Marko Helenius ja Juhani Paavilainen
(toim.)

Tietoturvallisuuden erityiskysymyksiä 2004

TIETOJENKÄSITTELYTIETEIDEN LAITOS
TAMPEREEN YLIOPISTO

B-2004-8

TAMPERE 2004

Sisällysluettelo

Johdanto

Tietojärjestelmät ovat yhä enemmän osana jokapäiväistä elämää. Tietoturvallisuudesta[1] on vastaavasti tullut kasvavasti merkittävä tekijä tietojärjestelmiä suunniteltaessa, rakennettaessa ja käytettäessä. Tietojärjestelmien avoimuus ja tietoturvasuunnittelun puute ovat osaltaan johtaneet tälle ajalle tyypillisiin tietoturvaongelmiin. Tietoturvaongelmien vuoksi tarvitaan tutkimusta ja opetusta. Tietoturvallisuutta käsittelevät syventävät opinnot ovat mielestämme tärkeä osa sekä tutkimusta että opetusta.

Tämä julkaisu sisältää Tampereen yliopiston tietojenkäsittelytieteen laitoksella keväällä 2004 pidetyn seminaarin tietoturvallisuuden erityiskysymyksiä seminaarityöt. Opiskelijat saivat seminaarin aikana ohjausta ja palautetta työstään. Seminaarin yhtenä tarkoituksena onkin valmentaa opiskelijoita opinnäytetyön tekemistä varten. Seminaarissa olivat vierailijaluennoijina toimitusjohtaja Pekka Sarvela Asapsoft Netsystems Oy:stä ja apulaisprofessori Cestmir Halbich Prahan maatalouskorkeakoulun informaatioteknologian laitokselta.

Opiskelijat saivat valita seminaarityön aiheen vapaasti, joten aiheet vaihtelevat paljon. Seminaaritöiden aiheet käsittelevät terveydenhuollon tietojärjestelmien tietoturvallisuutta, XML:n ohjelmakirjaston tietoturvaominaisuuksia, käyttäjän tunnistautumisen hallintaa, yrityskonsernin tietoturvallisuutta, tietoturvallisuutta peruskäyttäjän näkökulmasta, sosiaalista tietomurtautumista, roskapostia ja sen torjuntaa, TETRA-viranomaisverkon tietoturvallisuutta, vakoiluohjelmia ja RSA-salausalgoritmin faktorointiongelmaa. Opiskelijat pitivät seminaarin lopuksi noin 35 minuutin esityksen seminaarityöstään, minkä jälkeen yksi tai kaksi opiskelijaa opponoi seminaarityön. Arviomme on, että seminaaritöiden taso on pääsääntöisesti erinomainen. Myös pidetyt esitykset ja niistä syntynyt keskustelu on ollut kiitettävää. Opiskelijoiden osaaminen ja motivaatio ovat näkyneet seminaarissa.

Tampereella 4.6.2004

Marko Helenius ja Juhani Paavilainen

[1] Tietoturvallisuudella tarkoitetaan niitä hallinnollisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys sekä yksityisyyden suoja.

Johdanto terveydenhuollon tietojärjestelmien integrointiin tietoturvanäkökulmasta

Niila Mäkelä

Tämä artikkeli pyrkii tuomaan esille tietoturvaan liittyviä seikkoja, jotka tulee huomioida terveydenhuollon tietojärjestelmien integrointiprojekteissa. Artikkelin alkuun on liitetty keskeisimmät määritelmät selityksineen, jotta terveydenhuoltoon tai tietoturvaan perehtymätönkin lukija pystyisi seuraamaan artikkelia. Koska aihe on hyvin laaja ja sen yksityiskohtainen käsittely vaatisi paljon laajemman esityksen kuin yhden seminaarityön, tämä artikkeli toimii eräänlaisena johdantona aiheeseen. Tekstissä käydään lävitse terveydenhuollon tietojärjestelmien erityispiirteet, jotka vaikeuttavat järjestelmien integrointia. Tutkimalla viitteitä lukija voi perehtyä tarkemmin tarpeellisiksi katsomiinsa kohtiin.

Avainsanat ja -sanonnat: Terveydenhuollon tietojärjestelmät, integrointi, tietoturva, aluetietojärjestelmä.

Sisällys

1. Johdanto

Terveydenhuollon tietojärjestelmiä tullaan integroimaan tulevaisuudessa entistä enemmän. Tällaiseen kehitykseen painostavat: tarve käsitellä potilaan tietoja eri terveydenhuollon yksiköissä, kustannussäästöt, joihin tähdätään järjestelmien päällekkäisten osien karsimisella sekä suurten ikäluokkien siirtyminen eläkkeelle, jonka seurauksena terveyspalveluiden kysyntä oletettavasti kasvaa. Potilastietojen saatavuus eri yksiköissä mahdollistaa joustavat (/saumattomat) palveluketjut [STAKES], jotka edelleen tehostavat terveydenhuollon palveluiden nopeutta ja nostavat potilaiden saaman palvelun laatua.

Terveydenhuollon tietojärjestelmien integroiminen synnyttää kuitenkin joukon ongelmia. Tässä artikkelissa käydään lävitse tietoturvaan ja etenkin tietosuojaan liittyviä ongelmia. Artikkelin lyhyydestä ja ongelmakohtien määrästä johtuen ongelmiin ei paneuduta yksityiskohtaisesti. Ongelmakohdat pyritään kuitenkin näyttämään, jotta niihin voitaisiin sovelluskohtaisesti paneutua tarkemmin. Artikkeli voi toimia eräänlaisena oppaana siihen, miten tietoturvaongelmat esiintyvät integrointiprojekteissa.

1.1. Määritelmät

Artikkelissa käytetyistä määritelmistä keskeisimmät ovat lueteltuina Liitteessä I. Määritelmät ovat pääosin lainattu Stakesin terminologiasanastosta [STAKES], jotta määritelmät vastaisivat mahdollisimman pitkälle suomalaisessa terveydenhuollossa vakiintunutta sanastoa. Liitteen määritelmät on pyritty esittämään sellaisessa järjestyksessä, jotta asiaan perehtymätönkin lukija pystyisi sisäistämään ne mahdollisimman helposti.

2. Terveydenhuollon tietojärjestelmät

Tässä kappaleessa kerrotaan ensin hieman terveydenhuollon tietojärjestelmien taustoista. Tämän jälkeen siirrytään käsittelemään terveydenhuollon tietojärjestelmien tietoturvan kannalta oleellisia erityispiirteitä.

2.1. Tietojärjestelmien tausta terveydenhuollossa

Terveydenhuollon tietojärjestelmät ovat jakautuneet eri ryhmiin niiden käyttötarkoitusten ja järjestelmää käyttävän organisaation mukaan. Järjestelmät voidaankin karkeasti luokitella erikoissairaanhoidon, perusterveydenhuollon, työterveyshuollon ja yksityisen sektorin järjestelmiin. Tässä artikkelissa keskitytään lähinnä kahteen ensin mainittuun luokkaan.

Aiemmin terveydenhuollon (etenkin erikoissairaanhoidon) tietojärjestelmät rakennettiin usein räätälöimällä. Näitä vanhoja järjestelmiä kutsutaan nykyään perinnejärjestelmiksi. Useiden perinnejärjestelmien ongelmina ovat hankalat merkkipohjaiset käyttöliittymät sekä järjestelmien välisen yhteistyön puuttuminen. Etenkin perusterveydenhuollon ja erikoissairaanhoidon välinen tietoliikenne on ollut ongelmallista. [Tuuri, 2003] Näitä perinnejärjestelmiä on edelleen käytössä sekä erikoissairaanhoidossa (esim. Aho, Musti, Saimi ja Sapo) että perusterveydenhuollossa, joten paineita järjestelmien uudistamiseksi on olemassa.

Nykyiset järjestelmät ovat usein modulaarisesti koottuja kokonaisuuksia, jotka pyrkivät tarjoamaan käyttäjille paljon erilaisia palveluita. Esimerkkeinä tällaisista järjestelmistä mainittakoon Effica (erikoissairaanhoito) [Mäkelä, 2003] ja Pegasos (perusterveydenhuolto) [Vuorela, 2003]. *Potilaskertomukset* ovat edelleen suurelta osin paperilla, vaikka eräät järjestelmät tukevatkin ainakin osittain digitaaliseen muotoon siirtymistä (mm. Effica, Miranda, Musti Qkert). [Tuuri, 2003]

Terveydenhuollon tietojärjestelmien kehitys tulee jatkossakin parantamaan palveluiden laatua ja tehokkuutta. Potilaan tiedot ovat yhä helpommin käytettävissä sijainnista ja ajankohdasta riippumatta. Potilastiedot ovat luottamuksellista tietoa ja niiden käsittelystä säädetään Suomen laissa. Nämä seikat tulee huomioida myös tietoturvallisuuden kannalta järjestelmiä suunniteltaessa, käytettäessä ja ylläpidettäessä.

