Authentication (Password)

Friday, 26 January 2018 12:43 PM

- Information/ Person is indeed what it claims to be
- Authenticity implies integrity
- Works two ways, Alice vs. IVLE

Password

1. Bootstrapping
    - Establish password by sending via another comunicator
    - Default Password
    - Can be attacked
2. Password Authentication
    - Replay Attack (copy passcode)
    - Weak authentication
        - vs. Strong authentication (covered later)
    - Sniff and spoof
    - Guess from social information, dictionary attack

Attacks

- Bootstrap attack
- Social engineering, dictionary attack
- Side Channel Attack
    - Use information from physical surroundings
- Phishing vs. Spear phishing (targeted)
    - Vishing (Voice)
    - Smishing (SMS0
- Likelihood of attacks? Especially expensive zero-day vulnerabilities

Preventive Measures

- Strong passwords (guided by organisational password policy)
- Password files should be encrypted (or store hash + ID)
- Security Questions: fallback authentication/ self-service pw reset
    - Increase usability and reduces operational helpdesk costs
    - Opens another door for attackers to target
- ATM Cards: magnetic stripes follow a standard ISO protocol
    - Data can be copied to the spoofed card
    - ATM skimmer
        - Fake ATM -> fake ATM skimmer

Biometrics

- Password derived from physical appearance (who you are)
- Identification (recognition from database), verification (authentication)
- Type I vs. Type II error
    - False match/ non-match rate (FMR, FNMR)
- Liveness detection (fake fingers/ sending in password) via temperature, etc
- Cannot be revoked, unlike passwords

n-FA

- What you know (pw, pin)

- What you have (OTP): time-based more common
    - Secret key cannot be retrieved
- Who you are (biometric)