

Tietoturvan opetus suomalaisissa ammattikorkeakouluissa

Helsingin yliopisto
Opettajankoulutuslaitos
Aikuisopetukseen suuntautuvat
opettajan pedagogiset opinnot / seminaari

Antti Vähä-Sipilä

<avs@iki.fi>

Korjattu versio 8.6.2003

Ohjaaja: Riitta Jyrhämä

Opponentti: Rauni Varkia

English Abstract

Information Security Education in Finnish Polytechnics¹

Antti Vähä-Sipilä <avs@iki.fi>

As information technology becomes more and more pervasive on all areas of everyday living and computers become extensively networked, the importance of data security has grown even more important. Information security is not detached from the other areas of information technology - rather it is connected to all areas of information technology from corporate processes to programming. The focus of this work is the content and methods of information security education in Finnish polytechnics (vocational colleges/universities that offer Bachelor's degrees). The results are based on a survey and previously published foreign research and reports on information security education. This work suggests a four-axis model that provides a tool for comparing information security education styles.

Until recently, information security has been usually viewed from a rather solution-centric viewpoint and it has not been generally seen as an aggregate of various different areas. Due to the threats from viruses and data networks, the marketing message of information security has been reactive. In the reactive model, vulnerabilities are fixed as they appear. One of the targets of this work is to find out whether this problem also affects information security education. Information security issues in programming are also generally not very well understood. Another target for this study is to find out whether this is also true for programming education in polytechnics.

The results of the survey support the initial assumptions. Security in programming education is relatively scarce, and its importance is not very well recognised. Information security education in Finnish polytechnics is very strongly concentrated in practical network security methods, although security policies and processes are seen almost just as important. It is apparent that there is a desire for increasing the amount of information security education. Teaching the basics of information security to all students is seen as important. Practical laboratory exercises are a highly valued tool in information security education when supported with lectures.

Further information in English is available from the author.

¹Polytechnic educational institutions in Finland are vocational colleges/universities that provide more practically oriented education than traditional universities and typically offer a Bachelor's degree (whereas traditional universities offer Master's, Licentiate and Doctoral degrees).

Tiivistelmä

Tietoturvan opetus suomalaisissa ammattikorkeakouluissa

Antti Vähä-Sipilä <avs@iki.fi>

Tietoturva on tullut entistä tärkeämmäksi tietotekniikan ulottuessa yhä useammille jokapäiväisen elämän alueelle ja tietokoneiden verkottuessa yhä tiiviimmin. Tietotekniikan alalla tietoturva ei ole erillinen kokonaisuus vaan se liittyy lähes kaikkiin tietotekniikan osa-alueisiin aina yritysten prosesseista ohjelmointiin. Tässä työssä tutkitaan tietoturvallisuuden opetussisältöä ja opetusmenetelmiä suomalaisissa ammattikorkeakouluissa kyselytutkimuksen keinoin ja verrataan tuloksia ulkomaille julkaistuihin tietoturvan opetusta käsitteleviin tutkimustuloksiin ja raportteihin. Samalla esitän neljän akselin mallin, joilla tietoturvan opetustapoja voidaan luokitella.

Tietoturvaa on katsottu viime päiviin asti yleensä varsin ratkaisukeskeisestä näkökulmasta, eikä sitä ole käsitelty monien asioiden kokonaisuutena. Virusongelmien ja tietoverkkojen turvallisuusongelmien vuoksi tietoturvan markkinoinnissa on korostunut reaktiivinen lähestymistapa, jossa pyritään paikkaamaan haavoittuvuuksia sitä mukaa kun niitä ilmenee. Tutkimuksen tarkoituksena on selvittää, koskeeko tämä lähestymistapa myös tietoturvan opetusta. Myös ohjelmoinnin tietoturva-asiat ovat jääneet alalla liian pienelle huomiolle. Toinen tavoite tutkimuksella on selvittää, onko ohjelmoinnin turvallisuuden opettaminen ammattikorkeakouluissa vähäistä.

Tutkimuksen tulokset tukivat alkuoletuksia siltä osin, että ohjelmoinnin turvallisuuden opetus oli vähäistä eikä sen tärkeyttä tiedostettu kovin laajalti. Tietoturvan opetus ammattikorkeakouluissa keskittyy hyvin vahvasti tietoverkkojen turvallisuuden käytännön menetelmien opettamiseen, joskin myös tietoturvapoliittikat ja -ohjeistukset koetaan lähes yhtä tärkeinä. Laboraatiot ja muut käytännön harjoitukset ovat erittäin tärkeässä asemassa.

On ilmeistä, että tietoturvaopetusta halutaan lisätä ja ainakin sen perusasioiden opettaminen kaikille oppilaille nähdään tärkeänä. Sekä ulkomaiset raportit että kyselytutkimuksen tulokset osoittavat, että laboraatioita arvostetaan tietoturvan opetuksessa ja niitä pidetään luentojen tukemana pedagogisesti parhaana tapana opettaa tietoturvallisuutta.

Sisältö

1	Tietoturvan opetus tutkimusten valossa	5
1.1	Tietoturva tietotekniikan osana	5
1.2	Tietoturvan osa-alueet	6
1.3	Opetuksen lähtökohdat	6
1.4	Erytishuomioita tietoturvan opetuksesta	11
2	Tutkimustavoite ja -ongelmat	14
3	Tutkimuksen tulokset	15
3.1	Tutkimuksen suorittaminen	15
3.2	Tietoturvaopetuksen kohdeyleisö	15
3.3	Tietoturvakurssien koostumus	16
3.4	Mielipiteet sisällöstä	17
3.5	Laboraatioiden tilanne	19
3.6	Tietoturvan opettamisen kehitysnäkymät	20
4	Luotettavuustarkastelu	21
5	Pohdintaa	22
5.1	Laboraatioiden jatkotutkimusta	22
5.2	Tietoturvallisen ohjelmoinnin kriisi	23
5.3	Varoittavat esimerkit	24
A	Tietoturvakurssien sisältöjä	29
B	Kyselykaavake	31

1 Tietoturvan opetus tutkimusten valossa

1.1 Tietoturva tietotekniikan osana

Tietotekniikka eroaa tietojenkäsittelyopista siten, että tietotekniikka kattaa laajemmin käytännön sovelluksia. Suomalaisissa korkeakouluissa tietotekniikkaa on yleensä opetettu teknillisissä korkeakouluissa (nykyään teknillisissä yliopistoissa) ja tietojenkäsittelyoppia taas monitieteellisissä yliopistoissa. Tämä työ lähestyy tietotekniikkaa laajemmasta näkökulmasta, jolloin siihen kuuluvat sekä tietokonetekniikka (laitteistot eli *hardware*), ohjelmistotekniikka (*software*), tietotekniikan käyttöön liittyvät yritysten prosessit ja hallinto sekä tietotekniikkaa tukevat alat kuten esimerkiksi matematiikka.

Tietoturva on ollut viime aikoina lujassa nousukiidossa monesta syystä: tietotekniikka on tunkeutunut yhä useammille elämän osa-alueille muodossa, jossa tekniikan pettäminen voi helposti aiheuttaa ihmishenkien tai suuren taloudellisen menetyksen ja toisaalta viime aikojen maailmanpoliittiset tapahtumat ovat luoneet epävarmuuden tunnetta, jota myös tietoturvayritykset yrittävät käyttää rahallisesti hyväkseen. Jopa informaationsodankäynnin kaltaiset termit vilahtelevat huomattavasti aikaisempaa useammin lehdistössä. Samaan aikaan Internetin huima suosion kasvu on aiheuttanut sen, että tietokoneet ovat entistä useammin yhteydessä toisiinsa tietoverkon välityksellä. Tulevaisuudessa myös nk. sulautetut järjestelmät eli tietokoneet, jotka on rakennettu osaksi jotakin muuta tietokonetta muistuttamatonta laitetta (esim. televisiot, jääkaapit ja puhelimet) ovat myös yhteydessä toisiinsa. Mikäli kyseiset laitteet ovat haavoittuvia hyökkäyksille², tämä luo erittäin suuria riskejä yhteiskunnan toiminnoille.

Olen kirjoittanut tämän seminaarityön myös yleisölle, joka ei ole teknisesti suuntautunut. Tästä johtuen olen pyrkinyt selittämään mahdollisesti oudot termit joko yleistävin kiertoilmauksin (josta johtuen teknisesti suuntaunut henkilö löytänee aiheetta pilkunviilaukseen joissakin kielikuvin) tai alaviitteinä (joita on tästä syystä varsin paljon). Työn pitäisi olla ymmärrettävissä myös ilman syvällistä tietotekniikan tuntemusta.

²Tietoturva-alalla ”hyökkääjä” on mikä tahansa taho, joka yrittää saada järjestelmän käyttäytymään haluamallaan tavalla järjestelmän ylläpitäjän tahdon vastaisesti. Termi ei (yleensä) viittaa sotilaalliseen toimintaan eikä hyökkääjä välttämättä ole ”paha”. Termi on tarkoituksenperäneutraali.

1.2 Tietoturvan osa-alueet

Tietoturvan määrittely lyhyesti ei anna oikeudenmukaista kuvaa alan laajuudesta. Tietoturvallinen järjestelmä voidaan määritellä esimerkiksi seuraavilla tavoilla:

- järjestelmä, joka toteuttaa annetun turvallisuuspolitiikan³ myös vihamielisessä ympäristössä (tekniseen toteutukseen perustuva määritelmä; Irvine, Chin, & Frincke 1998)
- järjestelmä, joka tekee määrittelynsä mukaiset toiminnot eli on laadukas ja käsittelee poikkeustilanteet hallitusti (laadun määritelmää laajentava määritelmä; Bishop 1997)
- järjestelmä, joka takaa tiedolle luottamuksellisuuden, eheyden ja alkuperätoennuksen (tiedon turvaamiseen perustuva määritelmä⁴)
- järjestelmä, jossa virhetoimintojen (hyökkäyksen) aiheuttamat kustannukset ovat pienemmät kuin sen suojaamisen kustannukset (riskitason määrittelyyn perustuva määritelmä; Schneier 2000, 301-302)

Paremmän kuvan tietoturvan alasta saa tutkimalla käytännön esimerkkejä, joiden tutkimisen ja toteuttamisen voidaan katsoa kuuluvan tietoturvaan. Liitteeseen A on koottu tietoturvan opetuksen osa-alueita useista tietoturvan opetusratkaisuja kuvaavista lähteistä (Irvine, Warren, & Clark 1997b; Bintziou, Alexandris, & Chrissikopoulos 1999; Bishop 2000; Bishop 1997; Yang 2001; Yasinsac 2001; White, Marti, & Hudson 1999; Irvine ym. 1998). Olen luokitellut osa-alueet isompien otsikkojen alle. Osa-alueiden lista ei varmastikaan ole täydellinen ja jaosta vallitsee useita eri käsityksiä - esimerkiksi käyttämässäni kyselylomakkeessa en jakanut osa-alueita pääotsikkojen alle.

