Sistemi di Autenticazione e MFA

Modulo TPSIT: Dalla Teoria all'Implementazione

Prof. Capolupo

3 marzo 2026

1. Identificazione vs Autenticazione

Identificazione: "chi sei"? (es. nickname, username).
Autenticazione: "chi certifichi di essere" (es. SPID)

I Tre Fattori di Autenticazione:

- **Conoscenza:** Qualcosa che **sai** (Password, PIN).
- **Inerenza:** Qualcosa che **sei** (Impronta digitale, iride, riconoscimento facciale).
- **Possesso:** Qualcosa che **possiedi** (Smartphone, Smart card, Token USB).

Esempio: In un portale sanitario (Traccia 2024), l'inserimento dello SPID combina conoscenza (password) e possesso (codice su app).

2. Multi-Factor Authentication (MFA)

Definizione: Uso combinato di almeno due fattori appartenenti a categorie diverse.

- **Perché usarla?** Se una password viene rubata (data breach), l'attaccante non può accedere senza il secondo fattore fisico o biometrico.
- **Meccanismi comuni:**
  - **OTP (One-Time Password):** Codice usa e getta via SMS.
  - **TOTP (Time-based OTP):** Codice che scade ogni 30-60 secondi (es. Google Authenticator).

Esempio: Per gestire da remoto i server delle start-up (Traccia 2018), MyStart richiede una password e un codice TOTP per evitare accessi non autorizzati via SSH.

3. Architettura AAA / RADIUS

Per gestire l'autenticazione su larga scala si usa il modello **AAA**:

1. **Authentication:** Chi sei?
2. **Authorization:** Cosa puoi fare? (Permessi).
3. **Accounting:** Cosa hai fatto? (Log degli accessi).

Protocollo RADIUS: Standard per centralizzare questi processi.

Esempio (Traccia 2016): Nel centro residenziale, un server RADIUS può autenticare gli utenti WiFi e tenere traccia di quanto traffico generano (Accounting).

4. Hashing e Salting delle Password

Le password **non** vanno mai salvate in chiaro nel Database.

- **Hashing:** Trasformazione unidirezionale della password in una stringa fissa (es. usando SHA-256 o BCrypt).
- **Salt:** Aggiunta di una stringa casuale alla password prima dell'hashing per prevenire attacchi con *Rainbow Tables*.

Esempio: Il database della Regione (Traccia 2024) memorizza solo l'*hash* delle password dei medici. Se il DB venisse rubato, le password reali resterebbero protette.

5. Inerenza e GDPR

L'autenticazione biometrica è potente ma solleva questioni di privacy.

- **Vantaggi:** Impossibile da dimenticare o smarrire.
- **Svantaggi:** Se un dato biometrico viene compromesso, non può essere "cambiato" come una password.
- **Normativa:** Il GDPR impone che i dati biometrici siano trattati come dati sensibili (particolari).

Esempio: L'accesso ai locali tecnici della sala server (Traccia 2018) tramite impronta digitale deve prevedere la cifratura del template biometrico per rispettare la normativa sulla privacy.