



Tietoturvallisuus

Kirja sivut 576-590



Mitä on tietoturva?

- Turvallisuus on omaisuuden ja ihmisten suojaamista
- Tietoturva on informaatio-omaisuuden suojaamista erilaisia uhkia vastaan
- Tietoturvaa ei voi tehdä mielekkäästi tunnistamatta suojattavaa informaatiota ja siihen kohdistuvia uhkia
 - Tietokoneiden ja verkkojen suojaaminen on osa tietoturvaa, mutta ei ydinasia



Tietoturvan perustavoitteet

- Ns. CIA-malli
- Luottamuksellisuus (Confidentiality)
 - Tiedon pitäminen salassa
- Eheys (Integrity)
 - Tiedon muuttamisen estäminen
- Saatavuus (käytettävyys, Availability)
 - Mahdollisuus käyttää tietoa
- Nämä vaatimukset ovat keskenään ristiriitaisia
 - Etenkin tiedon saatavuus on usein ristiriidassa muiden vaatimuksien kanssa



Tietoturvan muita peruskäsitteitä

- Tunnistaminen (identification)
 - Tiedetään henkilön tai olion identiteetti
 - Esim. cookie WWW-käytössä
- Todentaminen (authentication)
 - Varmennutaan henkilön tai olion identiteetistä
- Tapahtumien kirjaaminen (accounting)
 - Voidaan itse seurata mitä on tapahtunut
- Kiistämättömyys (non-repudiation)
 - Tapahtuma pystytään todistamaan myöhemmin muille
- Valtuutus (authorization)
 - Annetaan oikeutus suorittaa toimenpide
- Tietosuoja (privacy)
 - Henkilökohtaisen datan suojaaminen väärinkäytöksiltä



- Fyysiset vahingot hävittävät paljon tietoa
 - Kaikki kovalevyt hajoavat aikanaan
- Ihmiset tekevät virheitä, niin suunnittelussa kuin päivittäisissä toimissa
- Tahalliset hyökkääjät voivat lukea, muuttaa ja tuhota tietoa, huviksi tai hyödyksi
 - Ulkopuolisia tai omaa väkeä
- Oma henkilökunta on usein suurin ongelmalähde
- Uhka-analyysin kokonaisalue on laajempi, tässä keskitytään tietoverkkojen teknisiin uhkiin
 - Kannattaa muistaa, että palomuuuri ja salaus eivät estä omaa, luvallista käyttäjää kopioimasta tietoa paperille



- Tietoverkko (Internet) on kaksisuuntainen viestintäväline, verkon kautta voi:
- Murtautua tietojärjestelmään
 - Tunnettujen aukkojen hyödyntäminen on usein tuotteistettu ohjelmistoiksi
- Häiritä palveluiden toimintaa
 - Palvelunestohyökkäykset (Denial of Service, DoS)
 - Esim. kuormitus liikenteellä, virheellisesti rakennettujen viestien lähettäminen
- Lähettää vääriä viestejä esiintyen toisena tahona (spoofing)
 - Väärennettyä sähköpostia
 - Käyttää väärennettyjä IP-osoitteita



Uhat liikenteelle verkossa

- Salakuuntelu (eavesdropping)
 - Lähiverkoissa usein helppoa
 - Runkoverkossa melko hankalaa (paitsi valtioille)
- Siirrettävän tiedon manipulointi
 - Man-in-the-middle -hyökkäys
 - Hyökkääjä toimii välikätenä halliten tietoliikennettä kahden osapuolen välillä
- Uudelleenlähetys (replay)
 - Hyökkääjä lähettää kaappaamansa viestin uudestaan
 - Salaus ja eheyden varmistava allekirjoituskaan eivät auta välttämättä tähän



