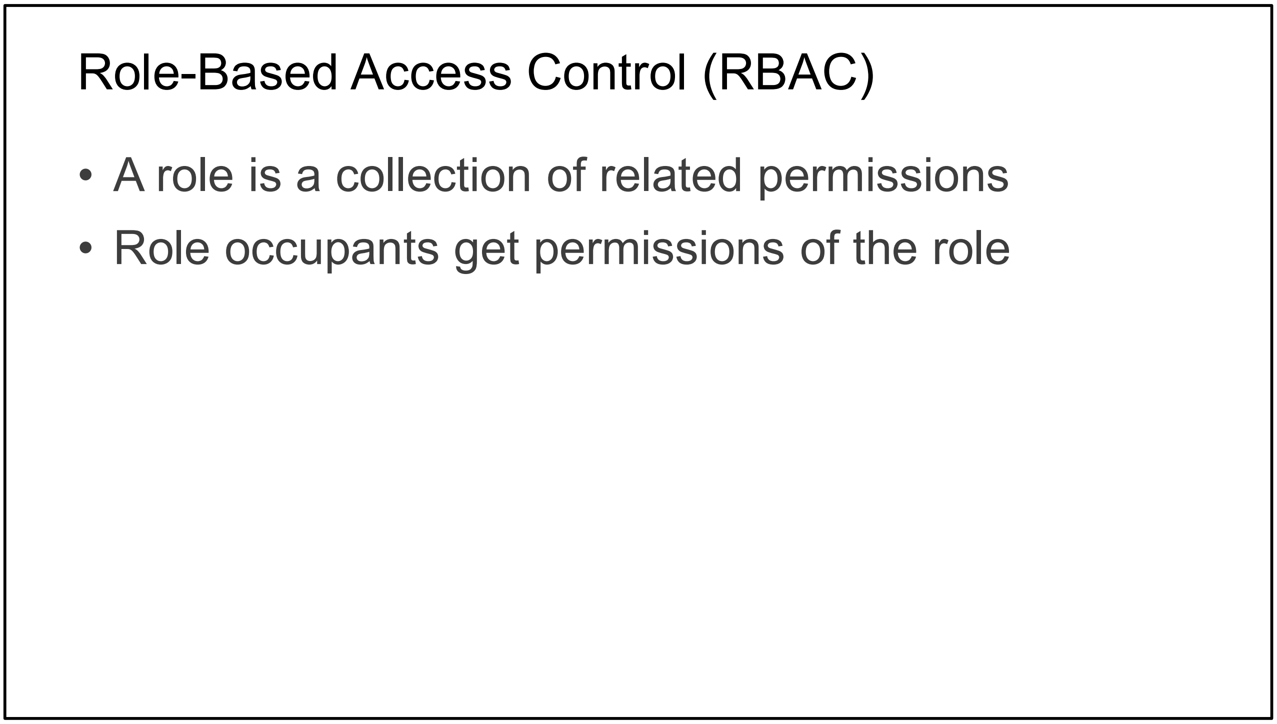
Credential Policies

- Defines who gets access to what
  - Employees
  - Contractors
  - Devices
  - Service accounts
  - Administrator/root accounts
    - Privileged access management (PAM)



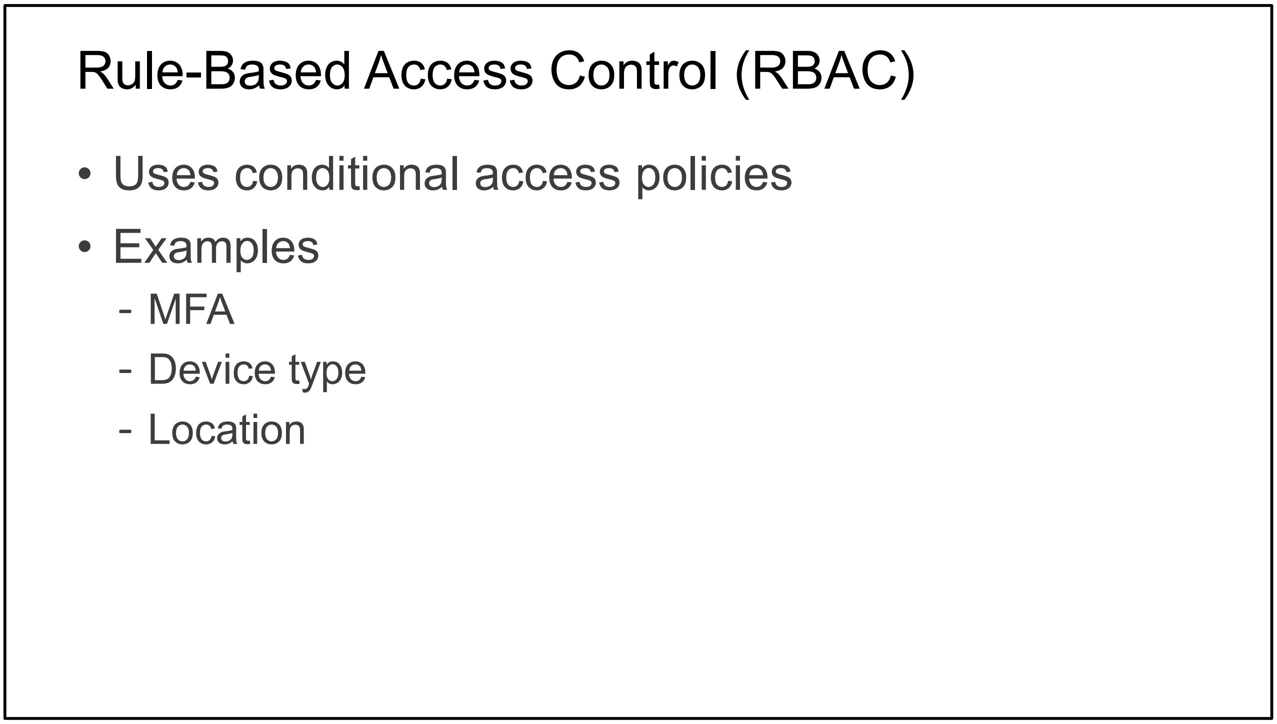
Attribute-Based Access Control (ABAC)

- Uses attributes to determine permissions
  - Example: date of birth or device type



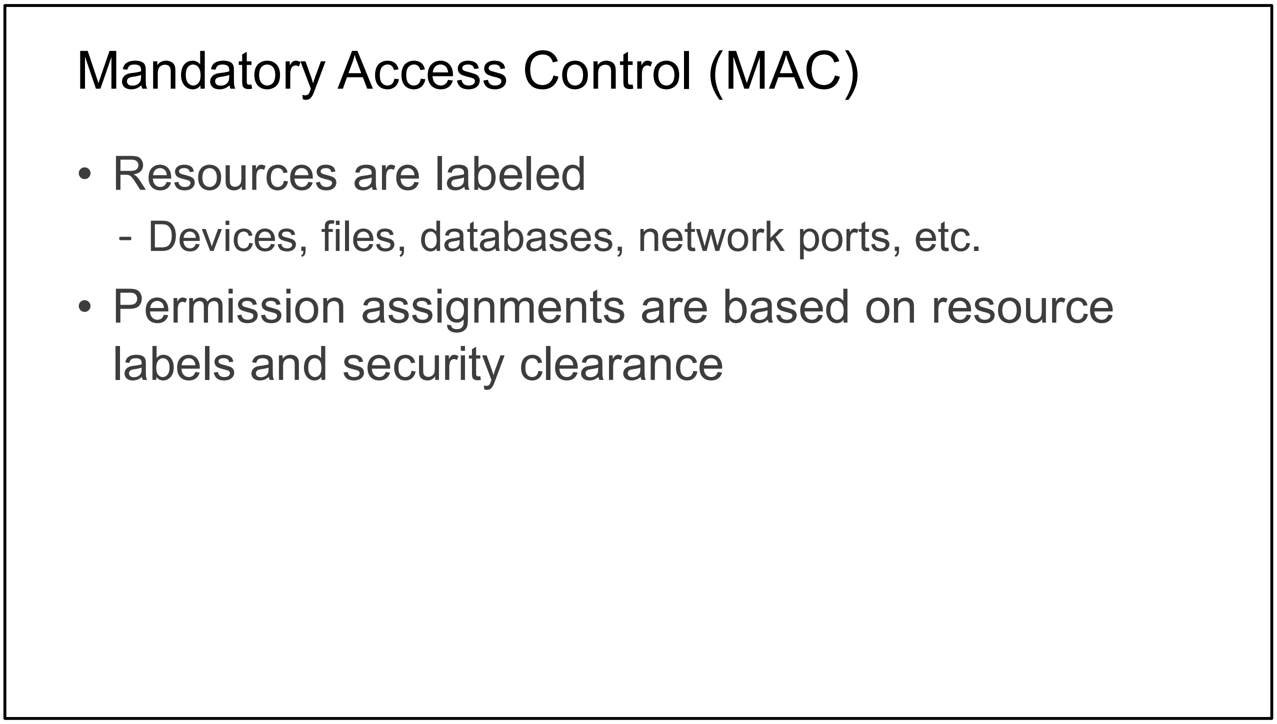
Role-Based Access Control (RBAC)

- A role is a collection of related permissions
- Role occupants get permissions of the role



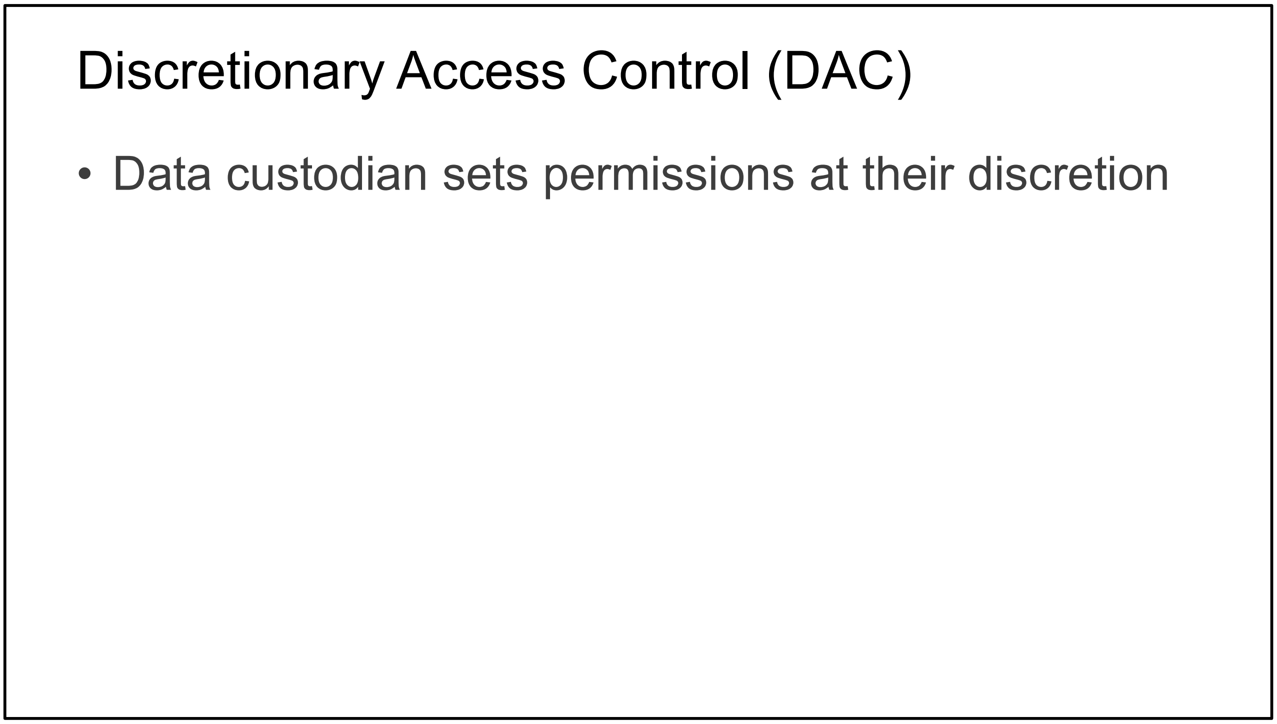
Rule-Based Access Control (RBAC)

