Lyhyt oppimäärä – mistä tietojen salauksessa on oikeasti kyse?

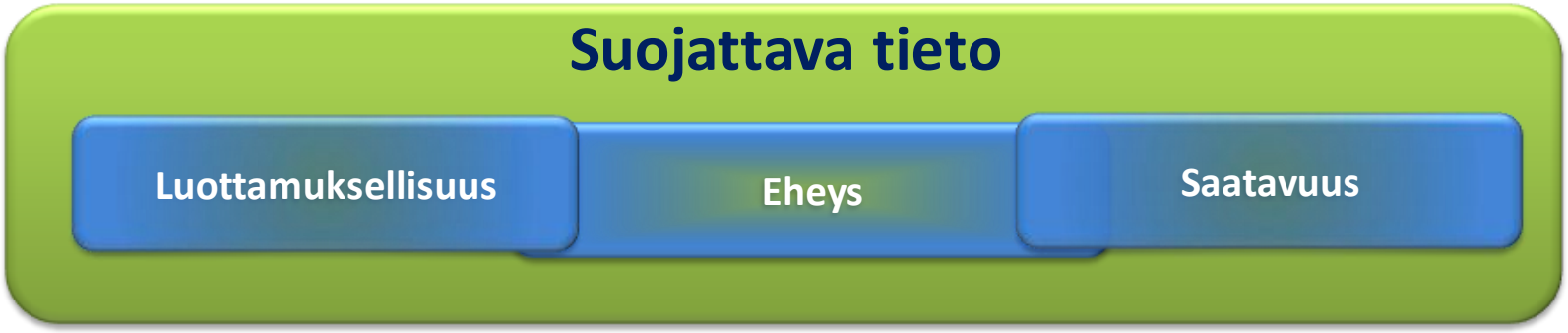
Risto Hakala, risto.hakala@ficora.fi

Kyberturvallisuuskeskus, Viestintävirasto

Sisältö

- Miten tietoa voidaan suojata?
- Mitä yksityiskohtia salausratkaisun toimintaan liittyy?
- Mitkä tekijät vaikuttavat salausratkaisun valintaan?
- Mitä haasteita salausjärjestelmän toteutukseen liittyy?
- Mihin suuntaan ala on kehittymässä?

Tietoturvan osa-alueet



Osa-alueiden merkitys riippuu tapauksesta.

Kryptologia

Kryptologia on tiede, joka tutkii

- salausmenetelmiä (kryptografiaa) ja
- salausten murtamista (kryptoanalyysiä).

Kryptografisilla menetelmillä tavoitellaan erityisesti

- luottamuksellisuutta,
- eheyttä ja
- autenttisuutta.

Missä kryptografiaa käytetään?

Kryptografisia menetelmiä käytetään mm.

- tiedon suojaamisessa, kun sitä siirretään yleisen verkon yli tai säilytetään laitteella, sekä
- henkilöiden ja laitteiden autentikoinnissa.

Esimerkkejä: nettipankit, nettikaupat, sirukortit, suojatut WLAN-yhteydet, VPN-yhteydet.

Kryptografiset menetelmät

- Luottamuksellisuus – salausmenetelmät
- Eheys – tiivistefunktiot
- Autenttisuus – sähköiset allekirjoitukset, MAC:t

Menetelmiä voi käyttää myös toisten menetelmien rakennuspalikoina.

Menetelmien lisäksi avaintenhallinnalla on suuri rooli salausjärjestelmissä.

Tunnettuja kryptografisia menetelmiä

- Salausmenetelmiä: 3DES, AES-128, AES-256, ...
- Tiivistefunktioita: SHA-1, SHA-256, SHA-512, ...
- Sähköisiä allekirjoituksia: RSA, DSA, ECDSA, ...
- Avaintenvaihtomenetelmiä: RSA, DH, ECDH, ...

Listaus käytetyistä menetelmistä ei kerro kaikkea.

Protokollat

- Menetelmiä ei valita toisistaan erillään, vaan käytetään jotakin protokollan tarjoamaa yhdistelmää.
- Protokollat sisältävät määrittelyn, miten kryptografisia menetelmiä käytetään yhteyksien suojaamiseen.
- Parametreihin on edelleen kiinnitettävä huomiota.
- Esimerkkejä: WEP, WPA, IPsec, TLS.

Kuvitteellinen VPN-salain

- Käyttää IPsec:iä virtuaalisen yksityisverkon muodostamiseen.
- *"Tieto salataan vahvoilla AES-128- ja SHA-256-algoritmeillä sekä 4096-bittisillä RSA-avaimilla."*
  - » Miten AES-128:ta ajetaan?
  - » Missä SHA-256:ta käytetään?
  - » Miten RSA:ta käytetään?
  - » Miten autentikointi tehdään?
  - » Miten avaintenvaihto tehdään?
  - » Miten avaimet luodaan?

IPsec ja IKEv2 todellisuudessa

- **Salausmenetelmät:** AES-CBC, AES-CTR, AES-GCM, ...
- **Satunnaislukugeneraattorit:** HMAC-SHA-256, HMAC-SHA-512, AES-128-XCBC, ...
- **Autentikointimenetelmät, sym.:** HMAC-SHA-256-128, AES-128-GMAC, ...
- **Autentikointimenetelmät, epäsym.:** RSA-SHA-256, ECDSA-SHA-256 (P-256), ...
- **Avaintenvaihtomenetelmät:** ECDHE (P-256), DH-4096, ...

Salausratkaisun valinta

- Valinnan ja käyttöönoton tulee perustua aina tarveanalyysiin (käyttötilanteet, reunaehdot).
- Kokonaisuudella on merkitystä – tietty menetelmä tai salausratkaisu ei tee järjestelmästä turvallista.
- Algoritmeihin, avainpituuksiin ja muihin konfiguraatioihin vaikuttaa mm.
  - tietojen merkitys,
  - käyttötarkoitus,
  - niihin kohdistuvat uhat ja
  - salausaika.

Salausratkaisu osana kokonaisuutta

Turvallisuuden kannalta merkittävää on myös

- avaintenhallinnan suunnittelu ja toteuttaminen,
- henkilöiden kouluttaminen tiedon ja päätelaitteiden käsittelyyn sekä
- aktiivinen valvonta – työkalut eivät itsessään takaa turvallisuutta.

Mikä tekee salausjärjestelmän toteuttamisesta vaikeaa?

- Menetelmillä on omat konfiguraationsa ja menetelmien tulee toimia yhdessä – toteutuksen kompleksisuus kasvaa.
- Yksityiskohdilla on merkitystä – ei oikaisuja! (WEP:n lyhyt IV)
- Usein on tehtävä kompromisseja käytettävyyden ja turvallisuuden välillä.
- Tekniikan rajat vaikeuttavat toteuttamista.

Tulevaisuuden näkymiä

- Tekniikan ja laskennallisten menetelmien (kvanttilaskenta, pilvet) kehittymisen takia uusia kryptografisia menetelmiä pitää kehittää jatkuvasti.
- Uusia käyttöympäristöjä (pilvet, IoT) ja käyttötapoja kehittyy jatkuvasti.
- Toteutusten ylläpito ja elinkaarenhallinta tulee monimutkaisemmaksi.

Toimiiko tiedonsalaus?

"Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."

— Edward Snowden

Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi