# Tietoturvan perusteita

14.4.2003

Sauli Takkinen

Informaatioteknologian tiedekunta

# Tietoturvaan mahdollisesti kohdistuvat hyökkäystyypit

- Eavesdropping
- Data Modification
- Identity Spoofing
- Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle
- Compromised-Key Attack
- Sniffer Attack
- Application-Layer Attack

## Eavesdropping

- Suomeksi: salakuuntelu.
- Salaamattomassa IP-liikenteessä paketit salaamattomia ja poimittavissa.
- Liikenteen seuraaja voi poimia väliltä haluamansa tiedot omaan käyttöönsä.
- Salakuuntelua voidaan estää käyttämällä esimerkiksi IPSec-suojausta.
- Myös älykkäät kytkimet osaavat estää salakuuntelun.

## Data Modification

- Suomeksi: tiedon muuttaminen.
- Liikenteen salakuuntelun jälkeen hyökkääjä voi muokata siirrettäviä paketteja haluamaansa muotoon.
- Tiedon muuttaminen on yleistä myös seuraavana esiteltävän identiteettihuijauksen yhteydessä.
- Tiedon muuttaminen on estettävissä salaamalla tai allekirjoittamalla paketit.

## Identity Spoofing

- Suomeksi: identiteettihuijaus.
- Hyökkääjä voi esittää käyttävänsä jotakin verkossa sallittua IP-osoitetta ja muuttaa, uudelleenreitittää ja tuhota osoitteen läpi kulkevaa liikennettä.
- Nykyisin liikenteen uudelleen reitittäminen vaatii murtautujalta pääsyn johonkin reitityslaitteeseen kuten kytkimeen tai siltaan. Eli pelkästään tietokoneeseen murtautuminen ei riitä.

## Password-Based Attacks

- Suomeksi: salasanapohjainen hyökkäys.
- Vanhemmat järjestelmät käyttävät käyttäjätunnistuksessa salaamatonta tekniikkaa, jonka takia käyttäjätunnistustiedot ovat hyökkääjän saatavilla.
- Hyökkääjän löytäessä järjestelmässä olemassa olevan käyttäjätunnuksen ja salasanan on hänen seuraava askeleensa on pyrkiä antamaan tälle tunnuksen ylläpitäjän oikeudet.

## Denial-of-Service Attack

- Suomeksi: palveluhyökkäys.
- Normaaliin järjestelmän käyttöön liittyvää väärinkäytöstä, jossa hyökkääjä toimii järjestelmän tarjoamien palvelujen avulla kyseistä verkkoa vastaan.
- Erona sovellustason hyökkäykseen on tässä hyökkäystyypissä käytössä ulospäin palveluja tarjoavat sovellukset, eikä mikä hyvänsä sovellus.

## Man-in-the-Middle

- Suomeksi: mies välissä -hyökkäys.
- Kyseessä on tilanne, jossa kahden tietoa välittävän käyttäjän välissä on kolmas osapuoli, jolla ei ole lupaa seurata, tallentaa tai muokata liikennettä.
- Esimerkki tällaisesta tapauksesta on, että joku lukee sähköpostin matkan varrella ja reitittää sen eteenpäin aivan kuin se ei olisi käynyt missään matkan varrella.

## Compromised-Key Attack

- Suomeksi: muokattu avain -hyökkäys.
- Murtautuja varastaa käyttäjän salaisen avaimen, jota muokkaamalla murtautujan on mahdollista esimerkiksi päästä käsiksi käyttäjän salaamiin tiedostoihin tai esiintyä kyseisenä käyttäjänä.
- Avain on salainen koodi tai numero, jonka tarkoituksena on taata salatun tiedon aitous.

## Sniffer Attack

- Suomeksi: snifferihyökkäys.
- Snifferi on työkalu, esimerkiksi laite tai ohjelma, jolla voidaan lukea, monitoroida ja kaapata verkossa liikkuvaa liikennettä.
- Liikennettä voidaan aina lukea, mutta jos käytössä on esimerkiksi IPSecin ESP-paketointi, niin pakettien sisältöä ei voida avata edes snifferillä.