- Uses conditional access policies
- Examples
  - MFA
  - Device type
  - Location



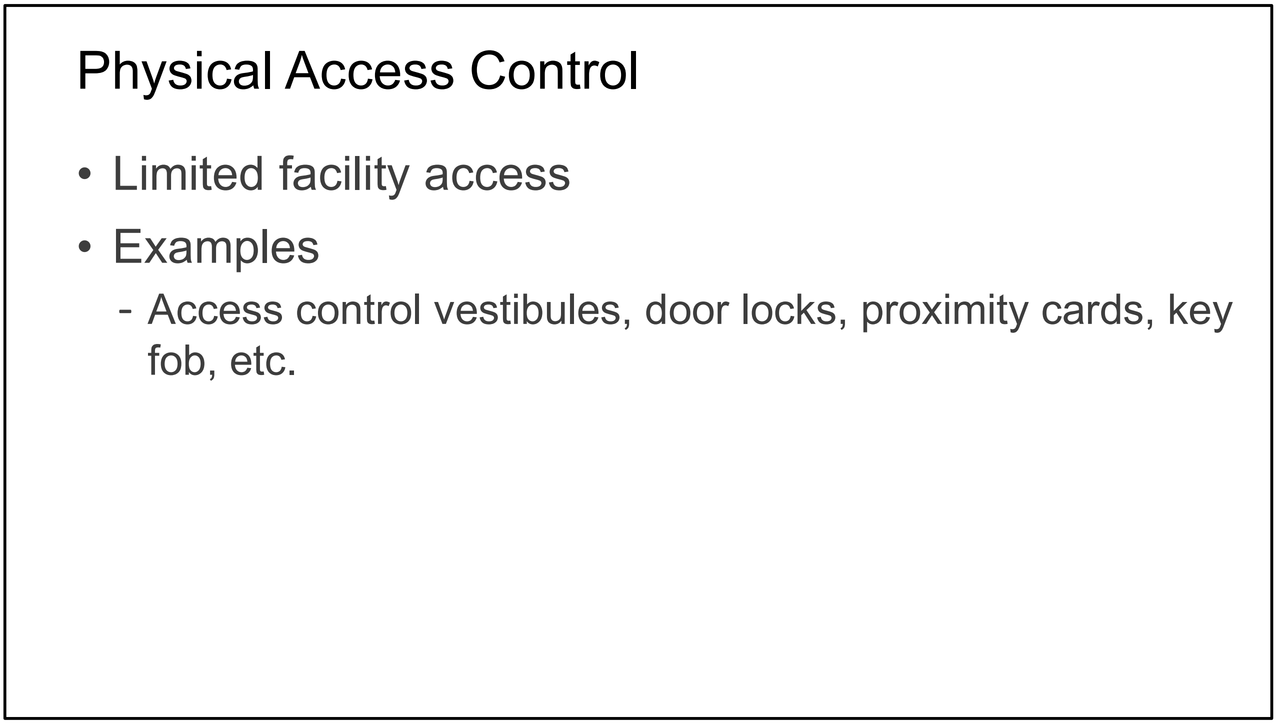
Mandatory Access Control (MAC)

- Resources are labeled
  - Devices, files, databases, network ports, etc.
- Permission assignments are based on resource labels and security clearance



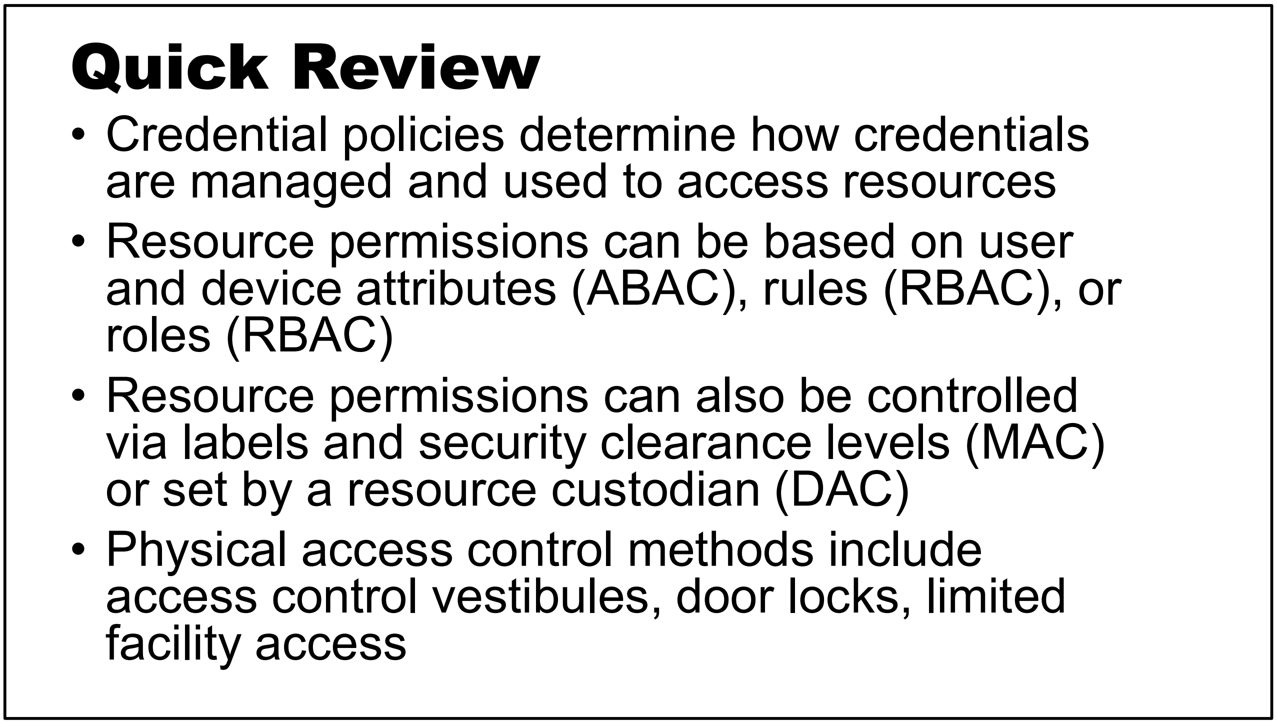
Discretionary Access Control (DAC)

- Data custodian sets permissions at their discretion



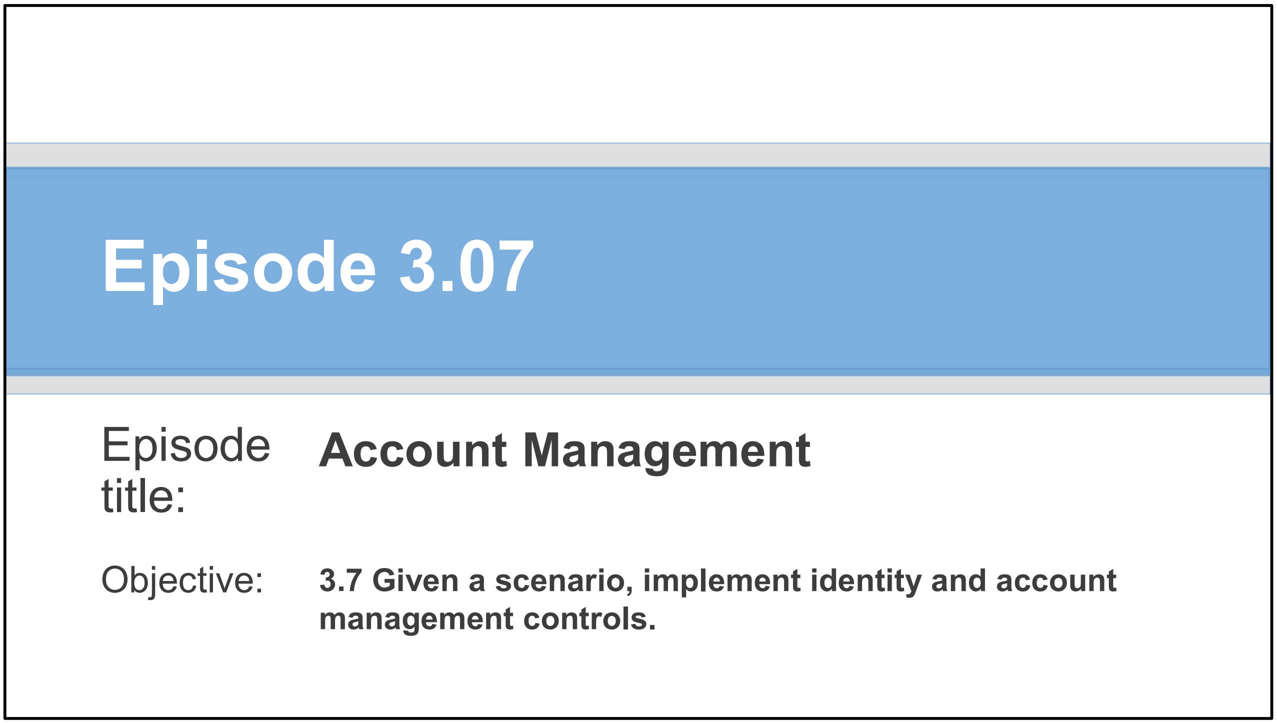
Physical Access Control

- Limited facility access
- Examples
  - Access control vestibules, door locks, proximity cards, key fob, etc.