Virukset ja muut haittaohjelmat

- **Haittaohjelmia on erilaisia**
 - Virukset ovat itseään kopioivaa ohjelmakoodia ja yleensä tarttuvat tiedostoihin (ohjelmiin tai dokumentteihin)
 - Madot ovat itsenäisinä ohjelmina verkossa liikkuvia viruksia, jotka murtautuvat koneisiin
 - Troijalaiset eivät leviä itsestään ja haittaominaisuudet on piilotettu
 - Mainosohjelmat (Adware) ei välttämättä ole pahantahtoista, mutta siitä on hankalaa olla varma
- **Haittaohjelmat saattavat**
 - Häiritä koneen toimintaa (syövät tehoa, muita häiriöitä)
 - Tuhota tietoja (tiedostoja)
 - Lähettää tietoa eteenpäin
 - Muuttaa tietoa



Tietoturvan ratkaisuja

- Suunnittelu
- Henkilöstö
- Ohjaus ja työprosessit
- Fyysinen suojaus
- Tietotekniset ratkaisut
 - Turvalliset asetukset
 - Turvallinen ohjelmointi
 - Palomuurit
 - Hyökkäyksen tunnistus
 - Virustentorjunta
 - Salaustekniikat



Tietoturvan suunnittelu

- Yksinkertaistaen
 - Tunnistetaan suojattavat kohteet
 - Laaditaan riskianalyysi
 - Päätetään suojaustoimenpiteet
- Suojattavan tieto-omaisuuden (assets) tunnistaminen on välttämätöntä suojauksien kohdistamiselle
- Riskianalyysissä
 - Tunnistetaan uhat tiedolle
 - Arvioidaan vahinkojen suuruus
 - Arvioidaan todennäköisyys
- Suojaustoimenpiteillä pyritään saamaan *jäännösriski* sopivalle tasolle



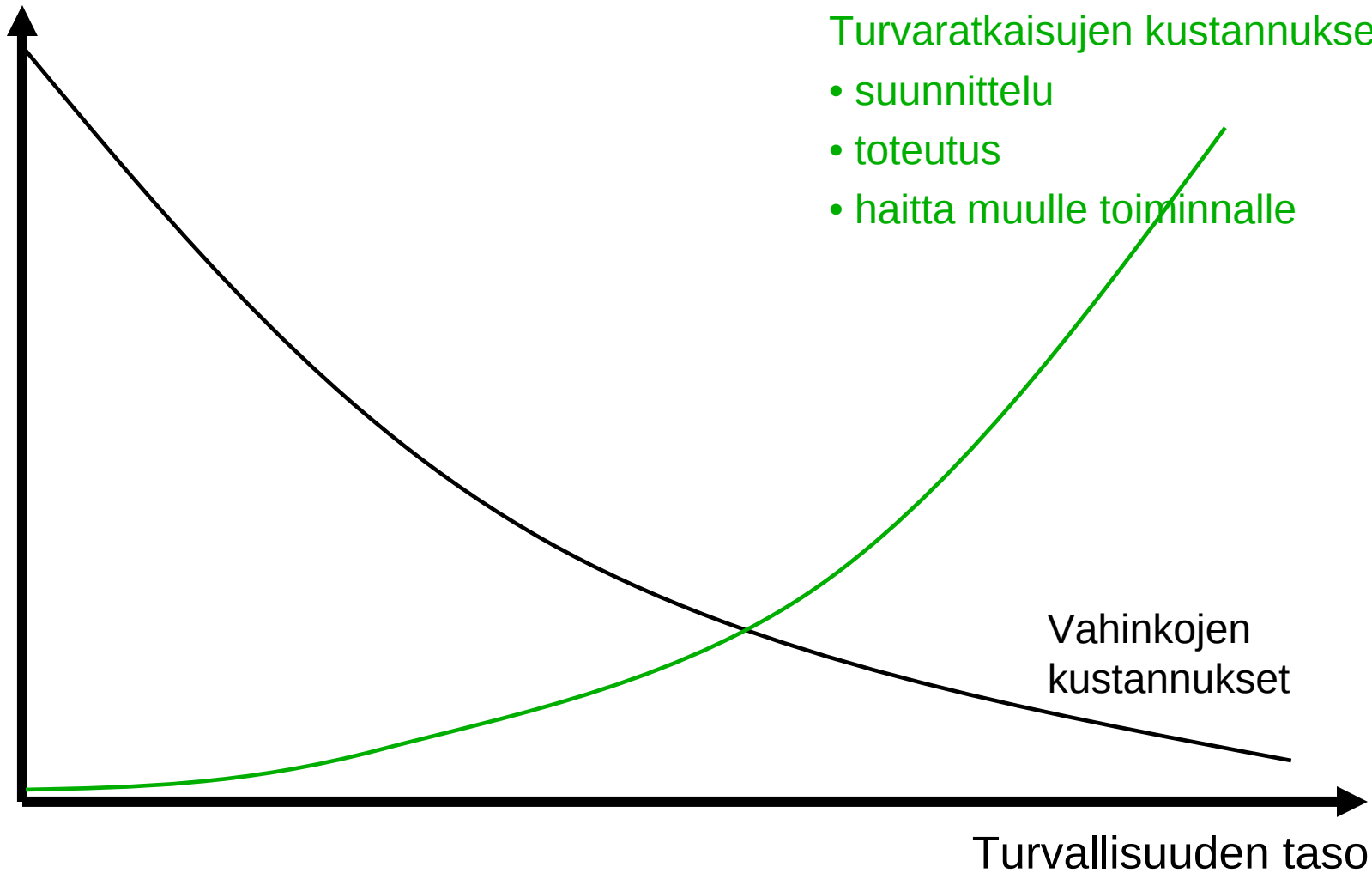
Turvallisuuspolitiikka (Security Policy)

