

Tietoyhteiskuntainstituutin raportteja

2/2005

**Tietoturvallisuuden tutkimus ja opetus**  
Nykytilanne ja kehittämismahdollisuudet

Selvitys

Marko Helenius

Tietojenkäsittelytieteiden laitos  
Tampereen yliopisto

ISBN 951-44-6219-X  
ISSN 1458-8943

Tampere 2005. Tampereen yliopisto.

Tampereen Yliopistopaino Oy.

*Tietojärjestelmät ovat kasvavassa määrin osa arkipäiväämme. Järjestelmien automatisoinnilla, integroinnilla ja langattomilla yhteyksillä saavutetaan kustannustehokkuutta sekä parannetaan käytettävyyttä. Samalla kuitenkin muodostuu aivan uudenlaisia ja ennalta arvaamattomia riskejä. Tietojärjestelmiä käytetään muun muassa maksuliikenteessä, sähkön ja lämmön ohjauksessa, puhelinliikenteessä, äänestämässä, logistiikassa, liikenteen ohjauksessa, puolustusjärjestelmissä ja yhä enemmän osana ihmiselämälle kriittisiä järjestelmiä. Käsiteltävä tieto voi olla myös muista syistä arkaluontoista. Tietojärjestelmien kansainvälisyys ja mahdollisuus järjestelmälliseen väärinkäyttöön aiheuttavat yhteiskunnallisesti merkittäviä uusia uhkia. Tietoturvallisuuden tutkimusta ja opetusta tarvitaan, jotta riskejä tiedostetaan ja pystytään ehkäisemään.*

*Tässä selvityksessä tutkimme Suomen yliopistojen tietoturvallisuuden opetusta ja tutkimusta sekä tietoturvallisuuden tutkimuksen rahoitusmahdollisuuksia. Tarkastelemme tietoturvallisuutta myös Euroopan unionin tukemassa tutkimuksessa. Pohdimme löydetyin perusteella mahdollisuuksia suunnata tutkimusta sekä tietoturvallisuuden tutkimuksen merkitystä. Tarkastelemme myös tietoturvallisuutta käsitteenä, kartoitamme tietojärjestelmien ongelmia sekä pohdimme tietoturvallisuutta ja etiikkaa.*

*Havaitsimme, että tietoturvallisuus on jatkuvasti kehittyvä alue, jonka opetus on vaihtelevaa eri yliopistoissa. Tietoturvallisuuden tutkimus on vasta kehittymässä.*



## Esipuhe

Tampereen yliopiston tietojenkäsittelytieteiden laitoksella käynnistettiin syksyllä 2002 Tietoturvakonsortio-hanke (2004). Koska Tietoyhteiskuntainstituutissa tiedostettiin tietoturvallisuuden merkitys, Tietoturvakonsortio sai vuonna 2003 Tietoyhteiskuntainstituutin (2004) tuen. Tietoyhteiskuntainstituutissa on korostettu tietoturvallisuuden merkitystä myös eTampere-hankkeen eri osa-alueilla.

Tietoturvakonsortiohanke perustettiin edistämään kansallista tietoturvallisuuden yhteistyötä erityisesti akateemisessa maailmassa. Hanke lähti liikkeelle havaitusta johdonmukaisen tiedon puutteesta suomalaisten korkeakoulujen toiminnoista tietoturvallisuuden alueella.

Tietoturvakonsortion tavoitteena on edistää tietoturvallisuuden tutkimusta, koulutusta ja yhteistyötä Suomessa. Keskeinen tavoite on koota yhteen tietoturva-alan tutkijat, opettajat ja tietoturvallisuuteen liittyvät tutkimuslaitokset ja välittää tietoa näiden välillä. Tietoa välitetään esimerkiksi verkkosivustolta löytyvien asiantuntijatietojen, päivitettävän julkaisulistan ja sähköpostilistojen kautta.

Tämä raportti tukee konsortion tavoitteita selvittämällä tietoturvallisuuden tilannetta. Useat henkilöt ovat osaltaan edistäneet tekemääni selvitystyötä. Haluan kiittää erityisesti seuraavia henkilöitä, jotka ovat olleet tärkeänä apuna selvityksen laatimisessa.

*Professori Ari-Veikko Anttiroiko, Tampereen yliopisto, yhdyskuntatieteiden laitos*  
*Professori Jarmo Harju, Tampereen teknillinen yliopisto, tietoliikennetekniikan laitos*  
*Toimitusjohtaja Timo Häkkinen, Contrasec Oy*  
*Professori Raija Järvinen, Tampereen yliopisto, oikeustieteiden laitos*  
*Tutkimusjohtaja Antti Kasvio, Tampereen yliopisto, tietoyhteiskuntainstituutti*  
*Kehityspäällikkö Leo Kaunisto, Tampereen teknillinen yliopisto, tietoverkkoinstituutti*  
*FT Jukka Koskinen, Tampereen teknillinen yliopisto, tietoliikennetekniikan laitos*  
*Projektsihteeri Hanna Liikala, Tampereen yliopisto, tietoyhteiskuntainstituutti*  
*Hanna Manni, Secgo Software Oy*  
*Professori Pirkko Nykänen, Tampereen yliopisto, tietojenkäsittelytieteiden laitos*  
*Tutkimusprofessori Pekka Ruotsalainen, Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus, Tietoteknologian osaamiskeskus*  
*OKT Jari Råman, Lapin yliopisto, oikeusinformatiikan instituutti*  
*Professori Mikko Siponen, Oulun yliopisto, tietojenkäsittelytieteen laitos*  
*FT Ilkka Tuomi, Institute for Prospective Technological Studies, Joint Research Centre*  
*Professori Teemupekka Virtanen, Teknillinen korkeakoulu, tietoliikenneohjelmistojen ja multimedian laboratorio*

Tampereella 13.1.2005

Marko Helenius



## Sisällysluettelo

1. Johdanto .....	1
1.1 Aihealueen kuvaus ja tärkeys .....	1
1.2 Tietoturvallisuuden puutteista aiheutuvat kustannukset .....	2
1.3 Selvityksen tavoite .....	3
1.4 Selvityksen metodi .....	3
1.5 Aikaisemmat selvitykset .....	4
1.6 Tulokset .....	4
2. Tietoturvallisuuden käsitteestä .....	5
3. Tietoturvallisuus ja etiikka .....	6
4. Tietoturvallisuus Suomen politiikassa .....	8
4.1 Viestintäviraston tietoturvaluusyksikkö .....	8
4.2 Kansallinen tietoturvastrategia .....	8
4.3 Valtionhallinnon tietoturvallisuuden johtoryhmä .....	9
4.4 Kansalaisvarmenne .....	9
4.5 Terveysturvallisuuden tietoturva .....	10
5. Tietoturvakonsortiossa mukana olevia yrityksiä .....	12
5.1 Asapsoft Netsystems Oy .....	12
5.2 Contrasec Oy .....	12
5.3 F-Secure Oyj .....	12
5.4 Giwano Computers Ltd .....	13
5.5 Secgo Software Oy .....	13
6. Tietoturvallisuus Euroopan unionin politiikassa .....	14
6.1 EU:n tietoturvavirasto .....	14
6.2 Cybersecurity .....	14
6.3 IPSC .....	15
7. Tietoturvallisuuden tutkimusta Suomen yliopistoissa .....	16
7.1 Helsingin yliopisto: .....	16
7.2 HIIT (Helsinki Institute for Information Technology) .....	16
7.3 Jyväskylän yliopisto .....	17
7.4 Kuopion yliopisto .....	17
7.5 Lapin yliopisto .....	17
7.6 Oulun yliopisto .....	17
7.7 Tampereen teknillinen yliopisto .....	18
7.8 Tampereen yliopisto .....	18
7.9 Teknillinen korkeakoulu (Otaniemi) .....	18
8. Tietoturvallisuuden opetus Suomen yliopistoissa .....	20
8.1 Helsingin yliopisto .....	20
8.2 Jyväskylän yliopisto .....	21
8.3 Kuopion yliopisto .....	22
8.4 Lapin yliopisto .....	22
8.5 Lappeenrannan teknillinen yliopisto .....	23
8.6 Oulun yliopisto .....	24
8.7 Tampereen teknillinen yliopisto .....	26
8.8 Tampereen yliopisto .....	28
8.9 Teknillinen korkeakoulu (Otaniemi, Espoo) .....	30
8.10 Turun yliopisto .....	34
8.11 Vaasan yliopisto .....	34
8.11 Helsingin kauppakorkeakoulu .....	34

8.12 Turun kauppakorkeakoulu .....	35
8.13 Muut yliopistot.....	35
9. Mahdollisia tutkimusaiheita.....	36
9.1 Palvelunestohyökkäykset.....	36
9.2 Sähköinen äänestäminen.....	36
9.3 Tietoturvallisuus ja laki .....	36
9.4 Tietosodankäynti.....	37
9.5 Haitallisten ohjelmien torjunta.....	37
9.6 Vertaisverkot.....	37
9.7 Matkapuhelinlaitteet .....	38
9.8 RFID-teknologia .....	38
9.9 Paikantaminen.....	39
9.10 Terveystieteiden tietoturvallisuus .....	39
9.11 Tietoturallinen ohjelmointi .....	39
9.12 Roskaposti.....	39
9.13 Identiteettivarkaudet .....	40
9.14 Tietoturvallisuus osana käytettävyyttä.....	41
9.15 Digitaalisen television tietoturvallisuus.....	41
9.16 Ohjauksjärjestelmien yhdistäminen turvattomiin verkkoihin.....	41
9.17 Laitteistotason tietoturvallisuus .....	41
9.18 Käyttäjien tietoturva-asenteet .....	42
9.19 Biometrinen tunnistaminen.....	42
9.20 Yritysvakoilu .....	43
9.21 Kotikäyttäjän tietoturva .....	43
9.22 Yksityisyyden suoja.....	43
10. Keskustelu.....	44
10.1 Tulokset .....	44
10.2 Rajoituksia .....	44
10.3 Suositukset jatkotoimenpiteiksi .....	45
Lähteet .....	46
Liite 1: Määritelmiä .....	52
Liite 2: Haitallisen ohjelmakoodin luokitus.....	54

# 1. Johdanto

## 1.1 Aihealueen kuvaus ja tärkeys

Tietoturvallisuuden tekee erityisen mielenkiintoiseksi tarkastelualueeksi sen yhteys lähes kaikkiin tietojenkäsittelyn osa-alueisiin. Tietoturvallisuuden osaamista tarvitaan esimerkiksi tietoliikenteen turvaamisessa, tietojärjestelmien käytettävyyttä suunniteltaessa, ohjelmoitaessa, osana johtamista sekä tietojärjestelmiä käytettäessä. Toisaalta tietoturvallisuus ja sen tutkimus ovat vielä aloina nuoria.

Järjestelmiä on rakennettu ja rakennetaan edelleen toteuttamatta tietoturvallisuutta riittävästi. Kun ohjelmistoja tai laitteistoa toteutetaan projektissa, tyypillisesti pyritään tekemään se, mitä on luvattu ja tietoturvallisuudesta pyritään saavuttamaan ainoastaan minimivaatimukset. Tämä on toisaalta ymmärrettävää, koska projektin itsensä tavoitteiden saavuttaminen vaatii jo sinänsä usein aivan tarpeeksi työtä. Käyttäjien tulisi kuitenkin pystyä myös luottamaan toteutettujen ratkaisuiden turvallisuuteen. Koska jo tehdyn korjaaminen on työlästä ja puutteet voivat aiheuttaa vaikeasti korjattavaa vahinkoa, paras kustannustehokkuus saavutetaan, kun tietoturvallisuus sisällytetään osaksi suunnittelua.

Pohdimme seuraavaksi, minkälaisia puutteita nykyisistä tietojärjestelmistä on löydettävissä:

- *Tietojärjestelmissä käytetään yhä sellaisia vanhentuneita tekniikoita, joita ei ole alun perin tarkoitettu massiiviseen tietoliikenteeseen ja tiedonkäsittelyyn.* Esimerkiksi TCP/IP-protokollassa tietoturvallisuutta ei ole otettu huomioon muuten kuin varmistamalla tiedon kulku useita vaihtoehtoisia reittejä pitkin.
- *Kriittisiä järjestelmiä yhdistetään turvattomiin järjestelmiin.* Internetin suosion vuoksi monia kriittisiä järjestelmiä, kuten pankkijärjestelmät, sähkönsiirron valvonta, osakejärjestelmät, liikenteen ohjaus ja terveydenhuollon järjestelmät, on yhdistetty Internetiin siten, että Internetin tietoturvaongelmat voivat vaikuttaa kriittisten järjestelmien toimintaan. Älykodit ja älykkäät tietolaitteet, joiden kommunikointi toimii julkisten verkkojen kautta, tuovat helppokäyttöisyyden lisäksi myös omat tietoturvaongelmansa.
- *Miljoonissa tietokoneissa ympäri maailman on sama käyttöympäristö.* Tämän seurauksena tietojärjestelmissä on myös samat tietoturvaongelmat ja sama alusta haittaohjelmille ja järjestelmiin tunkeutumiselle.
- *Valtava ja jatkuvasti kasvava laskentakapasiteetti sekä muistitila.* Nykyiset koteihin ja organisaatioihin hankittavat tietojärjestelmät vastaavat suoritusteholtaan muutaman vuoden takaisia supertietokoneita. Muistikapasiteetti on kasvanut moninkertaiseksi muutamassa vuodessa ja kehitys vaikuttaa jatkuvan. Käyttäjän on yhä vaikeampi ja usein jopa mahdoton havaita suoritustehon tai muistitilan väärinkäyttöä, ja toisaalta pahantahtoisiin ja laittomiin tarkoituksiin on tarjolla valtava ja jatkuvasti kasvava kapasiteetti.
- *Nopeat ja avoimet tietoliikenneyhteydet.* Nopeat tietoliikenneyhteydet yhdistettynä avoimuuteen mahdollistavat haitallisten ohjelmien nopean levittämisen sekä laskentakapasiteetin ja tiedonkäsittelyn maailmanlaajuisen yhdistämisen laittomiin tarkoituksiin.

- *Mobiilien tietolaitteiden yleistyminen.* Langattomien tietolaitteiden yleistyminen aiheuttaa kasvavia tietoturvariskejä, koska laitteiden suoritusaste, ohjelmoitavuus ja kapasiteetti kasvavat. Tällöin laitteet ovat alttiita varkauksille, tietomurroille ja haitalliselle ohjelmakoodille. Laitteiden liikuteltavuus ja kytkeminen sisäverkkoihin aiheuttavat tietoturvaongelmia.
- *Puutteellinen tieto järjestelmien toiminnasta.* Järjestelmien monimutkaisuuden takia niiden toimintaa ei voi edes ammattilainen täysin hallita ja ymmärtää, saati sitten peruskäyttäjät.
- *Tietoturvaperiaatteiden heikko noudattaminen.* Keskeisenä vaikeutena tietoturvasäännöissä ja tietoturvapoliitikassa on saada käyttäjät noudattamaan niitä.
- *Laitteistotason tietoturvaratkaisujen puute.* Tietoturvallisuus on tehokkainta silloin, kun se on rakennettu osaksi itse laitteistoa (Helenius 2003), sillä pelkästään ohjelmistojen oikeaan toimintaan ei voida luottaa. Laitteistoarkkitehtuurit ovat kuitenkin tyypillisesti varsin avoimia ja niihin sisällytetyt turvaratkaisut ovat toistaiseksi harvinaisia.

Nopeat yhteydet, saastuneet tietokoneet ja osaamattomuus ovat vaarallinen yhdistelmä. Esimerkkinä nykyisistä ongelmista voidaan mainita Internetissä leviävät tietokonemadot (ks. liite 2, joka sisältää haitalliseen ohjelmakoodin liittyviä määritelmiä). Voidaankin kysyä, miten on mahdollista, että suhteellisen yksinkertainen ja rajoittuneesti leviävä pieni ohjelma kaataa Internetin juuripalvelimia tai että tietokonevirus voi pysäyttää pankkijärjestelmät (Reiss 2003), vaikeuttaa juna- ja lentoliikennettä sekä päästä ydinvoimalan tietojärjestelmään (Mannila 2003). Entä tulevaisuudessa, kun langaton tietoliikenne lisääntyy ja yhä useampia laitteita ja järjestelmiä etäohjataan Internetin ja matkapuhelinverkkojen kautta?

## 1.2 Tietoturvallisuuden puutteista aiheutuvat kustannukset

Nykyisessä mallissa, jossa perussuunnittelun heikkouksia parannetaan tilapäisillä ratkaisuilla, tietoturvallisuus aiheuttaa kansantaloudellisesti merkittäviä kustannuksia. Nämä kustannukset seuraavat ylimääräisestä työkuormasta, joka ongelmista aiheutuu käyttäjille, ylläpitäjille ja ohjelmistojen valmistajille.

Esimerkiksi otamme tietokoneviruksen, joka leviää Internetissä maailmanlaajuisesti tietoturva-aukon kautta. Kustannusten todellista suuruutta on vaikea arvioida. Jonkinlaista kuvaa kustannusten laajuudesta saamme kuitenkin jakamalla kustannukset seuraaviin osiin:

- Virustentorjuntaohjelmien valmistajien työkuorma, joka veloitetaan muun muassa tuotteiden hinnassa.
- Tietoturva-aukkojen etsimisestä aiheutuva työkuorma (mm. yritysten ja tutkimuslaitosten käyttämät resurssit)
- Tietoturva-aukkojen paikkaamisesta aiheutuva työkuorma
- Hallinnollinen työ, kun tietoturva-aukoista ja viruksista tiedotetaan ja tiedotuksia seurataan.
- Käyttäjien työ, kun viruspäivitykset asennetaan ja tietoturva-aukot paikataan.
- Käyttäjien ja ylläpitäjien työ, kun virus poistetaan
- Viruksen aiheuttama työn keskeytys

- Mahdollisesta tuho-operaatiosta tai muusta haitallisesta toiminnosta aiheutuvat kustannukset
- Mahdollisesta luottamuksellisen tiedon vuotamisesta aiheutuvat kustannukset. Virus voi sisältää toimintoja, jotka johtavat luottamuksellisen tiedon paljastumiseen tai epäilyyn sen paljastumisesta.
- Tietoliikenteen hidastumisesta tai estymisestä aiheutuvat kustannukset
- Torjuntaohjelmien ja palomuurien käyttämät resurssit (laskentakapasiteetti ja muistitila)

Voimme tämän perusteella päätellä, että tietokonevirusten aiheuttamat vahingot ovat maailmanlaajuisesti ja kansantaloudellisesti merkittäviä.

Tietoturvallisuuden kokonaiskustannuksia on tätäkin vaikeampi määrittää. Jotain voimme päätellä kuitenkin tietoturvaluustuotteisiin käytetystä rahasummasta. International Data Corporationin (IDC) tekemän tutkimuksen mukaan vuonna 2003 tietoturvallisuuteen käytettiin 220 miljoonaa euroa Pohjoismaissa, mikä tekee tietoturvallisuuden taloudellisesta painoarvosta yhtä suuren laitteisto- ja ohjelmistomarkkinoiden kanssa (Karvonen 2004). IDC arvioi myös, että kustannukset tulevat kasvamaan 21 prosenttia vuodessa.

### 1.3 Selvityksen tavoite

Tässä raportissa tavoitteena on selvittää, miten tärkeitä tietoturvallisuuden opetus ja tutkimus ovat sekä minkälaista tietoturvallisuuden tutkimusta ja opetusta on Suomen yliopistoissa. Tavoitteena on myös selvittää, mihin tutkimusalueisiin tarvitsee erityisesti kiinnittää huomiota. Raportissa painotetaan yliopistoissa tapahtuvaa tutkimusta ja opetusta, vaikkakin myös yritysnaökoulma on mukana tarkastelussa.

### 1.4 Selvityksen metodi

Tutkimus- ja opetustietoa haettiin yliopistojen tieteellisen toiminnan rekistereistä sekä yliopistojen ja niiden alaisten laitosten kotisivuilta. Tiedonhaussa keskityttiin tietojenkäsittelytieteen alan laitosten kotisivuihin. Lisäksi tietoa hankittiin Tietoturvakonsortio-hankkeen yhteydessä muodostuneiden yhteyksien avulla. Tutkimuksen tukena käytettiin myös Internetissä olevaa lähdemateriaalia ja alan kirjallisuutta.

Tutkimus- ja opetustietojen haut tehtiin yliopistojen Internet-sivuilta. Tähän tiedonkeruumenetelmään päädyttiin, koska on oletettavaa, että kurssien kuvaukset ovat julkisesti saatavilla jo sen vuoksi, että opiskelijoiden tulee pystyä saamaan tietoa kursseista Internetistä. Myös tutkimushankkeiden perustietojen voidaan olettaa löytyvän Internetistä, joskin on hyvä huomata, että tutkimushankkeiden tietoja ei julkisteta yhtä avoimesti ja systemaattisesti kuin kurssitietoja.

Tutkimushankkeita haettiin yliopiston hakukoneen avulla tai, jos yliopiston sivuilla ei ollut hakukonetta, haut tehtiin Google-hakukoneella siten, että haut rajattiin kohteena olevan yliopiston Internet-sivuille. Jos yliopistolla oli käytössä tieteellisen toiminnan rekisteri, hakuja tutkimushankkeista tehtiin myös rekisteristä. Hakutermeinä käytettiin hakutermejä ”tietoturva”, ”tietoturvallisuus” ja ”security”. Jos hakutermi antoi liian

useita vaihtoehtoja, käytettiin yksilöivämpiä hakutermejä, kuten ”*information security*” ja ”*data security*” siten, että molempien sanojen tuli esiintyä haun kohteessa samanaikaisesti. Haut tehtiin aikavälillä kesä–lokakuu 2004 kuitenkin siten, että lokakuun aikana tarkistettiin tilanne ja tehtiin tarvittavat muutokset.

Raportti lähetettiin 16.10.2004 kommentoitavaksi tietoturvakonsortio-hankkeen aikana muodostuneelle yhteyshenkilöverkostolle. Henkilöillä oli noin viikko aikaa toimittaa kommenttinsa, joita käytettiin täydentämään raporttia.

### **1.5 Aikaisemmat selvitykset**

Vastaavaa selvitystyötä ei liene tehty aiemmin. Hieman eri näkökulmasta toteutettuja selvityksiä kuitenkin voidaan löytää. Esimerkiksi Vähä-Sipilä (2004) on tutkinut ammattikorkeakoulujen tietoturvallisuutta. Vähä-Sipilä havaitsi, että opetus oli pääasiassa eriytettyä eli tietoturvallisuutta opetettiin lähinnä erillisillä kursseilla sen sijaan, että opetus olisi yhdistetty osaksi muita kursseja. Toinen havainto oli, että opetus painottui tietoverkkojen turvallisuutta edistävien käytännön menetelmien opetukseen. Tietoturvallista ohjelmointia (katso liite 1, joka sisältää määritelmiä termeistä) ei juuri opetettu.