Quick Review

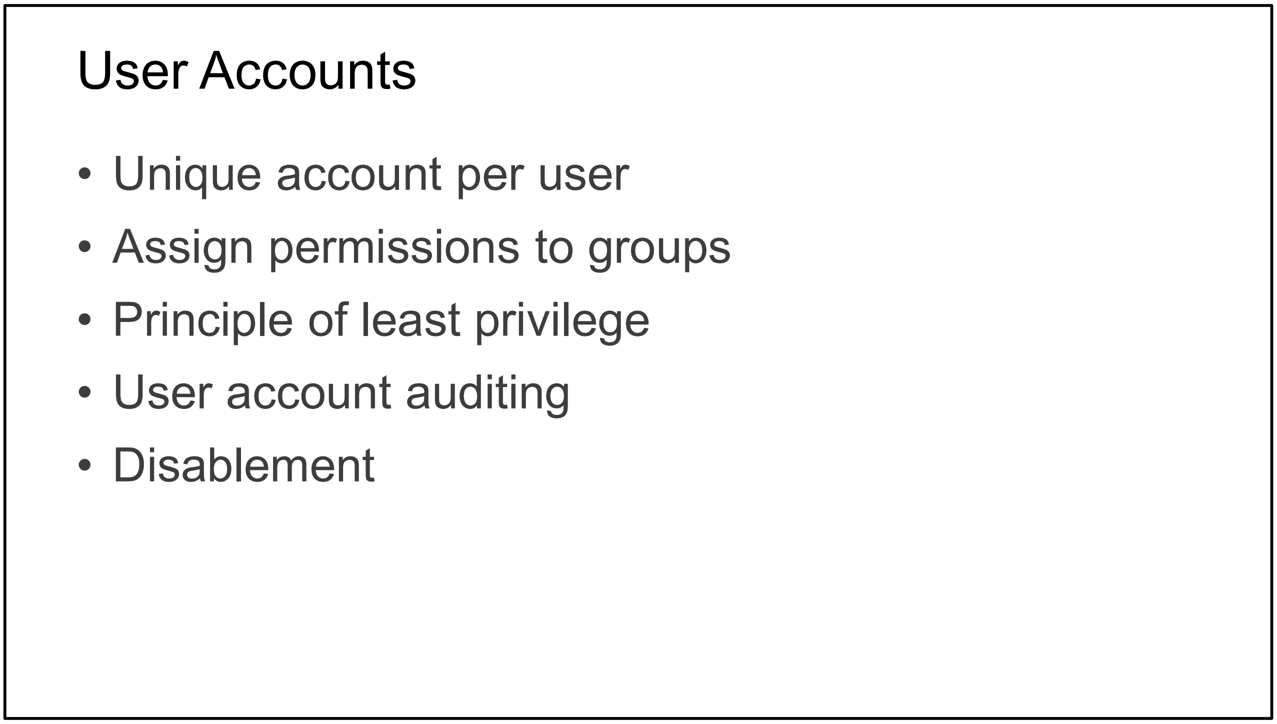
- Credential policies determine how credentials are managed and used to access resources
- Resource permissions can be based on user and device attributes (ABAC), rules (RBAC), or roles (RBAC)
- Resource permissions can also be controlled via labels and security clearance levels (MAC) or set by a resource custodian (DAC)
- Physical access control methods include access control vestibules, door locks, limited facility access



Episode 3.07

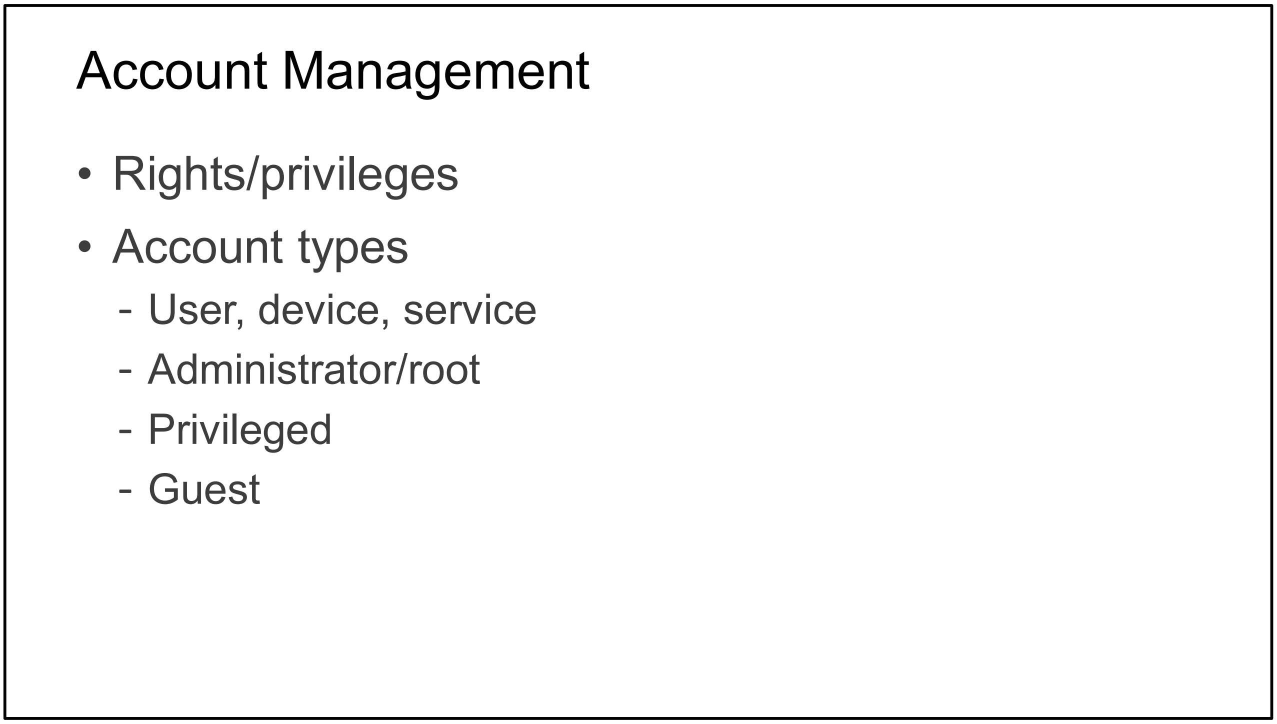
Episode title: **Account Management**

Objective: **3.7 Given a scenario, implement identity and account management controls.**



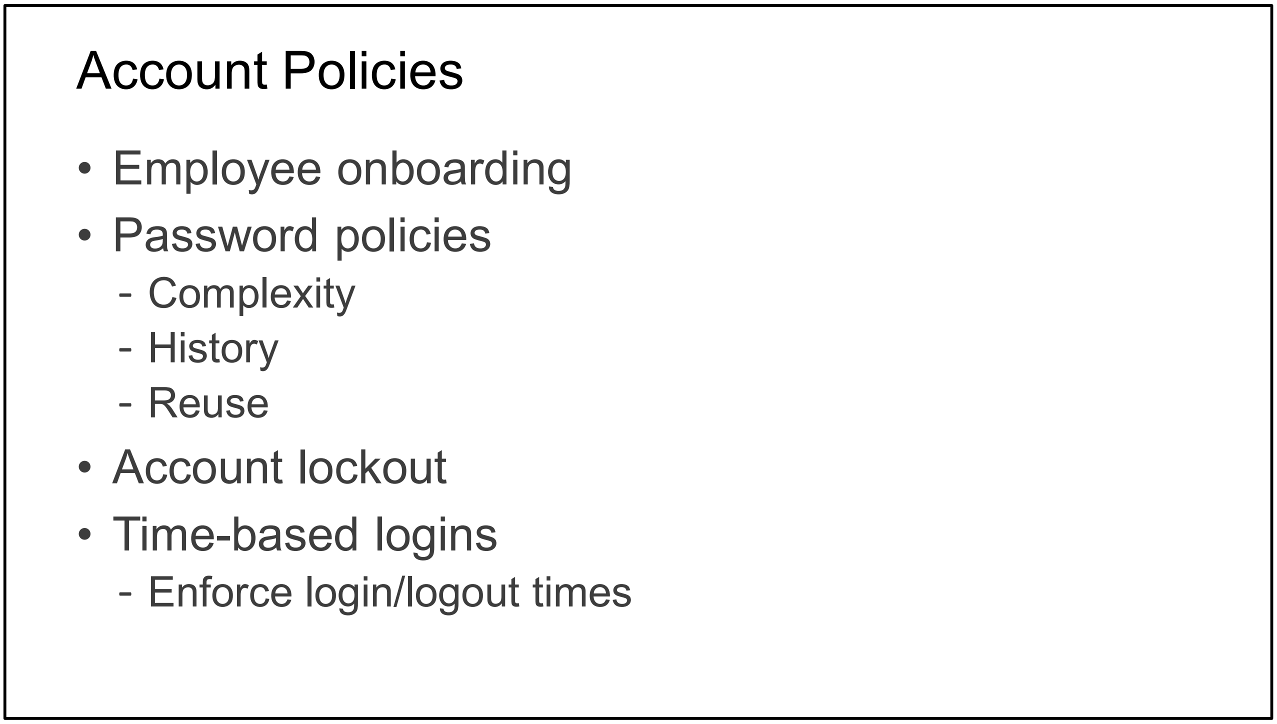
User Accounts

- Unique account per user
- Assign permissions to groups
- Principle of least privilege
- User account auditing
- Disablement



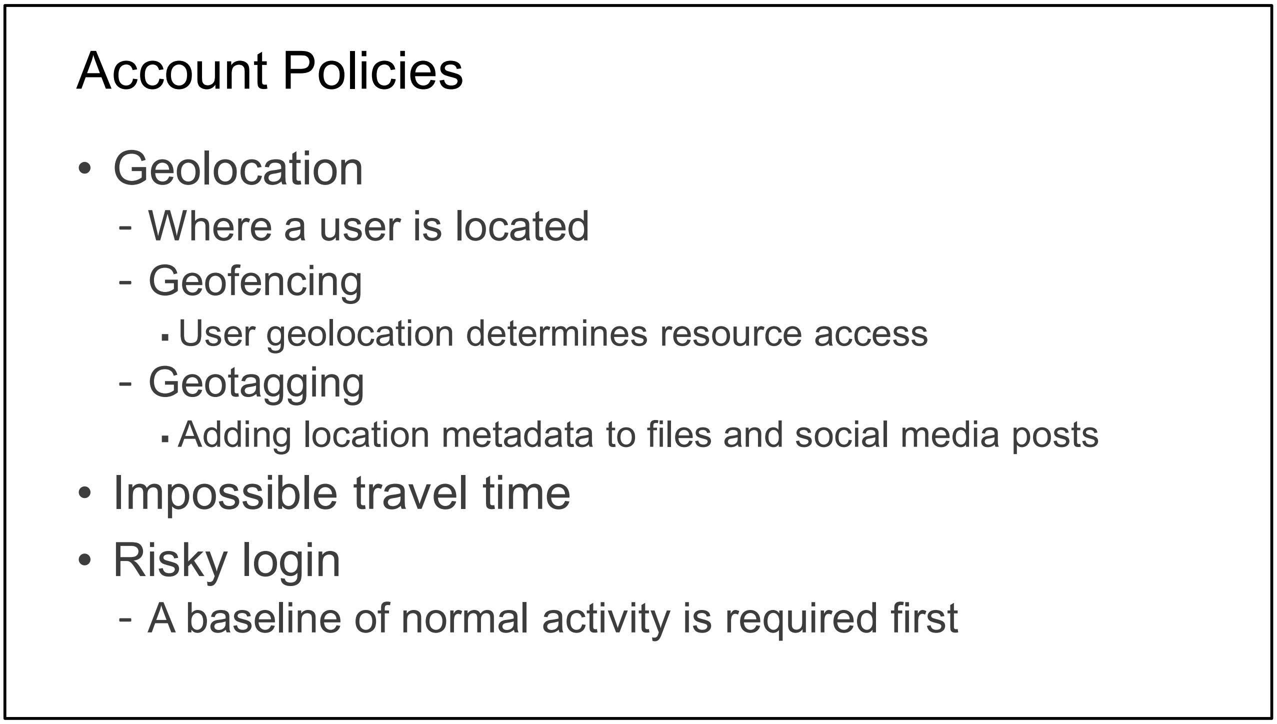
Account Management

- Rights/privileges
- Account types
  - User, device, service
  - Administrator/root
  - Privileged
  - Guest



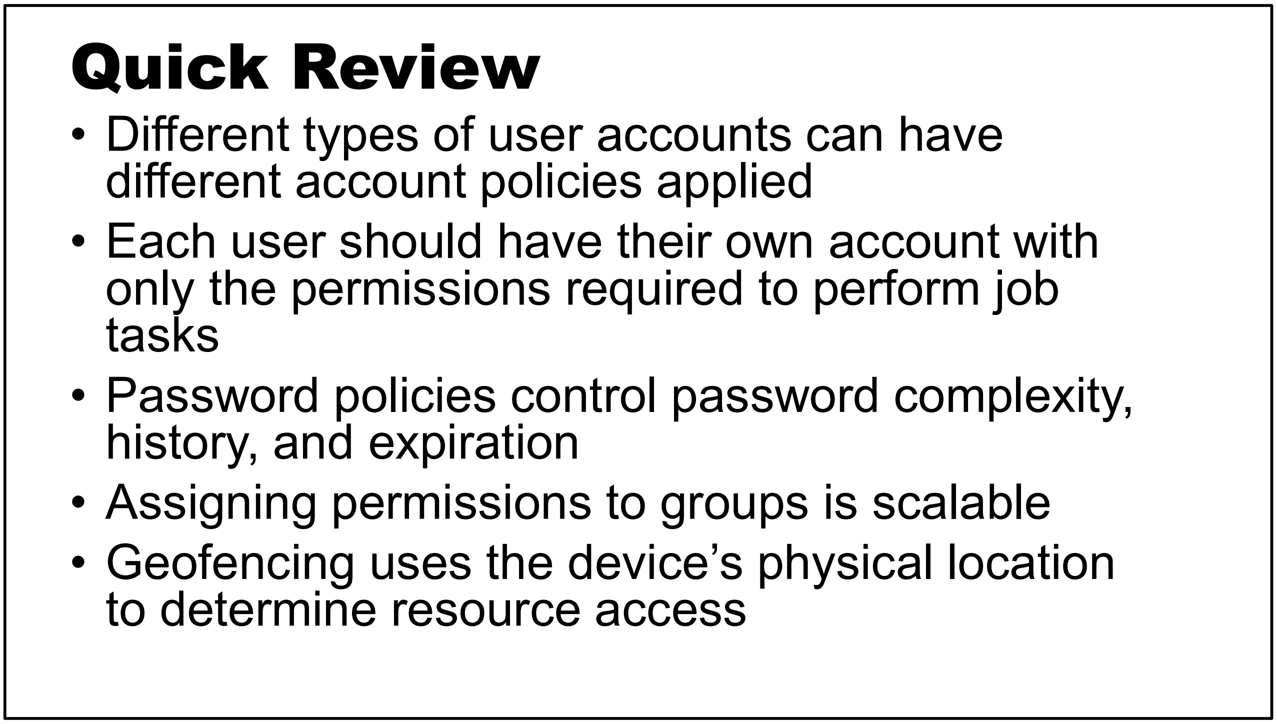
Account Policies

- Employee onboarding
- Password policies
  - Complexity
  - History
  - Reuse
- Account lockout
- Time-based logins
  - Enforce login/logout times



Account Policies

- Geolocation
  - Where a user is located
  - Geofencing
    - User geolocation determines resource access
  - Geotagging
    - Adding location metadata to files and social media posts
- Impossible travel time
- Risky login
  - A baseline of normal activity is required first



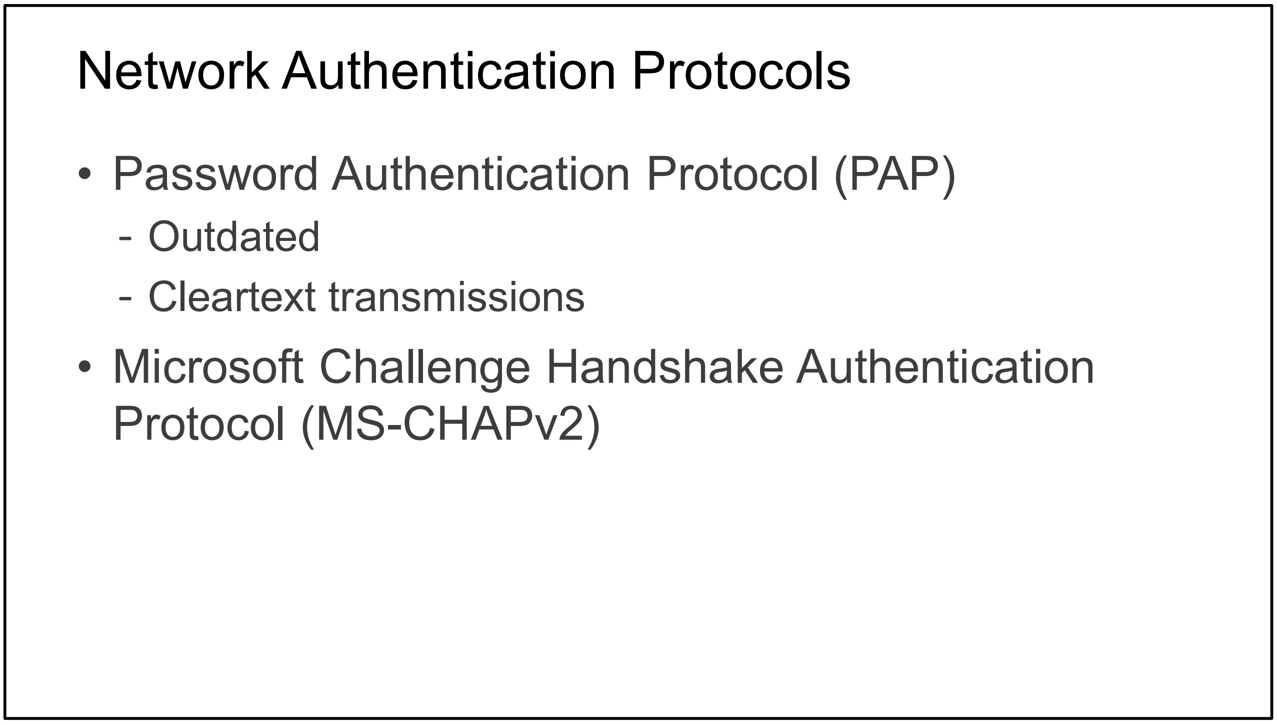
Quick Review

- Different types of user accounts can have different account policies applied
- Each user should have their own account with only the permissions required to perform job tasks
- Password policies control password complexity, history, and expiration
- Assigning permissions to groups is scalable
- Geofencing uses the device’s physical location to determine resource access

Episode 3.08

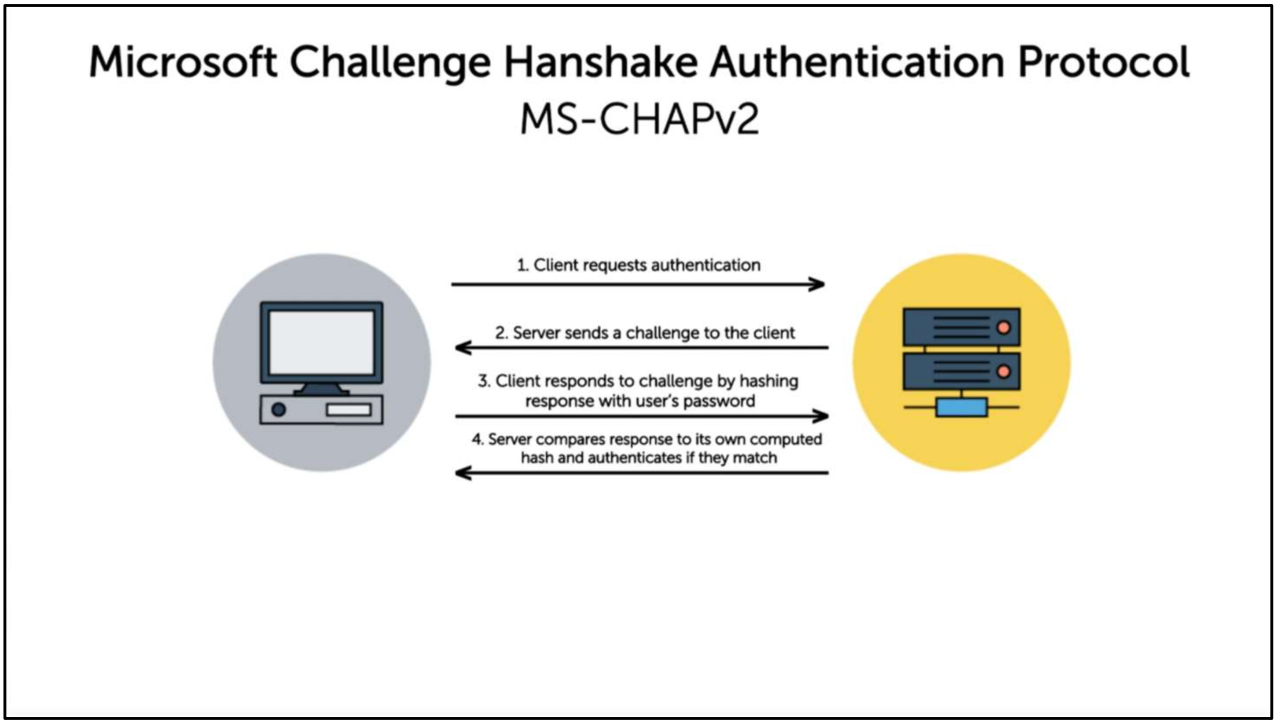
Episode title: **Network Authentication**

Objective: **3.8 Given a scenario, implement authentication and authorization solutions.**



Network Authentication Protocols

- Password Authentication Protocol (PAP)
  - Outdated
  - Cleartext transmissions
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2)



