Aalto-universitetet
Högskolan för
teknikvetenskaper

Tietoturva

Jyry Suvilehto

T-110.1100 Johdatus tietoliikenteeseen ja multimediatekniikkaan
kevät 2011

Luennon sisältö

1. Tietoturva, johdanto
2. Tietoturvauhkia
3. Tietoturvaratkaisuja

Osa luennosta perustuu Tuomas Auran ja Timo Kiravuon opetusmateriaaliin
Osa kaavioiden kuvista Public Domainia openclipart.orgin käyttäjiltä ARTMAN ja dur2250

Miksi tietoturva

- Yrityksillä ja yksilöillä on tietoa, jolla on arvoa
  - Voi olla myös dataa tai informaatiota, tässä kontekstissa semantiikka ei niin olennaista
  - Informaatioekonomiasta on tutalla ja Aalto-yliopiston kauppakorkeakoulussa kursseja
  - Esim. kopiointi vähentää (tai ei vähennä) tiedon arvoa
- Koska tiedolla on arvoa, sitä pitää suojata
  - Vaikka tiedolla ei voi tehdä rahaa, sille saatetaan määrittää arvo, esimerkiksi väärinkäytössakolla

Tietoturva vs. Turvallisuus

- Tietoturva on yksi turvallisuuden osa-alue, jota ei voida erottaa suoraan muista osista
  - Jos talo palaa, kyseessä on turvallisuusongelma
  - Jos pankki tositteineen, tietokoneineen ja lokeineen palaa, kyseessä on myös tietoturvaongelma

Terminologiaa

- Suojattavalle kohteelle (engl. Asset) saattaa tapahtua pahoja asioita
- Potentiaalista ei-toivottua tapahtumaa kutsutaan uhkaksi (threat)
- Uhka toteutuessaan aiheuttaa kustannuksen (cost, impact)
- Riski = P(uhka)*C(uhka)
  - Probability, Cost
- Tahallaan toteutettu uhka on hyökkäys
- Haavoittuvuus on ominaisuus joka tekee hyökkäyksestä helppoa

Risk Management

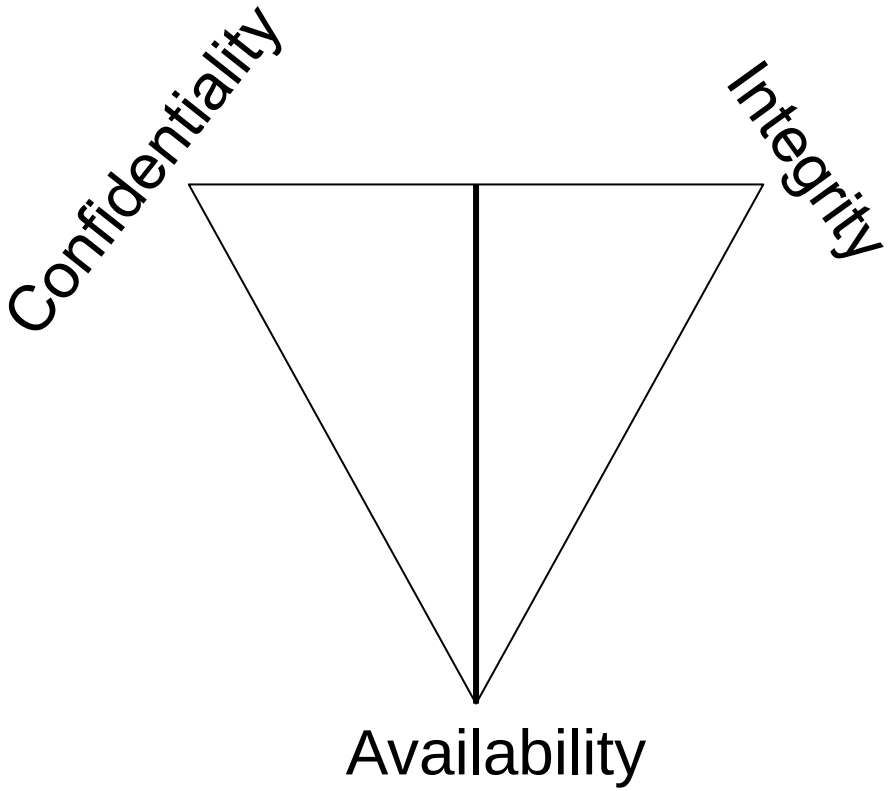
- Ihmiset ovat järjettömän huonoja arvioimaan riskejä intuitiivisesti
  - C(uhka) saa unohtamaan P(uhka):n tasapainottavan vaikutuksen
  - Lento-onnettomuuteen joutuminen
  - Useimmat fobiat
- Evolutiivisesti hyödyllistä
- Kun riskiä ei voida välttää, ihmiset eivät huolehdi
  - Arkipäivän vaarallisuus
  - Padon varjossa asuminen
- Ihmiset haluavat uskoa olevansa turvassa
  - ”security theater” http://en.wikipedia.org/wiki/Security_theater
  - http://xkcd.com/651/

Terminologiaa

- Luottamuksellisuus (Confidentiality):
  - ”Tietoa pääsevät näkemään vain henkilöt, joilla on siihen oikeutus ”
- Eheys (Integrity):
  - ”Vain oikeutetut henkilöt voivat muokata tietoa”
- Saatavuus (Availability)
  - ”Tietoon on mahdollista käsiksi silloin kun sitä tarvitaan”
- Nämä muodostavat tietoturvassa laajasti käytetyn CIA-mallin

CIA-malli

- CIA-mallia voi soveltaa ajattelemalla kolmiota, jonne tieto sijoitetaan
- Osittain harhaanjohtava C ja I eivät aina ole toisensa poissulkevia, CI ja A taas yleensä ovat
- Huono tietoturva-asiantuntija unohtaa tasapainottaa



CIA-malli, esimerkkejä

- Opintorekisterin ja pankkitilin tärkein ominaisuus on eheys
  - Tilille ei tule hyväksymättömiä tapahtumia
- Ennen tenttiä tenttikysymysten luottamuksellisuus on tärkeää
  - Uudet kysymykset voi tehdä nopeasti
  - Kuka haluaisi muuttaa tenttikysymyksiä?
- Noppa-palvelussa ei ole mitään hirveän salaista tai pysyvää
  - Saatavuus on tärkeää