### **1.6 Tulokset**

Raporttia varten on selvitetty tutkimuksen ja opetuksen tilaa Suomen yliopistoissa. Raportissa esitellään lokakuun 2004 tilanne. Myös eri tutkimusalueita sekä tietoturvallisuutta Suomen ja EU:n politiikassa on kartoitettu. Selvityksessä havaittiin, että tutkimusta on vaihtelevasti eri yliopistoissa ja alue on jatkuvasti kehittyvä. Tutkimusalueita kartoitettaessa huomattiin, että on useita tutkimusalueita, joiden kansallinen tutkimus on vähäistä. Eniten akateemista tutkimusta vaikuttaa olevan tiedon salauksen ja tietojärjestelmien haavoittuvuuksien testaamisen alueella.

### **1.7 Raportin rakenne**

Loppuosa raportista jakautuu lukuihin seuraavasti. Luvussa 2 tarkastellaan tietoturvallisuuden käsitettä. Luvussa 3 pohditaan tietoturvallisuuden suhdetta etiikkaan. Luvussa 4 käsitellään tietoturvallisuutta kansallisessa politiikassa. Luvussa 5 kuvataan lyhyesti Tietoturvakonsortio-hankkeessa mukana olevia tietoturvallisuusalan yrityksiä. Luvussa 6 tarkastellaan tietoturvallisuutta Euroopan unionin politiikassa tutkimuksen näkökulmasta. Luvussa 7 tarkastellaan tietoturvallisuuden tutkimusta Suomen yliopistoissa ja luvussa 8 tietoturvallisuuden opetusta Suomen yliopistoissa. Luvussa 9 pohditaan mahdollisia tietoturvallisuuden tutkimusaiheita. Luvussa 10 esitetään johtopäätöksiä sekä pohditaan tutkimuksen rajoituksia.

## 2. Tietoturvallisuuden käsitteestä

Tietoturvallisuus on käsitteenä laaja ja yksiselitteinen rajanveto siinä, minkä asioiden voidaan katsoa lukeutuvan tietoturvallisuuden piiriin ja minkä ei, on mahdotonta. Jotta voimme tarkastella asiaa laajemmin, on kuitenkin hyvä olla jonkinlainen käsitys siitä, mitä tietoturvallisuudella tarkoitetaan. Tarkastelemme seuraavaksi muutamia toisistaan sanamuodoiltaan hieman poikkeavia määritelmiä. Määritelmistä on hyvä huomata, että ne eivät ole tutkijoiden laatimia eivätkä siten heijasta tutkimuksista saatuja tuloksia. Määritelmiä ovat kuitenkin pohtineet useat henkilöt.

Valtiovarainministeriö (2004) pitää yllä myös Tietoturvasanastoa, joka sisältää seuraavan määritelmän tietoturvallisuudelle:

1. Asiantila, jossa tietojen, tietojärjestelmien ja tietoliikenteen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhat eivät aiheuta merkittävää riskiä.
2. Keinojen ja toimenpiteiden kokonaisuus, joiden avulla pyritään varmistamaan tietoturvallisuus niin normaali- kuin poikkeusoloissa.

*Huom.* Tietoturvallisuuden toteuttamisessa erotetaan kahdeksan toimenpidealuetta: hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus.

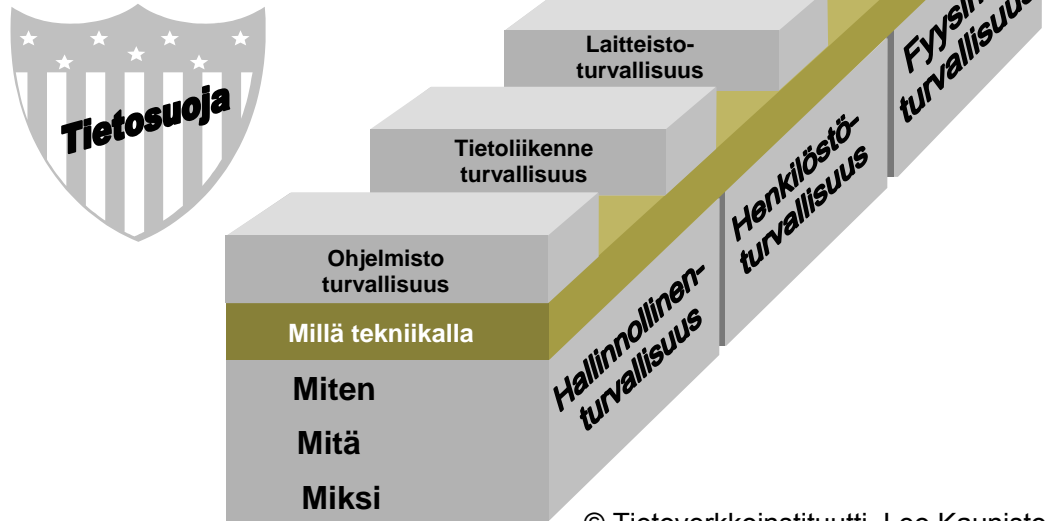
Valtiovarainministeriö (2004) käyttää myös seuraavaa tietoturvallisuuden määritelmää: ”Tietoturvallisuuden osa-alue, johon kuuluvat mm. tietoliikennelaitteiston kokoonpano, sen luettelointi, ylläpito ja muutosten valvonta, ongelmatilanteiden kirjaus, käytön valvonta, verkon hallinta, pääsyn valvonta, viestinnän salaaminen ja varmistaminen, tietoturvallisuuden kannalta merkityksellisten tapahtumien tarkkailu, kirjaus ja selvittäminen sekä tietoliikenneohjelmien testaus ja hyväksyminen.”

Viestintävirasto (2004) käyttää määritelmää ”Tietoturvalla tarkoitetaan niitä hallinnollisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys.” Samassa yhteydessä määritellään myös tietosuojat. ”Tietosuojalla tarkoitetaan henkilön yksityisyyden suojaamista henkilötietojen käsittelyssä. Tätä tarkoitusta varten henkilötiedot on suojattava oikeudettomalta tai henkilöä vahingoittavalta käytöltä.”

Kaunisto (2004) käyttää kuvan 1 mukaista havainnollistusta tietoturvallisuudesta. Organisaation tietoturvallisuuden peruselementeiksi Kaunisto kuvaa hallinnollisen turvallisuuden, henkilöstöturvallisuuden ja fyysisen turvallisuuden (katso liite 1). Pyrittäessä hyvään tietoturvallisuuden tasoon on välttämätöntä tarkastella myös miten tietoaineistoturvallisuus, käyttöturvallisuus, laitteistoturvallisuus, tietoliikenneturvallisuus ja ohjelmistoturvallisuus vaikuttavat haluttuun kokonaisuuteen. Lisäksi tulee pohtia, miksi tietoturvallisuutta toteutetaan, miten tietoturvallisuutta toteutetaan sekä mitä teknisiä tai hallinnollisia ratkaisuja tarvitaan halutun tietoturvallisuuden tason saavuttamiseksi.

# ”Tietoturvan muuri”

## ja ”Tietosuojaan kilpi”



Kuva 1. Kauniston havainnollistus tietoturvallisuuden käsitteestä

### 3. Tietoturvallisuus ja etiikka

Seuraavaksi tarkastellaan tietoturvallisuuden ja etiikan välistä suhdetta. On hyvä huomata, että tässä luvussa ei käydä täsmällistä filosofista keskustelua, vaan esitetään joitakin pohdintoja tietoturvallisuuden ja etiikan välisestä suhteesta.

Tietoturvallisuutta tarkasteltaessa voidaan ajatella, että mitä parempi turvallisuus saavutetaan, sitä vähemmän nykyisen muotoista turvallisuuden ylläpitoa, kehittämistä, tutkimusta ja koulutusta tarvitaan. Näin voidaan olettaa tapahtuvan siitä syystä, että kerran saavutetut helposti monistettavat kokonaisvaltaiset ratkaisut vähentävät tietoturvallisuuden kehittämisen tarvetta. Tämä ristiriita korostaa moraalin merkitystä osana tietoturvallisuutta. Toisaalta tietoturvallisuuden merkitystä ei huomata ennen kuin jotakin tapahtuu. Helposti saattaa unohtua esimerkiksi työntekijöiden aiheuttama yrityksen sisäinen uhka.

Houkutusena voi olla esimerkiksi turvallisuudella rahastaminen toteuttamalla vaillinaisia ratkaisuja, jotka lähinnä paikkaavat joitakin ongelmia mutta eivät paranna turvallisuutta kokonaisuutena. Tästä voi olla esimerkkinä ohjelman julkistaminen tietoturvallisuudeltaan puutteellisena, minkä jälkeen vähitellen paikataan ohjelmassa olevia virheitä. Uudet rahastusmahdollisuuden tarjoavat ongelmat ovat siis väistämättä edessä. Tässä yhteydessä on kuitenkin hyvä muistaa, että aina kyse ei ole puhtaasta hyödyn tavoittelusta vaan kokonaisvaltainen ongelmien ratkaisu edellyttäisi niin perustavanlaatuisia muutoksia järjestelmien suunnittelussa ja käytössä, että muutoksien aikaansaaminen edellyttäisi useiden vuosien turvallisuusalan, kehittäjien ja käyttäjien kokonaisvaltaista yhteistä panostusta.

Yksi mahdollinen vaara on myös, että sellaisten innovaatioiden edistäminen estetään, joiden katsotaan parantavat tietoturvaluottuutta liikaa kerralla. Tällöinhän sellaiset ratkaisut, jotka perustuvat jatkuvaan tietoturvan tarpeeseen kärsivät. Siksi näen tarpeellisena tukea sellaista akateemista tai muuten riippumatonta tutkimusta, joka pyrkii parantamaan tietoturvaluottuutta mahdollisimman puolueettomasta näkökulmasta. Jos kokonaisvaltaisia parannuksia saavutetaan, ne ovat kansantaloudellisesti suureksi hyödyksi, koska oikein toteutetusta tietoturvaluottuudesta hyötyy jokainen.

Pahimmillaan edellä käsitelty tietoturvaluottuuden etiikan laiminlyönti voi johtaa siihen, että tietoturvaluottuutta tuottamuksellisesti heikennetään tai vaillinaista suojausta käytetään hyväksi. Esimerkiksi tietokonevirusten ja niiden torjunnan alalla eräs ajoittain esitetty väite on, että virustentorjunta-alan yritykset luovat viruksia edistääkseen tuotteidensa myyntiä. Epäilemättä jos osaa toteuttaa torjunnan viruksia vastaan, on varmasti osaamista myös haittaohjelmien luomiseksi. Houkutus väärinkäyttöihin voi olla suuri, jos tarkastellaan lyhytaikaista taloudellista hyötyä. Kuitenkin virustentorjujat ovat luoneet kiinteän tutkimusyhteisön, jossa ei katsota hyvällä virusten kirjoittamista ja levittämistä tai tällaisten toimintojen suosimista. Epäeettinen käyttäytymisen seurauksena yksilö tai yritys joutuu väistämättä tutkijayhteisön ulkopuolelle.

Ilmiöstä on mahdollista löytää analogia myös poliisien tai lääkärien toimintaan. Ei voida katsoa hyvällä poliisia tai lääkäriä, joka tekee rikoksia<sup>1</sup> tai laiminlyö auttamisen. Vastaavalla tavalla tietoturvaluottuuden ammattilaisilta tulee vaatia toimimista moraalisesti oikein. Työllisyyden parantamisen tai muun hyödyn ei tule olla motiivina epäeettisyyteen.

---

<sup>1</sup> Lain rikkominen tulee suhteuttaa myös siihen, mikä on moraalisesti oikein (vertaa esimerkiksi diktatuurissa säädettyyn lakiin). On myös hyvä huomata, että laki ja moraalit eivät ole kumpikaan eettinen totuus, vaikka ohjaavatkin toisiaan.

## **4. Tietoturvallisuus Suomen politiikassa**

Tietoturvallisuuden edistämiseen on herätty myös Suomen politiikassa. Näkyvinä merkkeinä tästä ovat Viestintäviraston tietoturvallisuus-yksikön perustaminen, valtiovarainministeriön Vahti-ohjeisto ja kansallinen tietoturvastrategia.

### **4.1 Viestintäviraston tietoturvallisuusyksikkö**

Hallitus päätti 14.6.2001 tietoturvallisuuden hallinnollisia vastuita käsitellessään, että vastuu tietoliikenneturvallisuudesta ja tietoturvaloukkausten käsittely keskitetään Viestintävirastolle vuoden 2002 alusta lähtien (Viestintävirasto 2004).

Tietoturvan ja tietosuoja-alueella Viestintävirastolla on kolme hallinnollista työryhmää, jotka ovat CERT (Computer Emergency Response Team), COMSEC (Communications Security) ja Varmennepalvelut. Lisäksi on yksi standardointiryhmä: telekuuntelun tekninen toteuttaminen.

CERT-työryhmä (Viestintävirasto 2004) toimii yhteistyöelimenä tietoturvaloukkausten havainnoinnissa ja ratkaisemisessa. Lisäksi CERT-työryhmä seuraa ja edistää alan yleistä kehitystä. Työryhmän tehtäviin kuuluvat tietoturvauhkien ja loukkausten ehkäisyyn liittyvät asiat sekä tekninen yhteistyö tietoturvaloukkausten havainnoinnissa ja ratkaisemisessa.

COMSEC-työryhmän (Viestintävirasto 2004) toiminta sisältää kaikki ne toimenpiteet, joiden avulla pyritään turvaamaan tieto- ja telejärjestelmissä siirrettävien tietojen luottamuksellisuus, eheys ja käytettävyys. Toiminta kattaa siis sekä salaamisen laadun varmistamisen ja valvonnan että tietoliikenneverkkojen käytön luotettavuuden ja turvallisuuden valvonnan.

Varmennepalvelut-työryhmä (Viestintävirasto 2004) selvittää tarvetta Viestintäviraston määräyksille ja suosituksille sähköisistä allekirjoituksista annetusta laista ja kartoittaa myös yhteisten toimintatapojen selkeyttämisen tarvetta.

Sähköisessä kaupankäynnissä Viestintäviraston tehtävänä on valvoa, että tietoyhteiskunnan palveluntarjoajat täyttävät tiedonantovelvollisuutensa. Sähköisessä kaupankäynnissä on noudatettava myös kuluttajansuojalain säännöksiä. Näiden noudattamista valvoo kuluttaja-asiamies. Kuluttaja-asiamies (2004) on laatinut verkko-kauppiaille ohjeen, jossa pyritään opastamaan verkkokauppapaikan mallikelpoisessa pystyttämisessä.

### **4.2 Kansallinen tietoturvastrategia**

Valtioneuvosto on tehnyt 4.9.2003 periaatepäätöksen kansallisesta tieturvastrategiasta (Liikenne- ja viestintäministeriö 2004). Liikenne- ja viestintäministeriön asetettiin valmistelemaan strategia. Strategian tavoitteiksi mainitaan:

- edistää kansallista ja kansainvälistä tietoturvallisuusyhteistyötä
- edistää kansallista kilpailukykyä ja suomalaisten tieto- ja viestintäalan yritysten toimintamahdollisuuksia

- parantaa tietoturvallisuusriskien hallintaa
- turvata perusoikeuksien toteutuminen ja kansallinen tietopääoma
- lisätä tietoturvallisuustietoutta ja -osaamista

Tietoturvallisuusstrategia on saanut kansainvälistä arvostusta, kun RSA-konferenssi (RSA Security Inc., 2003) palkitsi kansallisen tietoturvallisuusstrategian parhaana eurooppalaisena turvallisuustoiminnan periaatteena.

### *Kansallinen tietoturvapäivä*

Yhtenä konkreettisena tietoturvallisuusstrategian saavutuksena on 13.2.2004 järjestetty kansallinen tietoturvapäivä, joka näkyi muun muassa julkisissa tiedotusvälineissä. Päivän teemana olivat loppukäyttäjien tietoturvatoinenpiteet. Kun loppukäyttäjä suojaa koneensa hyvin, hän tekee merkittävän palveluksen myös muille: yhteisvastuullisuus on siis tärkeä osa tietoturvaa. Päivän aikana kansalaisille jaettiin ilmaiseksi käyttöjärjestelmien ja sovellusten päivitys-cd:tä sekä joka kodin tietoturvaopas -vihkosta. Cd:ssä ongelmallista oli sen nopea vanhentuminen sekä se, että se toimii ainoastaan suomenkielisissä Windows-järjestelmissä. Cd:n avulla opetetaan kuitenkin käyttäjiä huolehtimaan järjestelmän tietoturvapäivityksistä sekä poistetaan tekoajankohtaan mennessä järjestelmissä havaittuja tietoturva-aukkoja.

Yksi tietoturvapäivän tärkeä saavutus on Internet-sivusto, jota päivitetään jatkuvasti (Tietoturvaopas 2004). Internet-sivusto opastaa käyttäjiä tietoturvallisuuden perusasioissa.

Yleinen linjaus loppukäyttäjän vastuullisuudesta vaikuttaa olevan, että lainsäädännöllisesti ei voida edellyttää, että loppukäyttäjä huolehtii oman tietokoneensa turvallisuuden tasosta. Tätä perustellaan yksilön vapaudella sekä sillä, että vanhoihin tietokoneisiin ja käyttöjärjestelmiin voi olla vaikea saada ajanmukaisia päivityksiä. Operaattorin tulee kuitenkin nykyisen lainsäädännön perusteella huolehtia tietoverkon toiminnasta. Lainsäädäntöä on tulkittu niin, että operaattori voi sulkea verkosta pois järjestelmän, joka aiheuttaa häiriötä tietoverkon toiminnalle.

### **4.3 Valtionhallinnon tietoturvallisuuden johtoryhmä**

Valtiovarainministeriö ohjaa ja sovittaa yhteen valtionhallinnon tietoturvallisuutta ja sen kehittämistä. Valtionhallinnossa on laaja yhteinen tietoturvallisuusohjeisto, joka kattaa kaikki tietoturvallisuuden osa-alueet. Ohjeita kehittää valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI), joka on Valtiovarainministeriön asettama ja tietoturvallisuuden asiantuntemusta laajapohjaisesti edustava ryhmä.

### **4.4 Kansalaisvarmenne**

Kansalaisvarmenteella tarkoitetaan Väestörekisterikeskuksen luonnolliselle henkilölle myöntämää laatuvarmennetta, jonka tietosisältö on määritelty väestötietolaisissa (FINLEX 2004). Jokaiselle kansalaiselle on luotu salainen ja julkinen salausavain, joiden avulla pystytään julkisen salauksen periaatteiden mukaisesti todistamaan käyttäjän henkilöllisyys, tekemään sähköinen allekirjoitus ja salaamaan tietoa. Luotettuna kolmantena osapuolena toimii Väestörekisterikeskus. Salainen avain sijoi-

tetaan mikrosirulle, joka voi olla esimerkiksi henkilökortissa, pankkikortissa tai matkapuhelimen SIM-kortissa. Tietokoneessa tulee olla toimikortinlukija, jotta varmenteen sisältämää henkilökorttia voidaan käyttää.

Väestörekisterikeskus (2004) on perustanut sähköistä henkilökorttia varten Internet-sivut. Kansalaisvarmenteen laajassa käyttöönotossa on ollut ongelmana, että tarvittavia palveluita ei ole ollut eikä tietokoneissa ole oletusarvoisesti lukulaitteita. Lisäksi on mahdollista, että tekniikan turvallisuuteen ja toimivuuteen ei luoteta tarpeeksi.

Varmenne on syyskuusta 2003 lähtien automaattisesti mukana kaikissa uusissa henkilöllisyystodistuksissa. Ajan kuluessa kansalaisvarmenne voi hyvinkin yleistyä. Lokakuussa 2004 voimassa olevia varmenteita oli 49 400 (Väestörekisterikeskus 2004). Väestörekisterikeskus (2004) kehittää yhteistyössä matkapuhelinoperaattoreiden kanssa myös mobiilivarmennetta eli matkapuhelinpalvelua henkilön sähköiseen tunnistamiseen. Tavoitteena on, että mobiilivarmenne tulee kuluttajien saataville vuoden 2004 aikana.

Julkisen avaimen salausjärjestelmissä on kyettävä luottamaan siihen organisaatioon, joka varmentaa avaimet eli todentaa kenelle mikin avain kuuluu. Sirukorttia käytettäessä jonkun on myös luotava avaimet kortille, ja tässä tapauksessa siis Väestörekisterikeskuksella on pääsy avaimiin. Suomessa on kuitenkin hyvä luottamus viranomaisiin, mikä osaltaan edistää varmenteen käyttöä.

#### *Paikallinen esimerkki: eKortti*

Paikallisena esimerkkinä julkisen avaimen salauksen hyödyntämisestä on eTampere-hankkeessa kehitetty eKortti (Tampereen kaupunki 2004). Kortti oli vuonna 2003 pilottivaiheessa ja 5 000 henkilön käytössä. Korttia voi käyttää muun muassa kaupungin liikennelaitoksen ja yhteistariffiliikenteen linja-autoissa, uimahalleissa, kirjastossa ja opiskelijaruokaloissa. Kortti sisältää sähköisen kukkaron, ja kortilla voi käyttää joitakin kaupungin sähköisiä palveluita (mielipidekyselyt, aloitteet, virallinen asiointi ja opiskelijapalveluita mukaan lukien opiskelijoiden terveydenhuollon konsultaatio). Kortilla olevien sovellusten määrä on minimoitu, jotta kortin joustava käyttö voidaan taata.

### **4.5 Terveydenhuollon tietoturva**

Alla erittelen terveydenhuollon tietoturvallisuuden tutkimusta Stakesissa (Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus) sekä Terveydenhuollon tietosuojaryhmän toimintaa.

#### *Stakes*

Stakesin tietoteknologian osaamiskeskus (OSKE, Stakes 2004) tekee tutkimustyötä seuraavilla terveydenhuollon tietosuojan ja tietoturvallisuuden alueilla:

- Tietoturvallinen sähköinen arkistointi
- Terveydenhuollon tietoturvallinen tiedonvälitys

Yhdessä Tampereen yliopiston kanssa OSKE tutkii ja kehittää terveydenhuollon informaatiojärjestelmien tietoturvallisuuden arvioinnin menetelmiä. Sosiaali- ja terveydenhuollon sähköisen asiointin strategioissa tietoturvallisuudella ja henkilötietojen käsittelyn luottamuksellisuudella on keskeinen asema. Tietosuoja käsitellään muun muassa Sosiaali- ja terveydenhuollon tietoteknologian hyödyntämisstrategiassa (Sosiaali- ja terveysministeriö 1995) sekä työryhmämuistiossa Saumaton hoito- ja palveluketju (Sosiaali- ja terveysministeriö 1998). Kansallisen terveysprojektin sähköisen potilaskertomushankkeen yhteydessä OSKE on laatinut vaatimukset terveydenhuollon toimintayksiköiden välisen tiedonvaihdon tietoturva- ja tietosuojavaatimuksiksi. OSKE on osallistunut myös kansainväliseen terveydenhuollon informatiikan tietosuojan standardisointityöhön (ISO-TC 215 Health Informatics, WG4 Security).

Sähköisen potilaskertomuksen käyttöönottoprojektin julkaisussa *Tietoturvallinen kommunikaatioalusta: Suositus kansallisesti noudatettaviksi standardeiksi* (Ensio & Ruotsalainen 2004) on nimetty terveydenhuollon sähköisen asiointin kannalta keskeiset standardit. Tietoteknologian osaamiskeskus on saanut sosiaali- ja terveysministeriöltä tehtäväksi koordinoita tietoturvallisuuden ja tietosuojan alueellisia toteutushankkeita. Parhaillaan noin puolet Suomen sairaanhoitopiireistä ottaa käyttöön julkisen avaimen salauksen arkkitehtuuria.

OSKE on julkaissut suosituksen terveydenhuollon kansalliseksi tietoturva-arkkitehtuuriksi (Ruotsalainen 2002). Parhaillaan OSKE laatii kansallista ohjeistusta terveydenhuollon toimintayksiköiden henkilötietojen käsittelyn tietoturvapoliittiseksi.

#### *Terveydenhuollon tietosuojaryhmä*

Tietosuojavaltuutetun toimisto on perustanut myös terveydenhuollon tietosuojaryhmän (TELLU-ryhmä, Tietosuojavaltuutetun toimisto 2004). TELLU käsittelee terveydenhuollon tietosuoja- ja tietoturvakysymyksiä sekä laatii alaan liittyviä hyvän käytännön ohjeistuksia sekä järjestää terveydenhuollon ammattihenkilöille suunnattua koulutusta.

## **5. Tietoturvakonsortiossa mukana olevia yrityksiä**

Seuraavassa esittelemme joitakin tietoturvallisuusalan yrityksiä sekä niiden toimintamuotoja. Tarkoituksena ei ole esittää kattavaa jäsenystä koko tietoturvallisuusosalasta vaan rajata käsittely niihin yrityksiin, joihin on muodostunut yhteyksiä Tietoturvakonsortio-hanketta koordinoidessani.

### **5.1 Asapsoft Netsystems Oy**

Asapsoft Netsystems Oy (2004) on sähköisten liiketoimintajärjestelmien toteuttamiseen erikoistunut suomalainen ohjelmistotalo. Yrityksen ASAP- ja NETTA-ohjelmistot ovat liiketoimintakriittisiin verkkopalveluihin soveltuvia sähköisen liiketoiminnan järjestelmiä. Tietoturvallisuus on yrityksen toteuttamissa ratkaisuissa keskeinen tekijä. Henkilöstö omistaa yrityksestä 80,1% ja Aldata Solution Oyj 19,9%. Liiketoiminta siirtyi Asapsoft Netsystems Oy:n nimiin 1.9.2002.

### **5.2 Contrasec Oy**

Contrasec Oy (2004) on syksyllä 2001 perustettu asiantuntijayritys, joka tuottaa korkeaa ammattitaitoa vaativia koulutus- ja konsultointipalveluita asiakkailleen. Koulutuksen painopistealueita ovat tietoturva ja tietoliikenne. Yrityksen tilat sijaitsevat Tampereella, mutta käytössä on yhteistyökumppaneiden tiloja myös muissa suurissa kaupungeissa. Lisäksi käytettävissä on siirrettävä opetusluokka. Yritys on yksi harvoista tietoturvaan erikoistuneista koulutusyrityksistä Suomessa. Yrityksellä on osaamista tietoturvatapahtumien selvityksessä.

### **5.3 F-Secure Oyj**

F-Secure Oyj (2004) on hajautettujen, keskitetysti hallittavien tietoturvaratkaisujen toimittaja. F-Securen tuotevalikoima sisältää keskitetysti hallittavia virustentorjunta-, tiedosto- ja verkkosalaustuotteita, sekä hajautettuja palomuurituotteita yritysten kaikille keskeisille laitealustoille, työasemista verkkolaitteisiin ja palvelimista langattomiin taskutietokoneisiin.

F-Securen tuotteet sopivat erinomaisesti yritysten IT-osastojen, jälleenmyyjien ja palveluntarjoajien kautta jaettaviksi. Loppukäyttäjälle tuotteet ovat näkymättömiä, automaattisia, luotettavia, aina päällä ja päivitettyjä. Järjestelmän haltijalle tuotteet tarjoavat laajalle hajautetun käyttäjäkunnan keskitetyn hallittavuuden sekä ajantasaisen raportoinnin.

Yritys on perustettu 1988 ja noteerattu Helsingin pörssissä. Yhtiön pääkonttori sijaitsee Helsingissä sekä Pohjois-Amerikan pääkonttori San Josessa, Kaliforniassa. Yhtiöllä on lisäksi toimistot Saksassa, Japanissa, Ruotsissa ja Englannissa sekä jälleenmyyjiä yli 90 maassa eri puolilla maailmaa.

#### **5.4 Giwano Computers Ltd**

Giwano Computers Ltd (2004) valmistaa turvatietokoneita ja ohjelmistoja korkeaa tietoturvaa vaativien yritysten ja yhteisöjen tarpeisiin. Yrityksen avaintuote on Giwano-turvatietokone. Tietokone koostuu kahdesta erillisestä yksiköstä sisäisiä ja ulkoisia yhteyksiä varten. Kone mahdollistaa helpon mutta silti turvallisen tiedonsiirron yksiköiden välillä ja toimii erinomaisena alustana korkean turvataso verkkoratkaisuille.

#### **5.5 Secgo Software Oy**

Secgon ohjelmistoilla rakennetaan tietoturva- ja liikkuvuudenhallintaratkaisuja muun muassa etäkäyttö-, WLAN- ja VoIP-järjestelmiin. Secgon tuotteet ovat laajalti käytössä vaativilla toimialoilla, kuten julkishallinnossa, pankki- ja rahoitussektorilla, teollisuudessa ja puolustushallinnossa. Secgon ohjelmistot toimitetaan yhä useammin osana suurten tietotekniikkatoimittajien ratkaisuja, kuten Atea, Fujitsu, TeliaSonera ja IBM.

## 6. Tietoturvallisuus Euroopan unionin politiikassa

Myös EU:ssa on huomattu tilanteen vakavuus ja suhtauduttu myönteisesti tietoturvallisuuden edistämiseen. Merkkeinä vakavasta suhtautumisesta ovat muun muassa EU:n tietoturvaviraston perustaminen, poliittista päätöksentekoa tukeva tietoturvallisuuden tutkimus sekä tietoturvallisuuden ottaminen mukaan tutkimusohjelmiin (katso esimerkiksi CORDIS NEWS 2004).

### 6.1 EU:n tietoturvavirasto

Yhtenä merkkinä ongelmien vakavuudesta ja EU:n vakavasta suhtautumisesta tietoturvallisuuden edistämiseen on EU:n päätös perustaa tietoturvavirasto. EU:n tietoturvavirasto eli ENISA (European Network and Information Security Agency, ENISA 2004) on yksi virastoista, jotka on jaettu eri EU-maihin. Tietoturvavirastolle on varattu määrärahaa 34,3 miljoonaa euroa viidelle ensimmäiselle vuodelle (vuodet 2004–2008).

Tietoturvaviraston yhtenä ehdokasmaana oli Suomi, mutta EU-maiden johtajat päättivät lopulta viraston sijoittamisesta Kreikkaan. Erkki Liikasen (2003) mukaan tietoturvavirasto keskittää toimintansa seuraaviin alueisiin:

- Komission ja jäsenmaiden avustaminen ja ohjaaminen tietoturvallisuudessa ja yhteyksissä yrityksiin laitteisto- ja ohjelmistotason tietoturvallisuuden ongelmissa
- Tietoturvatapauksista ja uusista riskeistä saatavan tiedon kerääminen ja analysoiminen Euroopassa
- Riskien hallinnan ja johtamisen menetelmien edistäminen, jotta mahdollisuudet käsitellä tietoturvauhkia paranevat
- Tietoisuuden ja yhteistyön kasvattaminen eri osapuolien välillä sekä erityisesti julkisen ja yksityisen sektorin kumppanuuden kehittäminen

Tietoturvaviraston ensimmäiseksi johtajaksi valittiin Andrea Pirotti Italiasta ja varajohtajaksi Ferenc Suba Unkarista. Kristiina Pietiläinen Suomesta valittiin johtokunnan puheenjohtajaksi.

### 6.2 Cybersecurity

JRC (Joint Research Center, 2004) tukee Euroopan komission poliittista päätöksentekoa puolueettomalla tieteellisellä ja teknisellä osaamisella. JRC:n alaisuudessa on töissä noin 2 000 henkilöä, ja sen vuotuinen budjetti on yli 300 miljoonaa euroa. JRC koordinoi seitsemää tutkimuslaitosta, joista yksi on Espanjan Sevillassa sijaitseva IPTS (Institute for Prospective Technological Studies 2004). Yksi IPTS:n tieteellisistä osa-alueista (ISA, Integrated Scientific Area) on tietoturva (*Cybersecurity*) (2004). Osa-alueen tavoitteiksi mainitaan:

- Lainsäädännön viitekehyksen muodostaminen tukemaan kansalaisten yksityisyyden suojaa
- Tietoyhteistyö CERT-keskusten (Computer Emergency Responce Team, 2004) kanssa

- Tiedon kokoaminen tietorikoksista
- Kuluttajien suojeleminen sähköisessä kaupankäynnissä. Tämä sisältää kuluttajiin kohdistuneiden huijausten käsittelyn sekä valitusten käsittelyn toteuttamisen.
- Nousevien uhkien tunnistaminen ja näistä varoittaminen sekä tulevien suuntausten löytäminen
- Sosioekonomisten vaikutusten arvioiminen ja tulevaisuuden teknologioiden tutkiminen

*Cybersecurityn* alaisuudessa mainitaan seuraavat tutkimusprojektit:

*Cybersecurity skills and training needs and the impact on employment*

Tutkimuksen tarkoitus on tunnistaa ja analysoida tulevaisuuden tietoturvallisuuden tarpeita koulutuksen ja osaamisen osalta. Tutkimus jatkui vuoden 2002 kesäkuusta tammikuuhun 2003.

*Identity management systems*

Tutkimuksen kesto oli heinäkuusta 2002 tammikuun 2003. Tuloksena syntynyt tutkimusraportti (ICPP, 2004) käsittelee tunnistamisen hallintaa Internetissä. Projektissa on tutkittu tunnistamisenhallintajärjestelmiä sekä tehty kyselytutkimus 80 ammattilaiselle.

*A Network of Excellence for the Future of IDentity in the Information Society (FIDIS)*

FIDIS-hanke on Euroopan Unionin kuudennen puiteohjelman tukema Network of Excellence -tyyppinen projekti. Projektin kesto on 60 kuukautta alkaen maaliskuusta 2004 eteenpäin. Projektin tutkimuskohteena ovat teknologiat, jotka tukevat tunnistautumisen hallintaa, tunnistautumisen ja autentikoinnin keskinäistä toimimista, identiteettivarkauksien (katso liite 1) torjumista, yksityisyyden suojaa, turvallisuutta sekä profiilien keräämistä ja väärinkäytösten jäljittämistä (FIDIS 2004).

*Security and privacy for the citizen in the post-September 11 digital age*

Tämä tutkimus on tehty Euroopan Parlamentin LIBE-komitealle (Committee on Citizens' Freedoms and Rights, Justice and Home Affairs). Tutkimuksen perusteella on syntynyt raportti, jossa selvitetään syyskuun yhdennentoista terrori-iskun vaikutuksia kansalaisen yksityisyydensuojaan ja turvallisuuteen (Clements et al. 2003).

*Virtual residence*

IPTS:n alaisuudessa on myös virtuaaliseen minän tutkimusta, jossa painopiste on yksityisyyden suojassa identiteetin hallinnan alueilla. Skenaarioita on viety eteenpäin muun muassa käsitteellistämällä ajatusta ”digitaalisista territorioista” (Besley & Hakala 2004).

### 6.3 IPSC

JRC:n tietoturvaan liittyvään toimintaan kuuluu myös Italiassa sijaitseva Institute for the Protection and Security of the Citizen (IPSC 2004), jossa tutkitaan muun muassa kuluttajansuojan tietoturvallisuutta. IPSC:ssä tutkimuksen painotus on fyysisessä turvallisuudessa, mutta myös tietoturvallisuus on mukana.

## **7. Tietoturvallisuuden tutkimusta Suomen yliopistoissa**

Käsitykseni on, että nimenomaan tutkimustyöllä pystytään luomaan teorioita ja innovaatioita, jotka edistävät tietoturvallisuutta. Toisaalta tutkimusta säätelevät rahoitus ja henkilöiden suuntautuminen. Tarvitaan siis ihmisiä, jotka ovat aidosti kiinnostuneita tietoturvallisuuden tutkimuksesta ja toisaalta rahoittajia tutkimustyölle. Tutkimustyö ei ole pelkästään korkeakoulujen sisäistä tutkimustyötä, vaan myös yrityksiä on usein mukana.

Tutkimustyön ei pitäisi perustua vain jo tunnetuille alustoille, vaan tietoturvallisuutta pystytään edistämään parhaiten luomalla aivan uudenlaisia ratkaisuja. Olen kuvannut joitakin konkreettisia tapoja, joilla tietoturvallisuuden parantaminen on mahdollista (Helenius 2003). Näitä ovat esimerkiksi tarkistussummien ja sähköisen allekirjoituksen menetelmien ottaminen osaksi tietojärjestelmien turvallisuutta, integroidut varmistusjärjestelmät, integroitu käynnistys turvalliselta alustalta, laitteistotason ratkaisut tukemaan käyttöoikeuksien hallintaa, ohjattu laitteistotason eristäminen ja ilmaisimet, joita ei voi ohjelmallisesti ohittaa.

Seuraavaksi käsittelem tietooni tulleet yliopistojen tutkimushankkeet Suomessa. Tässä kohdin on hyvä huomata, että lista ei välttämättä kata kaikkia olemassa olevia hankkeita.

### **7.1 Helsingin yliopisto**

Helsingin yliopiston hanketietokannasta (2004) löytyi hakutermillä ”tietoturva” hanke ”Sähköisen asioinnin oikeudelliset ongelmat”.

”Sähköisen asioinnin oikeudelliset ongelmat” on kansainvälisen talousoikeuden instituutin hanke, jota kuvataan seuraavasti ”Tutkimuksen tarkoituksena on kartoittaa ja analysoida keskeisimmät ajankohtaiset oikeudelliset ongelmat, joita liittyy sähköiseen asiointiin. Selvitettäviä kysymyksiä ovat muun muassa sähköinen identiteetti, yksityisyydensuoja, menettelysääntely, asiakkaan oikeudet ja oikeusturva sekä tietojen luovutukseen liittyvät kansainväliset näkökohdat.” Tutkimus on toteutettu vuosina 1999–2000 kahdentoista kuukauden työjaksona.

### **7.2 HIIT (Helsinki Institute for Information Technology)**

Helsingin yliopiston ja teknillisen korkeakoulun yhteisessä HIIT-tutkimusinstituutissa (Helsinki Institute for Information Technology) mainitaan yksi tietoturvallisuutta tutkiva hanke: Security Technologies and Attitudes in Mobile IPR (Rantanen et al. 2003, s. 20). Hanke on toteutettu vuosina 2002–2003. Projektin rahoittajina olivat Tekes Nokia ja Elisa Communications. Hankkeessa tutkittiin informaation validiteettia sekä yksityisyyden suojaa välitettäessä tekijänoikeudella suojattua sisältöä asiakkaiden tietolaitteille. Hankkeen tavoitteissa mainitaan hankkeen suuruudeksi 163 miestyövuotta (STAMI 2004).

### **7.3 Jyväskylän yliopisto**

Jyväskylän yliopiston tietotekniikan laitoksella tietoturva mainitaan yhtenä osa-alueena tieteelliseen laskennan tutkimuksessa (Jyväskylän yliopisto 2004). Samassa yhteydessä mainitaan myös yksi konkreettinen tutkimushanke nimeltä ”Tietoturvamenetelmät”: ”Selvitetään ja kehitetään erilaisia ratkaisuja verkon palveluiden suojaamiseen. Tämän tutkimuksen pääpaino on palomuuritekniikoiden toimintamallien, konfiguraatioiden ja niiden tarjoaman tietosuojan selvittäminen tuotantoverkoissa. Tulevaisuudessa tullaan käyttämään älykorttipohjaisia ratkaisuja, joita tämän tutkimuksen avulla myös selvitetään ja kehitetään. Projekti on alkanut vuonna 1998. Mukana Sonera ja Nokia.”

### **7.4 Kuopion yliopisto**

Kuopion yliopiston (2004) terveyshallinnon ja -talouden laitoksen yhtenä tutkimuskohteena mainitaan terveydenhuollon tietoturvaprosjekti (PKI), jonka tavoitteena on terveydenhuollon tietojärjestelmien tietoturva- ja suojaratkaisujen kehittäminen ja mallintaminen.

### **7.5 Lapin yliopisto**

Oikeusinformatiikan instituutissa tietoturvasuhteisuus on ollut keskeisellä sijalla valtiovarainministeriölle tehdyssä selvityksessä ”tietoturvasuhteisuus ja laki” (Saarenpää ja Pöysti 1997), jossa kartoitettiin tietoturvasuhteisuuden sääntelyn tilannetta ja tulevasuutta. Lisäksi instituutissa tehdään selvitystä liikenne- ja viestintäministeriölle perusoikeuksien huomioonottamisesta tietoturvasuhteisuuden sääntelyssä ja viranomaisten sähköisissä palveluissa.

### **7.6 Oulun yliopisto**

Oulun yliopistossa on kolme professuuria, joiden erikoistumisalueena on tietoturvasuhteisuus. Professori Juha Röning vastaa OUSPG-yksiköstä (Oulu University Secure Programming Group 2004), professori Juha Kortelainen vastaa tietoturvasuhteisuuden opetuksesta tietojenkäsittelytieteiden laitoksella ja professori Mikko Siponen on keskittynyt tietoturvasuhteisuuden tietojärjestelmätieteen näkökulmasta.

Juha Röningin vetämä OUSPG-yksikkö tutkii, arvioi ja kehittää menetelmiä toteutus-tason tietoturva-aukkojen paikantamiseen. Projektin kotisivuilla esitellään kaksi tutkimusprojektiä: ”PROTOS – Security Testing of Protocol Implementations” ja ”FRONTIER-COMPAT – Inferring Causal Relationships in Complex Systems”.

PROTOS-projektin tavoitteena on tutkia protokollista löydettäviä tietoturvasuhteuteita. PROTOS-projekti on Oulun yliopiston ja VTT Elektronikan yhteinen projekti, jonka rahoittajina olivat vuosina 1999–2001 TEKES ja kaksi telealan yritystä. Yhteenlaskettu rahoitus oli näinä vuosina noin 320 000 euroa. Vuosina 2002 ja 2003 projektia on jatkettu yritysten tuella. Projektiä ovat tukeneet Microsoft Research ja Codenomicon Ltd.

FRONTIER-COMPAT-projektin tavoitteena on toteuttaa menetelmiä, joilla voidaan päätellä monimutkaisissa tietoverkoissa olevia tietoturvaluutteita. Projekti on TEKES-rahoitteinen ja sen rahoitus on ollut vuosina 2002–2004 noin 100 000 euroa vuodessa.

### **7.7 Tampereen teknillinen yliopisto**

TTY:n tietoliikennetekniikan laitoksella tietoturvatutkimusta on tehty professori Jarmo Harjun (2004) johtamassa Tekesin NETS-ohjelmaan kuuluvassa ICEFIN-projektissa. Erityiskohteena ovat olleet julkiset langattomat verkot, niissä tapahtuva autentikointi sekä pääsynvalvonta niiden kautta muihin järjestelmiin.

### **7.8 Tampereen yliopisto**

Tampereen yliopiston tietojenkäsittelytieteiden laitoksella on Tietoturvakonsortiohankkeen lisäksi maanpuolustuksen tieteellisen neuvottelukunnan (Puolustusministeriö 2004) rahoittama projekti vuodelle 2003, jossa on tutkittu hajautetun palvelunestohyökkäyksen havaitsemis- ja torjumismahdollisuuksia sekä mahdollisuuksia tekijöiden jäljittämiseen.

Samoin tietojenkäsittelytieteiden laitoksen yhteydessä toimii virustutkimusyksikkö, jossa on muun muassa arvioitu tietokonevirusten torjuntaohjelmien virustentorjuntakykyä sekä tehty kansainvälistä yhteistyötä virustentorjuntaohjelmien valmistajien kanssa. Virustentorjuntaohjelmien vertailun aktiivinen aika on ollut vuosina 1994–1999.

### **7.9 Teknillinen korkeakoulu (Otaniemi)**

Teknillisessä korkeakoulussa on kolme tietoturvallisuuden alueen professuuria, joten tämä heijastuu myönteisesti sekä tutkimukseen että opetukseen. Helger Lipmaa (2004) on kryptologian professori teoreettisen tietojenkäsittelyn laboratoriossa ja johtaa kryptologian tutkimusryhmää. Teemu-Pekka Virtanen (2004) on turvallisuuden professori tietoliikenneohjelmistojen ja multimedian laboratoriossa. Hannu Kari (2004) on osa-aikainen professori tietojenkäsittelyteorian laboratoriossa.

Lipmaan tutkimusryhmällä on ulkopuolisella rahoituksella toteutettava tutkimushanke (aiemmin Krypto) nimellä CYDAMI (Cryptology and Data-Mining). CYDAMI-hanke on saanut Suomen Akatemian rahoituksen vuosille 2004–2007 kolmeksi ja puoleksi vuodeksi.

Ohjelmistoliiketoiminnan ja -tuotannon laboratoriossa on käynnissä NETPROSEC-projekti. Projektin Internet-sivuilla (SoberIT 2004) on kuvattu projektin taustaa:

”NETPROSEC-projektissa tutkitaan tietosuojan toteutumista erilaisissa tietojärjestelmissä, tiedonsiirrossa sekä käyttöympäristöissä. Lähtökohtana ovat lainsäädännön asettamat tietosuoja- ja tietoturva vaatimukset. Osana tutkimusta analysoidaan yrityksissä ja organisaatioissa toteutettuja tai suunnitteilla olevia internet- ja verkkopalveluja, muita viestintäpalveluja sekä asiakastietojen hallintaa. Lisäksi perehdytään mm. varmennepalveluihin ja tietoturvatoteutuksiin sekä arvioidaan niiden merkitystä tietosuojan toteutumisessa.”

Projektissa ovat mukana Alma Media Oyj, Elisa Communications Oyj/Kolumbus Oy, Väestörekisterikeskus, liikenne- ja viestintäministeriö, Nixu Oy ja tietosuojavaltuutetun toimisto. Projektin tavoitteet kuvataan seuraavasti:

”NETPROSEC-projektin tavoitteena on tuottaa toimintamenetelmä ja työkalun prototyyppi tietosuojan ja tietoturvan toteuttamiseen yrityksissä ja organisaatioissa. Projektin työssä kehitettävää menetelmää ja sitä tukevaa työvälinettä hyödyntävät ensisijaisesti sovelluksia, toteutus- ja turvaamisteknologiaa kehittävät yritykset sekä palvelujen tuottajat tuotekehityksessään, palvelujen tuottamisessa ja ylläpidossa. Sen avulla varmistetaan suojattu ja turvallinen tiedon kulku läpi koko toiminta- tai palveluprosessin ja tieto- ja tiedonsiirtojärjestelmän.”

Ohjelmistoliiketoiminnan ja -tuotannon laboratoriossa (2004) toimii myös Muppet-projekti (Managing Privacy and Trust in P2P Communication). Projektia kuvataan seuraavasti:

”Vertaisverkkoteknologiat tarjoavat radikaaleja uusia mahdollisuuksia erilaisiin viestintätilanteisiin, olkoon kyseessä sitten yleisradiolähetys, ryhmien välinen tai henkilökohtainen viestintä. Uusi, hajautettu viestintäteknikka tuo mukanaan kuitenkin myös monia viestinnän luottamuksellisuuden ja yksityisyyteen liittyviä haasteita ja ongelmia. Muppet-tutkimusprojekti tutkii näitä yksityisyyden ja luottamuksen ongelmia käyttäen sekä teknistä että taloudellista näkökulmaa yhdistettynä käytettävyyss-tutkimukseen.”

Ohjelmistoliiketoiminnan ja -tuotannon laboratoriossa (2004) on meneillään myös Go-Sec-projekti (GO Project 2004). Projektin tavoitteena on tutkia tietoturvaongelmia ja riskejä, jotka ovat osana langatonta Internet-yhteyttä. Projektin on tavoitteena myös toteuttaa ohjelmallinen SIM-kortti, jolla käyttäjä voidaan tunnistaa sellaisissa tietokoneissa, joissa fyysistä SIM-korttia ei voida käyttää.

## 8. Tietoturvallisuuden opetus Suomen yliopistoissa

Tietoturvallisuuden opetuksen merkitys on siirtää tietoa sekä luoda sellainen ympäristö, joka edistää tutkimustyötä. Opetuksella saadaan parhaimmillaan aikaan myönteinen ketjureaktio: Opiskelijat tulevat ensin tietoiseksi tietoturvallisuuden ongelmakentästä. Myöhemmin nämä opiskelijat ovat niitä, jotka suunnittelevat tietojärjestelmiä ja osallistuvat yhteiskunnan kannalta merkittäviin päätöksiin. Kun tietoturvallisuus on osa päätöksentekoa ja suunnittelua, tulee yhteiskunnastakin parempi paikka elää.

Yliopistojen yhteisiltä tietoturvasivuilta (U-Cert-työryhmä 2004) löytyvät muun muassa seuraavat kaikille yliopistoille yhteiset sääntöpaketit:

- Sähköpostin käsittelysäännöt
- Sähköpostin suodatusohje
- Toimenpiteet tietojärjestelmien käyttöoikeuden loputtua
- Ohjeet tiedostojen käsittelystä tietojärjestelmien käyttöoikeuden haltijan kuoltua
- Tietojärjestelmien ylläpitosäännöt
- Tietoturvapoikkeamiin reagoiminen
- Tiedottaminen poikkeamatilanteissa
- Tietotekniikkarikkomusten seuraamuskäytäntö
- Seuraamusasteikot (henkilökunta, opiskelija, muut) tietoturvaloukkaustilanteissa.

Seuraaviin taulukoihin on kuvattu tietoturvallisuuden opetusta Suomen yliopistoissa elokuun ja lokakuun 2004 aikana tehdyn kartoituksen perusteella.

### 8.1 Helsingin yliopisto

Helsingin yliopistossa tietoturvallisuuden opetusta on tietojenkäsittelytieteen laitoksella seuraavasti:

Kurssi / laitos	Laa-juus	Kuvaus	Suoritustapa
Tietoturva / Tietojenkäsittelytieteiden laitos	3 ov (S)	Tietoturva on valinnainen kurssi, joka soveltuu erityisen hyvin hajautettuihin järjestelmiin ja tietoliikenteeseen suuntautuille. Myös muiden erikoistumissuuntien opiskelijoille kurssi käy hyvin. Kurssilla pyritään käsittelemään tietoturvaprotokollia ja tunkeutumisen estämistä kryptografiaa kokonaan unohtamatta.	Luennot, harjoitukset, tentti
Tietoturvan jatkokurssi / Tietojenkäsittelytieteiden laitos	3 ov (S)	Tietoturvan jatkokurssi soveltuu niille, joilla on kurssin Tietoturva tiedot ja jotka ovat kiinnostuneita syventämään teoreettisia tietojaan tietoturvasta. Kurssilla ei käsitellä juuri lainkaan kryptografiaa eikä ylläpitoon liittyviä ongelmia. Sen sijaan keskitytään tietoturvan erilaisiin malleihin. Kurssia pyritään luennoimaan silloin tällöin, esimerkiksi parin vuoden välein. Eri luentokerroilla kurssin sisältö vaihtelee.	Luennot, harjoitukset, tentti

Seminaari: Tietoturvallisuus nykyaikaisessa liiketoimintaympäristössä	2 ov (S)	Seminaarissa perehdytään tietoturvan hallintaan sekä organisatoriselta että tekniseltä kannalta.	Seminaarityö, esitelmä
---	----------	--	------------------------

Taulukko 1: Tietoturvallisuuden kurssit Helsingin yliopistossa

Lisäksi Helsingin yliopistossa on ollut muita seminaareja, joista mainitaan verkkosivuilla: ”Selected topics in information security” (pidetty vuonna 2003, 2 ov), ”Research seminar on advanced topics in security and cryptography” (2 ov, peruttu), ”Security in distributed systems” (pidetty vuonna 2000, 2 ov) ja ”Hajautettujen järjestelmien tietoturva” (pidetty vuonna 1998, 2 ov).

## 8.2 Jyväskylän yliopisto

Tietojenkäsittelytieteen laitoksella on seuraavat kurssit:

Tietoturva	2 ov	Tietoturvan toteutusperiaatteet seuraavissa yhteyksissä: laitteet, käyttöjärjestelmä, ohjelmistot, tietokannat, tietokoneverkot, sähköposti, www-selaus, etäkäyttö, sähköinen kaupankäynti ja asiointi. Em. osa-alueiden teoreettisluonteisia täydennyksiä sekä kryptografian perusteita (joitain laskuharjoituksia).	Luennot 28 t, harjoitukset ja tentti
Tietokone ja tietoverkot työvälineenä	2 ov	Kurssin tavoitteena on antaa opiskelijalle sellaiset tiedolliset ja taidolliset perusvalmiudet, jotka mahdollistavat tiedekunnan oppiaineiden opetuksen seuraamisen ja omien valmiuksien jatkuvan kehittämisen tulevaisuudessa. Sisältö: 1) Agoranetin käyttö, virukset ja tietoturva; 2) WWW:n käyttö ja tiedonhaku; 3) Käyttäytymissäännöt verkossa, yksityisyys ja immateriaalioikeuksien alkeet; 4) Perus- ja työkaluohjelmistot (tekstinkäsittely, esitysgrafiikka, pakkausohjelmat); 5) WWW-sivujen tuottamisen alkeet.	Luennot, harjoitukset ja harjoitus-työ
Peruskäyttäjän tietoturva	0 ov	Mitä juuri minun tulisi tietää tietoturvasta? Teemoina mm. tietoturvariskit, tietojen suojaaminen, virustorjunta, ohjelmistot ja päivitykset.	

Taulukko 2: Tietoturvallisuuden kurssit Jyväskylän yliopistossa

Lisäksi tietoturvallisuutta on integroitu jonkin verran opetukseen mukaan. Tietoturvallisuus mainitaan yhdeksi osa-alueeksi ainakin kursseilla ”WWW-sovellukset” (2 ov), ”Tietokone ja tietoverkot työvälineenä” (2 ov, ECTS 4.0 cr) ja ”Johdatus tieto- ja viestintäteknologiaan” (2ov, Humanistisen tiedekunnan virtuaaliyliopistokurssi).

### 8.3 Kuopion yliopisto

Kuopion yliopisto tarjoaa seuraavat tietoturvallisuuden alueen kurssit:

Tietoturva / Tietojenkäsittelytie- teen laitos	3 ov / ECTS 4,5	Kurssi johdattaa keskeisiin salaisen avaimen salakirjoitusmenetelmiin (DES, IDEA, Blowfish...), salaisen avaimen salakirjoitusmenetelmiin (RSA, Diffie-Hellman, El Gamal...) ja hajautusmenetelmiin (MD5, SHA, HMAC...) kohtalaisella matemaattisella täsmällisyydellä. Kurssilla käsitellään autentikointiprotokollia (Kerberos, X.509) ja tietoturvaohjelmistoja (ssh, ssl, SET, IPSet, VPN...) sekä tietoturvapoliitikkaa.	Luennot 32 t, harj. 14 t, tentti
Tietosuoja ja -turva / Terveystieteiden ja -talouden laitos	3 ov / ECTS 4,5	Peruskäsitteet, tietosuojalainsäädäntö, erityisvaatimukset sosiaali- ja terveydenhuollossa, yksityisyyden suoja palveluketjussa, asiakkaan oikeudet ja asema, tietoturvapoliitikka, tietoturvan suunnittelu ja kehittäminen, tietoverkkojen turvallisuus, käytettävyys ja järjestelmien turvallisuus.	Luennot 12 t, harjoitukset 12 t. Hyväksytty oppi- mistehtävä.

Taulukko 3: Tietoturvallisuuden kurssit Kuopion yliopistossa

Lisäksi ainakin tietojenkäsittelytieteiden laitoksen kurssilla ”Tietotekniikka” (3 ov / 4,5 ECTS) mainitaan yhtenä osa-alueena tietoturva. Kuopion yliopistossa tarjotaan myös tuettua kaikille suunnattua tietoturvakoulutusta. Näistä mainitaan verkkosivuilla kaksi päivänmittaista seminaaria.

### 8.4 Lapin yliopisto

Lapin yliopistossa ei ole tietojenkäsittelytieteiden alan laitosta. Tietoturvallisuuden opetusta on kuitenkin osana muuta opetusta (mm. informaatioteknologian opinnot). Tietoturvallisuus on ollut jo 1980-luvulta lähtien mukana oikeustieteen kandidaatin tutkintoon pakollisena kuuluvassa oikeusinformatiikan perusopintojaksossa.

Tekijänoikeudet, tietosuoja ja tietoturva	1 ov (A)	Opiskelija tietää oikeudelliset velvoitteet materiaalin tuottamisessa ja käyttämisessä. Hän osaa soveltaa tietojaan opetustyössä ja tuntee vastuunsa juridisesta näkökulmasta. Opiskelijat perehtyvät tekijänoikeudellisiin kysymyksiin ja tietosuojan problematiikkaan. Tekijänoikeuksien syntyminen, siirtyminen, varmistaminen jne. - Tietosuoja - Yksityisyyden suoja ja henkilötietolainsäädäntö - Hyvä tietojenkäsittelytapa - Tietoturva	Luennot 6 t
Organisaatioiden tietoturvallisuus	3 ov (S)	Opintojakson suoritettuaan opiskelija ymmärtää tietoturvan luonteen, organisaation tietoturva-vaatimukset ja osaa koordinoita omaa toimintaansa vaatimusten edellyttämällä tavalla. Opiskelija ymmärtää tietoturvan osana organisaation laatu-järjestelmää, vallan ja vastuun merkityksen tietoturvan näkökulmasta sekä tietoturvan merkityksen liiketoimintaan.	Luennot luento- päiväkirjat ja tentti

Tietoverkkojen tietoturva	2 ov (S)	Opintojaksossa perehdytään tcp/ip-verkkojen, lähinnä Internetin ja intranetin, tietoturvan teknologiaan ja toteutukseen. Sisältö: Tietoturvan merkitys Internetissä ja Intraneteissä; kryptografia: perusteet, salausalgoritmit, julkisen avaimen menetelmä, VPN-verkot, Internet-sovellusten tietoturvaan liittyvät tekniikat, protokollat ja toteutukset; palomuurit: perustehtävät, käytännön esimerkkejä, kehittyneet palomuuriratkaisut.	Luennot, luentopäiväkirja ja aktiivinen osallistuminen tai kirjallinen kuulustelu
Tietosuoja ja tietoturvallisuus	6 ov	1. Yksityisyyden suojan ja henkilötietojen suojan oikeudellinen sääntely ja yleiset opit 2. Tietoturvallisuuden oikeudellinen sääntely ja yleiset opit	Luennot 10 t, tentti

Taulukko 4: Tietoturvallisuuden kurssit Lapin yliopistossa

Lisäksi tietoturvallisuus mainitaan kursseilla ”Johdatus tietoverkkoihin” (3 ov) ja ”TCP/IP-verkot” (3 ov). Myös tietosuojaa käsitellään muilla kursseilla.

Tietoturvallisuus on yksi keskeinen opintojakso myös instituutin järjestämässä kansainvälisessä oikeusinformatiikan LLM-tutkintoon johtavassa EULISP (European Universities Legal Informatics Study Programme) -koulutusohjelmassa. Niin tietoturvallisuuden kuin tietotekniikkarikostenkin osalta perusopetusmateriaalia on luotu ENLIST (European Network for Legal Information, Study and Training) -tietopankkiin (Lapin yliopisto 2004).

Instituutti järjestää yhdessä Lapin lääninhallituksen, Pohjan Viestikillan, poliisin tietohallintokeskuksen, Oulun yliopiston tietojenkäsittelytieteen laitoksen ja puolustusvoimien kanssa myös vuosittaisen Tietoturvallisuus ja laki -päivän. Päivä järjestettiin viidettä kertaa 9.11.2004.

### 8.5 Lappeenrannan teknillinen yliopisto

Lappeenrannan yliopistossa on seuraava tietoturvallisuuden kurssi.

Tietoturvan perusteet / Tietotekniikan osasto	2 ov (A)	Tavoitteet: Tutustuttaa opiskelija tietoturva-ajatteluun sekä esitellä menetelmiä halutun tietoturvan saavuttamiseksi Sisältö: Tietoturvan peruskäsitteet; perusmenetelmät tietoyhteyksien suojaamiseen; palomuurien perusteet; virukset ja niiltä suojautumismenetelmät; tietoturvapoliitikka.	
Suojatut tietoyhteydet / Tietotekniikan osasto	4 ov	Tavoitteet: Perehdyttää opiskelija laitteiston ja tietoyhteyksien suojaamiseen. Sisältö: Kryptografia ja sen perusmenetelmät; turvattu tiedonsiirto ja autentikointimenetelmät; sniffaus, skannaus ja spooffaus; tietomurron todentaminen; verkkoyhteyksien suojaus.	

Taulukko 5: Tietoturvallisuuden opetus Lappeenrannan teknillisessä yliopistossa

Lisäksi tietoturvallisuuden aihepiiriä käsitellään ainakin kurssilla ”Johdatus tietojenkäsittelyyn” (2 ov).

## 8.6 Oulun yliopisto

Kurssitarjonta ja opetuksen resursointi vaikuttavat olevan pisimmällä Oulun yliopistossa. Tietojenkäsittelytieteiden laitoksella on kaksi professuuria tietoturvallisuuden alueella. Lisäksi lehtorit ja tuntiopettajat osallistuvat tietoturvallisuuden opetukseen.

Tietoturvan perusteet / Tietojenkäsittelytieteiden laitos	3 ov (A)	<p>Kurssin tavoitteena on antaa tietoturvan perustietämys kaikille tietotekniikan parissa toimiville.</p> <p>Kurssilla esitetään käyttäjän tasolla:</p> <p>1) peruskäsitteet 2) käyttäjään kohdistuvat haasteet 3) toimiminen tietoturvaprosjekteissa 4) modernin organisaation tietoturvan hallinta 5) tietoriskit 6) henkilöturvallisuus 7) ohjelmistoturvallisuus 8) ulkoistamisen tietoturva 9) lainsäädäntöjen harmonisointi 10) biometriset menetelmät 11) intranetin tietoturva 12) tietoturva kilpailuetuna.</p> <p>Kurssilla on mahdollisesti vierailevina luennoijina teollisuuden ja hallinnon tietoturva-asiantuntijoita.</p>	Tentti, luennot 40 t, harj. 20 t
Turvallisten tietojärjestelmien suunnittelumenetelmät / Tietojenkäsittelytieteiden laitos	4 ov (S)	<p>Opintojakso syventää edeltävillä tietoturvakursseilla (mm. Tietoturvan hallinta) muodostunutta näkemystä turvallisten tietojärjestelmien kehittämisiongelmissä ja tietoturvan hallinnan ongelmista sekä niihin liittyvistä menetelmistä. Lisäksi kurssi täydentää ohjelmisto- ja tietojärjestelmäsuunnittelun kurseja (esim. Ohjelmistotekniikka, Oliosuuntautunut analyysi ja suunnittelu, Tietojärjestelmien suunnittelumenetelmät) opettamalla miten eri tietoturvamenetelmiä voidaan integroida olemassa oleviin ohjelmisto- ja tietojärjestelmäkehitysmenetelmiin. Siten kurssi sopii erinomaisesti ohjelmistotuotannon ja tietojärjestelmien suuntautumsvaihtoehdon opiskelijoille. Opintojakson suoritettuaan opiskelija I) ymmärtää miten tietoturvan hallinnan ja turvallisten tietojärjestelmien suunnittelumenetelmiä pystytään integroimaan tietojärjestelmä- ja ohjelmistokehitykseen, II) huomaa erilaisten tietoturvan hallinnan/turvallisten tietojärjestelmien suunnittelumenetelmäsukupolvien erot, III) osaa soveltaa erilaisia menetelmiä ja IV) osaa arvioida menetelmien käyttökelpoisuutta erilaisissa tilanteissa.</p>	Luennot 36 t, harj., harj. työ, tentti

Tietoturvasuus ja laki / Tietojenkäsittelytieteiden laitos	2 ov (A)	Kurssilla perehdytään tietoturvasuuden ja tietosuojan oikeudelliseen sääntelyyn ja tietoturvasuuteen oikeudellisena käsitteenä ja oikeusperiaatteena. Kurssin suoritettuaan opiskelija ymmärtää Suomen ja EY:n lainsäädännön merkityksen tietoturvasuudelle ja tietosuojalle. Opiskelija kykenee hahmottamaan informaatioteknologian ja oikeuden välistä suhdetta analysoimalla tietoturvasuutta oikeudellisena tavoitteena. Opiskelija ymmärtää tietoturvasuuden sekä yksityisyydensuojan ja omaisuudensuojan välisen vuorovaikutussuhteen sekä tunnistaa verkottuneen informaatioyhteiskunnan oikeudelliseen sääntelyyn liittyviä keskeisiä piirteitä.	Luennot 20 t, tentti
Langattoman tietoliikenteen tietoturva / Tietojenkäsittelytieteiden laitos	3 ov (A)	Langaton tiedonvälitys yleistyy nopeasti ja sitä tullaan käyttämään yhä enenevässä määrin jokapäiväisiin toimintoihin, kuten kaupankäyntiin ja informaationhankintaan. Kurssilla tarkastellaan sellaisia turvasuusongelmia, joita ei havaita tavanomaisissa verkkoympäristöissä.	Luennot 40 t, tentti, essee
Tietoturvan hallinta / Tietojenkäsittelytieteiden laitos	3 ov (A)	Kurssin tavoitteena on antaa tietoturvan tietämys niille henkilöille, jotka tarvitsevat sitä organisaation toiminnan tukena. Kurssilla esitetään 1) organisaation tietoturvaohjeistus 2) turvasuusmalli 3) tietoturvapoliittikka 4) turvasuuden organisointi 5) fyysinen ja ympäristöturvasuus 6) tietokoneiden ja tietoverkkojen hallinta 7) järjestelmään pääsyn valvonta 8) järjestelmien kehittäminen ja ylläpito 9) liiketoiminnan jatkuvuuden suunnittelu 10) vaatimustenmukaisuus 11) tietoturvasuuden hallintajärjestelmiä koskevat vaatimukset 12) valvontatoimet.	Luennot 30 t, harj. 20 t, tentti
Tietoverkkojen tietoturva / Tietojenkäsittelytieteiden laitos	3 ov (A)	Turvasuuteen liittyvät riskit ja uhkakuvat ovat este tietoverkkojen käytön kasvulle ja niiden tarjoamien palvelujen monipuolistumiselle. Verkkojen yleistyessä on myös kyseenalainen, jopa rikollinen toiminta niissä lisääntynyt; tietomurtojen ja virusten aiheuttamista vahingoista ovat joutuneet kärsimään niin yksityiset ihmiset kuin erilaiset organisaatiotkin. Tämä opintojakso esittelee nykytieteen ratkaisuja verkkojen tietoturvan ongelmiin. Perehdymme verkkojen rakenteeseen, tietoturvan peruskäsitteisiin, salaukseen, kryptografisiin algoritmeihin ja protokoliin sekä turvaratkaisuihin verkon eri tasoilla. Myös sovellusten (sähköposti, elektroninen kaupankäynti) turvakysymykset sekä palomuurit kuuluvat kurssin aihepiiriin.	Luennot 40 t, harj. 20 t, tentti

Tietoturvatutkimuksen suuntaukset ja menetelmät / Tietojenkäsittelytieteiden laitos	4 ov (A)	<p>Opintojakso käsittelee tietoturvatutkimuksen koulukunnallisia eroja (mm. käytetyt menetelmät ja tieteenfilosofiset oletukset) sekä uusimpia tutkimuksessa saavutettuja tuloksia tietokoneen, tietojärjestelmien ja kommunikaation turvallisuuden lisäämiseksi. Kurssimateriaali koostuu joukosta huolellisesti valittuja artikkeleita, jotka on poimittu alan johtavista tieteellisistä julkaisuista. Opintojakson alussa osallistujat jaetaan 2–3 hengen ryhmiin, ja kukin ryhmä voi annetuista aiheista vapaasti valita sen, johon haluaa perehtyä. Tämän jälkeen ryhmä valmistele julkaisuja lähdemateriaalina käyttäen esitelmän, joka pidetään, opponoidaan ja arvioidaan tavanomaista tieteellistä käytäntöä noudattaen. Kun esitelmä on pidetty, ryhmä vielä laatii valitsemastaan aiheesta joko suomen- tai englanninkielisen tutkielman; parhaat näistä pyritään kokoamaan yhteen ja julkaisemaan laitoksen raporttisarjassa.</p> <p>Opintojakson tavoitteena on syventää osallistujien näkemystä tietoturvatutkimuksen nykytilasta, perehdyttää tutkielman kirjoittamiseen ja johdatella tieteellisen tutkimuksen tekemiseen.</p>	Seminaarityö, osallistuminen
---	----------	--	------------------------------

Taulukko 6: Tietoturvallisuuden kurssit Oulun yliopistossa

## 8.7 Tampereen teknillinen yliopisto

Tampereen teknillisessä yliopistossa tietoturvallisuuden opetukseen on panostettu erityisesti tietoliikennetekniikan laitoksella sekä tiedonhallinnan laitoksella. Samoin opetusyhteistyötä on tehty Tampereen yliopiston tietojenkäsittelytieteiden laitoksen kanssa syventävissä opinnoissa.

Tietoturvallisuuden perusteet / tietoliikennetekniikan laitos	2–4 ov	<p>Tavoitteena on</p> <ul style="list-style-type: none"> <li>- tietoisuus tietoturvaan ja tietosuojaan liittyvistä uhista ja vastuista;</li> <li>- tietämys uhkien torjuntaan liittyvistä menetelmistä siinä määrin kuin on tarpeen tietotekniikan opinnoissa ja yhteiskunnassa.</li> <li>- hankkia valmiuksia löytää ja omaksua lisätietoja, kun niitä aikanaan työelämässä tarvitaan.</li> </ul> <p>Osa A, 2 ov: Yleisellä tasolla tietoturvan toteutusperiaatteita seuraavissa yhteyksissä: laitteet, käyttöjärjestelmä, ohjelmistot, tietokannat, tietokoneverkot, sähköposti, www-selaus, etäkäyttö, sähköinen kaupankäynti ja asiointi.</p> <p>Osa B, 1 ov: A-osan joihinkin kohtiin liittyviä teoreettisluonteisia täydennyksiä sekä kryptografian perusteita.</p> <p>Osa C, 1 ov: Tietoturvan ja -turvattomuuden ajankohtainen ilmeneminen arjessa ja yhteiskunnassa; uhkia ja ilmiöitä; erityisesti yksityisyyttä ja valvontaa, PKI-asiaa, lainsäädäntöä sekä eettisiä kysymyksiä.</p>	Luennot 14+14 t, verkko-keskustelu, tentti
---	--------	---	--

Tietoturvallisuuden jatkokurssi / tietoliikennetekniikan laitos	2-3 ov	<p>Tavoite on muuten sama kuin Tietoturvallisuuden perusteissa, mutta tietämisen lisäksi opitaan myös tekemään jotain ja samalla tietämystäkin syvennetään. Lisäksi näkökulma on soveltajan, palvelujen kehittäjän, suunnittelijan eikä enää vain opiskelijan ja kansalaisen. Tietoturvamekanismeja opitaan käyttämään, arvioimaan ja jossain määrin rakentamaan niistä kokonaisuuksia. Mekanismien kehittämistä tai luomista ei opetella.</p> <p>Osa A, 2 ov: Pääosin samat asiat kuin Tietoturvallisuuden perusteiden A+B:ssä, mutta uudella tasolla, vain vähän kerraten. Lisää erityisesti tietokannoista, ohjelmistoista, kryptologiasta ja protokollista sekä TT:n rakennusprosessista ja evaluaatiosta.</p> <p>Osa B, 1 ov: A-osan joihinkin kohtiin liittyviä teoreettisluonteisia täydennyksiä. Lisäasioina formalismeja (erityisesti ohjelmistojen näkökulmasta), tietoturvamalleja (erityisaiheina mm. monitasoisuus ja piilokanavat)</p>	Luennot 28+14 t, harj. 28 t, tentti
Verkon tietoturva / tietoliikennetekniikan laitos	3 ov	<p>Tavoitteena on oppia ja harjaantua valmiuteen ottaa vastuu jostain tietoverkosta tietoturvan osalta.</p> <p>Sisältö/luennot: Suunnitteluprosessi, politiikka, henkilöstö, toimilaitteiden ja niiden ohjelmistojen turvallisuus, fyysinen turvallisuus, tapahtumakirjanpito ja analyysi, auditointi, hyökkäykseen varautuminen, sellaisen havaitseminen, käsittely ja siitä toipuminen, näytön kerääminen.</p> <p>Harjoitukset: Haavoittuvuuksia ja vastatoimia eri protokollissa, kuten reitityksessä, verkonhallinnassa ja palveluissa kuten sähköpostissa, etäkäytössä, hakemistoissa ja www:ssä; hyökkäystyökalujen käyttö aukkojen etsinnässä; palomuurin asentaminen ja konfigurointi. Palvelunestohyökkäyksen käsittely.</p>	Luennot 14 t, harj. 28 t, harjoitustyö, tentti
Seminaarit, tietoliikenteen turvallisuus ja tietojenkäsittelyn turvallisuus / tietoliikennetekniikan laitos	2 ov	<p>Tavoitteena on tietoturvatietämyksen syventäminen tutustumalla tutkimustuloksiin jonkin erityisen aiheen puitteissa ja saman aiheen vieminen käytäntöön jonkin muun tietotekniikan kurssin tai työelämästä hankittujen tietojen pohjalta.</p> <p>Seminaarin teema valitaan vuosittain. Tietojenkäsittelyn turvallisuus -seminaarin teema rajataan sentapaiseen aiheeseen kuin käyttöjärjestelmät, tietokannat, tietojärjestelmien evaluointi tai pahat ohjelmat ja sisällöt. Tietoliikenteen turvallisuus -seminaarin aiheita voivat olla esim. reititys, verkonhallinta, tunkeutumisen havainnointi tai palvelunesto.</p>	Kaksi esitelmää

Kryptoprotokollat / tietoliikennetekniikan laitos	2-5 ov	Opitaan soveltamaan ja laatimaan kryptografisia protokollia tietoturvaongelmien ratkaisemiseksi. Huomataan, miten ratkaisut toisinaan aiheuttavat uusia tietoturvaongelmia. Tutustutaan suunnittelu- ja analyysimenetelmiin, joilla tätä voitaisiin välttää. Osa A, 2 ov: Perusongelmia, kuten autentikointi, avaimenvaihto ja anonymiteetti, eri muodoissaan ja yhteyksissä. Erityisongelmia, kuten äänestys, huutokauppa, liikkuvat agentit. Epäonnistuneita, vakiintuneita sekä tuoreita protokollia näihin ongelmiin. Näiden analyysia ja omien muunnelmien kehittelyä. Suunnitteluperiaatteita. Osa B, 1 ov: Lisää erityisongelmia ja protokollia, kuten monen osapuolen salattu laskenta ja reilu vaihto. Protokollan automaattinen verifiointi. Osa S, 1-2 ov: Kirjoitelma ja seminaariesitelmä aiheesta, joka sopii osan A tai B opiskelijoille sisällön jatkeeksi.	Luennot 28 t, harjoitukset 14 t, seminaarityö, tentti
Kryptologia / matematiikan laitos	3 ov	Tavoite: Tutustuminen tavallisimpiin kryptausmenetelmiin ja protokolliin sekä niiden matemaattiseen taustaan. Sisältö: DES, AES, RSA, ym. kryptausmenetelmiä. Protokollia. Tarvittavassa määrin lukuteoriaa ja algebraa.	Luennot 42 t, harjoitukset 28 t, tentti
Tietoturvallisuuden johtaminen/ tiedonhallinnan laitos	3 ov	Kurssin tavoitteena on antaa peruskäsitys tietoturvallisuuden johtamisesta. Sisältö: Kurssilla käsitellään erityisesti tietoturvapoliittikkaa ja -standardeja, tietoriskien hallintaa sekä turvallisuuden luomista tiedon avulla.	Luennot 21 t, harjoitukset 21 t, harjoitustyö ja tentti

Taulukko 7: Tietoturvallisuuden kurssit Tampereen teknillisessä yliopistossa

Tampereen teknillisen yliopiston alaisuudessa toimii myös tietoverkkoinstituutti (2004), jossa järjestetään tuettua ja kaikille suunnattua koulutusta. Koulutukseen on otettu yhtenä osana mukaan tietoturvallisuus. Koulutuksesta vastaavat Tampereen yliopiston täydennyskoulutuskeskus ja tietoverkkoinstituutti. Lisäksi kouluttajina toimivat muun muassa Tampereen ammattikorkeakoulu, Tampereen teknillisen yliopiston tietoliikennetekniikan laitos ja Tampereen yliopiston tietojenkäsittelytieteiden laitos.

## 8.8 Tampereen yliopisto

Tietojenkäsittelytieteiden laitoksella on seuraavat kurssit:

Tietoturvallisuuden perusteet / Tietojenkäsittelytieteiden laitos	2 ov (A)	Opintojakson tavoitteena on antaa yleiskuva tietoturvallisuudesta ja sen eri osa-alueista sekä tietoturvallisuuteen liittyvistä tekniikoista. Sisältö: Tieto ja tallenteet sekä näiden ominaisuudet tietoturvan kannalta, tietoturvan osa-alueet, turvallisuusluokitukset, salaustekniikan perusteet, tietoliikenneturvallisuuden perusteet, haitalliset ohjelmistot, ohjelmistoturvallisuuden perusteet.	Luennot 24 t ja tentti
---	----------	--	------------------------

Seminaari: tietoturvallisuuden erityiskysymyksiä / Tietojenkäsittely- tieteiden laitos	2 ov (S)	Seminaarissa perehdytään vapaasti valittavaan tietoturvallisuuden osa-alueeseen sekä valmistaudutaan opinnäytetyön ja tutkimuksen tekemiseen. Opiskelijat saavat valita seminaarityön aiheen vapaasti tietoturvallisuuden alueelta. Opiskelijat pitävät seminaarin lopuksi esityksen seminaarityöstään, minkä jälkeen yksi tai kaksi opiskelijaa opponoi seminaarityön.	Seminaari- työ, seminaari- esitys ja osallistu- minen
Kryptologian perusteet / Tietojenkäsittely- tieteiden laitos	3 ov (S)	Tavoite: Perehtyä kryptologisten menetelmien turvallisuuden perusteisiin. Sisältö: Kryptologia on matemaattinen tieteenala, jonka avulla tietoa voidaan turvata. Kryptologian johdantokurssi esittelee kryptologiaa tieteenalana ja antaa opiskelijalle perusymmärryksen aihealueeseen liittyvistä tutkimusaloista. Opintojaksolla tutustutaan sekä salaisen avaimen että julkisen avaimen salausmenetelmiin, keskeisiin salausalgoritmeihin, digitaalisiin allekirjoituksiin ja hash-funktioihin. Lisäksi aihealueisiin liittyviä matemaattisia perusasioita kerrataan sekä tutustutaan lukuteoriaan soveltuvin osin.	Luennot, harjoitukset ja tentti
Haitalliset ohjelmat ja niiden torjunta / Tietojenkäsittely- tieteiden laitos	4 ov (S)	Erilaiset haittaohjelmat, kuten tietokonevirukset, Troijan hevoset ja vakoiluohjelmat, ovat merkittävä tietoturvariski nykyisissä tietojärjestelmissä. Kurssilla perehdytään haitallisten ohjelmien toimintaperiaatteisiin sekä menetelmiin riskien vähentämiseksi. Kurssilla otetaan sekä käytännönläheinen että teorettinen lähestymistapa haittaohjelmiin ja niiden torjuntaan. Tavoite on, että opiskelija oppii tunnistamaan haittaohjelmien toimintatavat sekä keinot riskien vähentämiseksi sekä pystyy ottamaan haittaohjelmien aiheuttamat riskit huomioon järjestelmiä suunniteltaessa ja toteutettaessa.	Luennot, harjoitukset, harjoitustyö ja tentti
Riskienhallinnan perusteet / Oikeustieteiden laitos	3 ov / 5 ECTR (A)	Opintojaksolla esitellään riskienhallinnan käsitteet ja määritelmät. Tavoitteena on luoda laaja-alainen näkemys riskienhallinnan periaatteista ja merkityksestä arkielämässä, yhteiskunnassa ja yritys-elämässä. Opintojaksolla tuodaan esille riskienhallinnan erilaiset tarkastelunäkökulmat, kuten mm. matemaattinen, tekninen, taloudellinen ja psykologinen.	Luennot 30 t, tentti
Riskienhallinnan menetelmät / Oikeustieteiden laitos	3 ov (A)	Opintojakson tavoitteena on perehtyä erilaisiin riskienhallinnan menetelmiin ja oppia soveltamaan erilaisia keinoja ja menetelmiä varsinkin yritysten riskien hallinnassa. Tarkoituksena on oppia lähestymään riskienhallintaa kokonaisvaltaisesti ja analyyttisesti niin, että riskienhallintamenetelmiä yhdistelemällä ja vertailemalla löydetään erilaisissa tilanteissa kokonaisuuden kannalta optimaalinen ratkaisu. Opintojakso on harjoitustyöpainotteinen ja käytännön case-harjoitusten avulla toteutetaan kohdeyrityksessä riskienhallintaprosessi pääpiirteissään.	Luennot 20 t ja harjoitukset 25 t

Riskienhallinta ja turvallisuusjohtaminen / Oikeustieteiden laitos	3 ov / 6 ECTR (S)	Opintojakson tavoitteena on perehtyä turvallisuusjohtamisen viitekehykseen, globaaleihin riskeihin, kuten poliittiset riskit ja luonnon riskit, sekä erityisriskien ja uusien riskien tunnistamiseen sekä niiden hallintaan mm. ART:n avulla. Opintojakso tutustuttaa myös vakuutusorganisaatioiden omaan operatiiviseen riskinvalintaan ja niihin liittyviin teoreettisiin kysymyksiin sekä riskin psykologiaan. Opintojakson luennot toimivat kirjallisen materiaalin täydentäjinä ja johdatuksena jakson teemoihin.	Luennot 15 t
--	-------------------------	--	-----------------

Taulukko 8: Tietoturvallisuuden kurssit Tampereen yliopistossa.

Tutkinnonuudistuksen yhteydessä kurssi ”Tietoturvallisuuden perusteet” korvautuu muuhun opetukseen integroitavalla opetuksella. Tietoturvallisuus on osana ainakin kursseilla ”Johdatus WWW-tekniikoihin” (2 ov) ja ”Tietojärjestelmien ylläpito” (3 ov).

### 8.9 Teknillinen korkeakoulu (Otaniemi, Espoo)

Teknillinen korkeakoulu tarjoaa seuraavat tietoturvallisuuden alueen kurssit:

Tietoturvallisuustekniikka / Tietoliikenneohjelmistojen ja multimedialaboratorio	2 ov (A)	Tietoturvallisuustekniikka-opintojaksolla käydään läpi tietoturvallisuuden toteuttamisessa käytettäviä menetelmiä ja niiden soveltamista. Turvallisten järjestelmien kehittäminen. Tunnistaminen, todentaminen ja pääsynvalvonta. Kryptografian tarjoamat mahdollisuudet. Tietoturvamallit. Käyttöjärjestelmien ja palveluiden tietoturva.	Luennot, kotitehtävät, harjoitustyö ja tentti
Seminar on Network Security / Tietoliikenneohjelmistojen ja multimedialaboratorio	3 ov	Englanninkielinen seminaari, jonka teema vaihtelee.	Seminaarityö
Yritysturvallisuuden perusteet / Tietoliikenneohjelmistojen ja multimedialaboratorio	2	Yritysturvallisuuden perusteet -kurssi antaa perustietoa turvallisuudesta organisaatiossa. Siinä esitellään yleisesti turvallisuuden tavoitteita, keinoja ja rajoituksia. Näkökulmana on ”Mitä jokaisen diplomi-insinöörin tulisi tietää turvallisuudesta”.	Luennot, tentti

Tietojärjestelmien käytännön turvallisuuden erikoiskurssi	3 ov (S)	<p>Implementing and administering a secure system requires understanding of (1) assets being protected, and (2) threats, vulnerabilities, and attacks against the system. The goal of this course is to learn how to find vulnerabilities and how to protect against attacks exploiting the vulnerabilities. The approach towards this goal is to try exploiting vulnerabilities in practice, document the results of the attacks, and describe how the attacks could be prevented.</p> <p>Identifying vulnerabilities and finding information about them are valuable tools in practical information security. Assuming the viewpoint of an attacker helps the students learn how to defend against attacks. Because attacks are tried out in practice, students learn to assess difficulty of attacks and defenses more realistically.</p> <p>Students learn about vulnerabilities, attacks, and defenses in pairs. Course staff does not teach how to carry out attacks – one important goal for the students is to learn how to find information on their own.</p>	
Kryptologian perusteet / Teoreettisen tietojenkäsittelyn laboratorio	3 ov	<p>Kryptologia on tieteenala, joka tutkii tiedon suojaamisen menetelmiä. Näitä ovat: salaamisen menetelmät tiedon luottamuksellisuuden turvaamiseksi, tiedon alkuperän todentamisen menetelmät, tiedon eheyden turvaamisen menetelmät, tunnistamisen menetelmät, hajautetun tiedon käsittelyn turvaamisen menetelmät, avainten muodostamis- ja hallintamenetelmät, salaisen tiedon osittamisen menetelmät, sähköinen raha, aikaleimaus, copyright ja DRM.</p> <p>Kryptologia on mitä suurimmassa määrin matematiikkaa, varsinkin jos päämääränä on salausteknisten menetelmien vahvuuden ja turvallisuuden arvioiminen. Kurssin tarkoituksena on perehtyminen nykyaikaisten kryptologisten menetelmien turvallisuuden perusteisiin.</p> <p>Kurssi soveltuu erikoiskurssiksi tietotekniikan, matematiikan ja sovelletun matematiikan syventäviin aineopintoihin.</p>	Tentti, harjoitukset
Special Course on Cryptology / Teoreettisen tietojenkäsittelyn laboratorio	2-6 ov	<p>In this seminar, we are studying the security of symmetric cryptosystems: block ciphers, stream ciphers, hash functions, etc. The choice of this topic was motivated by the recent attacks (August 2004) on some fairly standard hash functions. We plan to cover those, among with attacks on other ciphers. We also study how to design provable secure ciphers, and whether "provable security" actually gives something.</p>	Seminaariryö, seminaariesitys

Cryptography and Data Security / Teoreettisen tietojenkäsittelyn laboratorio	3 ov	This is an introductory course on cryptology and data security. We plan to teach the course according to textbook, and our preliminary plan is to cover the first 12 chapters, and spend the last few lectures for "new and recent" material. It is also possible that we will have some famous cryptographer giving a minicourse in May. (In 2002, it was Phil Rogaway, in 2003, it was Vincent Rijmen.)	Luennot, seminaarityö
Safety-Critical Systems / Teoreettisen tietojenkäsittelyn laboratorio	2 ov	This is a basic course on Safety Critical Systems and the use of Formal Methods to verify and validate safety systems. Subjects covered this year are: Requirement Engineering, Hazard/Risk Analysis Methods, System Reliability, Safety Critical Hardware/Software and Verification/Validation Tools.	Luennot, kotitehtävät
Cryptography: Special Topics / Teoreettisen tietojenkäsittelyn laboratorio	2-6 ov	Englanninkielinen kurssi, jonka teema vaihtelee.	
Tietoturvallisuuden kehittämisprosessi / Tietoliikenne-ohjelmistojen ja multimedian laboratorio	3 ov	<p>Kurssin tarkoituksena on perehdyttää opiskelijat organisaation tietoturvallisuuden hallintajärjestelmän perusteisiin ja kehittämiseen. Kurssilla perehdytään organisaation tietoturvallisuuden tarpeiden ja vaatimusten määrittämiseen sekä tietoriskien kartoittamiseen ja analysointiin ja käydään läpi keskeisten lakien vaatimukset tietoturvallisuudelle. Kurssilla annetaan perustiedot organisaation tietomaisuuden ja tietojärjestelmien turvaamisesta sekä perehdytään tietoturvallisuutta ohjaavien käytäntöjen ohjeistamiseen, kuten tietoturvapoliittikka, jatkuvuus- ja toipumissuunnitelmat.</p> <p>Kurssilla keskitytään tietoturvallisuuden toimintatapoihin ja käytäntöihin. Kurssilla käydään läpi julkisuuteen tulleita liike-elämän tilanteita ja arvioidaan niiden syitä ja tarvittavia tietoturvallisuuden kehittämistoimia. Kurssi selvittää tietoturvallisuuden hallinnan ja kehittämisen osana jokaista toimintoa / prosessia.</p> <p>Kurssin suoritettuaan opiskelijalla on valmius suunnitella ja arvioida organisaation tietoturvallisuuden menettelytapoja. Kurssin jälkeen opiskelija hallitsee tietoturvallisuuden peruskäsitteet, ymmärtää tietoturvallisuuden merkityksen organisaation toiminnassa, tietää tietoja ja tietojärjestelmiä uhkaavat tietoriskit sekä tuntee toimintatavat ja -keinot.</p> <p>Harjoitustyössä perehdytään johonkin tietoturvallisuuden rajattuun osa-alueeseen.</p>	Luennot 28 t, harjoitukset, harjoitustyö tai tentti

Henkilöstö- ja toimitilaturvallisuus / Tietoliikenneohjelmistojen ja multimedian laboratorio	2 ov	Kurssilla käydään läpi yritysturvallisuuden perinteisiä menetelmiä, jotka ovat välttämättömiä myös tietoturvallisuudelle. Henkilöstön luotettavuuden varmistaminen ja tähän liittyvät oikeudelliset näkökohdat työuran eri vaiheissa. Toimitilojen turvallisuuden takaaminen ja parantaminen.	Luennot, tentti
Yritysturvallisuuden seminaari / Tietoliikenneohjelmistojen ja multimedian laboratorio	3 ov	Seminaarin tavoitteena on antaa osanottajille yleiskuva yritysturvallisuudesta osa-alueineen sekä turvallisuuden merkityksestä yrityksen toiminnan osana.	Luennot, seminaarityö ja esitys
Security evaluation	3 ov	The course provides an introduction to formal evaluations of computer security according to the Common Criteria (CC), the ISO/IEC standard for the evaluation of IT security. Basic concepts of security evaluation and assurance are provided, but the main focus shall be on the practical application of the CC evaluation process and in the assurance on the security features implemented in computer security products. Lectures shall be in English and the assignment is expected to be completed in English.	Luennot, harjoitustyö
Smart Card Application Development / Tietoliikenneohjelmistojen ja multimedian laboratorio	3 ov	The course provides an introduction to smart cards and smart card application development using the Java Card framework. Concepts of smart cards are introduced but the focus shall be on the development of smart card applications using the Java Card API and services. A simulation package shall be used to implement a simple smart card application that could be downloaded and installed on a Java Card. Lectures are in English and the assignment is expected to be commented and documented in English.	Luennot, harjoitustyö
Cryptographic protocols / Tietoliikenneohjelmistojen ja multimedian laboratorio	3 ov	The course, to be taught in English, will introduce common cryptographic protocols to the students. This consists of the identification of the basic concepts of cryptographic protocols, of the introduction of the main areas of application of cryptographic protocols, of the detailed survey of well known cryptographic protocols, and of an introduction of appropriate logics for analyzing security protocols.	Luennot, tentti

*Taulukko 9: Tietoturvallisuuden kurssit Teknisessä korkeakoulussa (Espoon Otaniemi)*

Lisäksi tietoturvallisuutta opetetaan ainakin Tietoliikenneohjelmistojen ja multimedian laboratorion kurssilla ”Verkkomedian perusteet” (3 ov). Teemu-Pekka Virtanen (2004) on koonnut ohjaamansa mm. tietoturvallisuudesta tehdyt diplomityöt Internet-sivuille.

Koulutuskeskus Dipolissa (2004) on myös laajaa maksullista tietoturvallisuusalan koulutusta. Dipolissa on tietoturvallisuuden koulutusohjelma, turvallisuusjohdon koulutusohjelma sekä turvallisuusalan pätevyitysohjelma Master of Security.

## 8.10 Turun yliopisto

Turun yliopistossa on seuraava tietoturvallisuuden alueen kurssi:

Tietoverkkojen tietoturva / Informaatioteknologian laitos	3 ov (A)	Kurssilla tarkastellaan laajasti tietojärjestelmien tietoturvakysymyksiä, erityisesti verkotetuissa ja hajautetuissa järjestelmissä. Kurssiin sisältyy katsaus erilaisiin tietoturvariskeihin, tietoturvaa parantaviin menetelmiin ja olemassa olevissa järjestelmissä käytettyihin ratkaisuihin.	Tiivistelmäluennot, kotitehtävät, kirjatentti.
---	----------	---	--

Taulukko 10: Tietoturvallisuuden kurssit Vaasan yliopistossa.

Lisäksi tietoturvan aihepiireihin perehdytään ainakin tietojenkäsittelytieteen laitoksen kurssilla ”Tietokoneverkot” (3 ov).

## 8.11 Vaasan yliopisto

Vaasan yliopistossa on seuraava tietoturvallisuuden alueen kurssi:

Tietoturvallisuuden perusteet / Tietotekniikan laitos	3 ov (A)	Sisältö: Yleiskuva tietoturvallisuudesta, peruskäsitteet ja mallit.	luennot 26 t, harj. 26 t ja tentti
Salausmenetelmät / Tietotekniikan laitos	3 ov (S)	Tavoite: Tutustutaan salauksen perusmenetelmiin ja erikoisesti moderneihin julkisiin salaustekniikoihin. Sisältö: Salausmenetelmien kehitys, julkiset salausmenetelmät.	luennot 30 t ja harj. 20 t ja tentti
ATK-tilintarkastus / laskentatoimi	2 ov	Tavoite: Antaa yleiskuva tietojärjestelmiin ja niiden ylläpitoon liittyvistä riskeistä, tietoturvan ja tietoriskien hallinnan käsitteistä, taloushallinnon tietojärjestelmiin liittyvistä erityisvaatimuksista, atk-tarkastuksen perusteista ja sisällöstä, atk-avusteisista tarkastusmenetelmistä. Sisältö: Atk-tarkastus, tietojärjestelmien kontrollit, tietoturvallisuus, tietojärjestelmät ja kirjanpito, yleisten atk-riskien hallinta, atk-avusteinen tarkastus.	Luennot 14 t, harj.

Taulukko 11: Tietoturvallisuuden kurssit Vaasan yliopistossa.

Lisäksi aihetta käsitellään ainakin tietojenkäsittelytieteen laitoksen ainakin kursseilla ”Tietotekniikan perusteet” (2 ov), ”Käyttöjärjestelmät” (3 ov) ja ”Tietoverkot” (3 ov).

## 8.12 Helsingin kauppakorkeakoulu

Kurssin ”Elektronisten kauppapaikkojen kehittäminen” yhteydessä mainitaan aihepiiri ”Tietoturva ja maksaminen”.

### 8.13 Turun kauppakorkeakoulu

Turun kauppakorkeakoulussa on seuraava tietoturvallisuuden alueen kurssi:

Internet rikollisuuden ja poliittisen vaikuttamisen välineenä / Tietojärjestelmä-tiede	3 tai 5 ov	Kurssilla luodaan katsaus Internetin haitallisiin vaikutuksiin ja käyttömuotoihin yhteiskunnan tasolla. Painopisteitä ovat Internetissä tapahtuva rikollisuus sekä Internetin kautta tapahtuva haitallinen poliittinen vaikuttaminen. Opetustavoitteena on kriittisen ja arvottavan lähestymistavan omaksuminen Internetin kehitykseen: paljon tutkittujen ja esille tuotujen Internetin hyötyjen ohella pitäisi osata tunnistaa myös sen haittapuolet. Pääpaino on Internetin haitallisen käytön toimintatapojen ymmärtämisessä, mutta esiin tuodaan myös, miten esim. yritykset ja yksilöt voivat suojautua Internetin vuoksi aiheutuville riskeiltä. Tärkeää osaa kurssissa näyttelee opiskelijoiden itse tuottama materiaali.	Kirjallinen kuulustelu luennot ja kirjat 3 ov, selvitystyö Internet-rikollisuus, seminaari 2 ov
--	------------	---	---

*Taulukko 12: Tietoturvallisuuden kurssit Turun yliopistossa.*

Kurssi ”Internet rikollisuuden ja poliittisen vaikuttamisen” välineenä on toteutettu yhteistyössä Turun yliopiston kanssa. Lisäksi tietoturvallisuus mainitaan ainakin kursseilla ”Tietotekniikan perusteet” (3 ov) ja ”Yrityksen tietohallinto” (5 ov).

### 8.14 Muut yliopistot

Joensuun yliopistosta, Taideteollisesta korkeakoulusta, Sibelius-Akatemiasta ja Kuva- taideakatemiasta ei löytynyt tietoturvallisuuteen viittaavaa opiskelijoille suunnattua opetusta.

## **9. Mahdollisia tutkimusaiheita**

Seuraavaksi tarkastellaan joitakin mahdollisia tutkimusaiheita, näiden ongelmia sekä mahdollisia uusia aiheita. Tässä yhteydessä ei ole tarkoitus käsitellä kaikkia mahdollisia tutkimusalueita, vaan ainoastaan antaa ajatuksia tutkimustyön kehittämiseen sekä kuvata ongelmien monimuotoisuutta. Painotus on sellaisissa tutkimusaiheissa, joissa kansallista tutkimusta ei juuri ole.

### **9.1 Palvelunestohyökkäykset**

Palvelunestohyökkäys ei vaikuta yksittäisen järjestelmän kannalta yhtä vakavalta kuin järjestelmään tunkeutuminen. Palvelunestohyökkäyksellä voi olla kuitenkin vakavat seuraukset kriittisissä järjestelmissä, kuten äänestysjärjestelmissä, sähköisen liiketoiminnan järjestelmissä ja avoimen verkon kautta toimivissa ohjausjärjestelmissä. Palvelunestohyökkäyksille on tyypillistä, että niistä kärsivät paitsi varsinainen kohde ja kohteen käyttäjät myös ne, joiden koneille murtaudutaan sekä ne, joiden tietoliikenne hidastuu.

Palvelunestohyökkäys voi kohdistua paitsi yksittäiseen kohteeseen myös verkon perusrakenteisiin. Esimerkiksi nopeasti leviävät virukset ovat kaataneet Internetin juuripalvelimia ja ruuhkauttaneet tietoliikennettä.

### **9.2 Sähköinen äänestäminen**

Äänestämisen siirtäminen Internetiin on houkuttelevaa kustannustehokkuuden ja tasarvoisen äänestysmahdollisuuden vuoksi. Äänestämisessä tulee kuitenkin säilyä äänestysalaisuus ja äänestämisen tulee olla virheetöntä. Olisi harmillista, jos esimerkiksi viaton henkilö joutuisi syytteeseen vaalivilpistä sen takia, että on joutunut identiteettivarkauden kohteeksi.

Yhdysvalloissa käynnistetty SERVE-äänestysjärjestelmä on asiantuntijoiden mukaan tietoturvaltaan puutteellinen muun muassa Internetin tietoturvuutteiden takia (Jefferson et. al. 2004). Järjestelmän mahdollistamia ongelmia ovat muun muassa äänestysalaisuuden loukkaaminen, virhetilanteet ja äänien muokkaaminen. Yksi vaikeasti ratkaistava ongelma on palvelunestohyökkäyksien aiheuttama uhka. Yhdysvallat on lykännyt äänestysjärjestelmäprojektin käyttöönottoa tietoturvuutteiden vuoksi. Yksi asiantuntijoiden esittämä vaatimus on, että äänestyksestä on jäätävä lokitieto paperille, jotta äänet pystytään varmistamaan.

Suomen suunnitelmana on sähköisen äänestämisen mahdollistaminen tulevaisuudessa (Oikeusministeriö 2004). Tietoturvaluuskysymykset muodostavat yhden merkittävän näkökohdan tätä mahdollisuutta kehiteltäessä.

### **9.3 Tietoturvaluus ja laki**

Lain avulla voidaan määrittää rajoja, joissa on luvallista liikkua. Lainsäädännöllä on ennaltaehkäisevä ja rajoittava vaikutus, mutta laki ei kuitenkaan kykene estämään haitallista käyttöä. Missä tahansa rikollisuuden muodossa on henkilöitä, jotka tuottamuksellisesti rikkovat lakia. Tiedon jakamisen helpottuminen on saanut aikaan

sen, että lain rikkoja voi olla missä päin maailmaa tahansa ja toisaalta pieni joukko ihmisiä saa aikaan merkittävää maailmanlaajuista vahinkoa. Valaisevana esimerkkinä tästä toimii roskaposti: Spamhaus-projektin (2004) arvion mukaan noin 500–600 henkilöä on vastuussa noin 90 % kaikesta roskapostista.

Kuten voidaan havaita, tietoturvaluus on tulossa tärkeäksi osaksi lainsäädäntöä muun muassa EU-maissa ja Yhdysvalloissa. Toisaalta lainsäädäntö ja sen tulkinta vaihtelee. Kansainvälisen lainsäädännön kehittämisessä ja tutkimisessa riittää työtä. Lainsäädäntöä tarvitaan muun muassa tietorikollisuuden torjuntaan ja immateriaali-oikeuksien määrittämiseen.

#### **9.4 Tietosodankäynti**

Tietosodankäynnillä tarkoitetaan tiedon, tietojärjestelmien ja tietoverkkojen käyttöä sekä aseina että kohteina konfliktissa. Tähän sisältyvät muun muassa toiseen valtioon tai muuhun osapuoleen kohdistuvat vihamieliset toimet, joilla pyritään tuhoamaan, lamauttamaan tai vahingoittamaan kohteen tieto- ja teleteknistä varustusta, tietojärjestelmiä tai niissä olevia tietoja sekä tietojärjestelmistä riippuvia toimintoja tai jotka toteutetaan tieto- ja teleteknisiä välineitä käyttäen (Valtiovarainministeriö 2004).

#### **9.5 Haitallisten ohjelmien torjunta**

Haitallisten ohjelmien torjunnan tutkimus on vasta aluillaan. Sekä Suomessa että kansainvälisesti haittaohjelmiin liittyvä akateeminen tutkimus on toistaiseksi vähäistä. Tästä aihepiiristä on löydettävissä tutkimuskohteita, joita voidaan yhdistää muihin tutkimusalueisiin. Esimerkiksi virusten avulla muodostetaan laittomia murrettujen koneiden verkostoja, joita käytetään palvelunestohyökkäyksiin, roskapostin lähettämiseen ja tiedon keräämiseen.

#### **9.6 Vertaisverkot**

Vertaisverkkojen periaatteena on helpottaa tiedonhakua sekä antaa oma tietokone tiedonvälitykseen. Vertaisverkoille on tyypillistä, että niissä levitetään laittomasti tekijänoikeudella suojattua materiaalia, mutta vertaisverkkojen periaate mahdollistaa myös laillisen hyötykäytön.

Vertaisverkot tyypillisesti kuormittavat verkkoliikennettä suuren tiedonvaihdon vuoksi. Lisäksi vertaisverkko-ohjelmista on löydetty tietoturva-aukkoja ja vakoilutoimintoja. Kuormitus-, tekijänoikeus- ja tietoturvaongelmien vuoksi vertaisverkkojen käyttö on kielletty useissa organisaatioissa. Laillisuuden rajoissa toimiva vertaisverkkojen käyttö on kuitenkin sallittua kotikoneissa.

## 9.7 Matkapuhelinlaitteet

Matkapuhelimet ovat olleet suljettuja ympäristöjä, mutta tämä on muuttumassa. Samalla, kun matkapuhelinten ohjelmointirajapinta yhtenäistyy, kasvaa myös tietoturvallisuuden merkitys. Yhtenä esimerkkinä on Cabir-virus (Virus Bulletin 2004), joka leviää Bluetooth-yhteyden kautta matkapuhelinten Symbian-käyttöjärjestelmään.

Pahimmillaan matkapuhelinlaitteiden tietoturvallisuus jätetään käyttäjien vastuulle vastaavalla tavalla kuin henkilökohtaisissa tietokoneissa. Tehokkaasti leviävä virus saattaa aiheuttaa samankaltaisia ongelmia kuin nykyiset Internet-virukset. Virus saattaa esimerkiksi tukkia puhelinlinjoja ja puhelinverkkoja tai kohdistaa palvelunestohyökkäyksiä kriittisiin kohteisiin, kuten hätänumeroihin. Vielä ei kuitenkaan tiedetä, toteutuvatko tämäntyyppiset virukset: paljon riippuu matkapuhelinlaitteiden tietoturvallisuuden kehittämisen onnistumisesta.

Yksi matkapuhelinten tietoturvaongelma on, että haitalliset ohjelmat saattavat tehdä luvattomia puheluita tai käyttää luvattomasti muita palveluita. Tällöin seuraa kysymys vastuusta. Onko vastuussa käyttäjä, operaattori, matkapuhelimen valmistaja vai ohjelmiston kehittäjä? Puhelut saattavat suuntautua ulkomaille, jolloin lainsäädännöllä voi olla vaikea puuttua veloitukseen.

## 9.8 RFID-teknologia

RFID-teknikka (*Radio Frequency Identifier*) perustuu langattomaan tunnistamiseen, jossa lukulaitteella luetaan mikrosirujen sisältämät tiedot. RFID-teknologiaa käytetään muun muassa kulunvalvontajärjestelmissä, maksukorteissa, eläinten tunnistamisessa, autojen lukitusjärjestelmissä, tavaroiden merkitsemisessä ja jopa ihmisten merkitsemisessä. Näistä erityisesti viimeksi mainittu saa yksityisyyden suojan puolustajat sekä uskonnolliset järjestöt varpailleen, mutta myös kaupan tuotteiden merkitseminen RFID-tunnisteilla on saanut aikaan vastustusta (Consumers Against Supermarket Privacy Invasion and Numbering 2004).

Maksukorteista esimerkkinä on Tampereen kaupungin liikennelaitoksen matkakortti. Edulliset mikrosirut voidaan sijoittaa myös esimerkiksi myytäviin tuotteisiin. Siruille voidaan myös tallentaa tietoa.

Samalla kun RFID-teknologia mahdollistaa uusia sovellusalueita, tiedon langaton lukeminen ja muuttaminen aiheuttavat ongelmia tietoturvallisuudelle. Riittävän voimakkaalla lukulaitteella voidaan lukea ja muuttaa sirujen tietoja. Luvaton lukeminen aiheuttaa muun muassa ongelmia yksityisyyden suojalle, koska siruilla olevien tietojen perusteella voidaan esimerkiksi ottaa selvälle, mitä tuotteita kuluttajalla tai yrityksellä on hallussaan ja missä ne sijaitsevat. Sirujen kloonaminen saattaa olla myös mahdollista.

Toisin kuin viivakoodien sisältämät tiedot RFID-siru sisältää jokaiselle sirulle yksilöllisen tunnisteen, joten yksittäisten tuotteiden sijainnin ja kulkureitin jäljittäminen on mahdollista. Myös henkilö saatetaan paikantaa sirujen avulla edellyttäen, että sirun tunnistetieto pystytään yhdistämään johonkin tiettyyn henkilöön.

Tiedon muuttamisesta aiheutuu monimuotoisia ongelmia. Esimerkiksi myymälävarkaat voivat kiertää hälytysjärjestelmät, tuotteista sirulle tallennettuja tietoja voidaan muuttaa ja yrityksen logistiikan hallinta sekä varastokirjanpito voidaan sekoittaa (Gattiker 2004). Yksi riski on myös, että kommunikointisignaaleja pystytään käyttämään väärin esimerkiksi kulunvalvontajärjestelmissä.

RSA Security Inc. kehittää menetelmiä, joiden avulla yksityisyydensuojan ongelmia voidaan ratkaista (RSA Security Inc. 2004). Näitä ovat muun muassa häirintäsirut, jotka aktivoiduttuaan estävät alkuperäisen sirun lukemisen.

RFID-teknologia on tulevaisuuden teknologia, jonka käyttöönottoon liittyvät tietoturvasasiat on hyvä ottaa huomioon mahdollisimman varhaisessa vaiheessa. RFID-teknologia mahdollistaa uusia luovia ratkaisuja. Jos samalla kuitenkin tietoturvallisuus unohdetaan, seurauksena voi olla vakavia uusia tietoturvauhkia. Täytyy myös muistaa, että RFID-siruja on erilaisia. Yksinkertaisimmillaan siru sisältää vain luettavan tunnisteen.

### **9.9 Paikantaminen**

Paikantaminen on esimerkki teknologiasta, jota voidaan käyttää sekä hyvään että pahaan. Matkapuhelinverkkoon tai satelliittijärjestelmiin yhteydessä olevat laitteet ja mikrosirut pystytään paikantamaan. Paikannustiedon avulla käyttäjä voi selvittää oman sijaintinsa, tuttavansa sijainnin tai esineiden sijainnin. Hälytysajoneuvot löytävät paikannustietojen avulla perille ja rikollisia sekä kadonneita henkilöitä pystytään jäljittämään. Varastetut esineet ja kulkureitit pystytään jäljittämään. Toisaalta yksityisyyden suoja on uhattuna. Paikannustietojen mahdollinen vuotaminen puolestaan mahdollistaisi uudet rikollisuuden ja vakoilun muodot.

### **9.10 Terveystietojen tietoturvallisuus**

Terveystietojen palveluja ollaan Suomessa entistä enemmän siirtämässä avoimeen verkkoon. Tästä ovat esimerkkeinä sähköinen resepti ja erilaiset neuvontapalvelut. Samalla tulee eteen aivan uudenlaisia tietoturvakysymyksiä, koska järjestelmiä yhdistetään turvattomiin verkkoihin. Tietojen arkaluontoisuuden takia tietoturvallisuus ja tietosuoja joudutaan ottamaan huomioon oikeastaan kaikessa terveydenhuollon toiminnassa. Lainsäädännössä määrätään terveystietojen suojasta tarkasti ja tietosuojavaltuutettu valvoo toimintaa. Terveystiedot ovat luottamuksellisia ja salaisia.

### **9.11 Tietoturvallinen ohjelmointi**

Tietoturvalliseen ohjelmointiin (katso liite 1) tutkimus voisi vähentää kriittisiä ohjelmistovirheitä. Tämä edellyttäisi tulosten soveltamista käytäntöön sekä tulosten popularisointia.

### **9.12 Roskaposti**

Myös roskaposti (katso liite 1) on muodostunut merkittäväksi ongelmaksi. Ongelman laajuutta kuvaa roskapostiliikenteen määrä. Spamhaus-projektin (2004) arvion perusteella 62 % Internetin sähköpostiliikenteestä on roskapostia. Kyseessä on siis merkittävä resurssien tuhlaus, kun verkkoliikenne kuormittuu, käyttäjät ja ylläpito

joutuvat huolehtimaan roskapostin poistamisesta sekä tärkeää sähköpostia häviää roskapostin sekaan.

Perusongelma on luotettavan autentikoinnin puuttuminen sähköpostiliikenteestä. Jos sähköpostiliikenteen alkuperä pystyttäisiin luotettavasti määrittämään, ei roskapostin lähettämisessä olisi enää mieltä, koska haitalliset viestit pystyttäisiin suodattamaan ja alkuperäinen lähettäjä saisi vastauksena virheviestejä. Roskapostiongelmia pyritään ratkaisemaan myös lainsäädännön avulla (katso Sorkin 2003). Tällöin tulee vastaan lainsäädännön monimuotoisuus ja valvonnan vaikeus.

OECD (Organisation for Economic Co-operation and Development 2004) on perustanut työryhmän roskapostiongelman ratkaisemiseksi. Työryhmän tavoitteiksi mainitaan:

- Tuottaa ”OECD Anti-spam Toolkit”
- Verkonhallinnan ratkaisujen pohtiminen
- Autentikoinnin ja teknisten ratkaisujen pohtiminen
- Matkapuhelinverkkojen ja pikaviestinnän (Instant Messaging) roskapostin torjunnan pohtiminen
- Kansainvälinen yhteistyö
- 

Myös Microsoft on suunnittelemassa ratkaisua sähköpostiongelman ratkaisemiseksi. Bill Gates (BBCNews 2004) on ottanut esille roskapostiongelman ratkaisemiseksi kolme eri menetelmää, joita Microsoft kehittää:

- Sellaisen haasteen luominen, jonka ratkaiseminen on ihmiselle mahdollista, mutta tietokoneelle vaikeaa
- Sellaisen haasteen luominen, jonka ratkaisemiseen tarvitaan laskentakapasiteettia
- Sähköpostin maksullisuus

Suomessa Internet-palveluntarjoajat ovat alkaneet käyttää ennakoivaa suodatusta (katso liite 1) haitallista tietoliikennettä vastaan. Lainsäädännön muuttuminen on mahdollistanut ja velvoittanut puuttumisen haitalliseen tietoliikenteeseen (Liikenne- ja viestintäministeriö 2004).

### **9.13 Identiteettivarkaudet**

Palveluiden sähköistyminen tarjoaa myös uusia mahdollisuuksia rikollisuudelle. Identiteetin varastaminen (katso liite 1) on sitä houkuttelevampaa, mitä helpommin se on toteutettavissa ja mitä suuremmat hyödyt siitä on mahdollista saada. Identiteettivarkaudet toteutetaan tyypillisesti postin tai asiakirjojen varastamisen, tietomurtojen, sähköpostin, Internet-sivujen ja puhelinten avulla. Identiteettivarkauden kohteelle aiheutuu haittaa muun muassa luottotietojen menetyksestä, virheellisistä rikosmerkinnöistä, varojen menetyksestä, ajanhukasta, byrokratiasta ja stressistä. Vastaavasti rahoituslaitokset ja yritykset joutuvat korvaamaan varkaiden aiheuttamia vahinkoja.

Yhdysvalloissa identiteettivarkauksista on tullut todellinen ongelma. Vuosittain identiteettivarkauksista aiheutuu arviolta noin viiden miljardin dollarin vahingot ja noin kymmenen miljoonaa asukasta joutuu identiteettivarkauden kohteeksi. Tarkempia tietoja identiteettivarkauksista sekä tilastoja löytyy FDC:n (Federal Trade Commission 2004) Internet-sivuilta.