Microsoft Challenge Hanshake Authentication Protocol

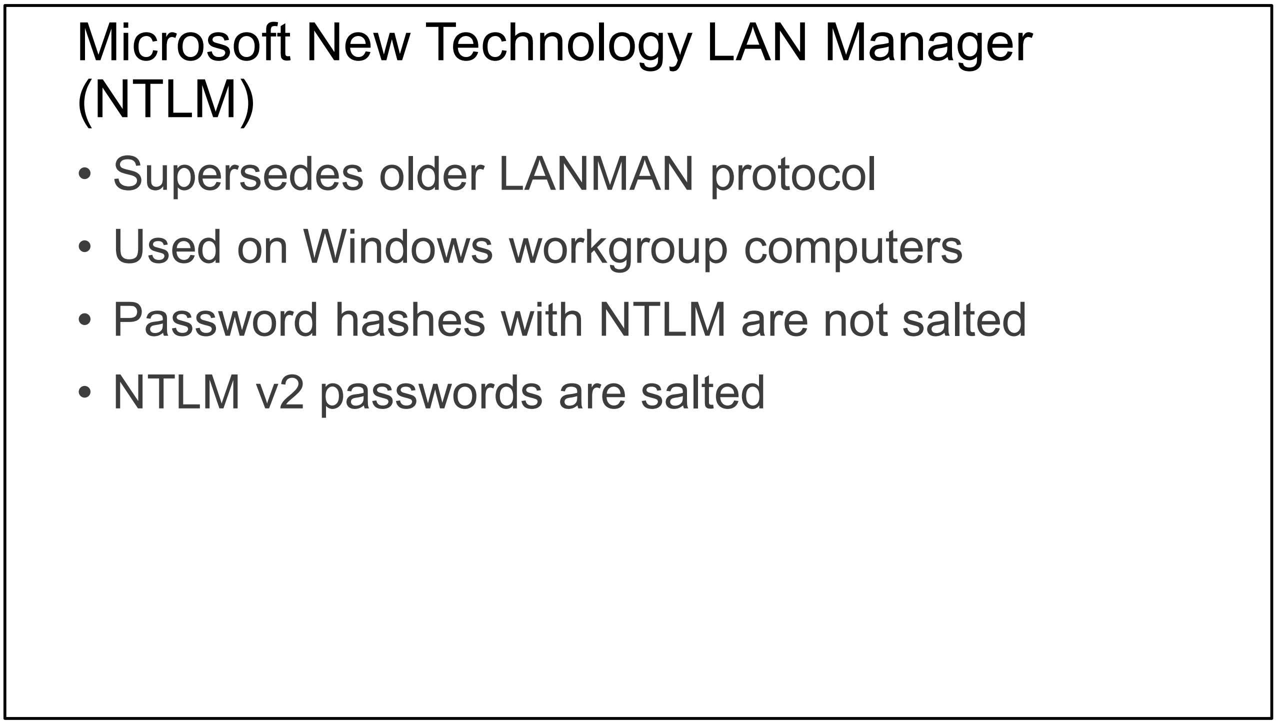
MS-CHAPv2

1. Client requests authentication

2. Server sends a challenge to the client

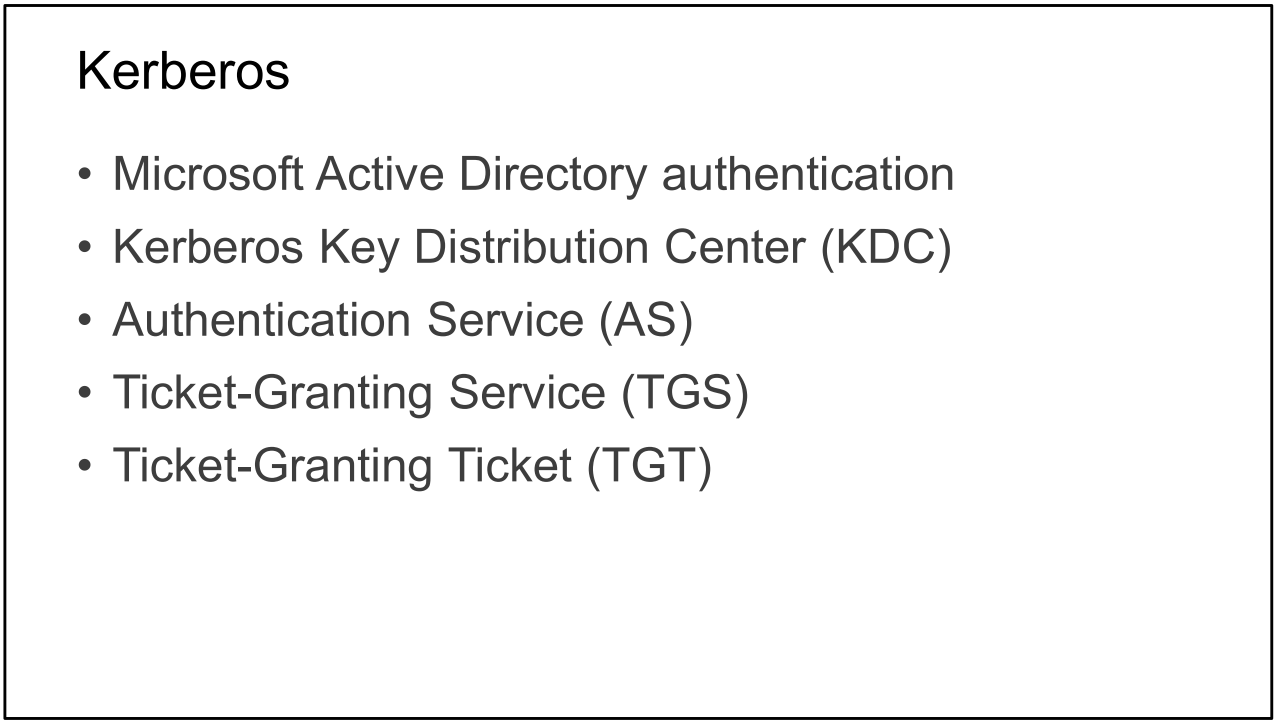
3. Client responds to challenge by hashing response with user's password

4. Server compares response to its own computed hash and authenticates if they match



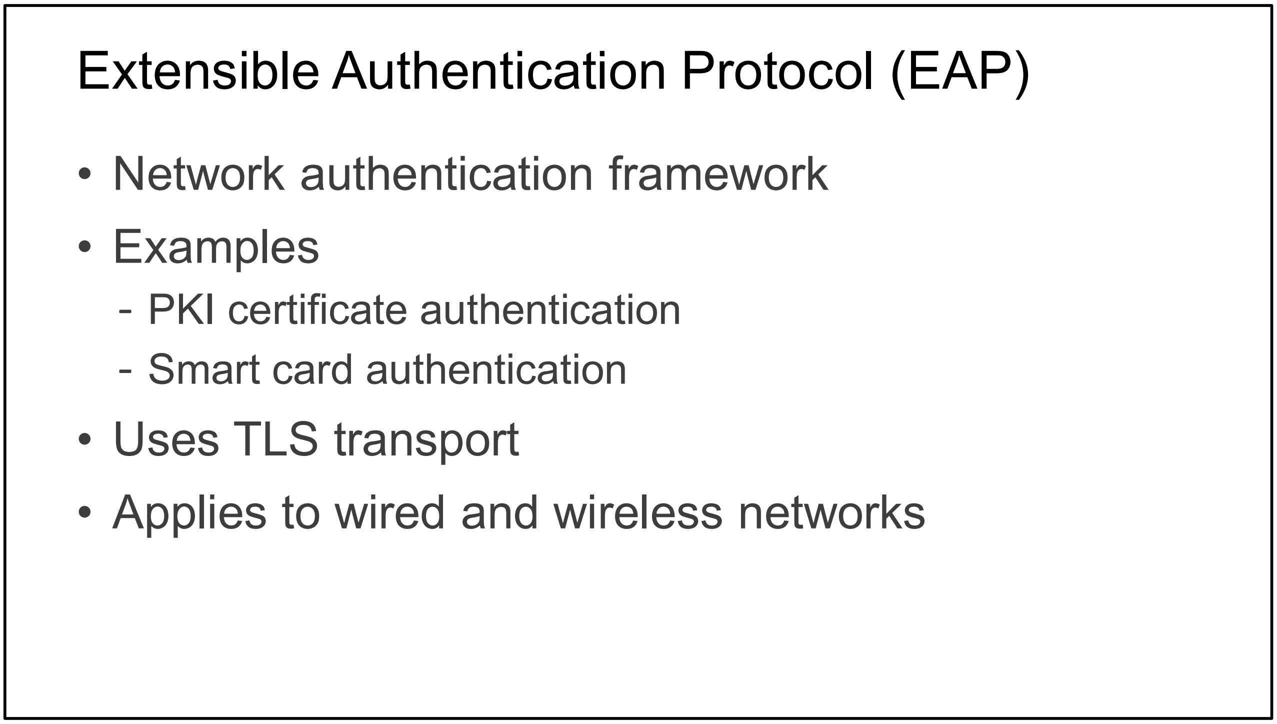
Microsoft New Technology LAN Manager (NTLM)

- Supersedes older LANMAN protocol
- Used on Windows workgroup computers
- Password hashes with NTLM are not salted
- NTLM v2 passwords are salted



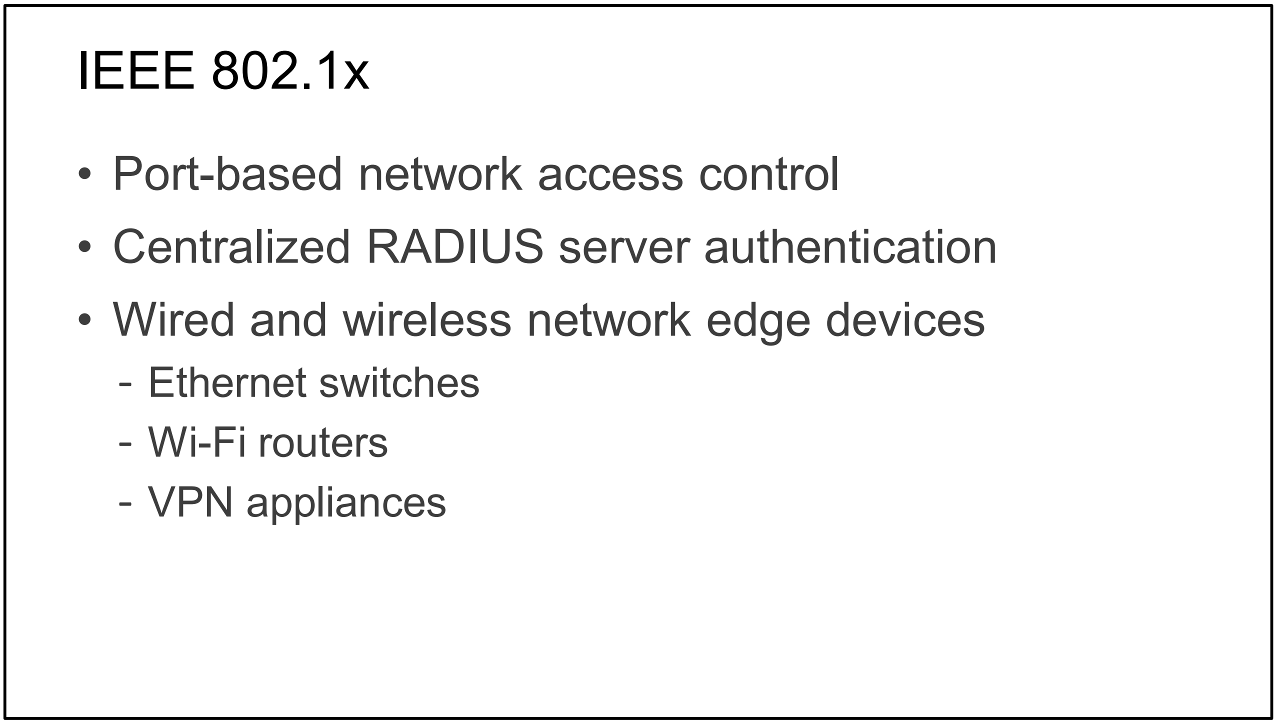
Kerberos

- Microsoft Active Directory authentication
- Kerberos Key Distribution Center (KDC)
- Authentication Service (AS)
- Ticket-Granting Service (TGS)
- Ticket-Granting Ticket (TGT)