Muita termejä

- CIA-malli ei riitä kaikkeen.
- Oikeutus (authorization)
  - Määritetään kuka saa tehdä ja mitä
- Tunnistaminen (authentication)
  - Tunnistetaan entiteetti jonkin perusteella
- Aitous (authenticity)
  - Onko tieto aitoa
  - Case okcupid
- Kiistämättömyys (non-repudiation)
  - Tapahtumaa ei voi kiistää jälkikäteen

Esimerkkejä

- Opintorekisterijärjestelmässä vain sihteereillä on oikeutus tehdä muutoksia opintosuorituksiin
  - Oletettavasti ei intressejä väärinkäytöksiin
  - Opettajat joutuvat viemään tulokset Oodiin sihteerien kautta
- Pankin kannalta sirukorttijärjestelmän tärkein ominaisuus on kiistämättömyys
  - Jos asiakas onnistuu kiistämään tehneensä maksun, pankki maksaa kauppiaalle
  - CHIP + PIN broken by Murdoch, Anderson & al

Turvallisuuspolitiikka

- Turvallisuuspolitiikka on organisaation (tai yksilön) turvallisuuden suunnittelussa käytetty dokumentti
- Määrittää
  - Suojattavat kohteet
  - Uhat
  - Ratkaisut
- Sisältää
  - Turvallisuuspolitiikan päämäärän
  - Resurssit
  - Vastuut
  - Ohjeet henkilökunnalle
- Teknisen toteutuksen

Miten tehdä turvallisuuspolitiikka

- Arvioi tilanne
  - Suojattavat kohteet
  - Olemassaolevat ratkaisut
- Arvioi riskit
- Päätä resurssit huomioon ottaen miten suojata kohteita

Yleisiä virheitä

- Tehdään asioita ”koska helposti voi”
- Politiikan tekijä päättää informaation arvon
  - Aina omistaja
- Politiikkaa käytetään jonkin oman agendan edistämiseen
  - Usein tietoturvapolitiikka on vallankäytön väline
- Esim. Aalto-yliopistossa opettajat ja tutkijat ovat olemassa täyttääkseen tietoturvapolitiikan vaatimuksen
  - P.o. Aalto-yliopistossa tietoturvapolitiikka on olemassa mahdollistaakseen opetuksen ja tutkimuksen
- Keskitytään tekniseen tietoturvaan
  - Suurin ongelma tietoturvassa...


On aina ihminen
YOU"

Tietoturva vs. käytettävyys

- Tietoturvapolitiikan on tärkeä ottaa ihmiset huomioon
- Ihmiset joko noudattavat ohjeita tai eivät noudata
  - On tietoturvapolitiikan tekijän tehtävä huolehtia siitä, että ohjeita on riittävän helppoa noudattaa
  - Esim. Avainpolitiikka
- Suurin haavoittuvuus ovat itseasiassa hyväntahtoiset käyttäjät (ref: Kevin Mitnick)
- Tietoturvan ja käytettävyyden ei aina ole pakko olla ristiriidassa
- Joskus turvavaatimukset oikeuttavat selkeitä käytettävyyshaittoja
  - Ydinaseiden laukaisukoodit
- Yhdysvalloissa ”kansallinen” ”turvallisuus” oikeuttaa ihan mitä vaan

TIETOTURVAUHKIA

Yleisiä tietoturvauhkia

- Verkkoliikenteen luvaton kuunteleminen
  - Mm. Harkoissa käytetyllä wireshark-ohjelmalla voi kuunnella myös luvattomasti verkkoa
  - Wlan-verkkoa voi kuunnella erityisen helposti
    - Tikkiläisten harrastus
- Valtaosa protokollista on suojaamattomia
- Yllättävän moni protokolla siirtää tunnuksia ja salasanoja selväkielisenä

Lisää uhkia

- Harjoituksissa tulikin jo esille, että sähköpostiviestin lähettäjä on triviaalia väärentää
  - Useissa sähköpostiohjelmissa ”käyttöä helpottava ominaisuus”
- Mikäli sovellus on huonosti tehty, oikeanlaisella sovelluskerroksen viestillä voidaan saada aikaan ongelmia
  - Buffer overflow
  - SQL Injection
    - http://xkcd.com/327/

Uhkakuvia

- Käyttäjien koneelle asentuvat ei-toivotut ohjelmat eli ns. Malware (virukset, vakoiluohjelmat, troijalaiset)
  - Ammattirikollisten heiniä: pankkitunnusten kalastelu ja botnet-hyökkäykset
- Tunnusten kalastelu (phishing)
- Palvelun ylikuormittaminen
  - Voi olla pahantahtoista, esimerkiksi botnetiä käyttämällä
  - Voi olla yllättävä suosion lisääntyminen, nk. Slashdot-efekti

Uhkakuvia

- Identiteettivarkaudet
  - Suomessa henkilön voi mm. Ilmoittaa kuolleeksi tietämällä henkilötunnuksen
    - Henkilötunnuksen saa selville varsin triviaalisti
  - Joissain maissa (Iso-Britannia) ei lainkaan kansallista henkilökorttijärjestelmää
  - Moni paikka perustaa autentikaation tietoihin, jotka julkisesti saatavilla

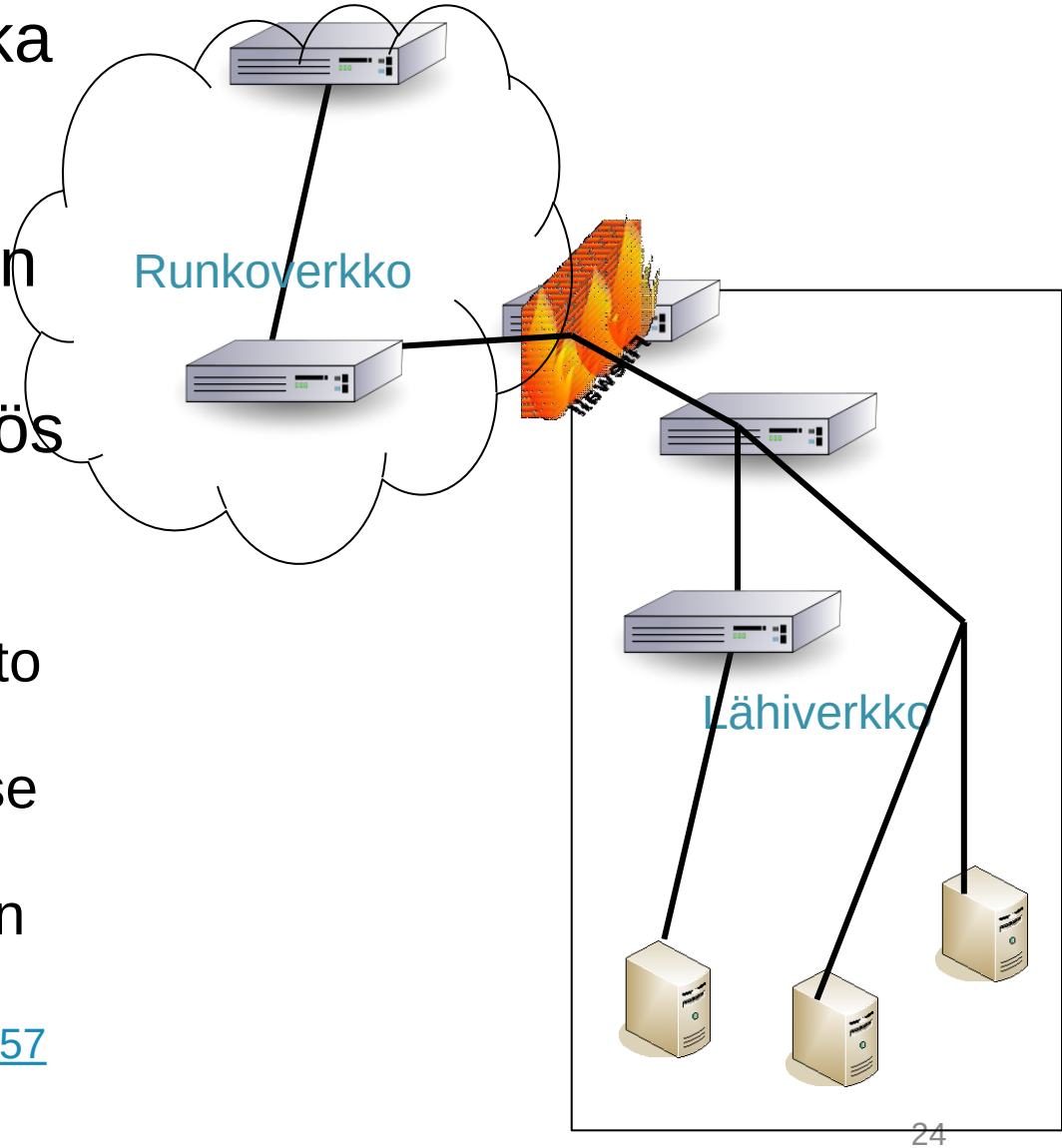
Yksityisyys

- Yksityisyys (privacy) liittyy olennaisesti identiteettivarkauksiin, mutta ei rajoitu siihen
- Onko oikeus tietää kaikki sinusta
  - Valtiolla?
  - Työntantajalla?
  - Vanhemmalla?
  - Vakuutusyhtiöllä?
  - Puolisolla?
  - Lemmenkipeällä tikkiläisellä?
- Yksityisyys on EU:n määrittelemä kansalaisoikeus

TEKNISIÄ RATKAISUJA TIETOTURVAUHKIIN

Palomuuri

- Palomuuri on laite, joka estää määritettyjen sääntöjen mukaan liikenteen verkon osien välillä
- Palomuuri voi olla myös ohjelmisto reitittimessä(vast)
  - Voi olla myös ohjelmisto yksittäisessä tietokoneessa, jolloin se säätelee liikennettä koneen ja muun verkon välillä
- http://www.schneierfacts.com/fact/657

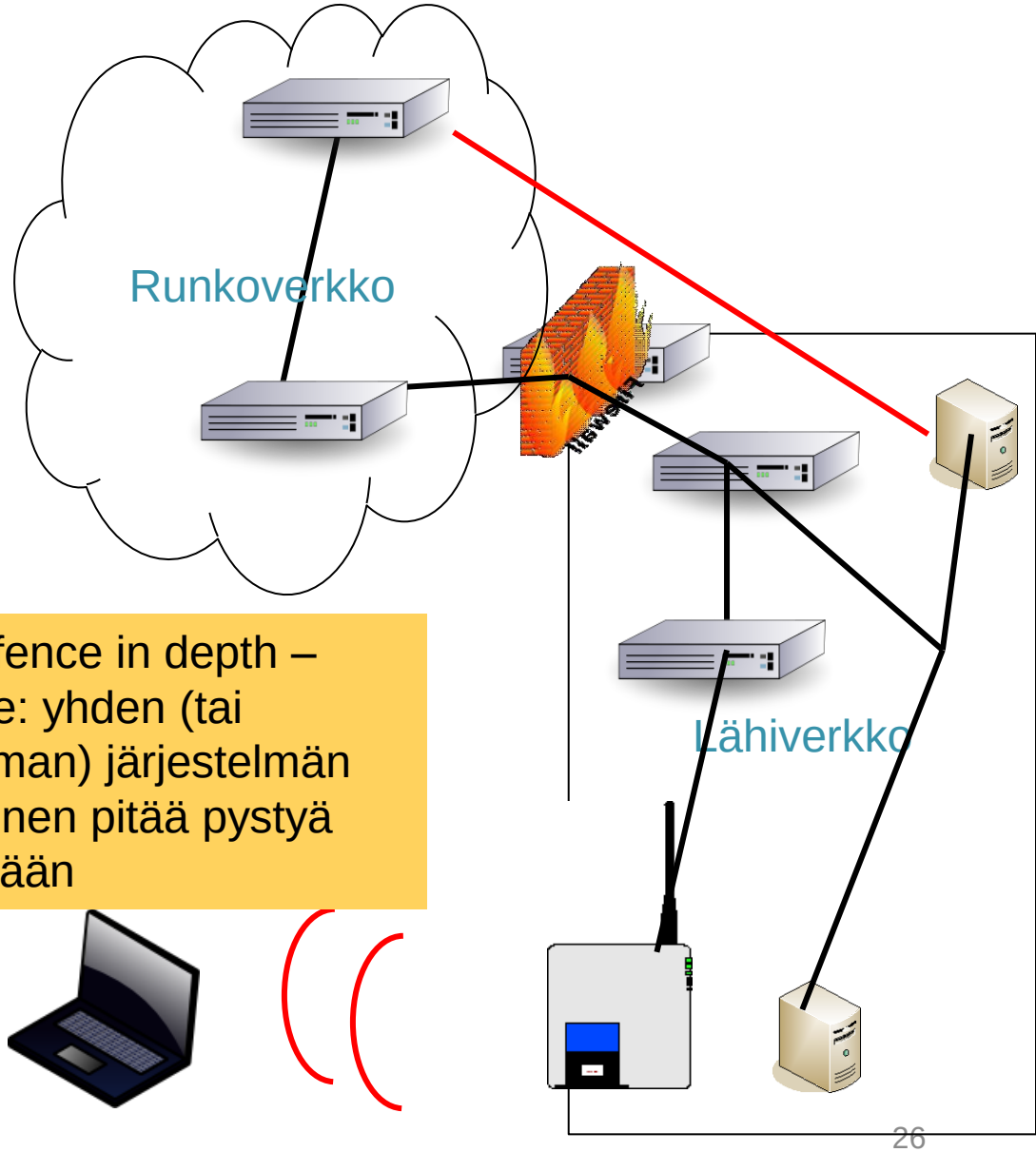


Linkkikerros	Verkkokerros	Kuljetuskerros	Sovelluskerros	Varsinainen data
-	Lähettäjä, vastaanottaja	Portti, TCP tai UDP, TCP:n liput	Protokollatiedot, esim. Tietty url, tietty lähettäjä, vastaanaottaja sähköpostissa	Kielletyt sanat

- Palomuuri tekee reitityspäätöksen eri protokollakerroksen tietojen mukaan
- Mitä korkeammalla tasolla, sitä kalliimpaa suodatus
  - EU:ssa puhutaan ISP-tasolla verkkokerroksen suodatuksesta
  - Kotiverkoissa/yrityksissä vähintään kuljetuskerroksen palomuuri
  - Kiinassa varsinaisen datan perusteella suodatusta

Palomuuri todellisuudessa

- Palomuuri on riittämätön turvaamaan verkon koneet
- Koneiden itsensä pitää olla suojattua koko ulkomaailmaa vastaan
- ”Constant vigilance!”
  - Prof. Alastor Moody



Nk. Defence in depth – periaate: yhden (tai useamman) järjestelmän pettäminen pitää pystyä kestämään

Autentikaatio

- Entiteetin tunnistaminen perustuu kolmeen pilariin
  - Johonkin, mitä entiteetti tietää (salaisuus, salasana, turvakysymykset)
  - Johonkin, mitä entiteetti omistaa (fyysinen avain, avainkortti)
  - Johonkin, mitä entiteetti on (biometrinen tunnistus)
  - Ei ole pakko olla ihminen, myös koneita (tai koiria) pitää tunnistaa
- Kahden tai useamman yhdistämistä kutsutaan usein vahvaksi autentikaatioksi
  - Käytännössä ei aina vahvaa

Hyvistä salasanoista

- Salasanan vahvuus perustuu sen *entropiaan*
  - Pituus ei auta jos esimerkiksi samaa merkkiä toistetaan
- Salasanan monimutkaisuus ja vaihtoväli määritellään tietoturvan tarpeen mukaan
- Ihmiset eivät luonnostaan muista salasanoja
  - Master-salasana avainrenkaalle(vast)
  - Salasanojen kirjoitus ylös
- Jos halutaan että ihmiset vaihtavat salasanansa uusiin, ne pitää saada kirjoittaa ylös
- Jos kielletään salasanojen ylöskirjoitus ja pakotetaan vaihtamaan usein, salasanan uusintamenetelmään pitää panostaa paljon
- http://www.schneierfacts.com/fact/27

Kryptografia

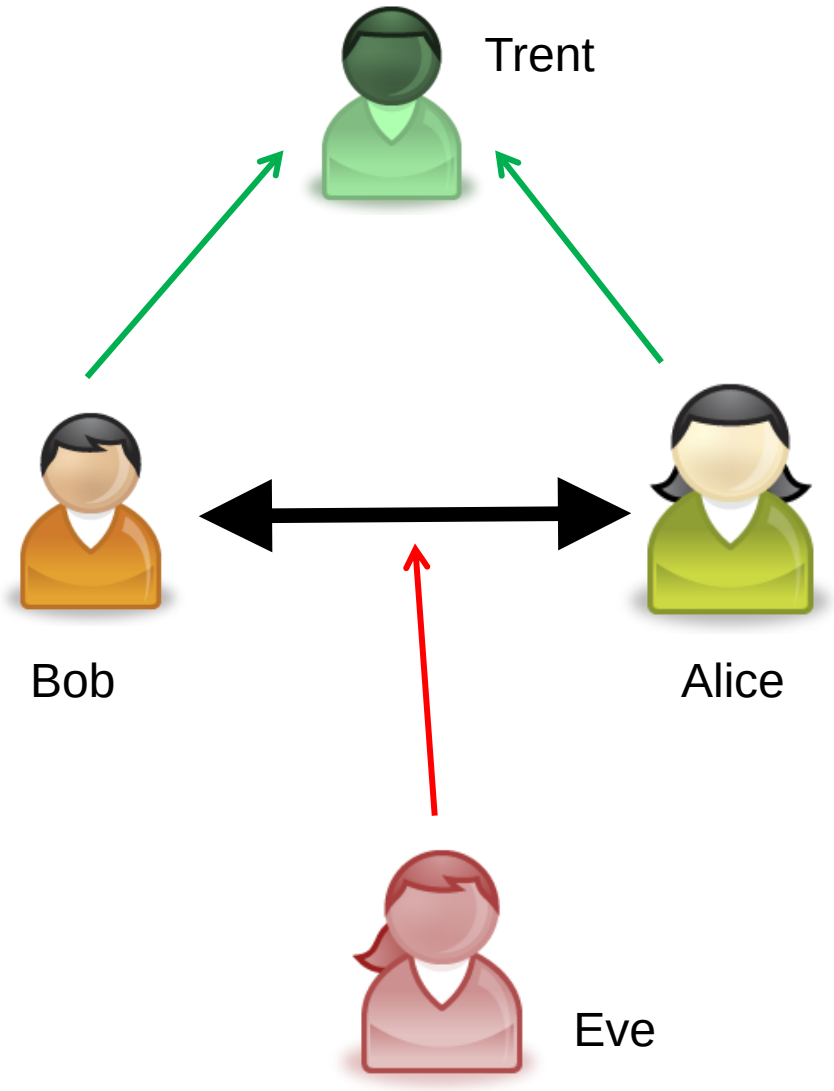
- Salaus suojaa tiedon *luottamuksellisuutta*
- Sähköinen allekirjoitus suojaa tiedon *eheyttä*
- Saatavuutta ei voi varmistaa kryptografialla
  - Jotkin salausohjelmistot lisäksi erittäin vaikeakkäyttöisiä
  - Optimaalisesti salausta ei huomaa

Salaus

- Salaus jakaantuu kahteen perusperheeseen
  - Symmetrisessä salauksessa kaikki osapuolet tietävät saman salaisuuden
  - Asymmetrisessä eli julkisen avaimen salauksessa jokaisella henkilöllä on julkinen ja salainen avain
    - Diskreettiin matematiikkaan perustuva yhteys avainten välillä
    - Perustuu alulukuihin ja luvun tekijöihin jakoon
      - http://www.schneierfacts.com/fact/24

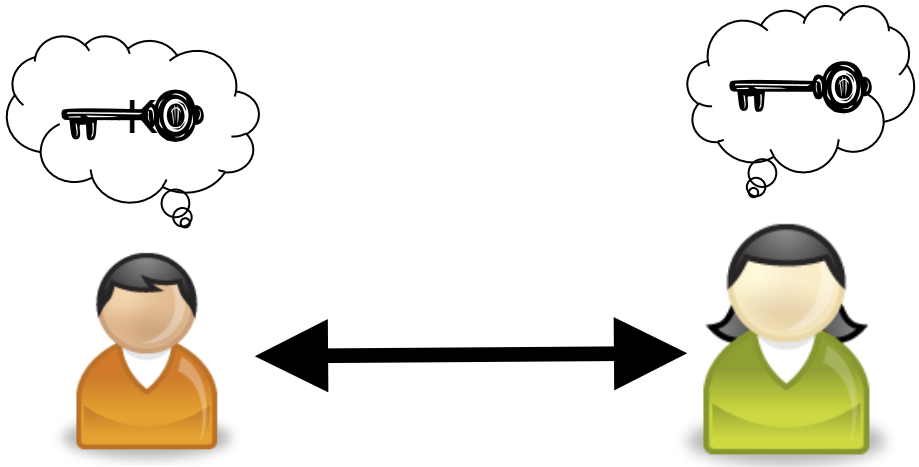
Nimeämiskäytäntöjä

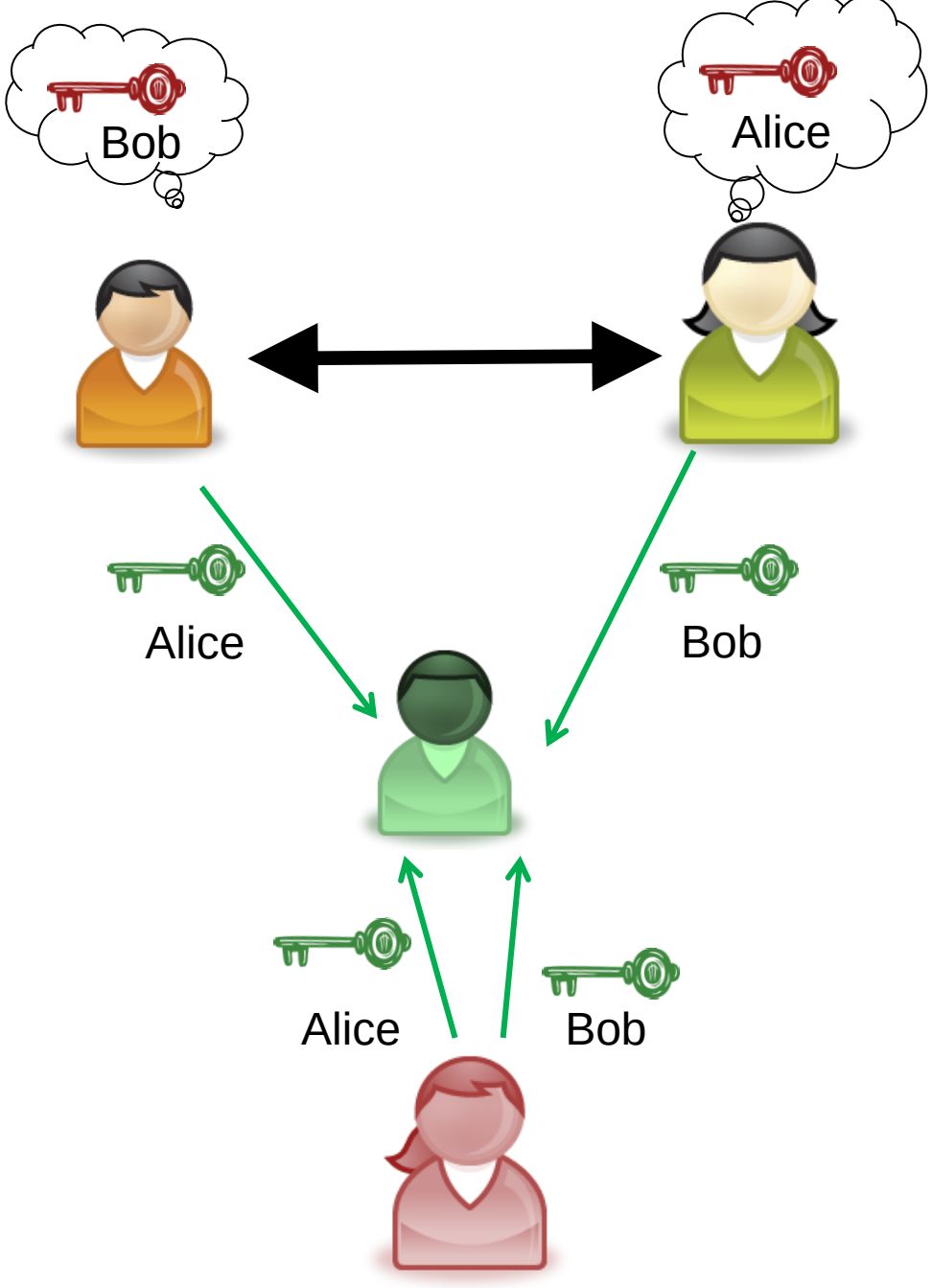
- Salausesimerkeissä Alice ja Bob yrittävät viestiä turvallisesti keskenään
- Pahantahtoinen Eve yrittää kuulee viestiliikenteen ja yrittää purkaa sitä
  - Mallory-niminen hyökkääjä voi myös muokata liikennettä
- Trent on Alicen ja Bobin luottama kolmas osapuoli
- Myös muita
- http://xkcd.com/177/



Symmetrinen salaus

- Symmetrisessä salauksessa Alice ja Bob tietävät jaetun salaisuuden K ja tavan, jolla K:lla salataan avain
- Eve tietää tavan, mutta ei tiedä K:ta
  - http://www.schneierfacts.com/fact/18
- Mikäli avain on viestin pituinen ja sitä käytetään vain kerran, mahdoton purkaa
  - Ns. One-time pad
  - http://www.schneierfacts.com/fact/2
- Ongelmaksi muodostuu salaisuusparien muodostaminen osapuolten välillä
  - N^2 avaintenvaihtoa N noodin välillä





Asymmetrinen salaus

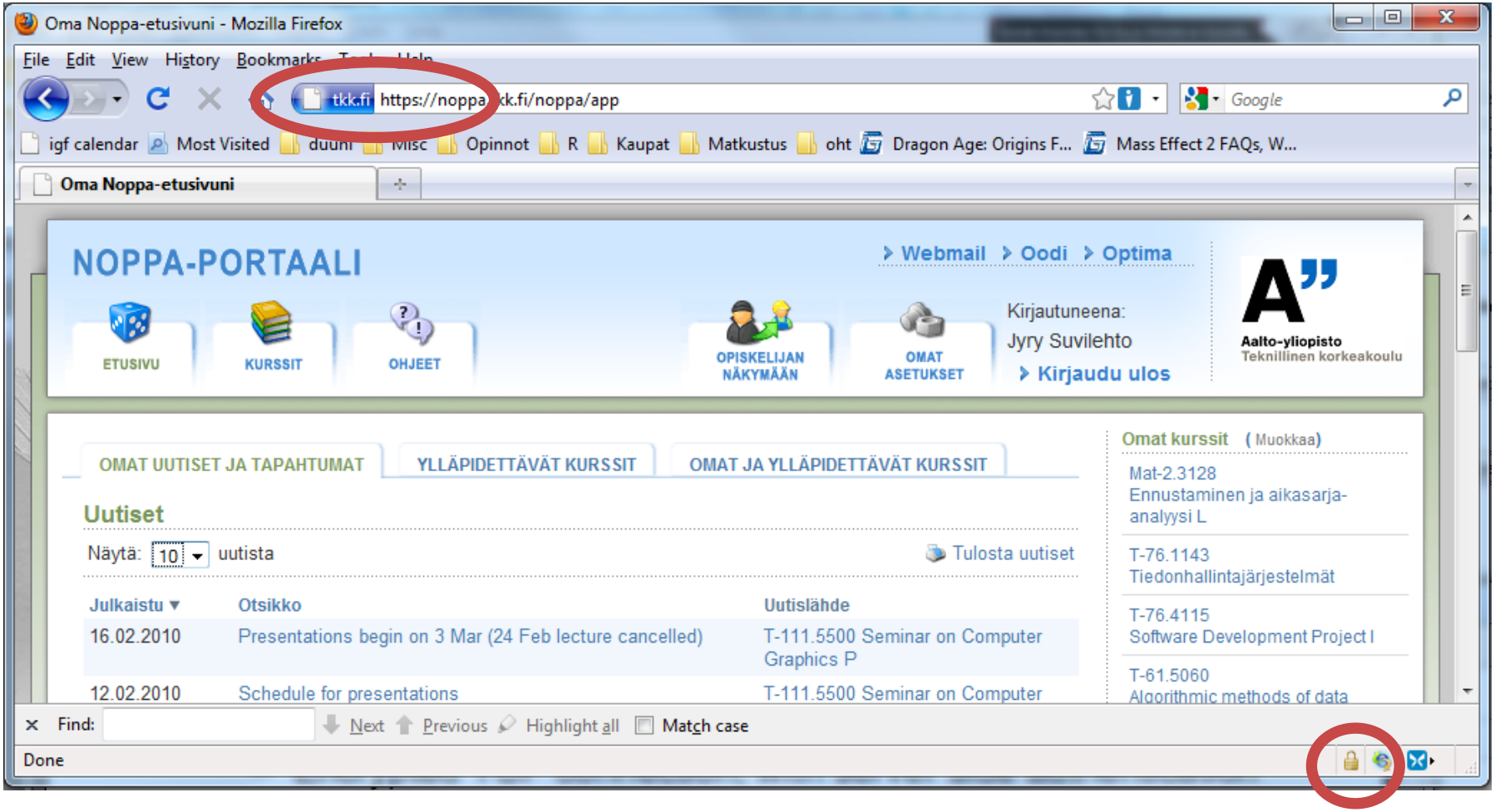
- Asymmetrisessä salauksessa Bobilla ja Alicella on
  - Julkinen avain
  - Yksityinen avain
- Julkisella avaimella salatun viestin voi avata vain salaisella avaimella
- Salaisella avaimella allekirjoitettu viesti aukeaa oikein vain julkisella avaimella
- Eve voi tietää julkiset avaimet, mutta ei voi murtaa salausta
- Mallory voi tietää julkiset avaimet mutta ei voi teeskennellä Bobia tai Alicea
- Ongelmaksi muodostuu luottamus Trentiin

http://www.schneierfacts.com/fact/101

PKI

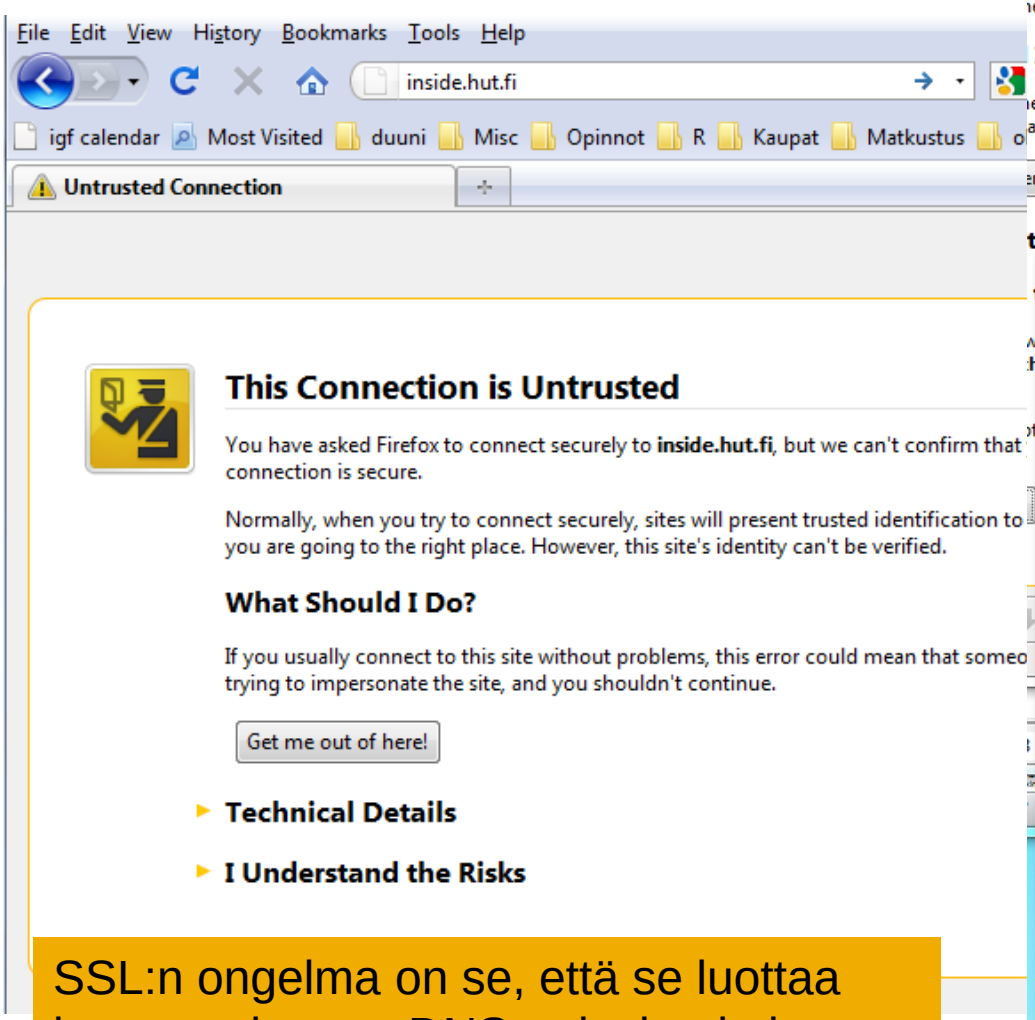
- Julkisen avaimen salauksessa ongelmaksi muodostuu se, että ei ole olemassa osapuolta, johon kaikki luottaisivat
- Erilaisia julkisen avaimen infrastruktuureja (Public Key Infrastructure, PKI) on monia
  - Esim. Hallitus voi vaatia kansalaisia luottamaan itseensä
- Jokin taho myöntää sertifikaatteja, joissa se digitaalisesti allekirjoittaa toisen tahon julkisen avaimen
  - Sertifikaatti voi sisältää esimerkiksi julkisen avaimen ja vastaavan palvelimen nimen