1.3 Opetuksen lähtökohdat

Tietoturvan opetusta ja soveltamista voidaan kuvata useilla erilaisilla akseleilla, joille kukin alalla toimija voi sijoittua suhteellisen vapaasti ja silti sanoa olevansa tietoturva-alalla. Seuraavassa kuvataan joitakin näistä akseleista ja esitellään kunkin lähestymistavan hyviä ja huonoja puolia.

³Politiikalla (*policy*) tarkoitetaan määrittelyjä, ohjeistusta ja toimintamalleja, jonka mukaan järjestelmä ja henkilöstö toimivat. Termillä ei viitata yleisesti poliittisiin ilmiöihin tai poliitikkoihin.

⁴Tunnetaan myös CIA-mallina: *confidentiality, integrity, authentication*

1.3.1 Prosessilähtöisyys - ratkaisukeskeisyys -akseli

Perinteisesti lähtökohdaksi on usein otettu se, että tietojärjestelmä on kuin harva seula, josta tehdään vedenpitävä tukkimalla reikiä yksi kerrallaan sen sijaan, että seulan sijasta käytettäisiin veden kauhomiseen esimerkiksi kauhaa tai kyseenalaistettaisiin tarve veden kauhomiseen kokonaan. Nykyään on kuitenkin yleisesti hyväksytty ajattelumalli, jonka mukaan ”turvallisuus syntyy prosesseista, ei tuotteista” (Schneier 2000, 273). Tämän mukaan tietoturvaluottelu lähtee ennen kaikkea oikeanlaisista toimintamalleista eikä niinkään tiettyjen teknisten ratkaisujen (tuotteiden) soveltamisesta.

Olisi tietenkin hurskastelua väittää, ettei tietoturvaluotteluja tarvittaisi. Ongelma onkin siinä, että monissa tapauksissa tietoturvaongelmaa lähestytään tuotteen näkökulmasta, jolloin unohdetaan esimerkiksi riskianalyysi ja taloudellisuus (joissakin tapauksissa hyökkäyksen kustannukset voivat olla pienemmät kuin suojauksen kustannukset) eikä oteta huomioon sitä, että kaikkia hyökkäysmahdollisuuksia ei ole otettu huomioon. Analogiana voisi toimia esimerkiksi risumaja, jossa on metalliovi ja munalukko. Hyökkääjä todennäköisesti kävelee seinän läpi ennemmin kuin alkaa polttoleikata ovea auki. Tällaiset ratkaisukeskeisestä ajattelutavasta johtuvat ongelmat saadaan minimoitua oikealla prosessien ja uhka-analyysien avulla ja prosessit voidaan jalkauttaa käytäntöön perustelluilla ratkaisuilla.

Opetuksessa ero näkyy siinä, opetetaanko ratkaisuja erillisinä ”temppeina”, kuten eräs tutkimukseen vastannut asian ilmaisi, vai annetaanko ratkaisuille peruste ja viitekehys. Ratkaisujen opettamista prosessilähtöinen ajattelu ei siis suinkaan sulje pois.

1.3.2 Integroituva - eriytyvä -akseli

Tietoturvaa voidaan opettaa joko yhdistäen tietoturvanäkökulmaa kaikkiin tietotekniikan olemassaoleviin kursseihin tai erillisenä kokonaisuutena, jossa tietoturva on ”arvo” sinänsä ja muita aiheita käsitellään nimenomaan tietoturvan näkökulmasta.

Tietoturvan integroinnilla muuhun opetussuunnitelmaan tarkoitetaan yleensä sitä, että tietoturva-asiat otetaan esille osana muita kursseja (esim. Irvine ym. 1998; Barnett 1996). Tietoturva-asiat nivoutuvat usein esimerkiksi luontaiseksi osaksi erityisesti tietoliikennekursseja (kuten tämän esityksen tutkimusosasta käy hyvin ilmi).

Tietoturva voi tulla kurssilla esille joko erillisenä aiheena, esimerkiksi yhden luennon aiheena, tai sitten esimerkiksi kurssin harjoitustyön aihe voi liittyä tietoturvan alaan. Integroidulla opetuksella on se hyvä puoli, että tietoturva-asiat tulevat vastaan ainakin jossakin muodossa ja laajuudessa lähes kaikille opiskelijoille ja aiheen toistaminen parantaa oppilaiden aiheenhallintaa. Ongelmaksi voidaan katsoa se, että varsinaisia tietoturva-asiantuntijoita ei tällä menetelmällä välttämättä synny. Kuitenkaan ihannetilanteessa erityisasiantuntijoiden leipominen ei välttämättä olisi edes tarpeellista: suurin osa tietoturvaongelmista johtuu tietoturvatietoisuuden puutteesta ja esimerkiksi laatuongelmista (NIST 2003). Mikäli tietoturvatietoisuus olisi korkeammalla tasolla yleisesti, ei ehkä tarvittaisi tietoturvaan erikoistuneita spesialisteja paikkaamaan syntyneitä reikiä. Integroitu lähestymistapa on todennäköisesti eriytettyyn malliin verrattuna paremmassa sopusoinnussa edellämainitun prosessilähtöisen ajattelumallin kanssa, sillä tällöin tietoturvallinen ajattelutapa sisällytetään kaikkeen toimintaan.

Integroivat mallit perustuvat myös usein jonkin ”punaisen langan” seuraamiseen kaikilla kursseilla. Esimerkiksi Irvine (1999b) ehdottaa nk. viitetarkkailijamallin (*reference monitor concept*, ks. myös Amoroso 1994, 90) ottamista käyttöön kaikkia tietoturvakursseja yhdistänä tekijänä. Mallin kuvaaminen ei liene tässä merkityksellistä, mutta oli valittu johtoajatus mikä hyvänsä, on ilmeisen tärkeää, että malli sopii sekä teknisten toteutusten suunnittelupohjaksi että prosessien ja tietoturvapoliittikkojen perusteeksi. Punaisen langan käyttöönotto varmistaa myös sen, että tietoturvasasioilla on looginen jatkumo, jolloin opetus ei lokeroidu (Irvine ym. 1997b). Haasteellisuutta lisää se, että mikäli kurssien suoritusjärjestys ei ole kiveen hakattu, tietoturvan osuus on rakennettava niin, että se samanaikaisesti mahdollistaa aiemmin opitun päälle rakentamisen mutta ei kuitenkaan estä kurssille osallistumista esitietojen puutteen vuoksi.

Integroitua mallia voidaan soveltaa myös niin, että oppilaiden todennäköisille tuleville työrooleille määritellään sopiva paketti tietoturvatietoutta ja tämä paketti jaetaan olemassaoleviin kursseihin siten, että tutkinnon suoritettuaan jokainen oppilas on saanut tarkoituksenmukaisen annoksen tietoturvaa (Irvine ym. 1998). Tietoturvan kannalta mahdollisia rooleja ovat esimerkiksi ”suuri yleisö”, yritysten tietohallintohenkilöstö, tietokoneasiantuntijat, järjestelmäylläpitäjät, tietoturvaongelmia hoitavien työryhmien⁵ jäsenet, turvallisten ohjelmistojen ja laitteistojen kehittäjät, systeemiarkkitehdit, systeemien sertifioijat, laki-ihmiset ja viranomaiset sekä tur-

⁵CERT, *Computer Emergency Response Team*. Esimerkiksi Suomessa Viestintävirastolla on CERT-FI -työryhmänsä ja monilla yrityksillä omat tietoturvaorganisaationsa.

vallisuustutkijat (Chin, Irvine, & Frincke 1997). Tosin vuosi edellisen luokittelun sisältäneen paperin julkaisun jälkeen yksi sen kirjoittajista varoittaa, että liiallinen tuleviin rooleihin perustuva oppisisällön määrittely voi johtaa *training* -tyyppiseen koulutukseen, jossa painopiste on liikaa jonkun tietyn tuotteen tai menettelytavan ulkoaoppimisella (Irvine 1999a). Lisäksi ”turvallisten” ohjelmistojen kehittäjien erottaminen muista ohjelmistokehittäjistä vahvistaa mielestäni vanhahtavaa mielikuvaa siitä, että olisi jotenkin hyväksyttävää tehdä ”turvattomia” ohjelmia.

Integroitu malli näyttäisi olevan myös työnantajien suosiossa. Eräät tietoturvan opetuksen tutkijat pyysivät vuosina 1996 ja 1997 kommentteja työnantajilta liittyen integroituun ja eriytyvään opetukseen. Tuloksena mainittiin mm.

Kaikki huomioita tehneet [työnantajat] täsmensivät, että turvallisuus ei ole erillinen tieteenala vaan paremminkin osa suurempaa insinööriyön ja tietotekniikan viitekehystä. (Irvine ym. 1998, oma suomennos; kyselyn tuloksista ks. myös Chin ym. 1997.)

Toinen tapa ajatella tietoturvaopetuksen asemaa opetussuunnitelmassa on eriytynyt malli. Tässä mallissa tietoturva-asiat on eriytetty omiksi kurseikseen. Kurseilla käsitellään tietotekniikan eri osa-alueita, esimerkiksi tietokantoja, tietoliikennettä ja ohjelmointia tietoturvan näkökulmasta. Eriytetty opetus saattaa tarjota paremman yleiskuvan tietoturvan alalta, mikäli kurssien teoreettinen pohja on tarpeeksi laaja. Tällainen pohja on tarpeen henkilöille, jotka toimivat esimerkiksi organisaatioiden tietoturvavastaavina. Riskinä on se, että kurseilla käydään läpi sarja ratkaisumalleja, jotka sopivat eri tilanteisiin, mutta opiskelijalla ei välttämättä ole vaadittavia perustietoja kaikista kurssin osa-alueista tietoturvamerkityksen todellista ymmärtämistä varten. Erillinen tietoturvakurssien opetus saattaa myös antaa tietoturvas-ta kuvan, jossa tietoturvallisuutta voidaan lisätä järjestelmiin jälkikäteen erillisten tietoturva-asiantuntijoiden toimesta. Tämä on tiukassa ristiriidassa aiemmin mainitun prosessinäkemyksen kanssa (Schneier 2000).

1.3.3 ”Miksi” - ”miten” -akseli (*Education - training -akseli*)

Äärimmäisyyteen vietyinä ratkaisukeskeinen ajattelutapa saattaa lähestyä *training* -tyyppistä koulutusta, joka keskittyy esimerkiksi yhden tietoturvatuotteen käyttöön, esimerkiksi palomuurituotteen⁶ käyttöönottoon. Training-tyyppinen koulutus saat-

⁶Palomuri (*firewall*) on verkkolaite, joka estää tai siistii verkkoliikennettä annettujen parametrien mukaan. Sillä pyritään suojelemaan laitteita, joiden tietoturva on puutteellinen.

taa hyvin toteutettuna antaa eväitä tehokkaaseen tietoturvaongelmiin reagointiin (Bishop 2002). Koska tietotekniikka kuitenkin kehittyy huimaa vauhtia, on yksittäisten tuotteiden nostaminen opetuksen keskiöön hieman kyseenalaista. Esimerkiksi Microsoft Windows 3.1:n osaaajille ei nyky maailmassa juuri ole enää käyttöä - käyttöjärjestelmien toimintaperiaatteita syvällisesti osaaville kylläkin. Tuotteiden käyttökokemusta tulisikin siis mielestäni korostaa lähinnä harjoitustöiden sivuvaikutuksena eikä sitä tulisi nostaa varsinaiseksi opetustavoitteeksi. Tätä ehdottaa myös Irvine (1999a): laboraatioiden suorittamisessa voisi olla tarpeellista käyttää tiettyjä turvallisuustuotteita, mutta niiden käytön oppiminen ei olisi varsinainen tavoite.