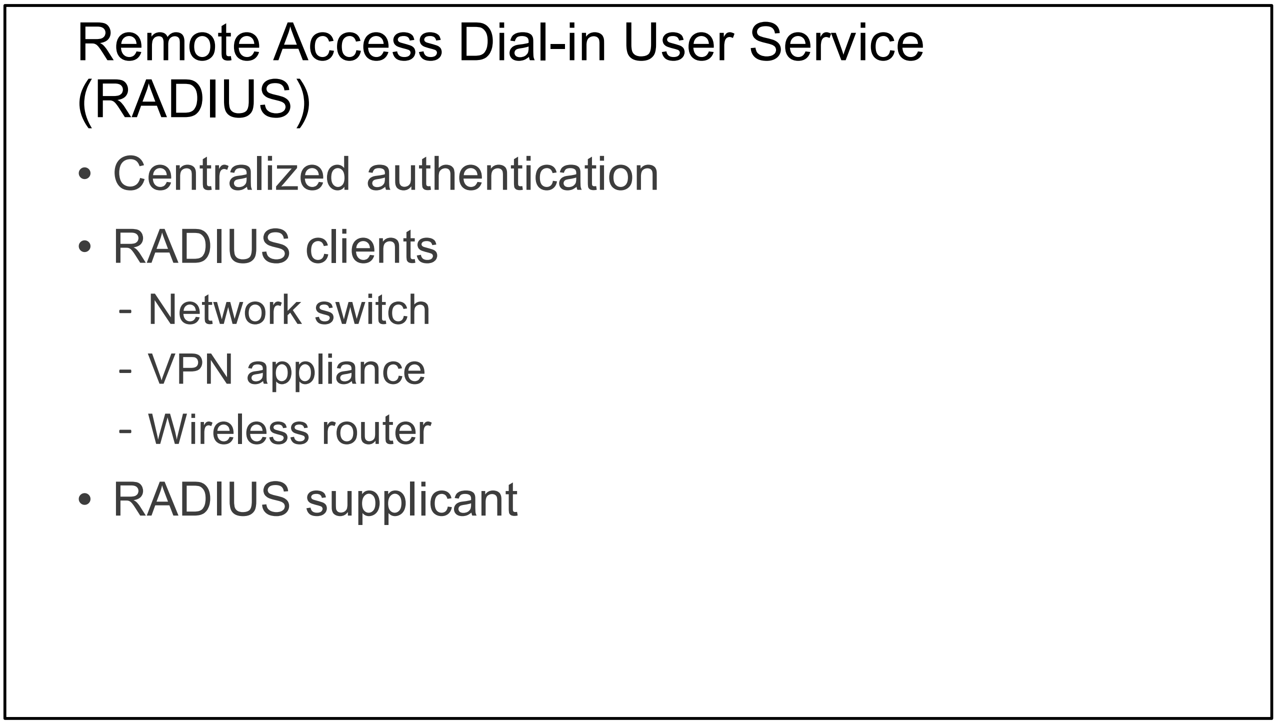
Extensible Authentication Protocol (EAP)

- Network authentication framework
- Examples
  - PKI certificate authentication
  - Smart card authentication
- Uses TLS transport
- Applies to wired and wireless networks



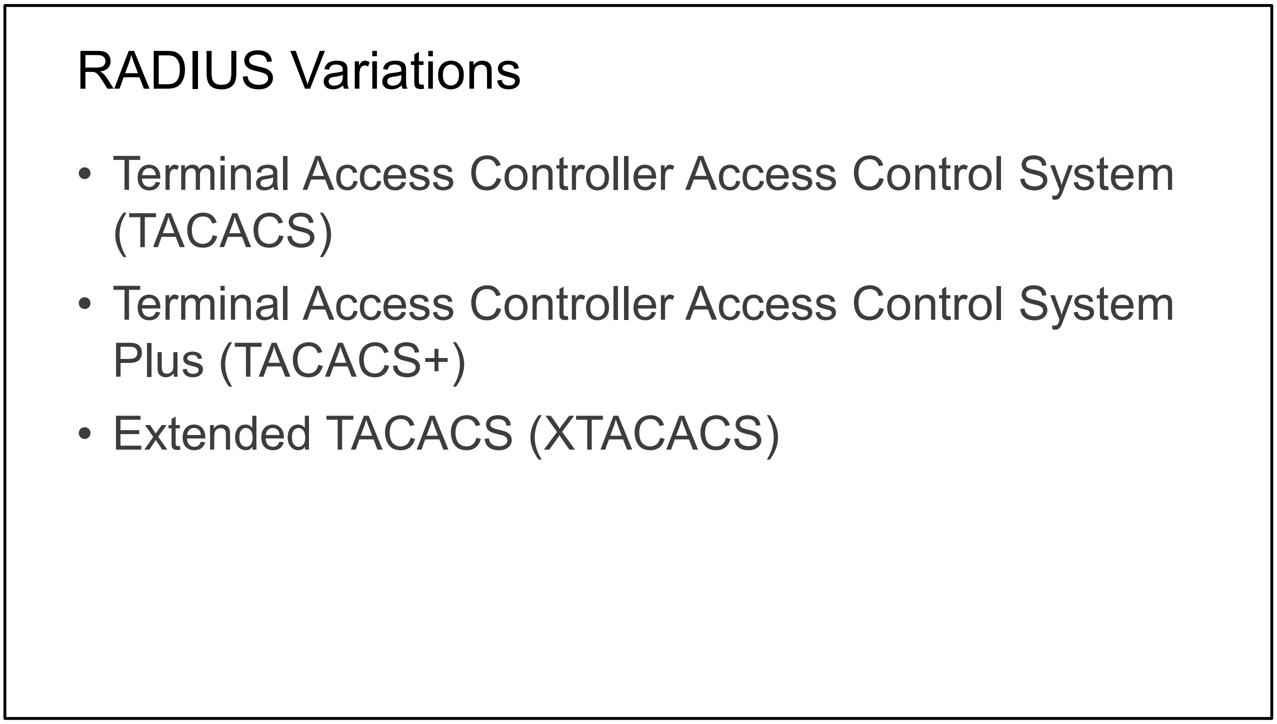
IEEE 802.1x

- Port-based network access control
- Centralized RADIUS server authentication
- Wired and wireless network edge devices
  - Ethernet switches
  - Wi-Fi routers
  - VPN appliances



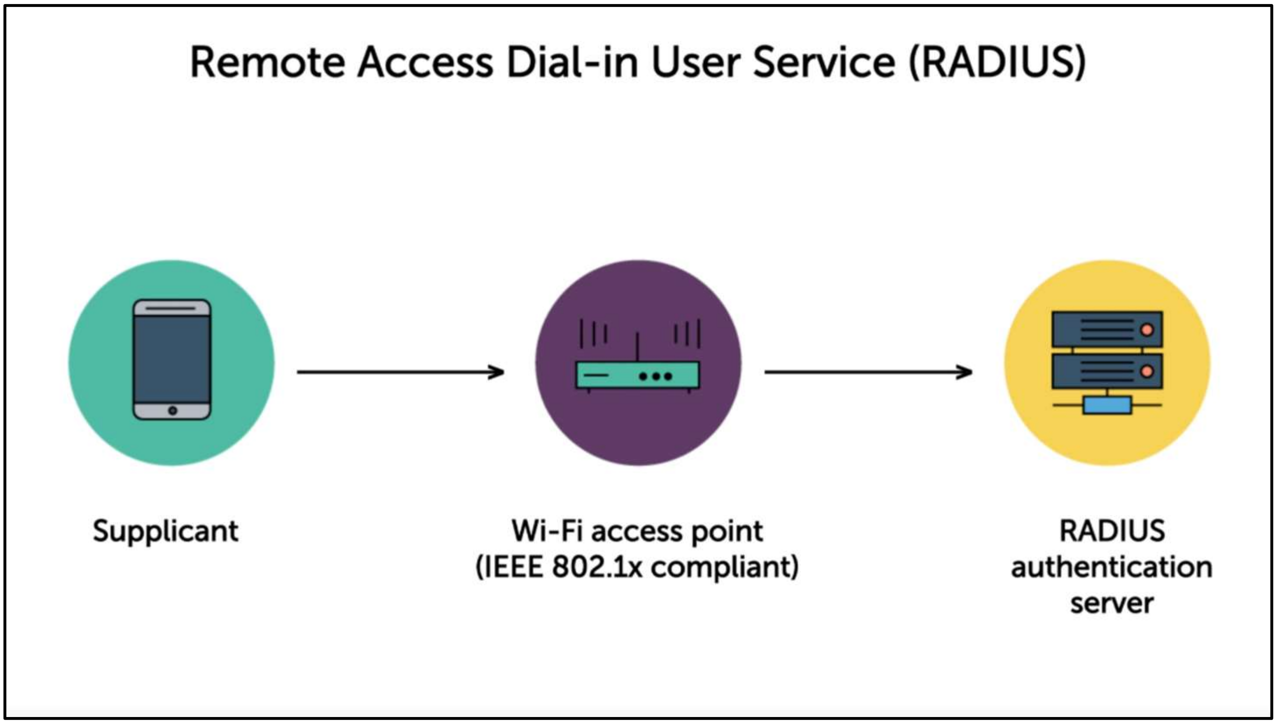
Remote Access Dial-in User Service (RADIUS)

- Centralized authentication
- RADIUS clients
  - Network switch
  - VPN appliance
  - Wireless router
- RADIUS supplicant



RADIUS Variations

- Terminal Access Controller Access Control System (TACACS)
- Terminal Access Controller Access Control System Plus (TACACS+)
- Extended TACACS (XTACACS)