2.2. Terveydenhuollon tietojärjestelmien erityispiirteet

Terveydenhuollon tietojärjestelmiin liittyy tiettyjä erityispiirteitä, jotka pitkälti määräävät, millaisia järjestelmien tulee olla. Nämä erityispiirteet luonnollisesti vaikuttavat myös järjestelmän tietoturvavaatimuksiinkin. Seuraavaksi käydään lävitse tärkeimmät näistä erityispiirteistä.

2.2.1. Käyttäjät

Terveydenhuollon tietojärjestelmiä käyttävät pääasiassa terveydenhuollon ammattilaiset. Heidän lisäkseen järjestelmiä käyttävät tietotekniikan ammattilaiset kuten ylläpitäjät ja tulevaisuudessa ainakin osaa järjestelmistä myös potilaat.

Järjestelmäintegraatio rakennetaan usein kahden tai useamman eri organisaation järjestelmien välille. Organisaatiokulttuurit voivat olla hyvinkin erilaisia ja tästä voi seurata monenlaisia ongelmia. Integraation yhteydessä työntekijät tarvitsevat usein lisää koulutusta, jotta uusien toimintatapojen omaksuminen olisi mahdollisimman tehokasta. Koulutuksen avulla pyritään myös ehkäisemään *henkilöturvallisuuteen* liittyviä riskejä.

Terveydenhuollon ammattilaisilla on hyvin vaihtelevat tietotekniikkataidot. Tämä johtuu työntekijöiden erilaisista taustoista ja työtehtävistä. Työntekijöitä koulutetaan työn ohessa käyttämään työtehtävissä tarvittuja järjestelmiä. Tämä koulutus ei kuitenkaan aina ole niin laaja kuin sen tulisi olla. Etupäässä tämä johtunee terveydenhuollon kovista työpaineista ja jatkuvasta kiireestä. Kun koulutus kattaa ainoastaan järjestelmän kriittisten osien käytön, jää työntekijältä helposti oppimatta lisäominaisuuksien käyttö, jotka mahdollisesti tehostaisivat työskentelyä, parantaisivat potilaiden saaman hoidon laatua ja tukisivat tietoturvaa.

Terveydenhuollon organisaatioilla tulisi olla tietoturvasäännöstöt osana *hallinnollista turvallisuutta*. Näiden sääntöjen tulee olla linjassa organisaation tietoturvapolitiikan kanssa. Sääntöjen olemassaolo ei kuitenkaan yksin riitä, vaan työntekijöiden on tunnettava nämä säännöt ja noudatettava niitä. Sääntöjen tulee olla kirjoitettuna helposti omaksut-

tavaan muotoon. Vaikka sääntöjen tarkoitus on parantaa tietoturvallisuutta, ne eivät saa liikaa hankaloittaa tai rajoittaa työntekijöiden työskentelyä.

Koska järjestelmiä käyttävät hyvin erilaiset ihmiset, joiden tietotekniikkataidot vaihtelevat hyvin paljon, tulee järjestelmät tehdä mahdollisimman helppokäyttöisiksi. Järjestelmien tulee olla hyviä *käytettävyydeltään*, jotta seuraavat tietoturvaa tukevat seikat toteutuisivat:

- Järjestelmää käytettäisiin tietoturvaohjeiden mukaisesti. Nykyiset järjestelmät ovat osittain niin hankalakäyttöisiä, että käyttäjät laiminlyövät tietoisesti tietoturvasäännöt helpottaakseen työskentelyään. Esim. sairaaloissa yleinen toimintatapa hoitaa kirjautumiset järjestelmiin on sellainen, että ensimmäinen työntekijä kirjautuu tunnuksillaan järjestelmään ja myöhemmät käyttäjät jatkavat samaa istuntoa. Näin työntekijät säästävät ajan, joka kuluisi toistuviin ulos- ja sisäänkirjautumisiin.