Vastakohtana *training*-tyyppiselle koulutukselle on ”akateeminen” (lähteissä *education*- tai *scholarly*-tyyppinen, Bishop 2002) koulutus, joka pyrkii antamaan oppilaille riittävän kokonaiskäsityksen, jotta yhden ratkaisumallin sijaan oppilaat ymmärtävät ongelman taustalla olevat periaatteet ja osaavat soveltaa useita eri ratkaisuja samaan ongelmaan. *Education*-tyyppisen opetuksenkaan ei tarvitse olla teoreettista. Jo pelkästään se, että oppilaat joutuvat esimerkiksi laboraatiossa miettimään ongelman syitä sen sijaan, että demonstraatiomielessä esimerkiksi asennetaan yksi tietty tietoturvaluote, auttaa oppilaita toimimaan tulevaisuuden muutuviissa haasteissa huomattavasti paremmin - mutta toisaalta ilman kokemusta yhdestäkään tuotteesta opiskelijat eivät ehkä osaa toimia riittävän nopeasti ja tehokkaasti.

On sinänsä valitettavaa, että monet yritykset yrittävät kouluttaa oppilaita vain oman yrityksensä tuotteiden erityisosaajiksi. Markkinointikikkana ajatus on varmasti erinomainen, mutta eettisesti tuotesidonnainen koulutus on mielestäni varsin arveluttavaa, ellei sitten koulutusta ole suunniteltu niin, että se korostaa ”miksi”-osuutta ”miten”-osuutta enemmän. *Training*-tyyppinen koulutus tähtää usein jonkin sertifiointin saamiseen, jonka on tarkoitus nostaa sertifikaatin haltijan haluttavuutta työmarkkinoilla. Ammatti- ja ammattikorkeakouluissa tällainen on varmasti erittäin hyvä argumentti, mutta tuotesidonnaisuus ja sertifikaatin mahdollinen vanhentuminen pidemmällä aikavälillä tulisi ottaa huomioon.

”Miksi” - ”miten” -akseli voidaan ymmärtää myös sinä tasona, johon teorian tieto abstrahoidaan. Tällä tarkoitan sitä tasoa, jonka perustana oleviin yksityiskohtiin ei enää kajota vaan niitä käsitellään kokonaisuutena. Esimerkiksi turvaprotokollien⁷ opetuksessa voidaan vetää raja protokollan sovelluskohteisiin, jolloin protokollan toteuttaviin algoritmeihin ei perehdytä. Toisena esimerkkinä palomuruin tutustuttaessa voidaan opetella vain perusperiaatteet (ja mahdollisen harjoitustyön tarvit-

⁷Protokollalla tarkoitetaan esimerkiksi tietokoneiden välisen liikennöinnin ”ohjesääntöä” eli miten koneet juttelevat toisilleen.

semat kehittyneemmät toiminnot) sen sijaan, että opetellaan tuotteesta joka ikinen pieni nippeli. Tällöin aikaa vapautuu monipuolisempien kokonaisuuksien käsittelyyn mutta tarvittaessa opiskelijalla on valmiudet syventyä yksittäiseenkin tuotteen myöhemmin työtehtävien niin vaatiessa.

1.3.4 Proaktiivinen - reaktiivinen -akseli

Proaktiivinen (ennaltaehkäisevä) opetuskäsitys painottaa sitä, että järjestelmistä pyritään rakentamaan turvallisia jo alusta lähtien, jotta myöhemmin ei tarvitse havaita puutteita turvallisuudessa (esim. Irvine ym. 1998). Reaktiivinen opetuskäsitys taas korostaa sitä, että ongelmien ilmetessä opiskelijoiden on osattava reagoida mahdollisimman nopeasti, tehokkaasti ja oikein.

Vaikka proaktiivinen malli kuulostaakin hyvin paljon prosessilähtöiseltä ajattelumallilta, erona on kuitenkin se, että proaktiivinen suunnittelu voi olla täysin teknisluonteista. Hyvin pitkälle viety proaktiivinen ajattelu kuitenkin todennäköisesti aiheuttaa näkemyksen siirtymisen prosessilähtöisyys -ratkaisukeskeisyys -akselilla kohti prosessilähtöisyyttä.

Barnett (1996) jakaa tietoturvahenkilöstön roolit kahteen luokkaan, joista toinen käsittelee ”pragmaattisia, operationaalisia asioita” lähinnä järjestelmien ylläpidossa ja toinen tuottaa varsinaisia tietoturvaratkaisuja tutkimuksen ja tuotekehityksen kautta. Järjestelmäylläpito ja verkkoja toteuttava henkilöstö siis hyötyisi tämän luokituksen perusteella enemmän reaktiivisesta painotuksesta ja ohjelmoijat ja testajat enemmän proaktiivisesta. Toisaalta sama artikkeli painottaa, että proaktiiviset menetelmät kuten riskienhallinta kuuluvat myös ylläpidon koulutukseen.

1.4 Erityishuomioita tietoturvan opetuksesta

1.4.1 Laboraatioiden ihanuus

Riippumatta siitä, missä kohtaa edellämainituilla akseleilla tietoturvaopetuksen näkemys sijaitsee, tutkittaessa tietoturvan opetuksesta kirjoitettuja papereita yksi didaktiivinen lähestymistapa nauttii jakamatonta suosiota. Laboraatiot eli yleensä valmiin tehtävänannon mukaan etenevät käytännön harjoitukset nähdään oleellisina tietoturvan opetuksessa. Lindskog, Lindqvist, & Jonsson (1999) ja Barnett (1996)

esittävät, että käytännön harjoitukset ovat välttämättömiä, koska oppilaiden on oltava valmistautuneita käytännön tilanteisiin. Tämän voi tulkita edustavan sellaisen organisaation tarpeita, joissa tietoturvaa lähestytään reaktiivisesti: organisaation tietoturva-asiantuntijalle annetaan uusia ongelmia ratkaistavaksi (siivilän reikiä tilkittäväksi) ja harjoituksista saadun kokemuksen avulla ongelman jäsenitys ja tietoturvaluokkien käyttö on tehokkaampaa ja helpompaa. Proaktiivista näkökulmaa edustavat Irvine, Stemp, & Warren (1997a), jonka mukaan käytännön harjoitukset ovat tarpeellisia, koska tietoturvan ylin tavoite on parantaa todellisten järjestelmien turvallisuutta ennaltaehkäisevästi. Lisäksi käytännön harjoitusten nähdään tukevan lopputöiden tekemistä. Fillery-James (1999) yhdistää käytännön harjoitteiden tarpeen yleiseen kasvatustieteelliseen näkemykseen, jonka mukaan oppimisprosessi vaatii käytännön kokeilemistä ja oppimista tapahtuu kokeiden tulosten tulkinnassa ja reflektoinnissa teorian pohjalta. Baskerville & Straub (1999) painottavat laboraatioiden lisäksi myös ryhmätöitä, jotka auttavat erityisesti ulospäinsuuntautuneita oppilaita jäsentämään omaa tietämystään aiheesta.

Laboraatiot⁸ on yleensä kytketty osaksi muuta kurssia (White ym. 1999; Irvine ym. 1997a; Barnett 1996; Baskerville & Straub 1999; Irvine 1999a), jolloin kurssin teemoja havainnollistetaan ja tehdään kiinnostavammiksi opiskelijoille (esimerkiksi Lindskog ym. (1999) menevät niinkin pitkälle, että kertovat oppilaiden katsoneen laboraatiot ”hauskoiksi” ja ”jännittäviksi”). Jos kyseessä on integroiva opetus, jossa tietoturva-asiat yhdistetään osaksi tavallisia kursseja, laboraatiot saattavat joissakin tapauksissa olla ainoa tapa käsitteellistää turvallisuusasiat niin, että oppilaat todella ymmärtävät ne (Irvine 1999a). Muuten ne saattavat jäädä irrallisiksi maininnoiksi, joilla ei ehkä ymmärretä olevan sovellutuksia todellisuudessa.

Irvine (1999a) jakaa laboraatiot viiteen pääluokkaan:

- järjestelmien heikkouksien käytännönläheinen tutkimus ja tunkeutumisanalyysiharjoitukset (esimerkiksi *white hat*-krakkerointi, julkaistujen hyökkäystyökalujen käyttäminen ja tutkinta jne.)
- turvallisuustestaus- ja turvallisuustuotteiden kokeileminen (vrt. aiemmin käsitelty *training* -malli)
- turvallisuuskäsitteiden ja -periaatteiden vahvistamiseen tarkoitettut harjoitukset (esimerkiksi uhka-analyysit, prosessikehitys, jne.)

⁸Erittäin hyviä ideoita laboraatioihin on esimerkiksi lähteessä Fillery-James 1999 ja murtautumisharjoituksia puolustavassa lähteessä Lindskog ym. 1999.

- turvallisten järjestelmien rakentamiseen käytettävien työkalujen tutuksi tekemiseen suuntautuvat harjoitukset
- projektit, joissa rakennetaan turvallisia järjestelmiä tai alijärjestelmiä (järjestelmiä, joiden määrittelyssä tietoturva vaatimukset ovat erikseen mainittuja)

Kahta ensimmäistä laboraatiotyyppeä varten tarvitaan yleensä erillinen laboratorioverkko tai tietojärjestelmä, koska testaaminen julkisessa verkossa tai edes koulun omassa sisäverkossa on varsin kyseenalaista. Kolmas, neljäs ja viides laboraatiotyyppi voidaan todennäköisesti yhdistää hyvin esimerkiksi osaksi ohjelmointiharjoitusta: ohjelmointikurssilla voidaan esimerkiksi edellyttää turvallisuustestaustyökalun käyttöä ohjelman testaamisessa, ohjelmointitehtävä voi olla jonkin järjestelmän turvalliseksi tarkoitettu osa-alue ja esimerkiksi Internet-sivustojen ohjelmoinnissa voidaan kiinnittää erityistä huomiota turvallisuustarpeisiin. Tietoturvalaboraatiot eivät siis välttämättä tarvitse mitään erillistä laboratoriota ollakseen mahdollisia, ainakaan jos kyse ei ole tietoverkkoturvallisuudesta.

