

Lecture 3 - notes

1. Importance of Authentication

- Confirms identity before granting access to systems.
- Prevents data breaches, malware installation, and regulatory noncompliance.
- Involves three steps:
- Identification: Username
- Authentication: Password, biometrics, or device
- Authorization: Verifies access rights

2. Core Authentication Operations

- Registration: Create identity, hash password, add salt, setup MFA.
- Authentication: Verify credentials via hashing and comparison.
- Recovery: Secure methods to regain access (email, backup codes, etc.).

3. Authentication Methods

- Password-based: Common but vulnerable.
- Certificate-based: Uses digital certificates.
- Biometric: Fingerprint, face scan.
- Token-based: Time-based one-time PIN (TOTP).
- OTP: Delivered via SMS/email.
- Push Notification: Approve/deny login.
- Voice Authentication: Verbal confirmation.
- Multifactor Authentication (MFA): Combines two or more methods.

4. Threats to Passwords

- Brute force & hash cracking
- Offline attacks
- Phishing, keyloggers, sniffers
- Password recovery abuse
- Social engineering
- Reuse of passwords
- Default passwords
- Passwords embedded in code

5. Keylogger Threats

- Hardware: Physical devices between keyboard and computer.
- Software: Form-grabbing, JavaScript injection, API hooks.
- Detection: Lag, unknown processes, elevated traffic.
- Prevention: Firewalls, updates, MFA, cautious behaviour.

6. Password Reuse Statistics

- ~57% of users reuse passwords across accounts.
- Main reasons: convenience, memory anxiety.
- Increases risk of credential stuffing.

7. Prevention Strategies

- Use 2FA/MFA
- Go password less
- Ban weak passwords
- Enable risk-based MFA
- Deploy SSO
- Apply least privilege principle
- Conduct regular audits
- Monitor suspicious activity

8. Secure Password Storage

- Hashing: One-way, preferred over encryption.
- Salting: Unique value per user to prevent reuse.
- Peppering: Shared secret not stored in DB.
- Work Factor: Adjust hashing difficulty.
- Legacy Hashes: Rehash on login or force reset.

9. Two-Factor Authentication (2FA)

- Combines:
- Something you know (password)
- Something you have (device)
- Something you are (biometric)
- Common methods:
- SMS codes
- TOTP apps
- Push notifications
- Hardware tokens
- Biometric + PIN

10. SMS-based 2FA

- Pros: Accessible, easy to deploy.
- Cons: Vulnerable to:
- SIM swapping
- MitM phishing
- SS7 exploits
- Recommendation: Use as fallback; prefer app/hardware-based 2FA.

11. Best Practices

- Educate users
- Use open standards (TOTP, FIDO2)
- Secure shared secrets
- Enable adaptive authentication
- Plan for password less future (e.g., passkeys)