- Käyttäjät tekisivät mahdollisimman vähän virheitä. Tämä on tärkeää tiedon eheyden säilyttämisen kannalta. Mikäli järjestelmä on sellainen, ettei käyttäjä voi helposti tarkistaa antamiaan syötteitä, tallentuu järjestelmään ajan myötä virheellistä tietoa kirjoitusvirheiden vuoksi. Tämä edelleen voi heikentää potilaan saaman hoidon laatua. Lisäksi Henkilötietolaki sallii vain virheettömän ja tarpeellisen tiedon käsittelyn. [Henkilötietolaki, 1999]

Muutoinkin henkilötietojen käsittelyn arviointi ja suunnittelu tulisi tehdä jo toimintaa ja tietojärjestelmää suunniteltaessa. Arviointi tulee toistaa silloin, kun järjestelmään tehdään muutoksia, jotka vaikuttavat henkilötietojen käsittelyyn. [Kleemola]

2.2.2. Potilastietojen luottamuksellisuus

Potilastiedot ovat luottamuksellista tietoa, eikä tietoja näin ollen saa katsella kuka tahansa. Tämän vuoksi järjestelmän käyttäjien toimia on valvottava ja rajoitettava. Tätä tarkoitusta palvelevat *pääsynvalvonta* ja *todennus*. Niiden avulla voidaan säädellä, ketkä pääsevät käsiksi järjestelmän tarjoamiin palveluihin ja tietoihin.

Pääsynvalvonta ja *todennus* ovat useissa järjestelmissä toteutettu käyttäjätunnusten ja salasanojen tai toimikorttien avulla. *Todennuksessa* voidaan myös hyödyntää PKI-tekniikoita (Public-Key Infrastructure, HST-kortit) tai biometristä tunnistusta. Nämä tekniikat ovat oikein toteutettuina tietoturvan kannalta parempia kuin salasanoihin perustuva tunnistaminen.

Käyttäjätunnusten mukaan työntekijöille on helppoa määritellä, millaiset oikeudet järjestelmän tarjoamiin palveluihin kukin työntekijä tarvitsee. Tämä ei kuitenkaan yksistään riitä integroidussa ympäristössä. Potilastietojen siirtäminen kahden eri rekisterinpitäjän järjestelmän välillä tulkitaan tietojen luovutukseksi. Tietojen luovuttamiseen tarvitaan potilaan antama *suostumus*.

Suostumusten pyytämiseen asiakkailta ei ehkä vielä ole vakiintunut kaikkein tehokkainta mahdollista rutiinia. Nykyisin potilaalta pyydetään suostumus usein paperille allekirjoitettuna. Tämä käytäntö tulee kuitenkin mahdollisesti muuttumaan tulevaisuudessa elektronisten HST-korttien myötä. Suostumuksiin liittyy toinenkin ongelma: Kenelle suostumus tarkalleen ottaen myönnetään? Suostumuksen saajan rooli saattaa muuttua kesken potilaan *palveluketjun*. Samoin palveluketjuun saattaa liittyä myöhemmin lisää hoitohenkilökuntaa.

Potilastietojen käsittelyä on valvottava. Tähän tarkoitukseen käytetään lokitiedostoja, joihin tallennetaan tieto siitä, kuka on katsellut mitäkin tietoa. Koska käyttäjä on *todentautunut* järjestelmään, täyttyy lokitiedostojen myötä myös *kiistämättömyysperiaatteen* vaatimukset. Käyttäjä ei näin ollen voi myöhemmin kieltää katselleensa järjestelmästä tietoja ilman suostumusta. Terveydenhuollon järjestelmät täytyy kuitenkin rakentaa niin, että tietojen katseleminen on mahdollista ilman potilaan myöntämää suostumusta, sillä mikäli potilas on tajuton, häntä tietysti autetaan kaikkia mahdollisia keinoja käyttäen, vaikkei potilas olisi erikseen ehtinyt antaa suostumustaan.

2.2.3. Järjestelmiin tallennettavan tiedon arkistointi

Terveydenhuollon tietojärjestelmiin tallennetaan paljon tietoa, sillä potilaita ja käyttäjiä on paljon. Lisäksi etenkin elektroniseen muotoon tallennetut kuvat vievät paljon tallennustilaa. Näistä syistä myös siirrettävää dataa on paljon. Integrointeja tehtäessä on syytä varmistaa jo suunnitteluvaiheessa, että suunniteltu ja jo olemassa oleva tietotekniikkalaitteisto vastaavat järjestelmän vaatimuksia. Järjestelmän kaikki mahdolliset pullonkaulat on käytävä lävitse, jotta ikäviltä yllätyksiltä säästyttäisiin. Tällaisia pullonkauloja voivat olla esim. järjestelmän tukemat rajalliset käyttäjämäärät tai riittämättömät tietoliikenneyhteydet.