# Application-Layer Attack

- Suomeksi: sovellustason hyökkäys.
- Sovellustason hyökkäyksen tarkoituksena on murtaa käyttöjärjestelmän suojaus aiheuttamalla virhe järjestelmän toimintaan.
- Sopivan virheen tuloksena voidaan ohittaa normaalin käyttäjän rajoitteet oikeuksissa ja päästään käsiksi järjestelmän tietoihin.
- Verrattuna Denial-of-Services-tyyppiseen hyökkäykseen on erona se, että tässä tapauksessa voidaan käyttää mitä hyvänsä sovellusta aiheuttamaan virheitä isäntäjärjestelmässä.

# Muita tietoturvaa uhkaavia tekijöitä

## Virukset

- Kanavia viruksien leviämisessä ovat sähköpostin liitetiedostot, piraattisovellukset sekä WWW-sivuille piilotetut ohjelmat.
- Uusia viruksia tehdään jatkuvasti, mutta onneksi virustentorjuntaohjelmien valmistajat pysyvät kohtuullisen hyvin tahdissa mukana.
- Eräs keino selvitä virusten kanssa on tunnetun valmistajan virustentorjuntaohjelmaa käyttäminen ja noudattaa varovaisuutta vieraiden tiedostojen kanssa.
- Yleinen harhaluulo on, että pelkkä palomuuri estää virusten tarttumisen kotikoneelle.
- Mikäli käyttäjä pystyy käyttämään palomuurin läpi esimerkiksi WWW-selainta ja lukemaan sähköposteja tulevat virukset sisään yhtä varmasti kuin ilman palomuuria.

## Käyttäjä tietoturva-aukkona

- Käyttäjien kouluttaminen tietoturvallisiin toimintatapoihin paras tapa välttää ongelmat.
- Myös normaalin käyttäjän oikeuksien rajoittaminen useimmiten välttämätöntä.

## Portit ja palvelut tietoturva-aukkoina

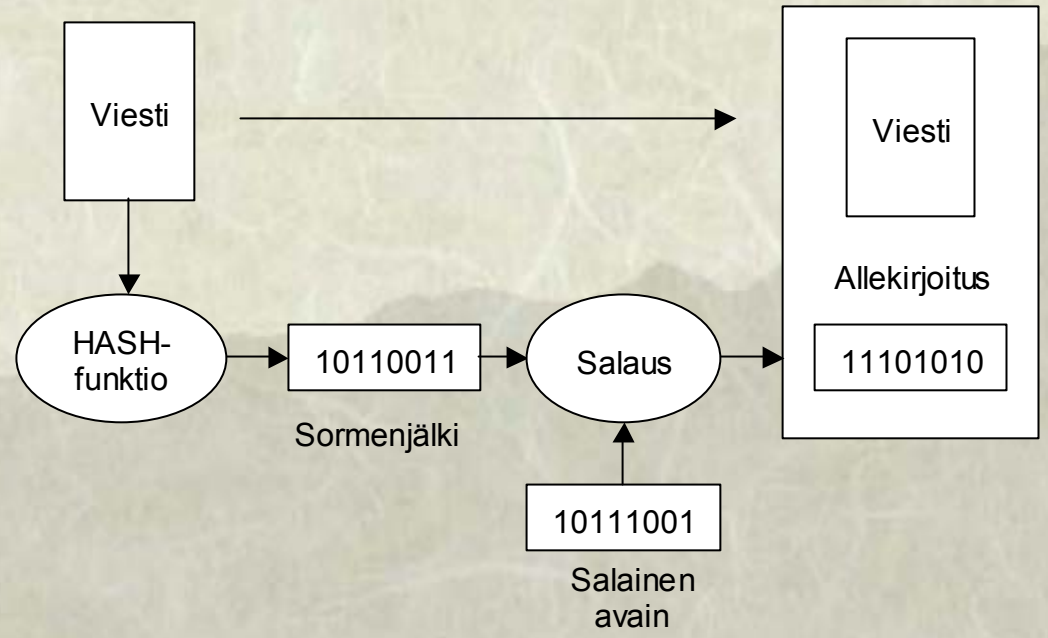
- Palveluiden kommunikointi ulkomaailmaan tapahtuu porttien kautta. Esimerkiksi *http*-protokollalla tapahtuva liikennöinti suoritetaan TCP-portin 88 kautta.
- Jokaiselle yleisesti tunnetulle palvelulle on varattu jokin tietty portti.
- Jokainen ylimääräinen avoinna oleva portti ja palvelu tarkoittaa yhtä uutta mahdollisuutta tulla järjestelmään sisälle luvatta.
- Tästä syystä järjestelmässä ei saa olla päällä yhtään tuntematonta eikä tarpeetonta palvelua.

# Keinoja tietoturvan parantamiseksi

## Eheyden tarkistaminen

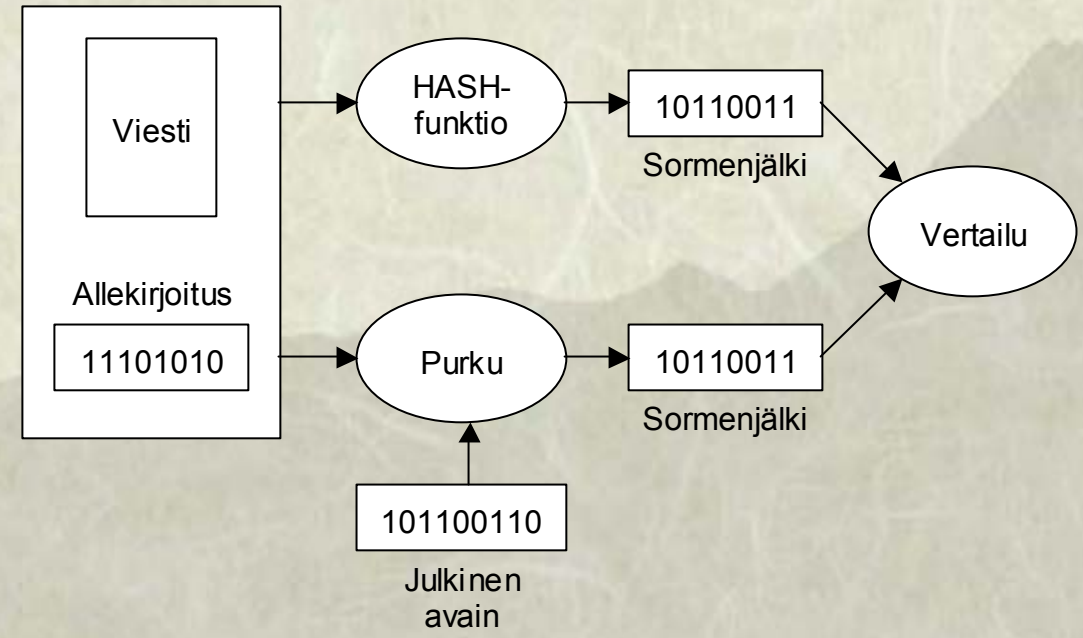
- Käyttämällä eheyden tarkistusta, voidaan varmistaa, että tieto ei ole siirron aikana joutunut ulkopuolisten muokkaukseen.
- Eheys voidaan tarkistaa esimerkiksi luomalla HASH-funktion avulla HMAC (Hash Message Authentication Codes).
- HMAC:lla voidaan siirrettävä paketti allekirjoittaa jolloin nähdään mikäli pakettia on muutettu tai, että paketteja ei ole hävinnyt tai tullut lisää matkan varrella.

# Digitaalisen allekirjoituksen luominen




- HASH-funktion avulla voidaan toteuttaa allekirjoitus, jonka avulla viestin vastaanottaja voi olla varma, että viesti on tullut viestin lähettäjältä.
- Tekniikka toimii niin, että HASH-funktion avulla tuotetaan viestistä vakiomittainen merkkijono eli sormenjälki.
- Tämä sormenjälki salataan lähettäjän salaisella avaimella ja liitetään viestin mukaan allekirjoituksena.

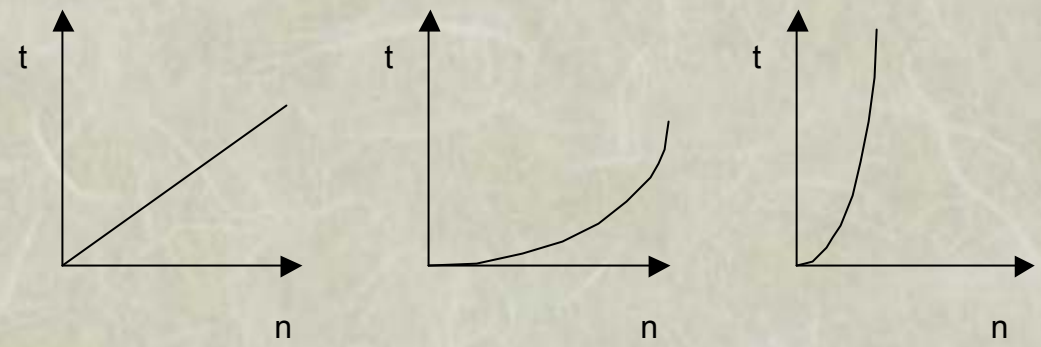
# Digitaalisen allekirjoituksen tarkistaminen




- Vastaanottaja erottaa allekirjoituksen ja purkaa sen lähettäjän julkisella avaimella.
- Tämän jälkeen vastaanottaja käyttää samanlaista HASH-funktiota kuin lähettäjä ja luo tämän avulla viestistä sormenjäljen, jota vertaa allekirjoituksena tulleeseen sormenjälkeen.
- Jos sormenjäljet täsmäävät voi vastaanottaja olla varma, ettei viesti ole muuttunut matkan varrella.

# Tiedon salaaminen

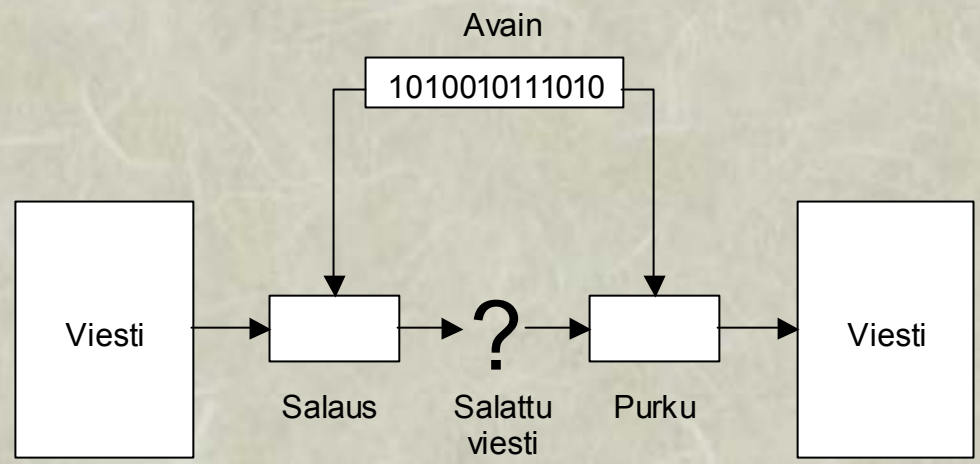
- Salaustekniikoita on kahta tyyppiä; symmetrisiä ja asymmetrisiä.
- Lisäksi on olemassa tekniikoita, jotka hyödyntävät näiden molempien yhdistelmiä.
- Salauksen purkaminen edellyttää salausfunktion käänteisfunktion löytämistä. Tämä pyritään tekemään mahdollisimman vaikeaksi eli NP-täydelliseksi ongelmaksi.




t = suorituksen aika ja monimutkaisuus
n = yrityskertojen määrä

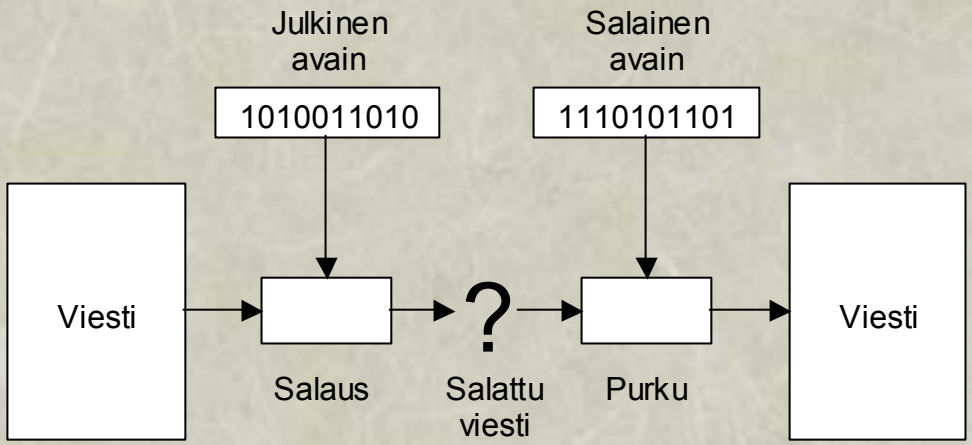
# Symmetrinen salaus

- Symmetrinen salaus perustuu siihen, että molemmat osapuolet tietävät salaamisessa käytettävän salaisen avaimen.
- Ongelmana järjestelmässä on se, että kuinka salainen avain saadaan molempien osapuolten tietoon varmaa reittiä pitkin.
- Käytössä olevia tekniikoita ovat esimerkiksi DES, 3DES, RC5, Blowfish ja Rijndael.



# Asymmetrinen salaus

- Käyttäjällä on olemassa kaksi avainta, salainen ja julkinen.
- Julkinen avain on tarkoitettu yleisesti jaettavaksi ja sillä julkisen avaimen jakajalle lähetettävä viesti salataan.
- Julkisella avaimella lähetetty viesti on avattavissa vain ja ainoastaan kyseiseen julkiseen avaimeen liittyvällä salaisella avaimella.
- Salainen avain täytyy säilyttää sellaisessa paikassa, ettei sitä pääse käyttämään kukaan muu kuin sen haltija.
- Viestin lähettäjän julkisen avaimen avulla voidaan puolestaan tarkistaa viestin allekirjoituksen täsmäävyys viestin alkuperän kanssa
- Käytössä olevia tekniikoita ovat esimerkiksi DSA ja RSA



# Palomuurit

- Palomuurin avulla voidaan estää liikennöinti sekä ulos- että sisäänpäin protokolla- tai porttikohtaisesti.
- Palomuureja markkinoidaan varsin voimakkaasti, mutta monesti unohdetaan se, että vaikka palomuurilla tukitaan liikennettä internetin raja-aidalla, paljon suurempia riskejä ovat käyttäjien toimet palomuurin sisäpuolella.
- Palomuuri ei tuo turvaa ulkoverkosta tuleville viruksille, niin kauan kuin normaali käyttö, kuten WWW-selaaminen tai sähköpostin lukeminen on mahdollista.
- Esimerkiksi WWW-palvelimen suojaaminen palomuurilla vaatii yleensä palvelimen hajauttamisen palomuurin molemmille puolille.
- NAT (Network Address Translate) -palvelu ei ole palomuuri.

# WWW-palveluiden tietoturva

- Kokonaistietoturva koostuu sekä palvelimen, että asiakaspään tietoturvasta
- Palvelin puolella vastuu on palvelun/palvelimen ylläpitäjällä, mutta kokonaistietoturvan kannalta yhtä tärkeää on asiakkaan tietoturvasta huolehtiminen.
- WWW-palvelut muodostava suurimman tietoliikenteessä olevan tietoturva-aukon.
- Peruskeinona WWW-palvelun tietoturvan parantamiseksi on salauksen käyttäminen esimerkiksi SSL (Secure Socket Layer) tai TLS (Transport Layer Security).
- Myös esimerkiksi ISAPI tai JAVA sovellusten käytöllä voidaan parantaa tietoturvaan, koska tällöin käyttäjätunnistus sekä arkaluontoisen materiaalin siirto on mahdollista suorittaa muuta kuin HTTP-liikennettä käyttäen.
- Toisaalta ISAPIn tai JAVAn käyttö siirtää vastuuta tietoturvasta asiakkaalle, koska sovellusten suoritus tapahtuu paikallisesti.

# SSL eli Secure Socket Layer

- Internetin laajimmin käytetty turvaprotokolla.
- Se mahdollistaa salauksen ja autentikoinnin ja käyttää X.509-sertifikaatteja.
- SSL toimii TCP-protokollan päällä ja sovellustason protokollien kuten HTTP:n tai FTP:n alla.

SSL rakentaa yhteyden asiakasohjelman (selaimen) C ja palvelimen S välille seuraavasti:

1.C --> S: "ClientHello": millaisia algoritmeja C:llä on käytettävissä.

2.S --> C: "ServerHello": minkä symmetrisen salausalgoritmin, moodin, hash-funktion ja kompressioalgoritmin S on valinnut - tai ilmoittaa kättelyn epäonnistumisesta.

3.S --> C: S:n julkisen avaimen sertifikaatti (kaikki sertifikaatit juurivarmentajan myöntämään asti)

4.[ S --> C: Pyytää S:n sertifikaattia. ]

5.[ C --> S: sertifikaatti - tai "no certificate", johon S reagoi lopettamalla, jos niin haluaa. ]

6.C --> S: Alustava symmetrinen avain k RSA:lla salattuna.

7.C --> S ja S --> C: Ilmoitukset valmiudesta ottaa käyttöön symmetrinen salaus k:sta lasketulla istuntoavaimella (avaimen laskennassa on mukana myös "Hello"-viesteissä esiintyneitä satunnaislukuja)

8.C --> S ja S --> C: Kättelyn lopetussanoma, jossa on tiiviste kaikesta edelläolevasta

Tämän jälkeen alkaa varsinaisen sovelluksen viestien vaihto. Kättely on lyhyempi kun saman yhteyden aikana käydään useita istuntoja ("Hello"-viesteissä on tunnisteet tätä varten). On myös mahdollista että palvelintakaan ei autentikoida. Tällöin yhteys on anonyymi ja avaimia vaihdetaan RSA:n sijasta Diffie-Hellman-protokollalla.

# ISAPI ja WWW lyhyesti

- ISAPI toimii käytännössä siten, että käyttäjän koneelle ladataan ohjelmatiedosto, joka suoritetaan.
- Suoritettavalla ohjelmatiedostolla voidaan esimerkiksi tehdä jotakin asioita paikallisessa koneessa tai suorittaa verkon yli toimenpiteitä jollekin palvelimelle.
- Käyttäjälle päin ISAPI-sovellus keskustelee normaalisti selaimen kautta, jolloin käyttäjä ei välttämättä erota tapahtuuko mahdollinen ulospäin liikennöinti HTTP- vai jonkin muun portin ja protokollan kautta.
- ISAPI-tekniikalla on hyvin helppoa rakentaa varsin tuhoisa virus, etenkin jos käyttäjä suorittaa kyseistä sovellusta pääkäyttäjän oikeuksin.

# JAVA ja WWW lyhyesti

- JAVA-sovelluksia voidaan ajaa, joko palvelimella tai asiakkaan työasemalla virtuaalikoneessa, käytetystä tekniikasta riippuen.
- Suoritettavalla ohjelmatiedostolla voidaan esimerkiksi tehdä jotakin asioita paikallisessa koneessa tai suorittaa verkon yli toimenpiteitä jollekin palvelimelle.
- Käyttäjälle päin JAVA-sovellus keskustelee normaalisti selaimen kautta, jolloin käyttäjä ei välttämättä erota tapahtuuko mahdollinen ulospäin liikennöinti HTTP- vai jonkin muun portin ja protokollan kautta.
- JAVA voidaan pitää jonkin verran ISAPI-sovellusta turvallisempana, koska virtuaalikoneella ei ole välttämättä kovin laajoja oikeuksia järjestelmään.
- Mutta myös JAVA-sovellusten avulla on mahdollista tehdä viruksia ja virtuaalikoneista on löytynyt ja löytyy runsaasti tietoturva-aukkoja.

# Autentikointi WWW-palvelussa

- Autentikoinnissa eli Käyttäjätunnistuksessa liikkuu AINA henkilökohtaista tietoa, joka täytyy suojata.
- Käytetystä tekniikasta riippumatta perustilanne on aina se, että asiakas joutuu lähettämään tunnistetietoja, jotka palvelin kuittaa.
- Autentikointitietojen välitysoperaatio täytyy suojata jollakin tekniikalla esimerkksi *SSL/TLS*.
- Usein autentikoinnissa käytetään WWW-palvelimen tarjoamia palveluja kuten esimerkiksi Apace-palvelimen *htaccess*.
- ISAPI- tai JAVA-sovellus voi suorittaa autentikointi jollakin yleisesti käytetyllä tekniikalla kuten esimerkiksi *kerberos* ja *netlogon*.
- Autentikoinnissa luotavan *session* elinikä (time to live) oleellinen tieto sekä käyttäjälle että palvelun ylläpitäjälle.

# Lähteitä


- Microsoft: Microsoft Windows 2000 Server TCP/IP Core Networking Guide, Microsoft Press, 2000
- Douglas R. Stinson: Gryptography Thetory and Practice, CRC Press 1995.
- Lewis, Papadimitriou: Elements of the Theory of Computation, Prentice Hall, Second Edition 1998.
- Edward Amoroso: Fundamentals of Computer Security Technology, Prentice Hall, 1994.
- Charles Pfleeger: Security in Computing, Prentice Hall, 1989. Second Edition 1996.
- Jim Keogh: Verkkotekniikat. Tehokas hallinta, IT Press, 2001.
- Terry Ogletree: Inside Verkot, IT Press, 2001.
- Microsoft.com, Microsoft Support Knowledge Base, saatavilla WWW-muodossa, <URL:http://support.microsoft.com/support/kb/>, 7.11.2001.