Suomessa ongelma ei ole akuutti eikä maksuliikenne perustu ainakaan toistaiseksi turvattomiin luottokorttiratkaisuihin vastaavassa laajuudessa kuin Yhdysvalloissa. Kuitenkin monet henkilökohtaiset tiedot ovat tyypillisesti julkisesti saatavilla (mm. osoitetiedot, verotiedot, puhelinnumerot, sähköposti, ajoneuvotiedot ja joissain tilanteissa jopa sosiaaliturvatunnus). Henkilön identiteetin varmentamisen perustuminen tällaiseen julkisesti saatavilla olevaan tietoon mahdollistaa monenlaisen ilkeilyn. Voi olla vain ajan kysymys, milloin identiteettivarkauksien aiheuttamat ongelmat kasvavat myös Suomessa. Nyt olisikin hyvä aika pohtia keinoja ongelman ennaltaehkäisemiseksi.

#### **9.14 Tietoturvallisuus osana käytettävyyttä**

Monelle lienee tuttu käsitys, että tietoturvallisuus heikentää käytettävyyttä. Näin ei kuitenkaan aina tarvitse olla. On löydettävissä tilanteita, joissa käytettävyys ja tietoturvallisuus paranevat yhdessä tai käytettävyyden heikkeneminen ei ole niin merkittävää, että tietoturvaluutta kannattaa heikentää. Esimerkiksi se, että käyttäjä löytää oikeat valinnat ja pystyy perumaan toimenpiteitä ja hallitsemaan tietojärjestelmää, lisää yleisesti ottaen tietoturvaluutta. Vastaavasti ohjelmistovirheiden karsiminen lisää sekä tietoturvaluutta että käytettävyttä.

#### **9.15 Digitaalisen television tietoturvallisuus**

Myös digisovitin, joka mahdollistaa televisiolähetysten vastaanottamisen, sisältää tietotekniikkaa. Tietoturvaongelmat saattavat mahdollistaa esimerkiksi lähetysten häiritsemisen ja muuttamisen. Samoin digisovittimien sisältämän tiedon vuotaminen voi tulevaisuudessa aiheuttaa ongelmia yksityisyyden suojalle, kun tietoliikenne on kaksisuuntaista. Digisovittimen toiminnan lamaantuminen virheellisen signaalin vuoksi on jo aiheuttanut ongelmia sekä luonut vaikeita vastuukysymyksiä (Erkkilä 2004).

#### **9.16 Ohjausjärjestelmien yhdistäminen turvattomiin verkkoihin**

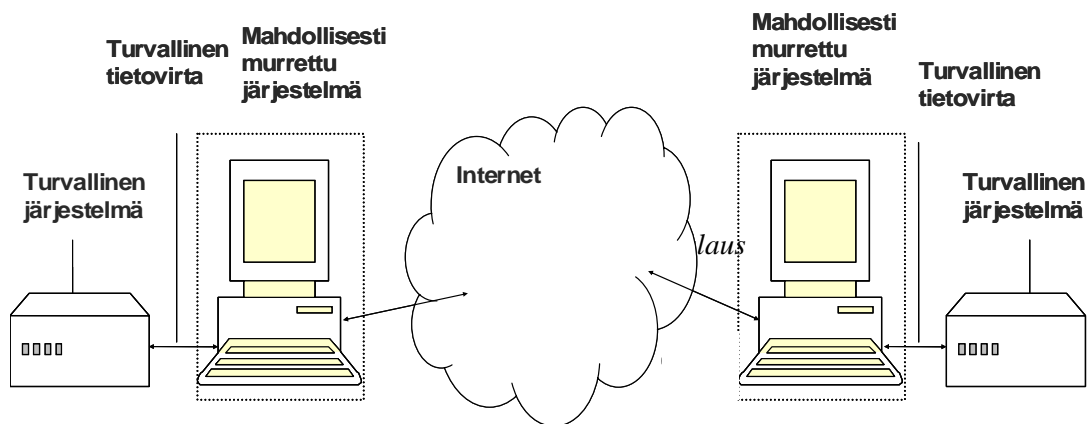
Silloin kun kriittisiä järjestelmiä ja niiden ohjausta yhdistetään avoimiin verkkoihin, syntyy uusia tietoturvariskejä. Esimerkiksi älykodeissa ohjausjärjestelmät kytketään tyypillisesti Internetiin tai matkapuhelinverkkoihin. Vastaavasti maksuliikenteessä sekä sähkön ja lämmön ohjauksessa käytetään Internetiä. Tällöin ilkeilyn, varkauden ja vakoilun mahdollisuus on olemassa, jos tietoturvaluudesta ei huolehdi.

#### **9.17 Laitteistotason tietoturvallisuus**

EICAR-konferenssissa (Helenius 2003) esitin pohdinnan, että tehokkain tietoturvaluutta saavutetaan vain siinä tapauksessa, että laitteisto tukee tietoturvaluutta. Pelkkiin ohjelmistoihin luottaminen on arveluttavaa, sillä ne sisältävät aina virheitä. Laitteistoratkaisutkin voivat sisältää tietoturva-aukkoja, jotka

ovat myöhemmin vaikeasti korjattavissa. Joka tapauksessa laitteistoratkaisuilla kyetään luomaan yksi turvakerrokseen ohjelmistojen tarjoaman suojan päälle.

Intel (2004) kehittää tietokonearkkitehtuuria, jossa laitteistokomponentit tukevat tietoturvallisuutta. Ohjelmistot suoritetaan omassa, fyysisesti eristetyssä tilassaan ja tiedot säilytetään ohjelmistosta erikseen. Vastaavasti Giwano Oy (2004) on kehittänyt turvatietokoneen, jossa kaksi tietokonetta on rakennettu samojen kuorien sisään. Yksiköiden välille on muodostettu helppo ja turvallinen tiedonsiirtojärjestelmä. Myös salaus voidaan tehdä turvallisesti vain, jos sekä salaus että salattava tieto säilytetään suojatussa järjestelmässä (kuva 2).



Kuva 2. Turvallinen salaus

## 9.18 Käyttäjien tietoturva-asetteet

Käyttäjien mahdollinen epäluottamus tietojärjestelmien turvallisuuteen vähentää järjestelmien käyttöä. Esimerkiksi Karjaluoto (2002, s. 33–35) toteaa, että käyttäjien asenteet turvallisuutta kohtaan ovat yksi merkittävimmistä esteistä Internet-pankipalvelujen käytölle. Kysymyksen voidaan olettaa aiheuttavan ongelmia myös kansalaisvarmenteen käytössä. Toisaalta osa peloista on aiheellisia ja osa riskeistä on sellaisia, että niihin eivät käyttäjät osaa varautua.

## 9.19 Biometrinen tunnistaminen

Biometrinen tunnistaminen voi onnistuessaan parantaa tietoturvallisuutta. Yhdysvaltojen vaatiessa passeihin biometrisia tunnistamistietoja asia on ajankohtainen myös tätä kautta. Tunnistuksen tulisi olla yksilöllistä eikä se saisi olla muutettavissa. Yhtenä ongelmana on mahdollisuus tunnistamistietojen vääräntäminen. Toinen näkökohta on yksityisyyden suoja. Esimerkiksi sormenjälkitunnistamistiedot saattavat vuotaa ulkopuolisille.

## **9.20 Yritysvakoilu**

Tiedon jakaminen on helpottunut, minkä vuoksi tieto voi myös vuotaa tehokkaasti. Tietoa voidaan nykyisin varastaa esimerkiksi pienen MP3-soittimen, digitaalikameran tai muun USB-liitäntäisen laitteen muistissa. Tieto voi myös levitä sekunneissa ympäri maailman.

## **9.21 Kotikäyttäjän tietoturva**

Samaan aikaan, kun tietokoneista on tullut entistä helppokäyttöisempiä, ovat käyttöjärjestelmien ominaisuudet ja samalla myös niiden monimutkaisuus kasvaneet. Seurauksena on, että tietokoneita käyttävät ihmiset, jotka tietävät entistä vähemmän tietoturvallisuudesta.

Jos kotitietokoneiden suojaaminen on puutteellista, tällä on vaikutusta koko Internet-verkon toiminnan kannalta. Suojaamattomia tietokoneita voidaan käyttää palvelunestohyökkäysten välineinä, palvelimina laittoman tiedon levitykseen, roskapostin levitykseen ja tietomurtojen jälkien peittämiseen. Ongelmana on luonnollisesti, että suojaamattomia tietokoneita löytyy ympäri maailman. Internetin luonteen vuoksi hyökkääjän näkökulmasta ei tyypillisesti ole merkitystä sillä, missä päin maailmaa suojaamaton tietokone sijaitsee.

## **9.22 Yksityisyyden suoja**

Yksityisyydensuojan turvaaminen on osana kaikkea tietojenkäsittelyä, jossa käsitellään henkilöä yksilöiviä tietoja. Aikaisemmin mainittujen kohtien lisäksi esimerkkejä ovat erilaisten tietokantojen käsittely, henkilöiden kuvaaminen ja henkilöitä yksilöivien tietojen käsittely. Yksityisyyden turvaamisen kysymyksissä joudutaan tasapainottelemaan rikollisuuden torjunnan ja yksilön oikeuksien kanssa. Esimerkiksi kamera-valvonta lisää turvallisuutta, mutta samalla tiloissa käyvät henkilöt pystytään tunnistamaan. Vastaavasti rikollisten liikkeitä pystytään jäljittämään erilaisten tietorekisterien ja paikannustietojen avulla, mutta samalla yksityisyyden suoja saattaa kärsiä. Lisäksi joudutaan tasapainottelemaan käytettävyyden ja henkilörekisterien suojan välillä.

Clements et al. (2003) ovat tarkastelleet vuoden 2001 syyskuun terrori-iskujen vaikutuksia yksityisyyden suojaan. Myös esimerkiksi tietoliikenteen suodatuksen ja yksityisyyden suojan kanssa joudutaan tasapainottelemaan. Viestintävirasto on koonnut tietosuojasta säädettyjä lakeja (2004).

## 10. Keskustelu

Seuraavaksi käsitellään yhteenvedonomaaisesti selvityksessä saadut tulokset, selvityksen rajoituksia sekä suositellaan jatkotoimenpiteitä.

### 10.1 Tulokset

Vaikuttaa siltä, että tietoturvallisuuden ongelmat tulevat jatkumaan ja syntyvien uusien ongelmien laatu jää pääasiassa arvailujen varaan. Toisaalta on merkkejä siitä, että tietoturvallisuutta otetaan vakavasti paikoin myös siellä, missä se on kustannustehokkainta: laitteistojen kehityksessä (esim. kehitteillä olevat tietoturva-arkkitehtuurit, katso Intel 2004), suurissa ohjelmistotaloissa (esim. Microsoftin trustworthy computing -ohjelma, Microsoft 2004) ja tietoliikenneyhteyksien tarjoajien piirissä (esim. Internet-operaattorien tekemä ennakoiva suodatus; katso myös Raiderin kuvaus Cisco Systemsin suunnittelemaasta tietoverkkoarkkitehtuurista 2004).

Selvitystä tehdessäni olen havainnut, että sekä tutkimus että opetus ovat jatkuvasti kehittyviä alueita. Tietoturvallisuuden perusopetusta tarjotaan jo monessa yliopistossa. Toisaalta tietoturvallisuuden tutkimukseen ja opetukseen ollaan vasta heräämässä.

Tietoturvallisuuden tutkimus on toistaiseksi ollut vähäistä Suomessa ottaen huomioon ongelmien laajuuden. Tutkimusalana tietoturvallisuus on Suomessa vielä nuori. Toisaalta merkkejä tutkimuksen kehittymisestä on nähtävissä. Lisäksi tutkimuksen rahoittajien kiinnostus tutkimusalueen tukemista kohtaan vaikuttaa kasvavan samalla, kun ongelmien laajuus aletaan tiedostaa.

Yliopistoista tietoturvallisuuden tutkimus vaikuttaa kehittyneen pisimmälle Otaniemen Teknillisessä korkeakoulussa sekä Oulun yliopistossa. Kummassakin yliopistossa on kolme tietoturvallisuuden professuuria, ja tämä heijastuu luonnollisesti sekä tutkimukseen että opetukseen. Tampereella ulkopuolisella rahoituksella tehtyä tutkimusta on ollut toistaiseksi vain pienessä mittakaavassa. Resursseihin nähden alan opetusta on Tampereella toistaiseksi järjestetty melko laajalti; opettajien mielenkiinto alaa kohtaan sekä paikallinen yhteistyö ovat tuottaneet hedelmää. Oulussa ja Otaniemessä on päästy professuurien voimilla näilläkin alueilla pitkälle. Näyttäisi, että tietoturvallisuus on sekä Oulussa että Otaniemessä kehittynyt pitkälti juuri professorien mielenkiinnon ansiosta.

Laajassa mittakaavassa tehtyä kansallista tutkimusta näyttää löytyvän toistaiseksi terveydenhuollon tietoturvallisuuden, haavoittuvuuksien ja tiedon salauksen alueilta. Näistä terveydenhuollon tietoturvallisuuden tutkimus keskittyy Stakesille.

### 10.2 Rajoituksia

Selvityksen painotus on *computer securityssä* tai ”tietotekniikan turvallisuudessa”. Jatkotutkimuksen aiheita olisi mahdollista löytää tietojärjestelmien luotettavuuden ja riskien alueilta (esim. *fail-safe, robust, self-monitoring & self-repairing computing, risk assessment methods*), tietoturvallisuuden taloudesta sekä organisatorisista ja sosiaalisista näkökulmista (*trust, law, management practices*).

Tietoturvallisuudesta on myös taloudellista ja yhteiskunnallista tutkimusta, jota kuitenkin ei ole systemaattisesti kuvattu. Näiden teknisten ja sosiaalisten, organisaattorien ja ekonomisten kysymysten väliin ei voida tehdä selvää rajaa, mikä on havaittavissa esimerkiksi avoimen lähdekoodin turvallisuusominaisuuksista käydyssä keskustelussa.

On hyvä huomata, että selvitys voi sisältää tiedon hankintatavasta ja alueen jatkuvasta muutoksesta aiheutuvia virheitä sekä kurssien että tutkimuksen alueella. Tietojen haussa vaikeutena oli selvittää, mitkä hankkeet liittyvät tietoturvallisuuteen: esillä oli useita hankkeita, joista tietoturvallisuuden olisi periaatteessa voinut kuvitella muodostavan yhden osa-alueen. Tästä seuraa kysymys: onko hankkeissa, joiden pääpainotus on muualla pyritty toteuttamaan tietoturvallisuudesta ainoastaan vähimmäistavoitteet? Tietoturvallisuuden integroiminen mukaan erilaisiin hankkeisiin ja opetukseen on kannatettava ajatus. Voidaan kuitenkin kysyä, tapahtuuko näin todella. Asian tarkempi tutkiminen vaatisi toisenlaista lähestymistapaa, kuten haastattelututkimusta.

Tutkimusaiheita kartoitettaessa lähtökohdaksi olisi myös voitu ottaa jonkin koulukunnan mukainen tutkimusote: esimerkiksi *security research*, *computer science security research*, *IS security research* tai *software engineering security research*.

Tutkimuksen näkökulmasta olisi ollut mahdollista syventyä tarkemmin tutkimusongelmiin sekä tarkastella tutkimuksia julkaisupainotteisesti. Tämä vaatisi hieman toisenlaista lähestymistapaa, jossa esimerkiksi otetaan tarkasteluun artikkeleita, tutkimusongelmia ja näiden merkitystä. Selvitystä lukiessa on hyvä huomata, että tutkimus ja koulutus ovat jatkuvasti muuttuvia alueita. Mainittujen rajoitteiden vuoksi selvitys ei anna täysin täsmällistä kuvaa tämän hetken tilanteesta.

### **10.3 Suositukset jatkotoimenpiteiksi**

Raporttia laadittaessa sekä tietoturvakonsortion koordinoitavuudessa on paljastunut useita uhkakuvia ja toisaalta myös tilanteita, joissa tietoturvallisuusnäkökohdat analysoidaan perinpohjaisesti. Selvää on, että nykyisessä tilanteessa tietoturvallisuuden tutkimusta ja opetusta sekä resursointia tarvitaan. On myös hyvä huomata, että tietoturvallisuuteen panostaminen merkitsee usein myös panostamista tulevaisuuteen. Tietoturvallisuuden asettaminen keskeiselle sijalle merkitsee tietorikollisuuden aiheuttamien kustannusten vähentyessä pidemmällä aikavälillä merkittäviä säästöjä kansantaloudelle.

Jos tilannetta mietitään paikallisesta näkökulmasta, huomaamme, että Tampereen alueelta puuttuu toistaiseksi tietoturvallisuuden professuuri. Jos tietoturvallisuuden opetuksen ja tutkimuksen kehitystä halutaan viedä eteenpäin, tämä professuuri on tarpeen. Vastaavasti resurssien suuntaaminen tietoturvallisuuden tutkimukseen ja yhteistyöhön on tarpeen, jotta alueelle saadaan osaamisen keskittymä. Tietoturvakonsortio-hankkeen vauhdittamana yhteistyötä on jo pystytty käynnistämään, ja tämä on näkynyt myönteisesti erityisesti opetuksessa sekä yhteyksien muodostumisessa. Toisaalta resursseja ei ole laajamittaiseen yhteistyöhön.

Tampereelle mahdollisesti perustettavat uudet resurssit olisi syytä suunnata niin, että ne täydentävät mahdollisimman tarkoituksenmukaisella tavalla jo muualla tapahtuvaa tutkimustyötä. Samalla tulisi ottaa huomioon ne tarpeet, jotka muilta Tampereen

vahvoilta tutkimus- ja koulutusaloilta kohdistuvat tietoturvallisuuden asiantunte-  
mukseen. Koulutuksen painopisteiden suuntaamisessa tulisi ottaa huomioon myös alan  
yrityksien tulevien vuosien tarpeet. Uusia virkaratkaisuja tehtäessä tulisi selvittää  
mahdollisuudet yhteistyöhön alueen eri yliopistojen kesken.

## Lähteet

- Asapsoft Netsystems Oy. 2004. Asapsoft Netsystems Oy – ohjelmistotalo alansa huipulta. Viitattu 14.9.2004 <http://www.asapsoft-netsystems.fi/yritys.htm>.
- Beslay, L. & Hakala, H. 2004. Digital Territory: Bubbles. draft article. Viitattu 27.10.2004 <http://cybersecurity.jrc.es/docs/DigitalTerritoryBubbles.pdf>
- Brightmail Incorporated. 2004. Spam Statistics. Viitattu 15.3.2004 <http://www.brightmail.com/spamstats.html>
- CBSNews. 2004. Gates: Spam To Be Canned By 2006. Viitattu 9.8.2004. <http://www.cbsnews.com/stories/2004/01/24/tech/main595595.shtml>
- Clements, B., Maghiros, I., Beslay, L., Centeno, C., Punie, Y., Rodríguez, C. & Masera, M. 2003. Security and Privacy for the Citizen in the Post September 11 Digital Age - A Prospective Overview Institute for Prospective Technological Studies. Viitattu 11.10.2004 <http://cybersecurity.jrc.es/pages/projectlibestudy.htm>
- Computer Emergency Response Team. 2004. CERT Coordination Center. Viitattu 22.9.2004 <http://www.cert.org/>
- Consumers Against Supermarket Privacy Invasion and Numbering. 2004. METRO Future Store Overview. Viitattu 29.10.2004 <http://www.spsychips.com/metro/overview.html>
- Contrasec Oy. 2004. Contrasec Oy. Viitattu 14.9.2004 <http://www.contrasec.fi/yritys.html>
- CORDIS News. 2003. Group of personalities discusses a security research strategy for Europe. 10.7.2003. Viitattu 3.9.2004 [http://dbs.cordis.lu/fep-cgi/srchidadb?ACTION=D&SESSION=215182004-2-2&DOC=1&TBL=EN\\_NEWS&RCN=EN\\_RCN\\_ID:21004&CALLER=EN\\_NEWS](http://dbs.cordis.lu/fep-cgi/srchidadb?ACTION=D&SESSION=215182004-2-2&DOC=1&TBL=EN_NEWS&RCN=EN_RCN_ID:21004&CALLER=EN_NEWS)
- Cybersecurity. 2004. Cybersecurity in a e-society. Viitattu 3.9.2004 <http://cybersecurity.jrc.es/>
- ENISA. 2004. ENISA: European Network Information Security Agency. Viitattu 3.9.2004 [http://www.enisa.eu.int/index\\_en.htm](http://www.enisa.eu.int/index_en.htm)
- Ensio, A. & Ruotsalainen, P. 2004. Tietoturvallinen kommunikaatioalusta: Suositus kansallisesti noudatettaviksi standardeiksi. Viitattu 27.10.2004 <http://www.oskenet.fi/uploads/qdnj9m1f15e7j.doc>
- Erkkilä, M. 2004. Digi-tv pimensi ruudut. Tietoviikko 15.4.2004. Viitattu 16.9.2004 [http://www.tietoviikko.fi/doc.ot?d\\_id=124100](http://www.tietoviikko.fi/doc.ot?d_id=124100)
- Federal Trade Commission. 2004. Welcome to the Federal Trade Commission: Your National Resource for Identity Theft. Viitattu 21.9.2004 <http://www.consumer.gov/idtheft/>
- FIDIS. 2004. FIDIS – Future of Identity in the Information Society. Viitattu 13.10.2004 <http://www.fidis.net/>
- FINLEX. 2004. Väestötietolaki 11.6.1993/507. Viitattu 6.9. 2004 <http://www.finlex.fi/linkit/ajansd/19930507>
- Gattiker, U. 2004. 09 Aug 2004 - W32 - Tool - Reading and Disabling RFID Tags on Products - Consumers Fighting for Privacy. Information Security This Week. August 15, 2004 Vol.5 No.34. ISSN 1600-1869. Viitattu 22.8.2004 <http://securitynews.weburb.dk/>
- Giwano Computers Ltd. 2004. Yritys lyhyesti. Viitattu 14.9.2004 <http://www.giwano.com/fi/company.htm>
- Go project. 2004. GO-SEC, Security subproject. Viitattu 26.10.2004 <http://go.cs.hut.fi/old-go/go-sec.html>

- Harju, J. 2004. ICEFIN Research Laboratory: WLAN & Security. Viitattu 25.10.2004  
<http://www.cs.tut.fi/tlt/npg/icefin/wlanetsecurity.html>
- Helenius, M. 2003. Realisation Ideas for Secure System Design. U. Gattiker (toim.) EICAR Conference Best Paper Proceedings. 10 sivua. Copenhagen: EICAR e.V.
- Helenius, M. 2004. Why Does E-mail Fail? Teoksessa U. Gattiker (toim.) EICAR 2004 Conference CD-rom: Best Paper Proceedings. 16 sivua. Copenhagen: EICAR e.V.
- Helsingin yliopisto. 2004. Osaamistietokannat. Viitattu 8.7.2004 <http://www-db.helsinki.fi/tuhti/>
- ICPP, Independent Centre for Privacy Protection. 2004. Identity Management Systems (IMS): Identification and Comparison Study. Viitattu 12.10.2004  
<http://cybersecurity.jrc.es/pages/projectsIMS.htm>
- Intel. 2004. LaGrande Technology (LT) for Safer Computing. Viitattu 22.9.2004  
<http://www.intel.com/technology/security/>
- IPSC. 2004. Institute for the Protection and Security of the Citizen. Viitattu 27.10.2004  
<http://ipsc.jrc.cec.eu.int/>
- Jefferson, D., Aviel, R., Simons, B. & Wagner, D. 2004. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). Viitattu 7.9.2004 <http://servesecurityreport.org/>
- Joint Research Center. 2004. Welcome to the Cybersecurity website of the IPTS ICT team. Viitattu 14.6.2004 <http://cybersecurity.jrc.es/>
- Joint Research Center. 2004a. Joint Research Center. Viitattu 16.6.2004 <http://www.jrc.cec.eu.int/>
- Jyväskylän yliopisto. 2004. Tietotekniikan laitos, tieteelliseen laskentaan liittyvät tutkimukset. Viitattu 24.9.2004 <http://www.jyu.fi/tdk/hallinto/tiedotus/tietekn.htm>
- Karjaluoto, H. 2004. Electronic Banking in Finland – Consumer Beliefs, Attitudes, Intentions and Behaviors. Dissertation. University of Jyväskylä. Jyväskylä Studies in Business and Economics.
- Karvonen, T. 2004. Tietoturva nousi tasoihin ohjelmistobisneksen kanssa Pohjolassa. IT-viikko 3.3.2004. IT-viikko-lehden uutisarkisto. Viitattu 26.1.2005  
<http://www.itviikko.fi/uutiset/uutinen.asp?UutisID=59740>
- Kaunisto, L. 2004. Tietoturvan muuri ja tietosuojaan kilpi. Kurssimateriaalista ProIT-Tietoturvakoulutus. Viitattu 4.10.2004 [http://show.tvi.tut.fi/kaunisto/TiTu\\_020604.pdf](http://show.tvi.tut.fi/kaunisto/TiTu_020604.pdf)
- Koulutuskeskus Dipoli. 2004. Turvallisuuskoulutus. Viitattu 26.10.2004  
<http://www.dipoli.hut.fi/turva/index.html>
- Kuluttaja-asiamies. 2004. Verkkokauppiiaan ohje. Viitattu 3.9.2004  
<http://www.kuluttajavirasto.fi/user/loadFile.asp?id=4733>
- Kuopion yliopisto. 2004. Terveystieteiden ja -talouden laitoksen tutkimuskohteet. Viitattu 8.10.2004  
<http://www.uku.fi/laitokset/tht/hankkeet.htm>
- Lapin yliopisto. 2004. EULISP-Koulutusohjelma. Viitattu 26.10.2004  
<http://www.ulapland.fi/home/oiffi/instituutti/eulisp.htm>
- Liikanen, E. 2003. European Network Security. Puhe 24.3.2004 CeBIT-tapahtumassa. Viitattu 13.6.2004 <http://europa.eu.int/rapid/pressReleasesAction.do?reference=SPEECH/04/148>
- Liikenne- ja viestintäministeriö. 2004. Kansallinen tietoturvastrategia. Viitattu 8.7.2004  
<http://www.mintc.fi/www/sivut/suomi/tele/tietoturvastrategia.htm>
- Liikenne- ja viestintäministeriö. 2004. Sähköisen viestinnän tietosuojalaki. Viitattu 24.9.2004  
<http://www.mintc.fi/oliver/upl752-Sähk.pdf>

- Lipmaa, H. 2004. The TCS@HUT Crypto Group. Viitattu 6.9.2004  
<http://www.tcs.hut.fi/Research/Crypto/>
- Mannila, M. 2003. Yhdysvaltain sähkökatko: Slammer sulki ydinvoimalan verkon tammikuussa. IT-Viikko 21.8.2003. Viitattu 19.8.2004 <http://www.itviikko.fi/uutiset/uutinen.asp?UutisID=56900>
- Microsoft. 2004. Trustworthy Computing. Viitattu 9.10.2004  
<http://www.microsoft.com/mscorp/twc/default.mspix>
- Microsoft. 2004. Trustworthy Computing. Viitattu 16.10.2004 <http://www.microsoft.com/mscorp/twc/>
- OECD. 2004. OECD Task Force to Coordinate Fight against Spam. Viitattu 7.9.2004  
[http://www.oecd.org/document/7/0,2340,en\\_2649\\_201185\\_33656711\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/7/0,2340,en_2649_201185_33656711_1_1_1_1,00.html)
- OECD. 2004. Background Paper for the OECD Workshop on Spam. Viitattu 7.9.2004  
[http://www.oelis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/\\$FILE/JT00157096.PDF](http://www.oelis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/$FILE/JT00157096.PDF)
- Oikeusministeriö. 2004. Viitattu 10.9.2004. Vaalitietojärjestelmän kehittäminen ja sähköinen äänestäminen. <http://www.vaalit.fi/14912.htm>
- Oulu University Secure Programming Group. 2004. Viitattu 7.9.2004 Oulu University Secure Programming Group. <http://www.ee.oulu.fi/research/ouspg/>
- ProIT. 2004. ProIT-Tietoturvakoulutus. Viitattu 7.9.2004 <http://proit.fi/titu/index.htm>
- Puolustusministeriö. 2004. Maanpuolustuksen tieteellinen neuvottelukunta Matine. Viitattu 7.9.2004  
[http://www.defmin.fi/index.phtml/page\\_id/125/topmenu\\_id/6/menu\\_id/125/this\\_topmenu/86/lanng/1/fs/12](http://www.defmin.fi/index.phtml/page_id/125/topmenu_id/6/menu_id/125/this_topmenu/86/lanng/1/fs/12)
- Rantanen, M., Mäntylä, M. & Mannila, H. (toim.) 2003. Helsinki Institute for Information Technology HIIT Annual Report 2003 Viitattu 12.10.2004  
[http://www.cs.helsinki.fi/hiit\\_bru/publications/annualreport2003/HIIT-Annual-Report-2003.pdf](http://www.cs.helsinki.fi/hiit_bru/publications/annualreport2003/HIIT-Annual-Report-2003.pdf)
- Reiss, M. 2003. Mato sulki 80 Nordean konttoria. IT-Viikko 14.8.2003. Viitattu 19.8.2004  
<http://www.itviikko.fi/uutiset/uutinen.asp?UutisID=56795>
- Raider, R. 2004. The Self-Defending Network. Viitattu 13.1.2005  
[http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac253/about\\_cisco\\_packet\\_feature0900aecd800e0153.html](http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac253/about_cisco_packet_feature0900aecd800e0153.html)
- RSA Security inc. 2003. RSA® Conference Europe announces the winners of the first annual European Information Security Awards. Viitattu 3.9.2004  
[http://www.rsasecurity.com/press\\_release.asp?doc\\_id=3239&id=1034](http://www.rsasecurity.com/press_release.asp?doc_id=3239&id=1034)
- RSA Security Inc. 2004. Protecting Consumer Privacy. Viitattu 27.8.2004  
<http://www.rsasecurity.com/rsalabs/node.asp?id=2119>
- Ruotsalainen, P. 2002. Ehdotus Sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi – terveydenhuollon PKI-arkkitehtuuri. <http://www.oskenet.fi/asp/empty.asp?P=326&PS=root>
- Saarenpää, A., Pöysti, T., Sarja, M., Still, V. & Balboa-Alcoreza, R. 1997. Tietoturvallisuus ja laki: Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä. Tutkimusraportti. Valtiovarainministeriö. Hallinnonkehittämisosasto. Lapin yliopiston oikeusinformatiikan instituutti. Helsinki: Edita.
- Secgo. 2004. Secgo. Viitattu 14.9.2004 <http://www.secgo.com/secgo/index.html>
- SoberIT. 2004. NETPROSEC. Viitattu 7.9.2004  
<http://www.soberit.hut.fi/NETPROSEC/indexFI.html>
- Sorkin, D. 2003. Spam Laws. Viitattu 9.8.2004 <http://www.spamlaws.com/>

- Sosiaali- ja terveysministeriö. 1995. Sosiaali- ja terveydenhuollon tietoteknologian hyödyntämisstrategia. STM:n julkaisuja 1995:27. Viitattu 13.1.2005  
<http://pre20031103.stm.fi/suomi/tao/julkaisut/hyodstra/tteknsis.htm>
- Sosiaali- ja terveysministeriö. 1998. Saumaton hoito- ja palveluketju. STM:n julkaisuja 1998:8. Viitattu 28.10.2004 <http://www.oskenet.fi/uploads/0gyxd5d8rr.pdf>
- Spamhaus. 2004. The Definition of Spam. Viitattu 8.9.2004 <http://www.spamhaus.org/definition.html>
- Spamhaus. 2004. The Spamhaus Project – ROKSO. Viitattu 14.9.2004  
<http://www.spamhaus.org/rokso/index.lasso>
- Stakes. 2004. Tietoteknologian osaamiskeskus. Viitattu 27.10.2004 <http://www.stakes.fi/oske/>
- STAMI. 2004. Security Technologies and Attitudes in Mobile IPR. Viitattu 13.10.2004  
<http://www.tml.hut.fi/Research/STAMI/>
- Swedberg, C. 2004. States Move on RFID Privacy Issue. RFID Journal. News 30.8.2004 Viitattu 24.9.2004 <http://www.rfidjournal.com/article/articleview/924/1/1/>
- Tampereen kaupunki. 2004. eKortti. Viitattu 14.9.2004 <http://www.etampere.fi/kortti/index.html>
- Tietoliikenneohjelmistojen ja multimedian laboratorio. 2004. Tml-tutkimus. Viitattu 26.10.2004  
<http://www.tml.hut.fi/Tutkimus/>
- Tietosuojavaltuutetun toimisto. 2004. TELLU - Terveystietosuojan ohjausryhmä. Viitattu 28.10.2004. <http://www.tietosuoja.fi/11209.htm>
- Tietotekniikan kehittämiskeskus. 2004. Tietoturva peruskäyttäjälle. Viitattu 18.9.2004  
<http://www.tieke.fi/tietoturvaopas/post.html>
- Tietoturvakonsortio. 2004. Tietoturvakonsortio. Viitattu 8.9.2004 <http://www.cs.uta.fi/fisc/>
- Tietoturvaopas. 2004. Kansalliset tietoturvatalkoot huipentuvat tietoturvapäivänä 11.2.2004. Viitattu 8.9.2004 <http://www.tietoturvaopas.fi/ajankohtaista/tietoturvatalkoot.html>
- Tietoturvaopas. 2004. Tietoturvaopas. Viitattu 3.9.2004 <http://www.tietoturvaopas.fi/>
- Tietoverkkoinstituutti. 2004. TVi etusivu. Viitattu 14.6.2004 <http://www.tvi.tut.fi/>
- Tietoyhteiskuntainstituutti. 2004. Tietoyhteiskuntainstituutti. Viitattu 22.6.2004  
<http://www.uta.fi/laitokset/ISI/>
- U-Cert-työryhmä. 2004. Yliopistojen tietoturvasivut. Viitattu 8.10.2004  
<http://www.yliopistojentt.uta.fi/>
- Valtiovarainministeriö. 2004. Tietoturvasanasto. Viitattu 3.9.2004  
<http://www.vm.fi/tietoturvasanasto/sisallys.htm>
- Valtiovarainministeriö. 2004. Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI). Viitattu 8.7.2004 <http://www.vm.fi/vahti>
- Viestintävirasto. 2004. Telestandardointi. Viitattu 3.9.2004 <http://www.ficora.fi/suomi/tele/n2405.htm>
- Viestintävirasto. 2004. Tietoliikenneturvallisuus (COMSEC). Viitattu 30.7.2004  
<http://www.ficora.fi/suomi/tietoturva/tietoliikenne.htm>
- Viestintävirasto. 2004. Tietoturva. Viitattu 24.6.2004 <http://www.ficora.fi/suomi/tietoturva/index.htm>
- Viestintävirasto. 2004. Tietoturvaloukkausten havainnointi ja ratkaisu (CERT-FI). Viitattu 3.9.2004  
<http://www.ficora.fi/suomi/tietoturva/cert.htm>
- Viestintävirasto. 2004. Tietoturva- ja tietosuojasäädökset Viitattu 28.10.2004  
<http://www.ficora.fi/suomi/tietoturva/saadokset.htm>
- Virtanen, T.-P. 2004. Teemupekka Virtanen. Viitattu 21.9.2004 <http://www.tml.hut.fi/~tpv/>

- Virus Bulletin. 2004. Virus Analysis 1: Cabirn Fever. Virus Bulletin Journal. August 2004.
- Väestörekisterikeskus. 2004. Mikä on sähköinen henkilöllisyys? Viitattu 11.10.2004  
<http://www.vaestorekisterikeskus.fi/vrk/home.nsf/0/6cef85151402ad98c2256c5c0028e63f?openDocument>
- Väestörekisterikeskus. 2004. Väestörekisterikeskus – Yleistä / Henkilökortti. Viitattu 11.10.2004  
<http://www.sahkoinenhenkilokortti.fi/>.
- Vähä-Sipilä, A. 2003. Tietoturvan opetus suomalaisissa ammattikorkeakouluissa. Helsingin yliopisto. Opettajankoulutuslaitos. Aikuisopetukseen suuntautuvat opettajan pedagogiset opinnot / seminaari. Korjattu versio 8.6.2003. Ohjaaja: Riitta Jyrhämä. Viitattu 8.7.2004  
[http://alpskari.vip.fi/~avs/tietoturva\\_ammattikorkeakouluissa.pdf](http://alpskari.vip.fi/~avs/tietoturva_ammattikorkeakouluissa.pdf)

## **Liite 1: Määritelmiä**

*Ennakoiva suodatus:* Tarkoittaa tietoliikenteen suodattamista siten, että haitallinen tietoliikenne ei päädy kohdejärjestelmään asti. Ennakoiva suodatus on sitä tehokkaampaa mitä varhaisemmassa vaiheessa se pystytään toteuttamaan, koska tällöin tietoverkon kuormitus jää mahdollisimman pieneksi. Esimerkiksi roskaposti ja virukset voidaan suodattaa eristämällä haitalliset tietokoneet ennen kuin haitallinen liikenne pääsee eteenpäin.

*Fyysinen tietoturvallisuus.* ”Henkilöiden, laitteiden, aineistojen, varastojen ja toimitilojen turvallisuus tuhoja ja vahinkoja vastaan.” (Valtiovarainministeriö 2004)

*Hallinnollinen tietoturvallisuus.* ”Tietoturvallisuuden osa-alue, joka käsittää toimintalinjaukset, periaatteet, organisaatiojärjestelyt, henkilöstön tehtävien ja vastuiden määrittelyn sekä tietoturvallisuuteen tähtäävän ohjeistuksen, koulutuksen ja valvonnan.” (Valtiovarainministeriö 2004)

*Henkilöstöturvallisuus.* ”Henkilöstöön liittyvien riskien hallinta henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta.” (Valtiovarainministeriö 2004)

*Identiteettivarkaus.* Jonkun toisen henkilön tunnistetietojen väärinkäyttö. Tyypillisiä väärinkäyttöön käytettyjä tietoja ovat: nimi, postiosoite, puhelinnumero, pankkitili, luottokortin numero ja sosiaaliturvatunnus.

*Käyttöturvallisuus.* ”Tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvä turvallisuus.” (Valtiovarainministeriö 2004)

*Laitteistoturvallisuus.* ”Tietoturvallisuuden alue, joka käsittää tietojenkäsittely- ja tietoliikennelaitteiden käytettävyyden, toiminnan, kokoonpanon, kunnossapidon ja laadunvarmistuksen.” (Valtiovarainministeriö 2004)

*Ohjelmistoturvallisuus.* ”Tietoturvallisuuden osa-alue, joka käsittää käyttöjärjestelmät, väliohjelmistot, sovellusohjelmat ja tietoliikenneohjelmistot. Alueeseen kuuluvat ohjelmistojen tunnistamis-, eristämisen-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt, ohjelmistojen laadunvarmistus sekä niiden ylläpitoon ja päivitykseen liittyvät turvallisuustoimet.” (Valtiovarainministeriö 2004)

*Roskaposti.* Ilman vastaanottajan suostumusta laajalle joukolle lähetetty sähköpostiviesti. Usein käytetty englanninkielinen sanamuoto on ”unconsolidated bulk e-mail”. On hyvä huomata, että määritelmässä on termejä, joita on mahdoton määritellä täsmällisesti. On vaikea todeta, miten suuri viestin levityksen tulee olla, jotta se voidaan luokitella roskapostiksi. Vastaavasti on vaikea todeta kaikissa tilanteissa, onko viesti lähetetty ilman vastaanottajan suostumusta. Se, mikä on yhdelle roskapostia, ei ole välttämättä sitä toiselle. Täsmällistä määritelmää roskapostille ei ole sovittu. Lisätietoa löytyy esimerkiksi Spamhaus-projektin verkkosivuilta (2004).

*Tietoaineistoturvallisuus.* ”Tietoturvallisuuden osa-alue, joka käsittää asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden, keinoina mm. tietoaineistojen luettelointi ja luokitus sekä tietovälineiden asianmukainen hallinta, käsittely, säilytys ja hävittäminen.” (Valtiovarainministeriö 2004)

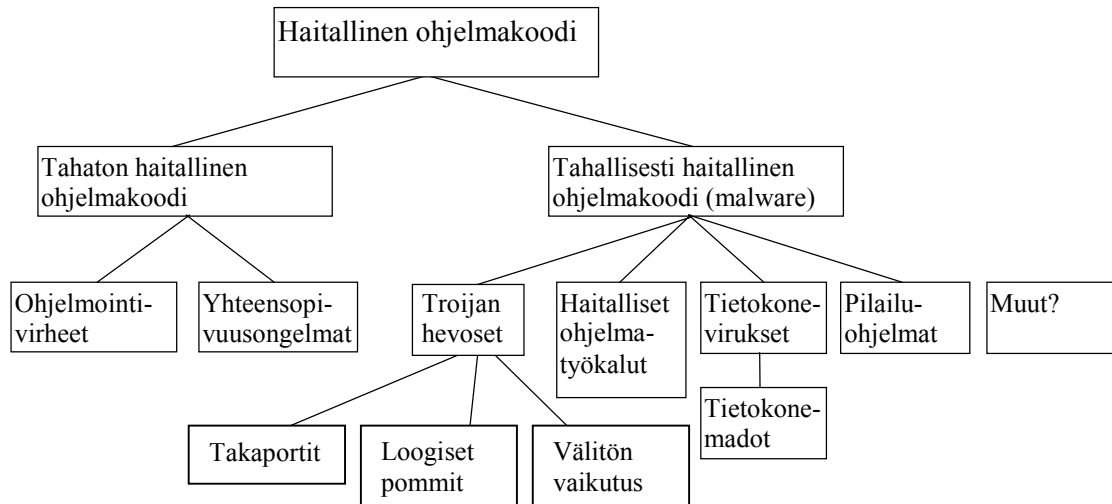
*Tietoliikenneturvallisuus.* ”Tietoturvallisuuden osa-alue, johon kuuluvat mm. tietoliikennelaitteiston kokoonpano, sen luettelointi, ylläpito ja muutosten valvonta, ongelmatilanteiden kirjaus, käytön valvonta, verkon hallinta, pääsyn valvonta, viestinnän salausta ja varmistaminen, tietoturvallisuuden kannalta merkityksellisten tapahtumien tarkkailu, kirjaus ja selvittäminen sekä tietoliikenneohjelmien testaus ja hyväksyminen.” (Valtiovarainministeriö 2004)

*Tietoturvallinen ohjelmointi.* Ohjelmointimenetelmä, jossa pyritään välttämään tietomurrot ja palvelunestohyökkäykset mahdollistavat virheet ohjelmakoodissa.

*VPN (Virtual Private Network) eli suojaverkko.* ”Avoimeen verkkoon tiettyjen käyttäjien välille muodostettu suljettu verkko, jonka sisäisessä liikenteessä käytetään salakirjoitusta ja käyttäjän todennusta. Näin verkko säilyy luottamuksellisena muilta avoimen verkon käyttäjiltä.” (Valtiovarainministeriö 2004)

## Liite 2: Haitallisen ohjelmakoodin luokitus

Haitallisen ohjelmakoodin luokitus selviää kuvasta 1. On hyvä huomata, että yleensä on vaikea löytää täysin poissulkevaa ja kattavaa luokitusta. Lisäksi eri tutkijoiden käyttämät määritelmät voivat vaihdella. Oheisilla määritelmillä on kuitenkin tarkasti mietitty tieteellinen pohja.



Kuva 3: Haitallisen ohjelmakoodin luokitus

*Haitallinen ohjelmakoodi.* Ohjelmakoodi, joka on toimii vastoin järjestelmän määri-tyksiä tai tarkoitettua toimintaa. Haitallinen ohjelmakoodi voidaan jakaa tahalliseen ja tahattomaan haitalliseen ohjelmakoodiin.

*Tahaton haitallinen ohjelmakoodi.* Ohjelmakoodi, joka on tehty tahattomasti haital-liseksi.

*Tahallinen haitallinen ohjelmakoodi.* Ohjelmakoodi, joka on tehty tarkoituksella haitalliseksi.

*Troijan hevonen.* Ohjelmakoodi, joka on naamioitu tekemään jotakin hyödyllistä, mutta joka sisältää piilotetun ja tarkoituksella tehdyn haitallisen toiminnon. Troijan hevonen voi aiheuttaa haitallisen vaikutuksen välittömästi (välitön vaikutus) tai tiettyjen ehtojen ollessa voimassa (loogiset pommit).

*Looginen pommi.* Troijan hevonen, jonka haitallinen toiminto aktivoituu vasta jonkin ehdon ollessa voimassa. Ehto voi olla aika, asetus, levytila, näppäinkoodi, laite, asennettu ohjelma tai mikä tahansa muu ohjelmallisesti tutkittavissa oleva järjestelmän tila. Laukeamisehtona voi olla myös erilaisten tilojen yhdistelmät.

*Takaportti.* Troijan hevonen, joka on tarkoituksella suunniteltu ohittamaan järjestelmän tai sovelluksen suojaustoimintoja.

*Tietokonevirus.* Ohjelmakoodi, joka kykenee leviämään itsekseen rekursiivisesti.

*Tietokonemato.* Tietokonevirus ilman isäntäohjelmaa, johon virus liittää itsensä tai korvaa omalla koodillaan. Tietokonemadot ovat tietokonevirusten osajoukko.

*Haitallinen ohjelmatyökalu.* Ohjelma, joka on suunniteltu helpottamaan tietojärjestelmiä vastaan tehtäviä hyökkäyksiä. Tällaisia ohjelmia ovat muun muassa haitallisten ohjelmien luontiohjelmat, tiedonkaappaajat ja hakkerointiohjelmat.