- Turvasuunnittelu tuottaa turvapolitiikan
 - Joukko säännöllisesti päivitettäviä dokumentteja
 - Osa saattaa olla sovellusohjeita, osa salaisia
- Turvallisuuspolitiikka sisältää suunnittelun dokumentoinnin
 - Suojattava tieto-omaisuus
 - Uhat
 - Riski-analyysi
 - Suojauksen tavoitteet
 - Suojauksen keinot
 - Vastuut
 - Resurssit



Turvallisuuden kustannukset

Kustannukset





Turvallisuuden toteutus on hyvissä prosesseissa

- Turvasuunnittelun perusteella pystytään toteuttamaan tekninen toteutus ja laatimaan prosessit henkilöstölle
- Molempien kohdalla vaikeutena on saavutetun tason säilyttäminen
 - Tekniikkaa on päivitettävä uusia uhkia vastaan
 - Ihmiset keskittyvät ensisijaisiin tehtäviinsä
- Turvallisuuspolitiikan toteutuksen on oltava realistinen
- Turvallisuutta on seurattava ja valvottava



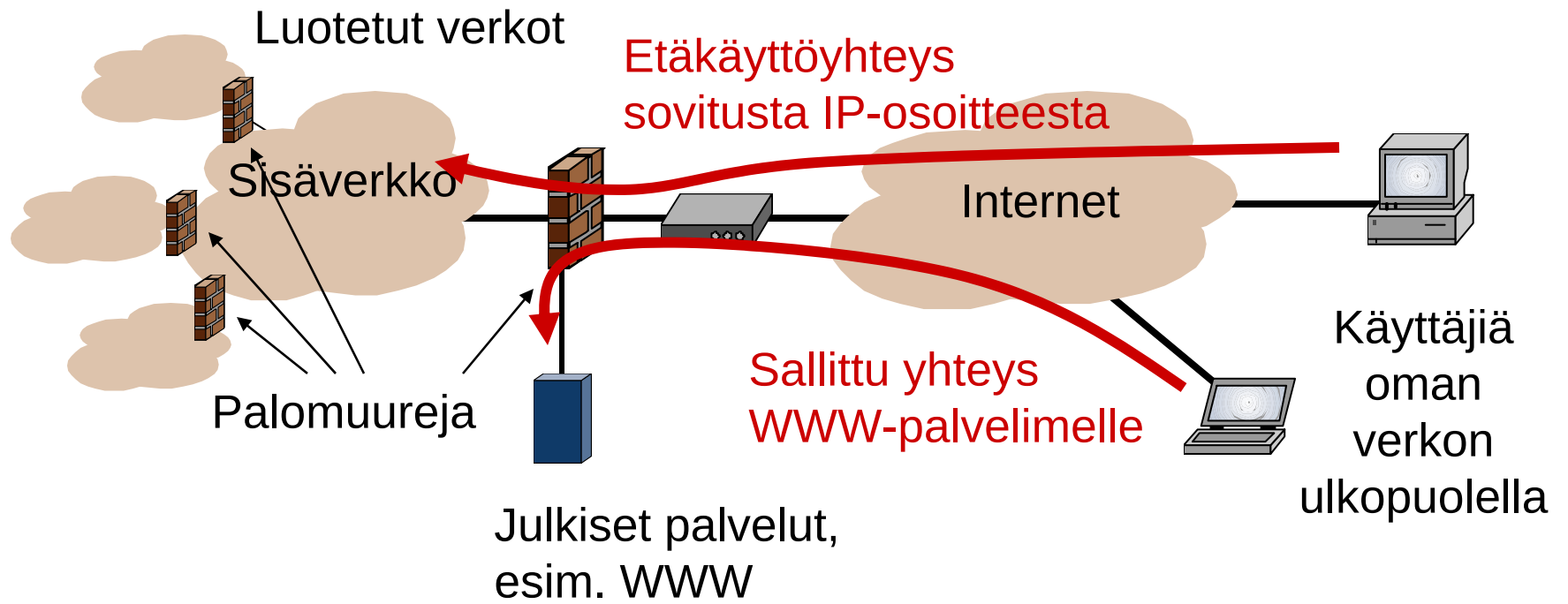
TEKNILLINEN KORKEAKOULU

Tietoturvan tekniset ratkaisut



Mikä on palomuri

- Laite (usein laite ja sovellus)
 - Rajoittaa tietoliikennettä verkkojen välillä
- Toteuttaa tietoturvapolitiikkaa





- Rajaavat liikennettä sääntöjen perusteella
- Kaksi perustyyppiä
 - *Pakettisuodattava* palomuuuri käsittelee paketteja yksitellen
 - Verkko- ja kuljetuskerroksen tasolla