1.4.2 Tietotekniikan etiikka

Tietotekniikan etiikka (*computer ethics*) olisi myös tärkeä osa tietoturvan opetusta, mutta se ei ole kovinkaan selvästi näkyvissä. Muutenkin tekniikan etiikan opetus on jätetty varsin vähäiselle painoarvolle. Esimerkiksi Tampereen teknillisessä korkeakoulussa 90-luvulla tekniikan etiikan kurssi oli täysin erillinen ja vapaaehtoinen opintojakso. Tämä on hieman erikoista, koska monilla tietotekniikan ammattilaisten järjestöillä on laajojakin eettisiä ohjeistuksia (esim. Tietotekniikan liitolla (Tietotekniikan liitto 2002) ja vanhimmalla alan järjestöllä Association for Computing Machineryllä (ACM 1998)).

Informaatiotekniikan etiikkaa tulisi opettaa jo huomattavasti ennen korkeakoulutusta, jo yleissivistävän koulutuksen aikana (Chin ym. 1997; Bintziou ym. 1999). Erään määritelmän mukaan tietotekniikan etiikan yleiskäsite informaatioetiikka kattaa suvaitsevuu-den, luottamuksen, huomioonottamisen ja säännöt (Bintziou ym. 1999). Suvaitseminen ja toisten huomioonottaminen ovat avainasioita esimerkiksi nk. netiketin (*netiquette*, verkkoviestinnän käyttäytymisohjeisto) opettamisessa ja näiden opettamisen tulisi olla luonteva osa sitä hetkeä, kun oppilaat peruskoulussa ensimmäistä kertaa alkavat käyttää tietokoneita viestintään. Säännöt taas liittyvät esimerkiksi lainsäädäntöön. Viime aikoina esimerkiksi tekijänoikeusasiat ovat olleet

pinnalla ja ne tulevat ajankohtaisiksi kun oppilaat tekevät ensimmäisiä kotisivujaan, esitelmiään tai muita tietokoneavusteisia esityksiään. Luottamusaspekti taas liittyy yksityisyyden suojaan ja tietosuojaan (*privacy*, Euroopassa erityisesti *data protection*) sekä siihen, mihin oppilaat voivat verkossa luottaa. Opetushallitus onkin julkaissut Suomessa DotSafe-hankkeen yhteydessä peruskouluille tarkoitetun materiaalikansion, joka sisältää netikettiohjeissaan jotakin tietotekniikan etiikan aiheita (Opetushallitus 2003).

Myöhemmässä tietotekniikan opetuksessa informaatioetiikan opetuksen voisi yhdistää vaikkapa lakiasioiden opetukseen. Esimerkiksi yksityisyyden suojaa säätelevät lait ja EU-direktiivit ovat tärkeitä kaikille verkkopalvelujen ja tietokantapalvelujen kehittäjille, tulevaisuuden mobiileista paikannuspalveluista puhumattakaan. Terveystieteidenhuoltoalan ammattikorkeakouluopetuksessa informaatioetiikka onkin edustettuna terveydenhuollon yksityisyyden suojan myötä.

2 Tutkimustavoite ja -ongelmat

Tutkimuksen tavoitteena on löytää vastauksia ainakin seuraaviin kysymyksiin:

- Onko tietoturvan opetusmenetelmissä havaittavia koulukuntia?
- Onko opetusmenetelmissä eroja riippuen siitä, mitä tietoturvan osa-alueita ollaan opettamassa vai ovatko menetelmät yhteisiä koko erityisalalle?
- Onko tietoturva-alalla ylikorostuneita tai aliarvostettuja osa-alueita? (Sisällöllinen kysymys, ei niinkään didaktinen.)
- Mitä kehittämisehdotuksia jo julkaistujen artikkelien kirjoittajat ovat esittäneet ja mitkä ovat pääsyyt näille kehittämisehdotuksille?

Tutkimushypoteesina oli, että tietoturvaopetus nykyisellään on varsin ratkaisulähtöistä ja keskittynyt virustorjuntaan ja verkkoturvallisuuteen, eikä prosessi- ja politiikkaopetusta juurikaan olisi. Lisäksi oletin turvallisen ohjelmoinnin opetuksen olevan puutteellista sen merkitykseen nähden.

3 Tutkimuksen tulokset

3.1 Tutkimuksen suorittaminen

Kysely suoritettiin sähköpostitse. Käytetty kyselylomake on liitteessä B. Kyselyn kohteeksi valittiin suomalaisia ammattikorkeakouluja, joissa on tietotekniikan opetusta tai muutoin tietoturvaan liittyviä kursseja. Alustava lista oppilaitoksista koostettiin tekniikan alan ammattikorkeakouluista ja näihin lisättiin kaikki ne ammattikorkeakoulut, joiden Internet-sivuilta löytyi viittauksia tietoturvan opettamiseen. Viittaukset etsittiin käyttäen Google-hakukonetta useilla eri termeillä. Oppilaitosten kokonaismääräksi muodostui näin 22 ammattikorkeakoulua.

Kysely pyrittiin lähettämään tietoturvakurssien opettajille. Mikäli opettajan yhteystiedot eivät selvinneet Internetin avulla (oppilaitoksen sivuilta tai Google-haulla), tiedustelu oikeasta henkilöstä lähetettiin oppilaitoksen neuvontaan tai alan yliopettajalle. Näillä menetelmillä oikea henkilö tavoitettiin 17 oppilaitoksesta. Viidestä oppilaitoksesta ei saatu mitään vastauksia sähköpostiin. Ainakin yhdessä tapauksessa kyse oli todennäköisesti siitä, että kurssista vastaava opettaja oli siirtynyt toiseen työpaikkaan.

Jäljelle jääneistä 17 oppilaitoksesta kolmen edustajat ilmaisivat halukkuutensa vastata, mutta eivät lopulta palauttaneet kyselylomaketta ajoissa. Kolmessa oppilaitoksessa ei kontaktihenkilön mukaan ollut tietoturvaopetusta ja yhden koulun edustaja kieltäytyi vastaamasta kyselyyn. Näin otokseksi jäi kymmenen ammattikorkeakoulua, joissa on tietoturvan opetusta. Kaikki vastaajat eivät vastanneet kaikkiin kvantitatiivisiin kysymyksiin, joten joissakin tutkimuksen tuloksissa (kysymykset 1.1, 1.2, 2.1) otos on yhdeksän vastausta.

3.2 Tietoturvaopetuksen kohdeyleisö

Tietoturvaopetusta löytyi ammattikorkeakouluista lähinnä tietotekniikan koulutusohjelmista. Joissakin kouluissa tietoturvakursseja löytyi myös hoitoalalta, sillä tietosuoja (yksityisyyden suoja) on oleellinen osa esimerkiksi terveydenhuollon tietojärjestelmiä, sekä kaupan ja hallinnon alalta. Suuntautumisvaihtoehdoista tietotekniikan tai tietojenkäsittelyn koulutusohjelmissa tietoturva kuului yli puolessa tapauksista tietoliikenteen alaan.

Tietoturvallisuuden opettajat haluaisivat kuitenkin tietoturvan osaksi kaikkien tietotekniikan opiskelijoiden opintoja. Vastaaajista seitsemän oli sitä mieltä, että tietoturvan perusteita tulisi opettaa kaikille. Syitä tähän olivat mm. se, että tietokoneiden ja tietoverkkojen käyttö edellyttää kaikilta niiden käyttäjiltä turvallisuuden perustuntemusta. Tietotekniikan alan sisältä ohjelmistotekniikka mainittiin kahdessa vastauksessa sellaisena alana, jossa tietoturvaopetusta tulisi lisätä.

3.3 Tietoturvakurssien koostumus

Tietoturvaopetuksen integrointia muihin kursseihin tutkittiin kysymällä suoraan opetettavien kurssien sisällöstä. Vastauksen antoi yhdeksän koulua, joista kolmessa tietoturvaopetus on eriytetty omiin kursseihinsa, kahdessa tietoturvaopetusta on ainoastaan muiden kurssien yhteydessä ja neljässä opetusta on sekä omina tietoturvakursseinaan että osana muiden kurssien opetussisältöä.

Niistä kuudesta koulusta, joilla opetusta oli ainakin jossakin määrin osana muita kursseja, viidellä tietoturvaopetus oli sisällytetty tietoliikenteen opetukseen. Muita integroivia kursseja olivat järjestelmäylläpitoon, kryptologiaan⁹ ja tietotekniikan perusteisiin liittyvät kurssit. Tulos ei liene mitenkään yllättävä: tietoturva on tullut ”joka kodin termiksi” nimenomaan verkottumisen seurauksena, joten tietoliikenteen yhteydessä on luontevaa puhua turvallisuudesta. Tietoturvaopetuksen kokonaisopintoviikkomäärät vaihtelevat alle yhden ja kahdeksan opintoviikon välillä keskiarvon ollessa noin kolme opintoviikkoa erillisille tietoturvakursseille. Muihin kursseihin integroidussa opetuksessa tietoturvan opetuksen osuus oli keskimäärin noin kaksi opintoviikkoa.

Tietoturvaopetuksen sisältö on esitetty taulukossa 1 (tekstin lopussa). Aiheiden suosituimmuusjärjestys tukee tulkintaa, jonka mukaan tietoliikenne on merkittävä tietoturvaopetuksen eteenpäin ajava voima. Yhdeksän suosituimman aiheen joukossa kolme aiheita liittyvät suoraan nimenomaan tietoliikenteen turvaamiseen. Muita suosittuja aiheita ovat sovellusten ja käyttöjärjestelmien tietoturva-asiat, joihin myös virukset kuuluvat (niin ikään kolme mainintaa suosituimpien yhdeksän aiheen joukossa). Tutkimusmenetelmästä johtuen pelkkiä mainintamääriä laskemalla ei kuitenkaan voida saada varmaa tietoa eri osa-alueiden suosituimmuudesta, sillä osa aiheista oli jaettu toisia hienosyisemmin. Suuntaa-antava tulos kuitenkin on.

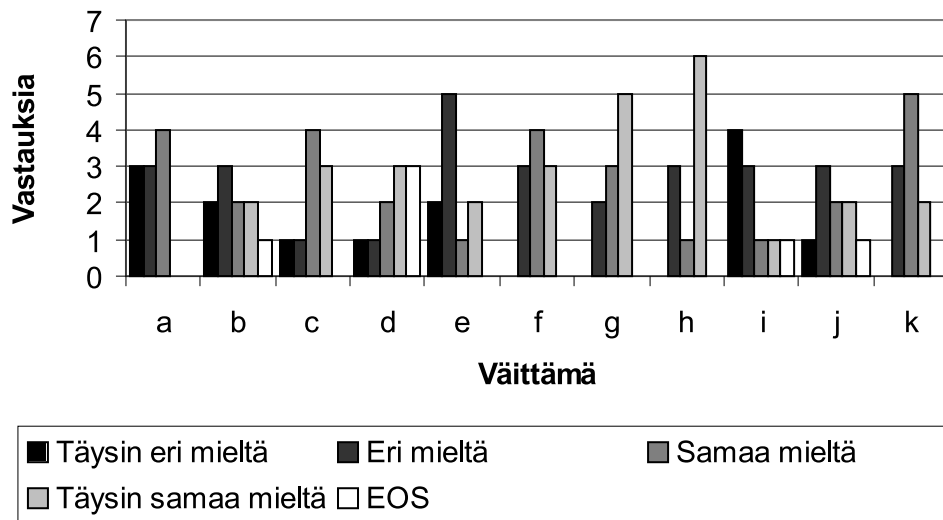
⁹Salaustiede.

Vastauksissa näkyy myös käytännönläheisyys: kryptografiaa käsitellään vain viidessä oppilaitoksessa ja niissäkin matemaattisiin periaatteisiin asti mennään vain yhdessä. Bell-LaPadula -mallin kaltaisia teoreettisia tietoturvamalleja ei käsitellä yhdessäkään vastanneessa koulussa.

Huomionarvoista on, että yhdessäkään vastauksessa tietoturva-asioita ei oltu otettu osaksi varsinaisia ohjelmointikursseja ja vain yhdessä koulussa ohjelmoinnin tietoturva otettiin yleensäkin esille.

3.4 Mielenpitoet sisällöstä

Vastaaajien mielestä tärkein tietoturvaan liittyvä opetuksen kohde on tietoverkkojen tietoturva. Toiseksi tärkeimpänä pidettiin tietoturvapoliittikoja ja tietoturvahallintoa. Nämä aiheet ovatkin edustettuna lähes kaikkien vastaaajien oppilaitoksissa. Useampia kuin kahden maininnan saivat virustorjunta, ohjelmistojen, käyttöjärjestelmien ja laitteiden tietoturva yleisesti, erilaisten teknisten suojausmenetelmien esittely (mukaanlukien kryptografiset menetelmät) ja tietoturvan uhkakartoitukset. Tietoturvapoliittikat, tietoturvahallinto ja uhkakartoitukset edustavat prosessilähtöistä ajattelua ja muut ehkä enemmän ratkaisukeskeistä ajattelua.



Kuva 1: Vastaukset väitelauseisiin

Opettajien arvomaailmaa tietoturvan suhteen tutkittiin myös muutamalla väitelauseella (ks. väitteet taulukossa 2 ja vastaukset kuvassa 1). Prosessilähtöisen tai ratkaisukeskeisen ajattelun vallitsevuutta tutkittiin väitteillä *a* ja *j*. Väitteseen *a* yli

puolet oli sitä mieltä, että tietoturvapoliitikkojen opetus ei ole vähemmän oleellista kuin teknisten menetelmien opetus ja väitteessä j vastaukset jakautuvat tasan. Tämä vahvistaa osaltaan aiemmin mainittua tulosta tärkeimmistä opetuksen aiheista.

Asennoitumista tietoturvaliseen ohjelmointiin tutkittiin väitteillä d ja i . Osittain ehkä yllättävästi vastaukset väitelauseisiin ovat hieman ristiriidassa toteutuneen opin-tosisällön kanssa, sillä kummassakin kysymyksessä enemmistö on sitä mieltä, että ohjelmoijat tarvitsevat tietoturvakoulutusta ja että ohjelmointivirheiden välttäminen on tärkeä viesti tietoturvakoulutuksessa. Kuitenkaan turvallinen ohjelmointi ei ole mukana nykyisessä tietoturvaopetuksessa, kuten aiemmin todettiin. Väittämäs-sä d oli suhteellisen paljon ”en osaa sanoa” -vastauksia, joka saattaa kieliä siitä, että ohjelmointivirheiden roolia tietoturvaongelmien alkusyynä ei ehkä aina tiedos-teta. Itse olen kuitenkin taipuvainen väittämään, että tämä on oleellinen osa-alue tietoturvassa (vrt. NIST 2003).

Väittämät b ja h mittasivat sitä, kuinka tarpeellista tietoturvallisuuden opetukses-sa on opettaa opiskelijoita ajattelemaan hyökkääjän tavoin. Vastausten perusteella käytännön harjoitukset järjestelmien suojauksesta ja murtautumisesta ovat tärkei-tä, mutta varsinaisesti hyökkääjän housuihin asettumista ei pidetä yksiselitteisesti hyvänä asiana. B -väitteen vastaus oli odotettu, sillä laboraatioita pidetään arvossa. Jälkimmäisen tuloksen tasaisuus on ainakin minulle itselleni yllättävä, koska hyök-kääjän ajattelumaailman tuntemista pidetään tärkeänä esimerkiksi riskianalyysime-netelmien käytössä (menetelmistä mm. Amoroso 1994, 17; Schneier 2000, 288-306, 318-333) ja c -väitteen mukaan tapahtuneiden turvaongelmien analysointia pide-tään tehokkaana menetelmänä. Tapahtuneiden ongelmien analysointihan kuitenkin on usein pitkälti kurkistamista hyökkääjien ajatteluun.

Teorian osuus tietoturvaopetuksessa on vastaajien mielestä tärkeää (enemmistö vas-tasi myöntävästi väitteeseen g) mutta mikäli opiskelija ei ole erikoistumassa tietoturva-alaan, teoriaa (mukaanlukien salausmenetelmien tuntemus) ei välttämättä tulisi opettaa (väite k). Enemmistön mielestä kryptografisten menetelmien toimintape-riaatteet eivät yleisestikään ole oleellisia (väite e). Turvaprotokollat, jotka tietenkin käyttävät kryptografisia algoritmeja, ovat kuitenkin enemmistön mielestä oleellisia opetuksessa (väite f). Tästä voitaneen päätellä, että ammattikorkeakouluissa teo-reettisen tietoturvan hyväksi nähty detaljitaso on jossakin protokollien toimintaperi-aatteiden ja algoritmien matematiikan välissä. Käytännön tietoturvatehtäviin tämä on mielestäni hyvä abstraktiotaso.

Opettajat arvioivat, että opiskelijoiden mielestä mielenkiintoisimmat aiheet poik-

keavat hieman tärkeimpinä pidetyistä sekä eniten opetetuista aiheista, joskin yhteneväisyyksiäkin löytyy. Eniten mainintoja (kolme kappaletta) saivat kryptografiset menetelmät eli salaustekniikat sekä virustorjunta. Seuraavaksi kiinnostavimpia olivat yleisesti tietoturvan tekniset toteutusmenetelmät (kaksi mainintaa), joista erityisesti mainittiin tietoturvakollat ja verkkojen suojaus palomuuerein. Tietoturvapolitiikkojen ja -prosessien opiskelua ei pidetty mielenkiintoisena yhdenkään vastauksen perusteella. Syyt tähän jäävät hämärän peittoon, koska tätä pitäisi todennäköisesti kysyä oppilailta itseltään. Voidaan kuitenkin arvailla, että kyse on siitä, että tekniikan opiskelijat ovat kiinnostuneita juuri tekniikasta ja että prosessiasioita pidetään jostakin syystä kuivina, byrokraattisina tai abstrakteina. Mahdollisesti tätä voitaisiin korjata sitomalla prosessiopetusta todellisiin projekteihin, jolloin prosessien käytännön merkitys ja sitominen jokapäiväiseen työhön kirkastuisi oppilaille.

3.5 Laboraatioiden tilanne

Kuten kirjallisuustutkimuksen perusteella oli odotettavissa, laboraatioita arvostetaan menetelmänä myös kyselyyn vastanneissa oppilaitoksissa. Luennot ja laboraatiot olivat käytetyimmät opetusmenetelmät (kahdeksan mainintaa). Laboraatiot määriteltiin kyselyssä ”valmiin tehtävänannon mukaan tehtävät, lähinnä ennustettavasti etenevät harjoitukset, usein koulun tiloissa”. Seuraavaksi suosituin opetusmenetelmä olivat harjoitustyöt (seitsemän mainintaa, määritelmänä ”valmiiseen tehtävänantoon perustuvat mutta oma-aloitteisesti etenevät työt, yleensä etätehtävinä”). Neljässä koulussa käytettiin projektitöitä (”itseohjautuvasti, mahdollisesti itse määriteltäviin tavoitteisiin tähtäävät harjoitustyöt, joskus ulkopuoliselle tilaajalle”) ja seminaareja tai tutkielmia. Kirjallisuuskuulusteluja tai -referaatteja teetettiin kolmessa koulussa. Kahdessa koulussa käytettiin laskuharjoituksia. Maininnan saivat myös opintokäynnit ja ohjelmointiharjoitukset. Lasku- ja ohjelmointiharjoitukset tosin saattavat sisältyä joissakin kouluissa laboraatioihin ja harjoitustöihin ja ne saattoivat tämän vuoksi jäädä erittelemättä. Kysymys tietokoneavusteisesta opetuksesta osoittautui hankalaksi, sillä tietotekniikan alalla miltei kaikki opetus tehdään jossakin määrin tietokoneella ja World Wide Webiä käytetään yleisesti.

Ylivoimaisesti suosituin laboraatioaihe (7 mainintaa) oli palomuurin pystytys. Muut tietoverkon turvallisuuteen liittyvät aiheet olivat myös suosittuja. Vastauksissa aiheet oli kuvattu vaihtelevalla tarkkuudella, joten tarkkaa suosituimmuusjärjestystä ei ole mahdollista tehdä. Karkealla luokittelulla voidaan kuitenkin havaita, että turvasovellukset (muun muassa turvasähköposti) olivat suosituimmuuslistalla seura-

valla tilalla ja kolmannen tilan jakoivat avaintenhallintainfrastruktuurit¹⁰, käyttöjärjestelmien turvallisuusominaisuudet sekä tietoturvapoliitikkojen luominen.

Tulos ei yllätä - palomuurihan on yksi tietoverkkojen turvallisuuden merkittävimmistä (reaktiivista) suojausmenetelmistä ja tietoverkkojen turvallisuushan oli kirjattu sekä suosituimmaksi että tärkeimmäksi tietoturvan opetuksen aiheeksi. Positiivista on mielestäni nähdä, että tietoturvapoliitikkojen tekeminen on myös laboraatioaihe. Viitaten aiempaan huomioon jonka mukaan prosesseihin liittyvät aiheet eivät ole opiskelijoiden suosiossa, näiden laboraatioiden kehittäminen saattaisi olla hyödyllistä.

Tietoverkkojen turvallisuutta opetetaan yleensä erillisessä laboratorioverkossa (suuren verkkolaittevalmistajan Cisco Academy-verkkoympäristö mainittiin kahteen otteeseen). Kuitenkaan neljässä vastanneessa koulussa ei ole erillistä ympäristöä tällaista harjoittelua varten. Kysyttäessä opettajilta, millainen olisi unelmatapa opettaa tietoturvaa, yhtä lukuunottamatta kaikki mainitsivat tietoturvalaboratorion. Laboratoriolta toivottiin suljettua laboratorioverkkoa joka koostuisi erilaisista koneista, reitittimistä ja palomuuereista ja jossa ei olisi muuta opetusta, jolloin verkossa voisi vapaasti käyttää muun muassa verkkoliikenteen tarkkailuun tarkoitettuja ohjelmia. Toinen suosittu toive oli yleensä erilaisten demonstraatioiden lisääminen. Tämä yhdistettiin edellämainittuun laboratorioympäristöön.