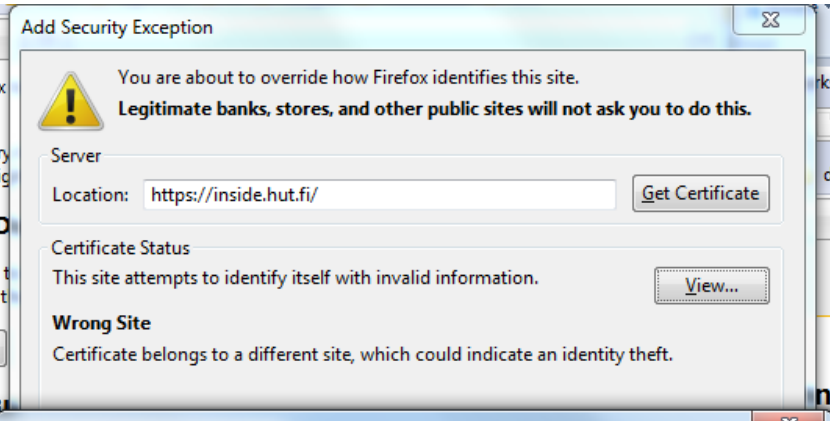
SSL

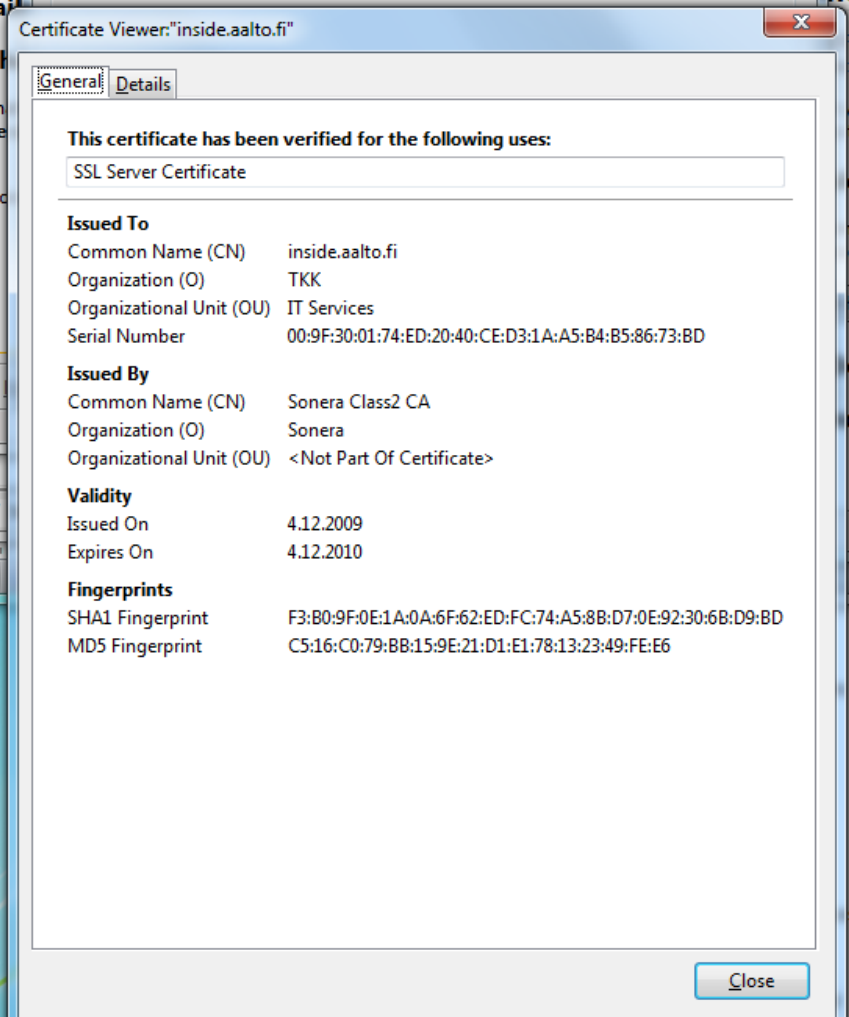


http://www.schneierfacts.com/fact/765

SSL

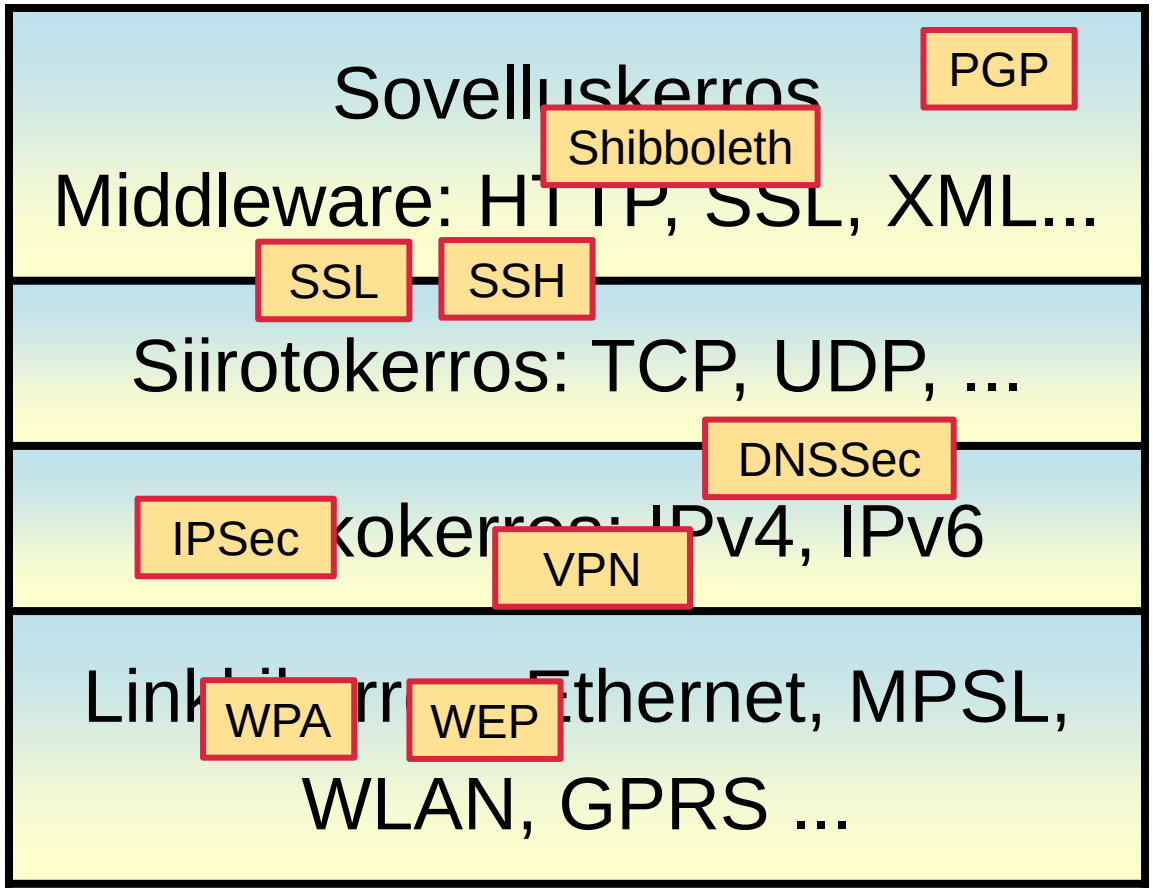






SSL:n ongelma on se, että se luottaa koneen nimeen. DNS-palvelu ei ole luotettava, joten koneen nimi on mahdollista väärentää.

Muita tietoturvaprotokollia



Mitä ajatella?

- Tietoturva on monipuolinen ala
  - Tekniset ratkaisut vain osa tietoturvaa
- Tietoturva vaatii suunnittelua
- Yksilön tietoturvan murtaminen on kannattavaa bisnestä
- Palomuurit rajoittavat liikennettä
  - Mitä korkeampi protokollataso, sen kalliimpaa
- Kryptografia suojaa tietoa siirron aikana

Ensi viikolla

- Olette joka iikka ilmoittautuneet välikokeeseen
  - Tarvitsemme tiedon osallistujista, jotta tilaa ja papereita riittää kaikille
- Televerkko
- GSM-verkko