 - IP-osoitteet, porttiosoitteet, Syn-, FIN-bitit
 - Pakettisuodatin voi olla tilaton tai tilallinen
 - Muistaa avatut tietoliikenneyhteydet
 - *Sovellustason* palomuuuri toteuttaa sovellusprotokollan ja sovelluksen logiikkaa
 - Virustarkistus sähköpostille
 - Aktiivisten WWW-komponenttien estäminen
- Tuotteissa on usein molempia ominaisuuksia



Palomuurin tarjoamaa suojaa

- Ulkopuolelta tulevat yhteydet voidaan käytännössä rajoittaa hyvin tehokkaasti
 - Palomuurin sisäpuolella olevat turva-aukot (esim. tavallisten käyttäjien työasemissa) eivät ole ulkopuolisten hyökkääjien käytettävissä
- Sisäpuolisten käyttäjien toimintaa voidaan rajoittaa
 - Motivoitunut käyttäjä pystyy kiertämään rajoituksia
- Oman verkon segmenttien väliset palomuurit suojaavat omalta henkilöstöltä ja sisään päässeeltä murtautujalta



Palomuurien ominaisuuksia

- Palomuurit häiritsevät Internetin päästä-päähän -arkkitehtuuria (end-to-end)
 - Jos palomuurista saa avata yhteyksiä vain ulospäin, kuinka kaksi eri palomuurien takana olevaa osapuolta voi kommunikoida?
- Palomuureissa on usein myös NAT-toiminto
 - Network Address Translation
 - Yksi julkinen IP-osoite jaetaan usean koneen käyttöön sisäverkossa käyttäen yksityisiä IP-osoitteita



