Autentisering, PKI och åtkomstkontroll

Del av kursen ETE352 Cybersäkerhet – grunder och medvetenhet som ges vid Linköpings universitet

Mikael Asplund

LINKÖPINGS UNIVERSITET

Autentisering

- Inte en egenskap utan en mekanism
  - Autenticitet finns som begrepp

- Kan användas för
  - Användare
  - Meddelanden
  - Interaktioner

Användarautentisering

- Att *säkerställa* identiteten för en användare

- Autentiseringsfaktorer
  - Kunskap – lösenord, pinkod
  - Besittning – telefon, säkerhetsdosa
  - Inneboende – biometri
  - Plats eller annan context

- Enfaktors eller flerfaktorautentisering

Meddelandeautentisering

- Att säkerställa riktigheten för ett meddelandes ursprung och innehåll

- Säkerställs genom kryptografisk signatur
  - Endast den avsändaren kan skapa signaturen
  - Alla kan verifiera om signaturen stämmer med innehållet

För interaktioner

- Om det inte finns någon användare?
- IoT-enheter som kopplar mot molnet
- Säkerställ att om enhet A tror sig ha interagerat med B så tror sig också B ha interagerat med A

Hantering av kryptonycklar

- Kryptografi nödvändigt för att säkerställa vissa egenskaper
- Hantering av identiteter och kryptonycklar en utmaning
- Grunden i dagens system: Public Key Infrastructure (PKI)

Grundläggande komponenter i PKI

- Publika och privata nycklar
  - Används för att signera och kryptera
- Certifikat för publika nycklar
  - Används för att vet att det är en legitim avsändare
- Certifikatutfärdare (CA)
  - Betrodd part
  - Utfärdar lista med utfärdade/återkallade certifikat

Åtkomstkontroll

- Vem ska ha tillgång till vad?
- Förutsätter fungerande autentisering
- Olika modeller för åtkomstkontroll
  - Roll-baserad (RBAC)
  - Attributbaserad (ABAC)
  - Diskretionär (DAC)

https://cybersakerhet-grund.ida.liu.se

LINKÖPINGS UNIVERSITET