3.6 Tietoturvan opettamisen kehitysnäkymät

Kysyttäessä, mihin suuntaan tietoturvan opetuksen tulisi kehittyä sisällöllisesti ja opetusmenetelmällisesti, viisi asiaa mainittiin ainakin kahdessa vastauksessa. Nämä olivat

- tietoturvan opetusta pitäisi olla tarjolla jokaiselle edes jossain määrin, sillä tietoturva on tärkeää kaikilla tietotekniikkaan liittyvillä osa-alueilla
- tietoturvan opetuksen määrää tulisi lisätä. Tämä koskee niin yleistä tietoturvan opetusta kuin myös erityiskursseja, joita tulisi opettaa vain alaan erikoistuville
- ohjelmoijien pätevyyttä pitäisi kehittää tietoturvan parantamiseksi

¹⁰Avaintenhallinta (*key management*) on tärkeä osa salausjärjestelmiä. Termi kattaa mm. salaus- ja todennusavainten luotettavan välittämisen tarvitsijoille.

- ammattikorkeakouluissa tietoturvan opetuksen tulisi lähestyä ongelmakenttää käytännön kannalta perustuen todellisiin uhkakuviin
- tietoturvan opetuksen tulisi ottaa lähtökohdaksi kokonaisuuden ymmärtäminen, jossa tarkastellaan uhkia, politiikkoja ja tekniikkoja yhdessä

Jos vastauksia verrataan aiemmin esiteltyihin tietoturvan lähestymistapojen akseleihin, toiveet pyrkivät siirtämään painopistettä eriytyneistä kursseista integroivammaksi. Toisaalta kokonaisvaltaisuuden korostaminen lähestyy prosessilähtöistä ajattelutapaa ja uhkien ja politiikkojen arviointi proaktiivista lähestymistapaa. Ammattikorkeakoulujen tavoitteiden kannalta painopisteen on luonnollista olla käytännönläheinen, joten ”miksi” - ”miten” -akselilta pitäisi löytyä sopiva tasapaino, jossa teoreettinen tausta on tasapainossa ratkaisujen kanssa. Haasteeksi saattaa muodostua tietoverkkojen turvallisuusopetuksen määrän suhteuttaminen muihin turvallisuusopintoihin kuten juuri prosessien ja ohjelmointiturvallisuuden opetukseen.

4 Luotettavuustarkastelu

Tutkimuksen luotettavuuden kannalta yksi kysymys on, oliko otos riittävän suuri. Vastauksia saatiin kymmenen kappaletta, joka on todennäköisesti riittävä edustus tietoturvaan opettavista ammattikorkeakouluista, joita on suurella todennäköisyydellä korkeintaan noin parikymmentä - mahdollisesti vähemmän (ks. kappale tutkimuksen suorittamisesta).

Tulosten tulkinnassa ei käytetty mitään erityisiä tilastollisia menetelmiä, koska vastausten määrät ovat laskettavissa kahden käden sormilla. Tähän liittyy riski siitä, että yhdenkin vastaajan puutteellinen vastaus saattaa vaikuttaa esimerkiksi taulukon 1 järjestykseen huomattavasti. Sen vuoksi esimerkiksi sisällön suosituimmuusjärjestyksessä eri aiheiden välistä suosituimmuutta kannattaa todennäköisesti ajatella asteikolla ”suosittu” ja ”ei suosittu” jättäen kaiken hienosyisemmän järjestyksen tulkinnan tekemättä.

Samoin vaihtoehtojen valinta vaikuttaa järjestykseen: jotkin asiat oli listattu vaihtoehtojen listaan hienojakoisemmin kuin toiset, joka luo taulukossa 1 illuusion siitä, että jotakin aihealuetta käsiteltäisiin paljon enemmän kuin jotakin toista. Esimerkiksi verkkoturvallisuuteen liittyviä aiheita oli useampia kuin virustorjuntaan liittyviä aiheita. Tämän takia kysymyksen tulokset ovatkin enemmän laadullisia kuin määrällisiä, ja ne pitäisi tällaisena tulkita.

Avokysymysten osalta tutkimus olisi todennäköisesti ollut parempi järjestää kahdes-
sa osassa niin, että ensin olisi kysytty avokysymyksiä ja sen jälkeen erikseen esimer-
kiksi opetussisältöä valmiilla listalla. On nimittäin mahdollista, että antamani lista
opetussisällöistä vaikutti avokysymysten vastauksiin joko niin, että jokin opetussi-
sältö, jota listalla ei ollut, unohtui myös avokysymyksistä tai sitten listalla olleet
opetussisällöt dominoivat myös avokysymysten vastauksissa.

Väitelauseisiin oli rakennettu vastapareja, joiden tarkoitus oli tutkia vastausten kes-
kinäistä validiteettia. Väitteet eivät olleet toistensa täydellisiä vastakohtia, mutta
silti vaikuttaa siltä, että väitevastausten keskinäinen validiteetti on kunnossa. Nämä
väiteparit olivat $d - i$ sekä $j - a$. Jos vertaillaan vastaajien vastauksia näihin väittei-
siin yksittäisten vastaajien tasolla ja jätetään huomiotta ”en osaa sanoa” -vastaukset,
vastaukset ovat $d - i$ -parissa yhtä ja $j - a$ -parissa kahta vastaajaa lukuunottamatta
samansuuntaiset (eli konsistentisti samaa/eri mieltä).

Avokysymyksissä tulkinnan hankaluus ilmeni vastausten koodaus- ja luokitteluvai-
heessa, sillä eri vastaajat korostivat asioita luonnollisesti eri tarkkuudella. Tämän
vuoksi jouduin luomaan vastauksille yläluokkia, jotka tietenkin poistivat joitakin
nyansseja vastauksista. Mikäli tutkimusta tehdessä olisi ollut aikaa tehdä selven-
täviä lisäkysymyksiä, yksityiskohtaisempien vastausten kysely olisi saattanut antaa
enemmän tutkimustietoa. Valitettavasti tähän ei ollut kerta kaikkiaan aikaa, mikäli
vastausaikaa olisi pitänyt antaa realistiset pari viikkoa.

5 Pohdintaa

5.1 Laboraatioiden jatkotutkimusta

Laboraatioiden opetuksellinen merkitys olisi mielenkiintoinen tutkimuskohde, erityi-
sesti se, helpottaako laboraation suorittaminen todella esimerkiksi luennolla anne-
tun teoreettisen pohjan omaksumista ja millä tavoin tähän tavoitteeseen päästäisiin
tehokkaimmin. Saattaa olla, että seminaarityyppinen esitys voisi auttaa laboraatioi-
den teoreettisen taustan selvittämisessä.

Prosessinäkökulman tuominen laboraatioiksi voisi myös olla kiinnostava kehitys- ja
tutkimuskohde. Saataisiinko tällä aikaan enemmän kiinnostusta yritysten tietoturva-
prosesseihin? Voisivatko opiskelijat oppia oikean elämän tietoturvaratkaisuista vielä
laboratorioverkkoakin enemmän?

5.2 Tietoturvallisen ohjelmoinnin kriisi

Miksi ohjelmissa on niin paljon turvallisuusaukkoja? Onko ohjelmat todella suunniteltu niin huonosti? Jälkimmäiseen kysymykseen vastaus on yleensä kielteinen. Vääränlaiseen ohjelmistosuunnitteluun perustuvia tietoturva-aukkoja syntyy melko harvakseltaan ja usein ne ovat luonteeltaan akateemisia eivätkä ole välttämättä helposti hyödynnettävissä. Sen sijaan ohjelmointivirheisiin (ohjelman koodissa oleviin ongelmiin, jotka aiheuttavat määrittelyn ja suunnittelun vastaista toimintaa) perustuvia tietoturva-aukkoja on hyvin paljon. Vuonna 2001 ainakin 60 % raportoiduista tietoturva-aukoista johtui suoraan ohjelmointivirheistä (NIST 2003).

Ohjelmointivirheistä aiheutuvat kustannukset ovat merkittäviä jo pelkästään tietoturvallisuusosalalla. Lähes koko reaktiivisen tietoturvamallin olemassaolon oikeutus perustuu siihen, että ohjelmiin ei voi luottaa vaan niiden turva-aukkoja on tukittava erilaisilla paikoilla ja suojauksilla. Esimerkiksi verkkoliikenne on ohjattava suodat-tavan palomuurin läpi, koska riski siitä, että koneessa on rikkinäisiä ohjelmia on niin suuri.

Miksi tietoturvallista ohjelmointia ei sitten painoteta enemmän? Hyvä kysymys. Suurin osa tätäkin työtä varten kerätystä lähdemateriaalista ei ota varsinaisesti ohjelmoinnin turvallisuusseikkoihin kantaa lainkaan. Ohjelmointiturvallisuuskurssien sisältö saattaa olla esimerkiksi erilaisten turvapalvelujen käyttöä tai ”kryptografista varmennusta”¹¹ (Yang 2001). Kuitenkaan turvapalvelujen tai kryptografisten primitiivien käyttö ei muuta ohjelmaa automaattisesti turvalliseksi vaan ohjelmointivirheiden (kuten puskuriylikuorojen¹², joka on merkittävin yksittäinen turvallisuusongelma) välttäminen tai turvallisemman ohjelmointikielen käyttäminen.

Tällaisten virheiden välttämiseen tähtäävän ohjelmointityylin (*robust programming*) tai turvallisten ohjelmointikielten opetus olisi siis mielestäni erittäin oleellisessa osassa ohjelmoijien tietoturvaopetusta. Se on tilastojen valossa tärkeämpää kuin esimerkiksi kryptologian perusteiden hallitseminen. Muita turvallisen ohjelmoinnin periaatteita ovat modulaarisuus ja tiedon kätchentä sekä siirrettävyys (Bishop 1997). Nämä kolme osa-aluetta kuuluisivat parhaassa tilanteessa jokaisen ohjelmoijan koulutukseen.

¹¹Mitä se ikinä tarkoittaakaan tässä yhteydessä. Todennäköisesti todennusta.

¹²Tämä tarkoittaa yksinkertaistettuna tilannetta, jossa ohjelma varaa tallennettavalle tiedolle liian vähän tilaa ja tieto vuotaa yli varatusta tilasta. Tämän kaltainen virhe on myös helppo korjata ja niiden etsimiseen on olemassa automaattisia ja puoliautomaattisia testityökaluja.

Jatkotutkimuksen aiheeksi voisi siis sopia, miten turvallista ohjelmointia voisi tehokkaasti tuoda osaksi ohjelmointikursseja. Tämä vaatisi myös erityistä syventymistä ohjelmoinnin opetuksen didaktiikkaan.

5.3 Varoittavat esimerkit

Tietoturvaa edistetään usein pelolla. Krakkerit saattavat murtautua järjestelmääsi, virukset saattavat lähettää henkilökohtaisia dokumenttejasi ulkopuolisille, tietosi saattavat tuhoutua ja niin edelleen. Tyypillisimmillään tietoturvattomuuspelottelu on alan yritysten markkinointimateriaalissa. Kaikki vastaajat kertoivat, että oikeiden tietoturvaongelmien läpikäynti oli vähintään esimerkkitasolla mukana opetuksessa ja kuvan 1 tulosten perusteella enemmistö pitää varoittavia esimerkkejä myös tehokkaana opetusmenetelmänä. On selvä ero siinä, onko oikeiden ongelmien läpikäynnillä tarkoitus pelotella vai onko ongelmista tarkoitus ottaa oppia. Vastausten valossa näyttää siltä, että ammattikorkeakouluissa esimerkit toimivat sekä mielenkiinnon herättäjänä että ponnistuslautana ongelmien analysointiin.

Jos tapahtuneita ongelmia aletaan analysoida esimerkiksi laboraatiossa, on mahdollista, että oppilaita ”opetetaan hakkeroimaan”. Ulkopuolisen silmissä tämä saattaa vaikuttaa varsin arveluttavalta (esim. Lindskog ym. 1999). Kuitenkin monet tietoturvasuunnittelusta kertovat teokset painottavat, että avain hyvään tietoturvasuunnitteluun on pystyä ajattelemaan samoin kuin hyökkääjä. Tällöin uhka-analyysi ja riskikartoitus, jotka ohjaavat järjestelmän suunnittelua, sisältävät ne uhat ja riskit, joita hyökkääjäkin käyttäisi hyväkseen. Tässä vaiheessa tietotekniikan etiikka on tärkeä ottaa esille. Hyviä käsiteltäviä asioita voisivat olla myös esimerkiksi haavoittuvuuksien raportointikäytännöt - esimerkiksi onko nk. *full disclosure* -periaate hyväksyttävä. (Periaatteen mukaisesti löydetty turva-aukko saatetaan heti julkiseen tietoon, jotta paineet aukon korjaamiseksi nousisivat riittävästi.)

Varoittavien esimerkkien tehon ja hyödyntämismenetelmien tutkiminen voisi olla mahdollinen tulevaisuuden tutkimusalue. Samalla huomion kiinnittäminen tietotekniikan etiikan opetuksen merkitykseen olisi hyödyllistä.

Viitteet

ACM (1998). Software Engineering Code of Ethics and Professional Practice. <http://www.acm.org/serving/se/code.htm>. Viitattu 15.4.2003.

- Amoroso, E. (1994). *Fundamentals of Computer Security Technology*. New Jersey: Prentice Hall.
- Barnett, S. F. (1996). Computer Security Training and Education: A Needs Analysis. Teoksessa *1996 IEEE Symposium on Security and Privacy*, 26–27.
- Baskerville, R., & Straub, D. (1999). Internet Groupware Use in a Policy-Oriented Computer Security Course. Teoksessa *IFIP TC11 WG 11.8 First World Conference on Information Security Education*.
- Bintziou, A., Alexandris, N., & Chrissikopoulos, V. (1999). Introducing IT-Security Awareness in Schools: The Greek Case. Teoksessa *IFIP TC11 WG 11.8 First World Conference on Information Security Education*.
- Bishop, M. (1997). Computer Security in Introductory Programming Classes. Teoksessa *ACM Workshop on Education in Computer Security*.
- Bishop, M. (2000). Education in Information Security. *IEEE Concurrency*, 8(4), 4–8.
- Bishop, M. (2002). Computer Security Education: Training, Scholarship, and Research. *IEEE Computer*, 35(4), 30–32.
- Chin, S.-K., Irvine, C. E., & Frincke, D. (1997). An Information Security Education Initiative for Engineering and Computer Science. Tekninen raportti, Naval Postgraduate School, Monterey.
- Fillery-James, H. (1999). Teaching Computer Security. Teoksessa *IFIP TC11 WG 11.8 First World Conference on Information Security Education*.
- Irvine, C. E. (1999a). Amplifying Security Education in the Laboratory. Teoksessa *IFIP TC11 WG 11.8 First World Conference on Information Security Education*.
- Irvine, C. E. (1999b). The Reference Monitor Concept as a Unifying Principle in Computer Security Education. Teoksessa *IFIP TC11 WG 11.8 First World Conference on Information Security Education*.
- Irvine, C. E., Chin, S.-K., & Frincke, D. (1998). Integrating Security into the Curriculum. *IEEE Computer*, 31(12), 25–30.
- Irvine, C. E., Stemp, R., & Warren, D. F. (1997a). Teaching Introductory Computer Security at a Department of Defense University. Tekninen raportti, Naval Postgraduate School, Monterey.

- Irvine, C. E., Warren, D. F., & Clark, P. C. (1997b). The NPS CISR Graduate Program in INFOSEC: Six Years of Experience. Teoksessa *NIST 20th National Information Systems Security Conference*, 22–30.
- Lindskog, S., Lindqvist, U., & Jonsson, E. (1999). IT Security Research and Education in Synergy. Teoksessa *IFIP TC11 WG 11.8 First World Conference on Information Security Education*.
- NIST (2003). ICAT Metabase. <http://icat.nist.gov/>. Viitattu 15.4.2003.
- Opetushallitus (2003). DotSafe-hankkeen (<http://dotsafe.eun.org>) materiaalikansio.
- Schneier, B. (2000). *Secrets & Lies: Digital Security in a Networked World*. New York: Wiley Computer Publishing.
- Tietotekniikan liitto (2002). Tietotekniikan ammattilaisen eettinen ohjeisto. <http://www.tt-tori.fi/pls/ttl/docs/F148570701/Eettisetohjeet3.htm>. Viitattu 15.4.2003.
- White, G. B., Marti, W., & Hudson, M. L. (1999). Incorporating Security Issues Throughout the Computer Science Curriculum. Teoksessa *IFIP TC11 WG 11.8 First World Conference on Information Security Education*.
- Yang, T. A. (2001). Computer Security and Impact on Computer Science Education. *The journal of computing in small colleges*, 16(4), 233–246.
- Yasinsac, A. (2001). Information Security Curricula in Computer Science Departments: Theory and Practice. Teoksessa *5th National Colloquium for Information Systems Security Education*.

9	mainintaa	Turvallisuuspalveluita toteuttavat verkkoprotokollat teoreettisen toiminnan tasolla (esim. avaintenvaihtoprotokollien toimintaperiaatteet tms.)
9		Lähiverkkojen jne. suojaus muilla kuin turvallisuuspalveluita toteuttavilla protokollilla (esimerkiksi palomuurit)
9		Virus- ja vastaavat uhat ja/tai niiden torjunta
8		Julkisen avaimen järjestelmien sovellukset (PKI, varmenteet)
8		Sovellukset, joilla voidaan tarjota turvallisuuspalveluja (sovelluksen, ei protokollan tasolla; esim. turvasähköpostin käyttö)
8		Yritysten/yhteisöjen tietoturvapoliittikat
7		Turvallisuuspalveluita toteuttavat verkkoprotokollat ja laitteet käytännön tasolla (esim. virtuaalisen yksityisverkon (VPN) toteutus käytännössä tunnetuilla protokollilla ja tuotteilla)
7		Käyttöjärjestelmien turvallisuusominaisuudet ja tietoturvaohjelmat
7		Yksityisyyden suoja ja tietosuoja (lainsäädäntö ja politiikat)
6		Sovellusten turvallisuusominaisuudet ja tietoturvaohjelmat
6		Yritysten/yhteisöjen tietoturvahallinto ja tiedonvarmistus (information assurance)
5		Kryptografiset algoritmit ilman matemaattisten periaatteiden tarkastelua
5		Tekijänoikeusongelmat ja digitaalisten oikeuksien hallinta (<i>digital rights management</i>)
5		Sähköiset maksujärjestelmät ja verkkokaupankäynti
4		Yksityisyyden suoja ja tietosuoja (tekniset toteutukset)
3		Kryptografian, kryptologian tai kryptoanalyysin matemaattiset periaatteet (mm. lukuteoria, abstrakti algebra, informaatioteoria jne.)
3		Tietotekniikkarikollisuus (<i>”cybercrime”</i>) ja tietotekniikan käyttö rikollisten apuna
2		Informaationsodankäynti tai -terrorismi
1		Turvallinen ohjelmointi (korkean tason kielet)
1		Turvallisen ohjelmasuunnittelun menetöt (<i>security design patterns</i>)
1		Muu: Kryptografisten sovellusten ja ohjelmistojen kehitys
0		Tietoturvan yleinen, ei-kryptografinen teoria (esim. Bell-LaPadula- ja Biba-mallit)
0		Turvallinen laitesuunnittelu (myös sulautettujen järjestelmien matalan tason koodin ohjelmointi ja piirisuunnittelu)

Taulukko 1: Tietoturvan opetuksen sisältö vastausten perusteella

Taulukko 2: *

Arvotusta mittaavat väitelauseet

-
- | | |
|---|---|
| a | Lainsäädännön ja tietohallinnon politiikkojen opetus ei ole niin oleellista kuin teknisten suojausmenetelmien opetus. |
| b | Tietoturvan opetuksessa oppilas on hyvä opettaa ajattelemaan hyökkäjän tavoin. |
| c | Varoittavat esimerkit ovat tehokas opetusmenetelmä. |
| d | Ohjelmointivirheiden välttäminen on tärkeä viesti tietoturvaopetuksessa. |
| e | On tärkeää, että oppilaat ymmärtävät kryptografisten algoritmien toimintaperiaatteet. |
| f | Tietoturvan opetuksessa on korostettava turvaprotokollien osuutta. |
| g | Tietoturvan opetuksessa on ensin lähdettävä liikkeelle tietoturvan perusteoriasta. |
| h | Käytännön harjoitukset tietojärjestelmien suojauksesta ja niihin murtautumisesta ovat keskeisiä. |
| i | Ohjelmoija ei välttämättä tarvitse erityistä tietoturvakoulutusta, mikäli hän ei toteuta tietoturvakomponentteja. |
| j | Tietojärjestelmän turvallisuudessa politiikka ja käyttäjät ovat tärkeämpiä kuin tekniset toteutusmenetelmät. |
| k | Teoreettiset mallit ja salausmenetelmien tuntemus eivät ole oleellisia muille kuin tietoturva-alan asiantuntijoille. |
-

A Tietoturvakurssien sisältöjä

Tämä lista on koottu lähteistä Irvine ym. 1997b; Bintziou ym. 1999; Bishop 2000; Bishop 1997; Yang 2001; Yasinsac 2001; White ym. 1999 ja Irvine ym. 1998.