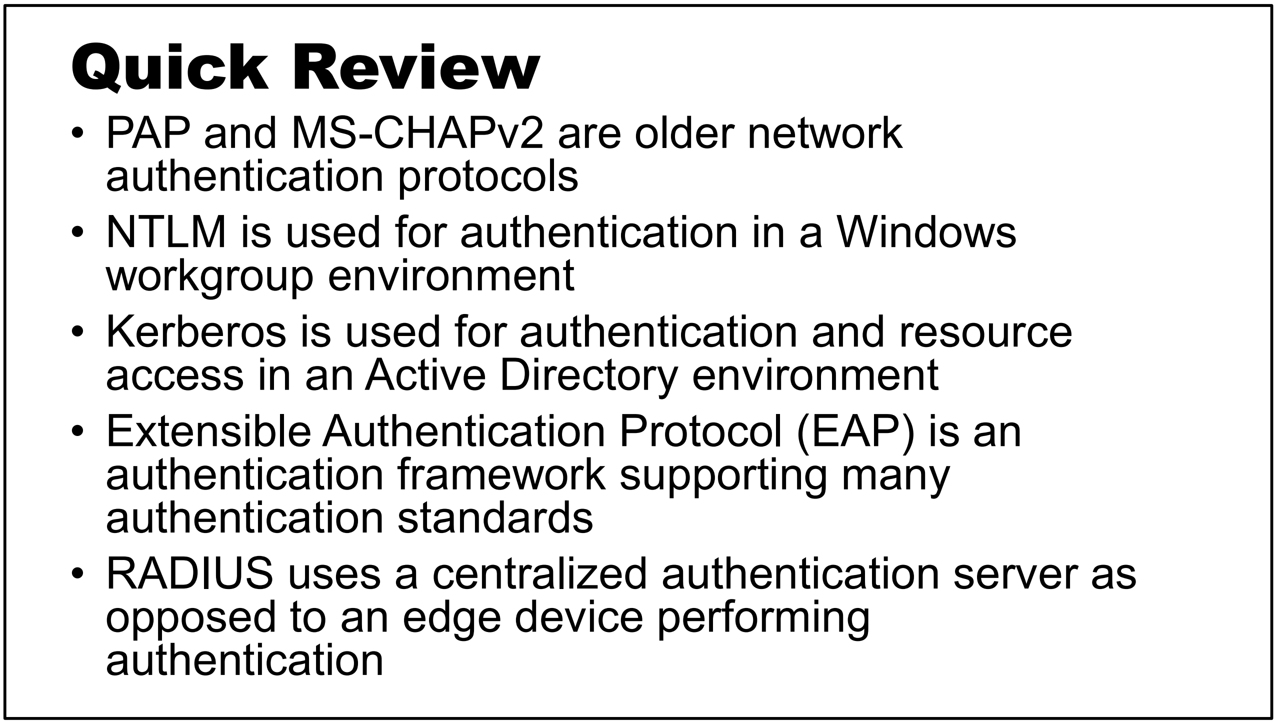


Remote Access Dial-in User Service (RADIUS)

Supplicant

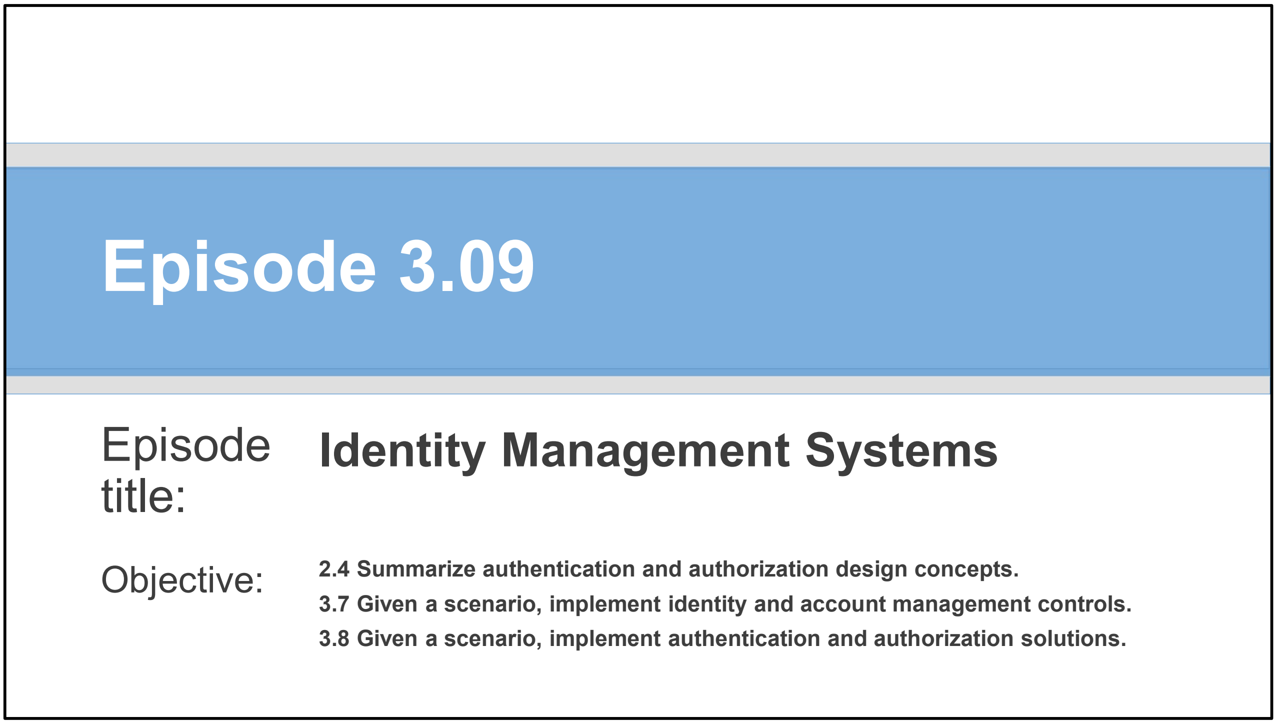
Wi-Fi access point
(IEEE 802.1x compliant)

RADIUS
authentication
server



Quick Review

- PAP and MS-CHAPv2 are older network authentication protocols
- NTLM is used for authentication in a Windows workgroup environment
- Kerberos is used for authentication and resource access in an Active Directory environment
- Extensible Authentication Protocol (EAP) is an authentication framework supporting many authentication standards
- RADIUS uses a centralized authentication server as opposed to an edge device performing authentication



Episode 3.09

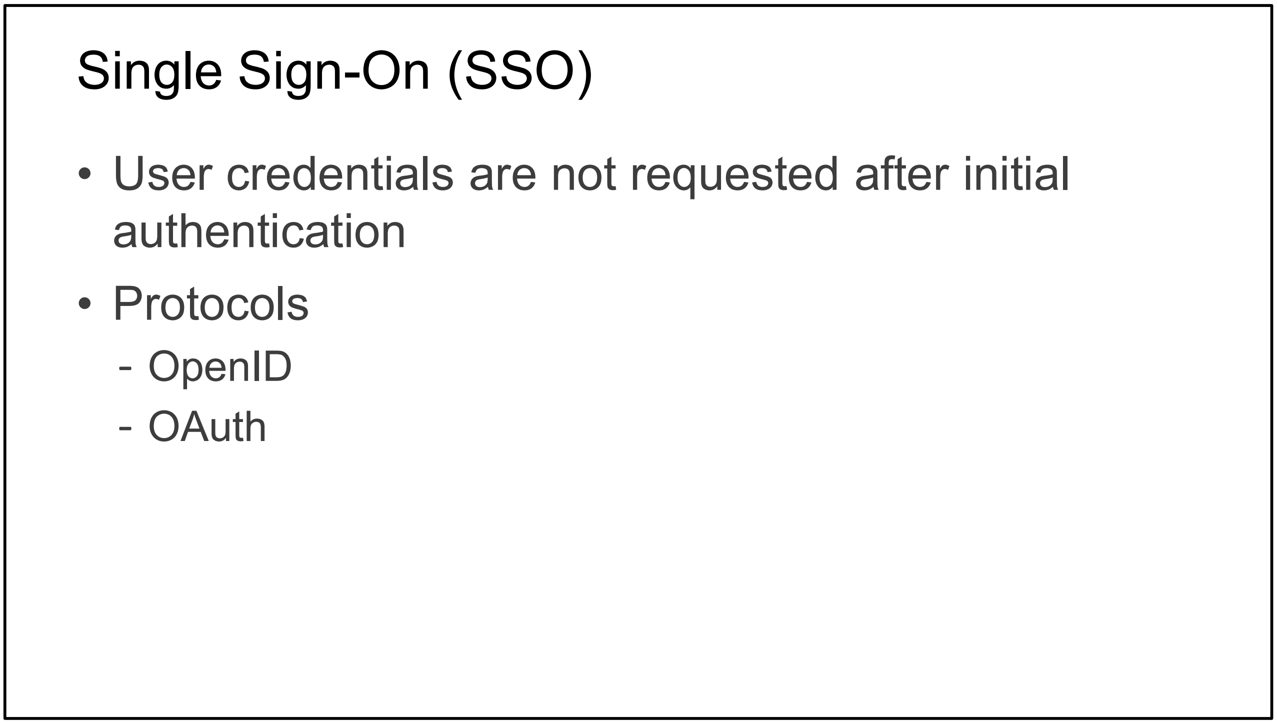
Episode title: **Identity Management Systems**

Objective:

2.4 Summarize authentication and authorization design concepts.

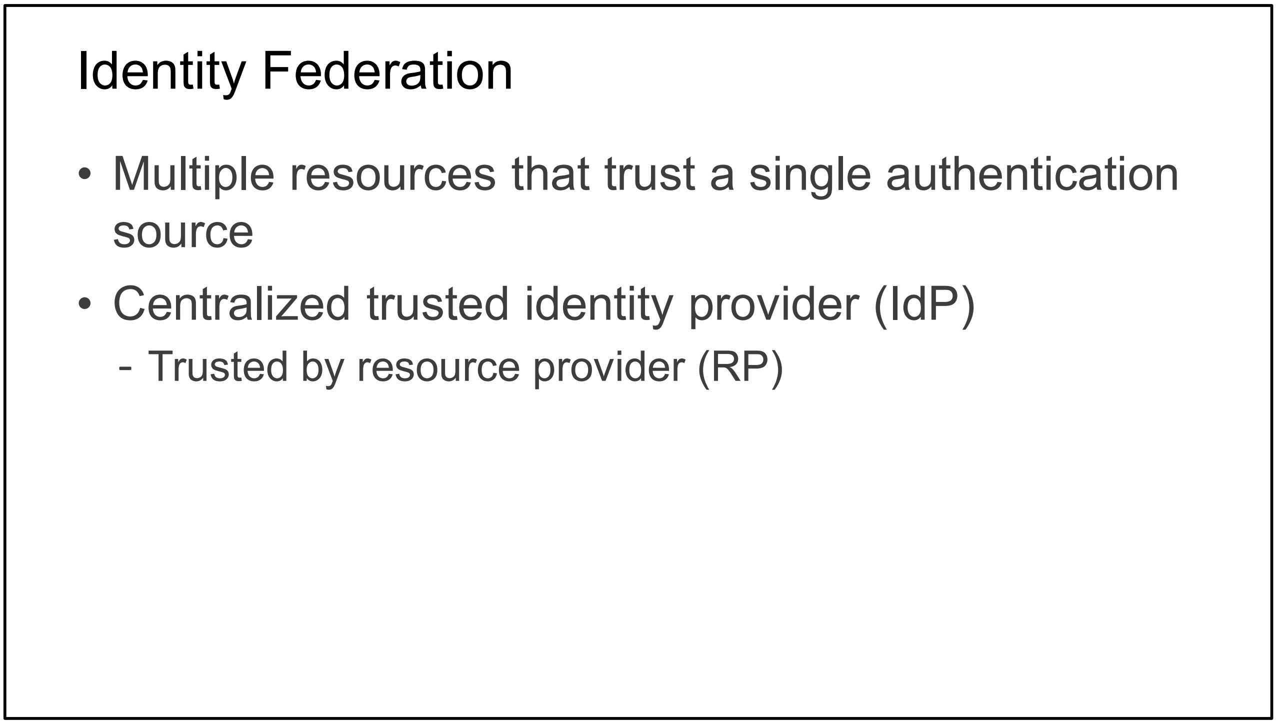
3.7 Given a scenario, implement identity and account management controls.