Yksittäisen tietokoneen turvaaminen

- Kaikkia koneita ei voi sulkea täysin palomuurien taakse
 - Palveluidenkin on oltava tavoitettavissa
- Verkkoon näkyvän koneen ensimmäinen suojaus on koneessa olevien ylimääräisten palveluiden poistaminen
 - Tavallinen Linux-asennus sisältää yli tusinan verkkoon näkyviä palvelinohjelmistoja
- Pääsyä jäljelle jääviin palveluihin voidaan rajoittaa
 - Ohjelmistopalomuuuri koneessa
- Palvelut on konfiguroitava oikein
 - Kaikki turhat ominaisuudet suljetaan
- Sisään päässyt murtautuja pystyy yleensä saamaan pääkäyttäjän oikeudet normaalisti ylläpidetyissä koneissa



Turvallinen palvelinohjelmointi

- Itse palvelinohjelmisto ja käyttöjärjestelmä on ohjelmitava kestämään hyökkäyksiä
 - Oma osaamisalueensa tämän kurssin ulkopuolella
- On oletettava, että hyökkääjä saattaa tehdä mitä tahansa, kuten
 - Aiheuttaa *puskurin ylivuodon* etsimällä lähdekoodista kohdan, jossa käyttäjän syöte luetaan puskuriin gets()-funktiolla
 - Syöttää WWW-lomakkeeseen SQL-kielisiä komentoja
 - Syöttää keskusteluforumille JavaScript-ohjelman
 - XSS, Cross Site Scripting
- Turvallisen ohjelmiston luominen alkaa jo suunnitteluvaiheessa
 - Oletukset ympäristöstä ja uhista
 - Arkkitehtuuri



Virus- ja haittaohjelmatorjunta

- Virukset ovat suosittujen ja ominaisuuksiltaan viruksia tukevien ympäristöjen ongelma
 - 80-luvulla Macintosh-ympäristö
 - 80-90-lukujen vaihteessa MS-DOS
 - 90-luvulla Windows
 - 2000-luvulla Microsoftin Office-ympäristö
- Virukset ja muut haittaohjelmat torjutaan nykyään ensisijaisesti viruksentorjuntaohjelmistoilla
 - Alan yritykset jakavat löytämänsä virukset keskenään
 - Kullekin virukselle luodaan tunnistet, joiden avulla ne voidaan tunnistaa ja toiminta estää
 - Tunnistetietokanta on päivitettävä säännöllisesti



- Tarkemmin seuraavalla luennolla
- Salauksella voidaan saavuttaa murtamaton luottamuksellisuus kahden osapuolen viestinnälle, jos osa puolilla on *jaettu salaisuus*
- Sähköisellä allekirjoituksella voidaan varmistaa viestien ja talletetun datan eheys
- Saatavuutta ei voida varmistaa salaustekniikoilla
- Salaustekniikat tarjoavat murtamattomia tekniikoita, mutta ei murtumattomia kiinnityspisteitä
 - Salaus ei ratkaise kaikkia ongelmia