Tietoturvallisuuden perusteet	Tietoturvatietoisuus Tietotekniikan etiikka (<i>computer ethics</i>) Historiallinen perspektiivi Yksityisyyden suoja (<i>privacy, data protection</i>)
Tietoturvahallinto ja tietoturvaprosessit	Lainsäädäntö Fyysinen turvallisuus Henkilöstöturvallisuus Tietoturvapoliittikat henkilöstö- ja teknisellä tasolla Riskianalyysi Tietoturvasertifiointi ja auditointi
Tietoturvamallit ja mekanismit	Turvallisuustason mittaaminen Formaalit mallit suunnittelussa yleisesti Luottamuksellisuus- ja eheysmallit (Bell-LaPadula, Biba- ja Clark-Wilson-mallit (esim. Amoroso 1994) Pääsynvalvonta ja pääsylistat Kyvyt (<i>capabilities</i>)
Ohjelmoinnin turvallisuus	Laatumittarit (mm. <i>capability maturity model</i>) Turvalliset suunnitteluperiaatteet suunnittelussa (<i>security design patterns</i>) Turvallisuuspainotteinen testaus Modulaarisuus ja tiedon kätkentä Jykevätekoinen (<i>robust</i>) ohjelmointi Ohjelmien oikeaksi todistaminen
Kryptografia	Konfiguraationhallinta Salaus, todennus ja eheyden takaaminen (CIA-malli) Avaintenhallinta Kryptografiset protokollat Julkisten avainten infrastruktuurit (<i>public key infrastructure, PKI</i>) Matemaattiset periaatteet (mm. lukuteoria)

Hyökkäys ja puolustus	<p>Haavoittuvuus- ja uhkamallit</p> <p>Turvallisuuspolitiikkojen tekninen toteuttaminen</p> <p>Tunkeutumiskokeet</p> <p>”Kyberterrorismi”, informaationsodankäynti</p> <p>Tietokonerikollisuus, piratismi</p> <p>Tietokonerikosten tutkinta</p>
Käyttöjärjestelmä- ja ajoympäristöturvalli- suus	<p>Virukset, troijan hevoset ja madot</p> <p>Dynaamisen sisällön (mm. skriptit) aiheuttamat ongelmat</p> <p>Virtuaalikoneiden turvamallit (mm. Java-kielen turvamalli)</p>
Verkkoturvallisuus	<p>Käyttöjärjestelmien turvallisuusominaisuudet</p> <p>Turvalliset toimintatavat tietoverkoissa</p> <p>Turvalliset verkkoarkkitehtuurit</p> <p>Verkkoprotokollien haavoittuvuus erilaisia hyökkäyksiä vastaan</p> <p>Palomuurit, suodattimet (mm. sähköpostisuodattimet)</p> <p>Palvelunriistohyökkäykset (<i>denial of service</i>)</p> <p>Verkonvalvonta</p> <p>Kryptografiset protokollat</p>
Palvelinturvallisuus	<p>Protokollien oikeaksi todistaminen</p> <p>Tietokantojen turvallisuus (mm. päättely- ja yhdistelyhyökkäykset)</p> <p>Hajautettujen järjestelmien (mm. WWW) turvallisuus</p> <p>Konfiguraationhallinta</p> <p>Murtautumisen havaitsevat ohjelmat (mm. Tripwire)</p>

B Kyselykaavake

OSA 1: OPETUKSEN SISÄLTÖ

1.1 Tietoturvan opetus järjestetään ensisijaisesti

- [a] Omina tietoturvakursseinaan
- [b] Osana jotakin muita kursseja
-> Mitä kursseja (nimet tai myös pelkästään alat riittävät)?

1.2 Seuraavassa valitse ne osa-alueet, joita opetuksessa käsitellään enemmän kuin maininnan tasolla.

Mitä tietoturvan opetus kattaa oppilaitoksessanne?

- [a] Turvallisuuspalveluita toteuttavat verkkoprotokollat teoreettisen toiminnan tasolla (esim. avaintenvaihtoprotokollien toimintaperiaatteet tms.)
- [b] Turvallisuuspalveluita toteuttavat verkkoprotokollat ja laitteet käytännön tasolla (esim. VPN:n toteutus käytännössä tunnetuilla protokollilla ja tuotteilla)
- [c] Lähiverkkojen jne. suojaus muilla kuin turvallisuuspalveluita toteuttavilla protokollilla (esimerkiksi palomuurit)
- [d] Kryptografian, kryptologian tai kryptoanalyysin matemaattiset periaatteet (mm. lukuteoria, abstrakti algebra, informaatioteoria jne.)
- [e] Kryptografiset algoritmit ilman matemaattisten periaatteiden tarkastelua
- [f] Julkisen avaimen järjestelmien sovellukset (PKI, varmenteet)
- [g] Tietoturvan yleinen, ei-kryptografinen teoria (esim. Bell-LaPadula- ja Biba-mallit)
- [h] Käyttöjärjestelmien turvallisuusominaisuudet ja tietoturvauhat
- [i] Sovellusten turvallisuusominaisuudet ja tietoturvauhat
- [j] Sovellukset, joilla voidaan tarjota turvallisuuspalveluja (sovelluksen, ei protokollan tasolla; esim. turvasähköpostin käyttö)
- [k] Turvallinen ohjelmointi (korkean tason kielet)
- [l] Turvallinen laitesuunnittelu (myös sulautettujen järjestelmien matalan tason koodin ohjelmointi ja piirisuunnittelu)

- [m] Turvallisen ohjelmasuunnittelun metodit (security design patterns)
- [n] Virus- ja vastaavat uhat ja/tai niiden torjunta
- [o] Yritysten/yhteisöjen tietoturvapoliittikat
- [p] Yritysten/yhteisöjen tietoturvahallinto ja tiedonvarmistus
(information assurance)
- [q] Yksityisyyden suoja ja tietosuoja (tekniset toteutukset)
- [r] Yksityisyyden suoja ja tietosuoja (lainsäädäntö ja politiikat)
- [s] Tietotekniikkarikollisuus (cybercrime) ja tietotekniikan
käyttö rikollisten apuna
- [t] Informaationsodankäynti tai -terrorismi
- [u] Tekijänoikeusongelmat ja digitaalisten oikeuksien hallinta (DRM)
- [v] Sähköiset maksujärjestelmät ja verkkokaupankäynti
- [w] Muut osa-alueet
-> Mitkä osa-alueet?

1.3 Mitkä osa-alueet ovat kaikkein tärkeimpiä tietoturvan alalla jos oppilaat ovat ammattikorkeakoulun tietotekniikan opiskelijoita? (Osa-alueiden ei tarvitse olla em. listasta vaan omat määrittelyt kelpaavat hyvin.)

1.4 Mitkä osa-alueet tuntuvat oppilaista kaikkein kiinnostavimmilta?

1.5 Mille muille oppilasryhmille (opintosuunnille) tietoturvan perusteita olisi syytä opettaa ammattikorkeakoulussa?

====

OSA 2: OPETUSMENETELMÄT

2.1 Mitä seuraavista opetusmenetelmistä käytetään tietoturvakursseilla tai tietoturvaa sivuavilla kursseilla tietoturvan opetuksessa? (Menetelmien nimet voivat vaihdella; nämä määritelmät vastaavat omia kokemuksiani. Määritelmä on tärkeämpi kuin menetelmän nimi.)

- [a] Luennot
- [b] Laboraatiot (valmiin tehtävänannon mukaan tehtävät, lähinnä ennustettavasti etenevät harjoitukset, usein koulun tiloissa)

- [c] Harjoitustyöt (valmiiseen tehtävänantoon perustuvat, mutta oma-aloitteisesti etenevät työt, yleensä etätehtävinä)
- [d] Projektit (itseohjautuvasti, mahdollisesti itse määriteltyihin tavoitteisiin tähtäävät harjoitustyöt, joskus ulkopuoliselle tilaajalle)
- [e] Laskuharjoitukset ja ohjatut teoreettiset pienryhmätyöt
- [f] Kirjallisuuskuulustelut ja -referaatit
- [g] Seminaarit ja tutkielmat
- [h] Tietokoneavusteinen opetus
 - > Mitkä ohjelmat/oppimisympäristöt?
- [i] Muut menetelmät
 - > Mitkä menetelmät?

2.2 Mikäli käytätte laboraatioita, harjoitustöitä, ryhmitöitä, tutkielmia, seminaareja tai projekteja, millaisia tehtävänantoja oppilaille annetaan? (Esimerkit aidoista tehtävänannoista ovat erittäin tervetulleita.)

2.3 Käytetäänkö luennoilla tai pienryhmien ohjauksessa todellisia caseja, varoittavia esimerkkejä tai vastaavia? Minkälaisia?

2.4 Käytetäänkö tietoturvan opetuksessa simuloituja tai laboratorioympäristöjä, joissa harjoitellaan tai demonstroidaan tietoturvaongelmia? Jos, niin minkälaisia ympäristöjä?

2.5 Onko jokin opetusmenetelmä selvästi muita tehokkaampi? Jos resurssit eivät rajoittaisi opetusmenetelmien valintaa, millainen olisi "unelmaopetusmenetelmä" tietoturvan alalla?

====

OSA 3: LÄHESTYMISTAPAPAINOTUKSET JA SUUNNITELMAT

3.1 Arvioi seuraavat väittämät asteikolla 1 .. 4

(1 = täysin eri mieltä, 4 = täysin samaa mieltä).

Jos asia on täysin yhdentekevä tai siitä ei ole tietoa, merkitse "?".

Jos haluat kommentoida väittämää ja antamaasi numeroa, voit

tehdä niin väittämän jälkeen.

- [a] Lainsäädännön ja tietohallinnon politiikkojen opetus ei ole niin oleellista kuin teknisten suojausmenetelmien opetus.
- [b] Tietoturvan opetuksessa oppilas on hyvä opettaa ajattelemaan hyökkääjän tavoin.
- [c] Varoittavat esimerkit ovat tehokas opetusmenetelmä.
- [d] Ohjelmointivirheiden välttäminen on tärkeä viesti tietoturvaopetuksessa.
- [e] On tärkeää, että oppilaat ymmärtävät kryptografisten algoritmien toimintaperiaatteet.
- [f] Tietoturvan opetuksessa on korostettava turvaprotokollien osuutta.
- [g] Tietoturvan opetuksessa on ensin lähdettävä liikkeelle tietoturvan perusteoriasta.
- [h] Käytännön harjoitukset tietojärjestelmien suojauksesta ja niihin murtautumisesta ovat keskeisiä.
- [i] Ohjelmoija ei välttämättä tarvitse erityistä tietoturvakoulutusta, mikäli hän ei toteuta tietoturvakomponentteja.
- [j] Tietojärjestelmän turvallisuudessa politiikka ja käyttäjät ovat tärkeämpiä kuin tekniset toteutusmenetelmät.
- [k] Teoreettiset mallit ja salaussuojauksien tuntemus eivät ole oleellisia muille kuin tietoturva-alan asiantuntijoille.

3.2 Mihin suuntaan haluaisitte tietoturvan opetuksen siirtyvän (sekä sisällöllisesti että opetusmenetelmällisesti) suomalaisissa ammattikorkeakouluissa, korkeakouluissa ja yliopistoissa?

3.3 Onko teillä muita, yleisiä kommentteja joko tietoturvan alueesta tai tästä kyselystä?