3.8 Given a scenario, implement authentication and authorization solutions.



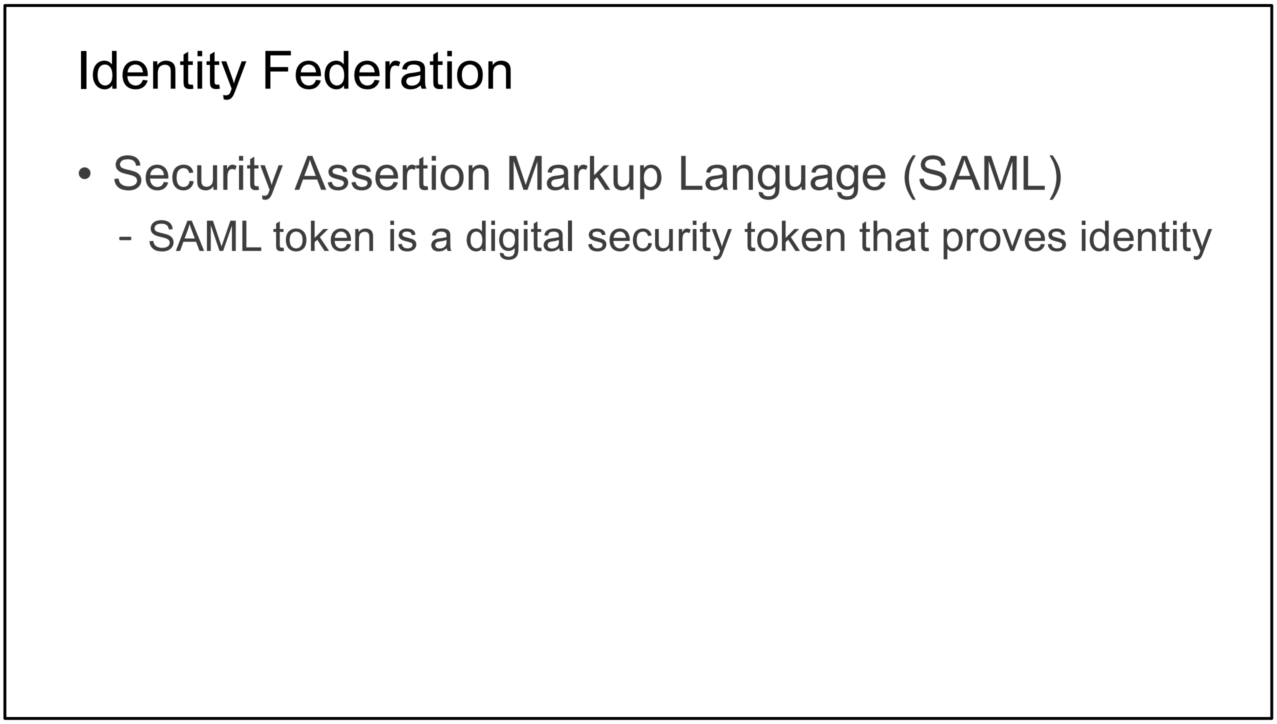
Single Sign-On (SSO)

- User credentials are not requested after initial authentication
- Protocols
  - OpenID
  - OAuth



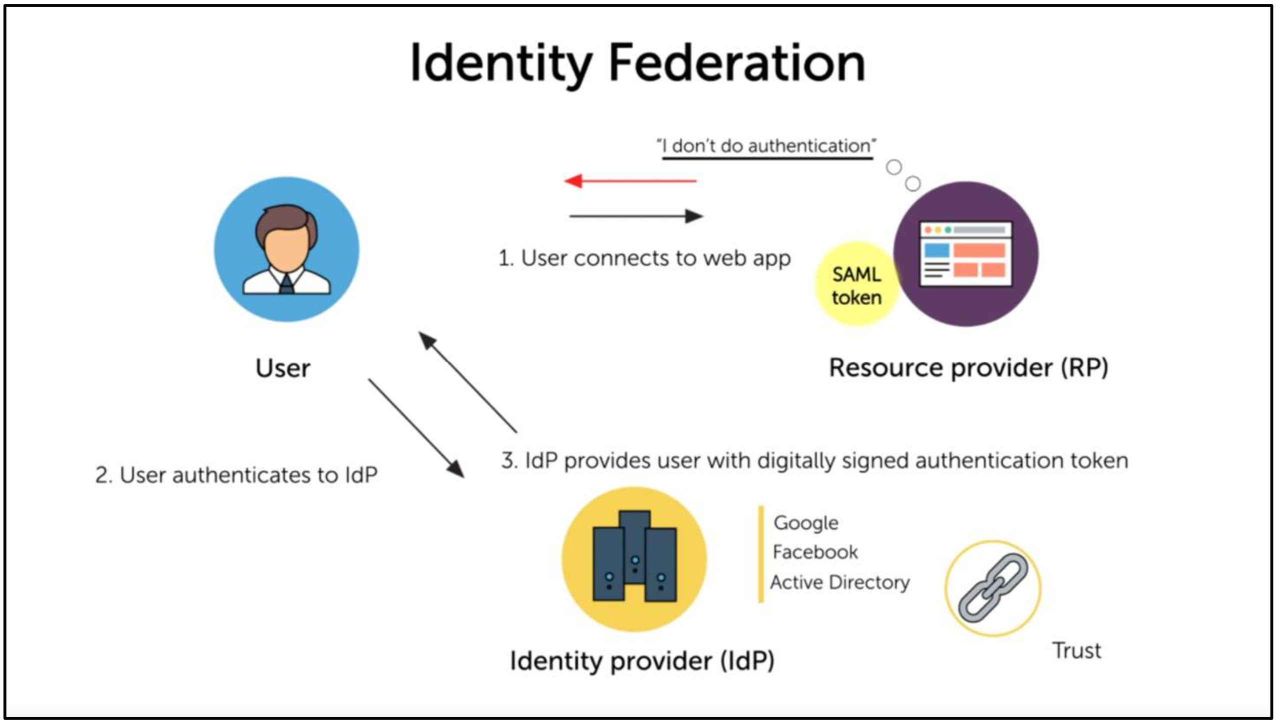
Identity Federation

- Multiple resources that trust a single authentication source
- Centralized trusted identity provider (IdP)
  - Trusted by resource provider (RP)



Identity Federation

- Security Assertion Markup Language (SAML)
  - SAML token is a digital security token that proves identity



Identity Federation

"I don't do authentication"

User

1. User connects to web app

SAML token

Resource provider (RP)

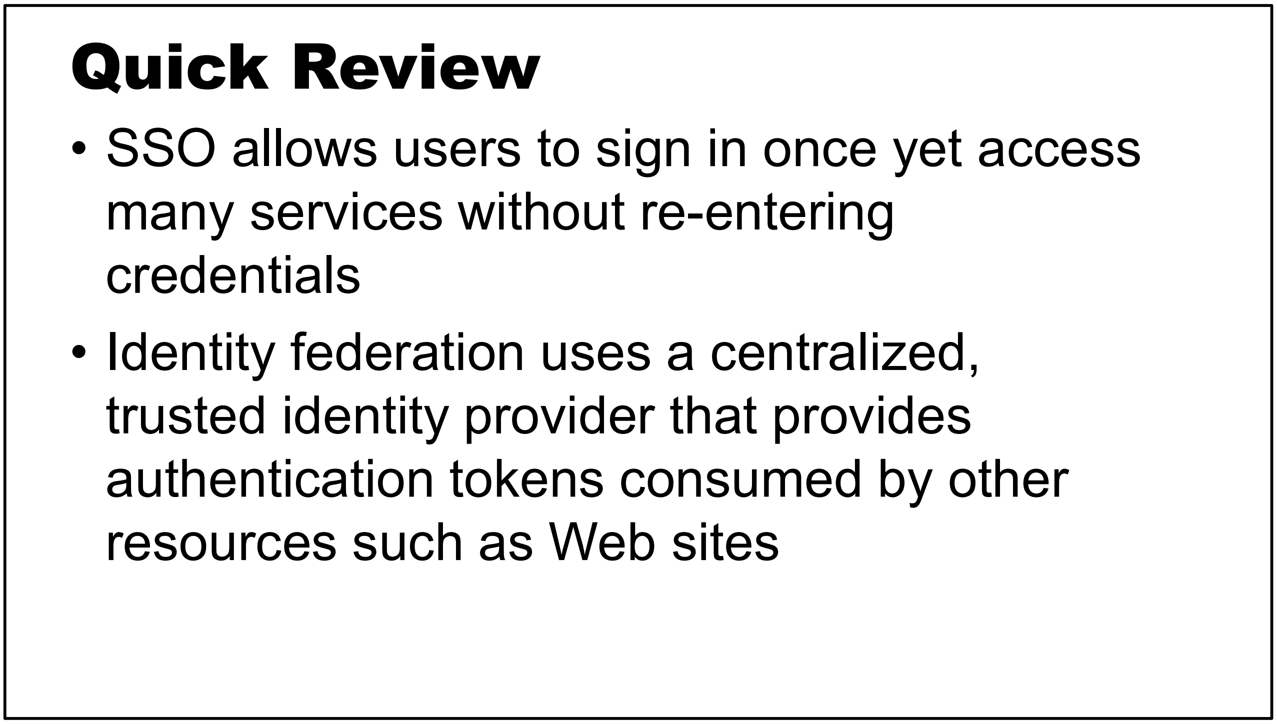
2. User authenticates to IdP

3. IdP provides user with digitally signed authentication token

Google
Facebook
Active Directory

Trust

Identity provider (IdP)



Quick Review

- SSO allows users to sign in once yet access many services without re-entering credentials
- Identity federation uses a centralized, trusted identity provider that provides authentication tokens consumed by other resources such as Web sites