TEKNILLINEN KORKEAKOULU

Esimerkkejä toteutuksista

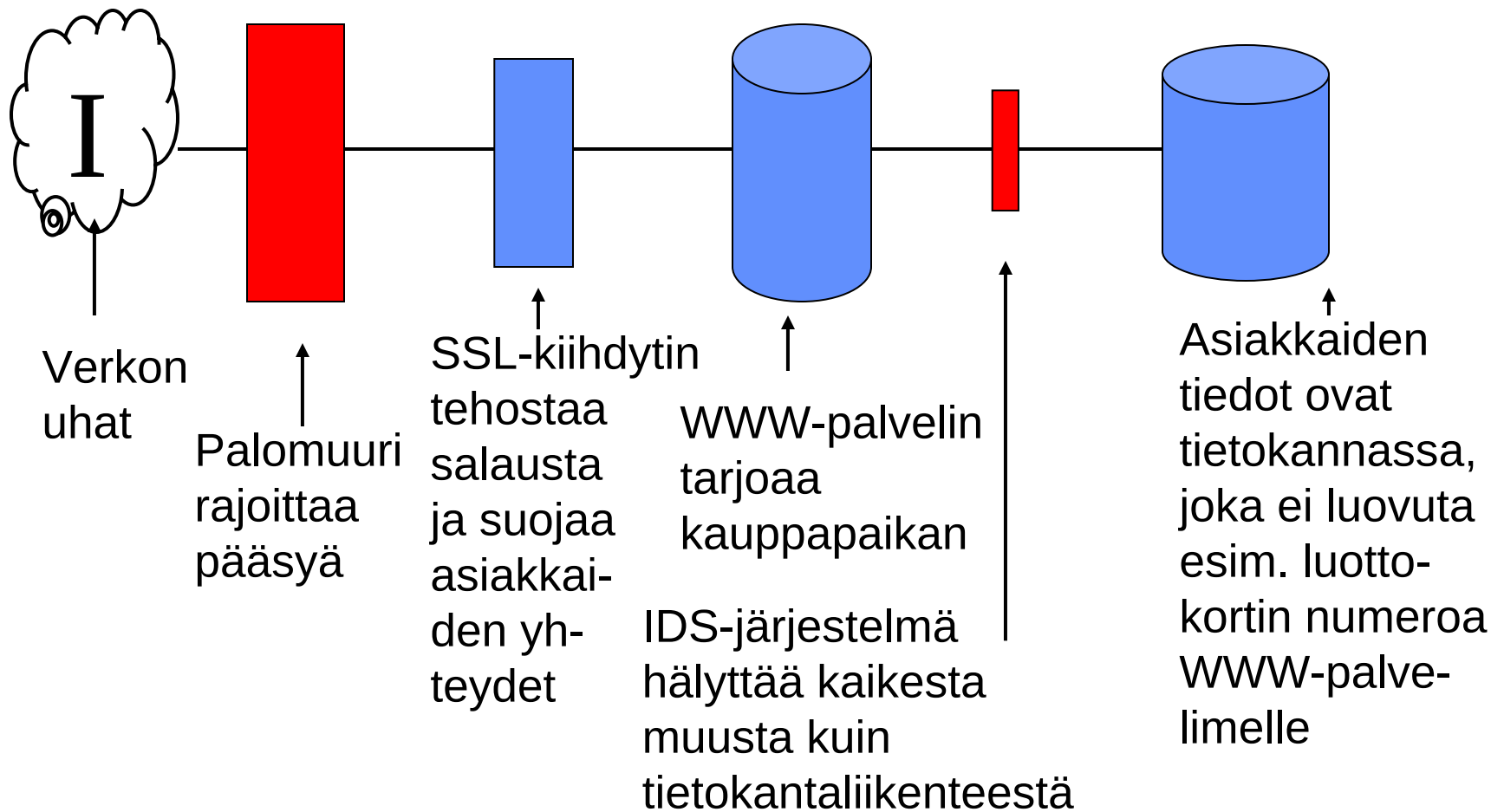


Kannettavien laitteiden tietoturva

- Kannettavat laitteet ovat organisaatiolle erityinen ongelma
 - Organisaation tietoa
 - Pääsy organisaation tietojärjestelmiin
 - Helposti hukattavia ja varastettavia
- Kannettavien (tietokoneet, PDA:t, viestimet) perussuoja on
 - Tietojen eheyden ja luottamuksellisuuden suojaaminen salaustekniikoilla
 - Tietojen saatavuuden suojaaminen tallentamalla kopio salausavaimesta organisaatiolle
 - Varmuuskopiointi
 - Koneen normaaleilla oikeuksilla käyttämisen estäminen ulkopuolisilta
 - Virus- ja haittaohjelmatorjunta
 - Ohjelmistopalomuuuri
 - Salanasuojaus
 - Käsittelyprosessi
 - Vain käsimatkatavarana,
 - Ei saa jättää vartioimatta



Verkkokaupan tietoturva





- Tietoturva on tiedon aspektien suojelemista
 - Luottamuksellisuus
 - Eheys
 - Saatavuus
- Tietoturva edellyttää suunnittelua
 - Pelkkä tekniikka on hyödytöntä
- Palomuurit turvaavat suuria osia verkosta
- Verkkoon näkyvät koneet on ohjelmoitava ja asennettava oikein
- Salauksella voidaan luoda suojattuja yhteyksiä