Potilastietojen tallentamisessa on huomioitava tietojen pitkä säilytysaika. Osaa potilastiedoista säilytetään 100 vuotta potilaan syntymästä asti ja osaa jopa pysyvästi. Tämä luo haasteita tiedon arkistoinnille. Tieto tulee olla jatkuvasti tallennettuna sellaiselle medialle, että sen palauttaminen luettavaan muotoon on mahdollista. [Ensio ja Ruotsalainen, 2003] Mainitun ehdon täyttäminen tulee olemaan haaste *tietoaineistoturvallisuuden* kannalta. Lisäksi suuri osa potilastiedoista on luonteeltaan sellaisia, ettei niitä saa muuttaa. Muutokset on tehtävä lisäämällä tietoa muuttamatta edellisiä merkintöjä. Näin potilaan oikeusturva on parempi hoitovirheen sattuessa.

Tietojen arkistoinnissa tulee huomioida myös *fyysinen turvallisuus*, eli tallennuslaitteiden on sijaittava fyysisesti suojaisessa paikassa, jossa esim. tulipalo ei pääse tuhoamaan tietoja. Järjestelmiä integroitaessa tallennuslaitteiden säilytystilojen erillään pitäminen on fyysisen turvallisuuden kannalta hyvä asia. Mahdollisen vahingon sattuessa ainakaan kaikkia tietoja ei menetetä, vaikka yhden yksikön tallennuslaitteet tuhoutuisivatkin. Tietojen menettämisen riskiä pyritään pienentämän myös kopioimalla tiedot varmistustallenteeksi.

2.2.4. Lainsäädäntö

Suomen lainsäädäntö säätelee monella tavalla terveydenhuollon tietojenkäsittelyä. Tässä artikkelissa ei kuitenkaan juurikaan käsitellä lakien vaikutuksia, sillä tämä artikkeli on julkaistu kokoelmassa, jossa on toinen, aiheeseen perehtynyt artikkeli. Tämä ei kuiten-

kaan tarkoita, että lainsäädäntöä tulisi väheksyä, vaan jo integraatioita suunniteltaessa on oltava hyvin perillä lainsäädännön asettamista rajoista.

2.2.5. Palvelun taukoamattomuus

Terveydenhuollossa on erityisen tärkeää, että potilaille pystytään antamaan mahdollisimman hyvää palvelua jatkuvasti. Tietojärjestelmien kannalta tämä tarkoittaa sitä, että tietojärjestelmän on oltava toimintavalmiudessa jatkuvasti. Järjestelmästä on aina saatava ulos potilaan hoidonkannalta kriittiset tiedot. Tämä vaatimus edelleyttää usein sitä, että rakennetaan erilaisia varajärjestelmiä, jotka paikkaavat varsinaisen järjestelmän osia häiriötilanteissa.

3. Terveydenhuollon järjestelmien integrointi

3.1. Tausta

Aiemmin terveydenhuollon tietojärjestelmiä yhdistettiin toisiinsa etupäässä sovittimilla, jotka mahdollistivat kahden järjestelmän välisen kommunikaation. Mikäli kahden järjestelmän muodostamaan verkkoon haluttiin liittää uusi järjestelmä, pahimmassa tapauksessa vanhoihin järjestelmiin piti kehittää sovittimet ja uuteen järjestelmään kaksi. Tällainen räätälöinti on aikaavievää ja kallista. Järjestelmien integroimista on hankaloittanut lisäksi se, että järjestelmien tukemat rajapinnat ovat olleet hyvin vaihtelevia. Lisäksi vaikka erilaisia standardeja on pyritty tukemaan, integrointiprojektit ovat olleet työläitä. Tämä on osittain ollut seurausta siitä, että järjestelmien toiminnot ja käsitteet sekä organisaatioiden toimintatavat ovat olleet erilaisia. Näistä syistä tietojärjestelmien välisen yhteistyön rakentaminen on ollut hankalaa etenkin alueellisella tasolla. [Tuuri, 2003]

3.2. Tavoitteet

Eräs tavoitteista, joihin pyritään järjestelmien integroinnilla, on sähköinen potilaskertomus. Järjestelmä mahdollistaisi potilaan tietojen katselemisen suoraan eri organisaatioissa ja näin ollen nopeuttaisi tiedonsaantia. Sähköisen potilaskertomuksen toteuttaminen vaatii sitä, että potilaan tiedot saadaan kerättyä nopeasti eri järjestelmistä aina tarvittaessa.

Suomessa on viimeaikoina integraation avulla rakennettu aluetietojärjestelmiä, joita käsitellään tämän artikkelin luvussa 3.3.

Järjestelmien integroinnilla pyritään myös siihen, ettei kaikkia palveluita tarvitsisi tuottaa joka yksikössä. Esim. HUS PACS (Helsingin ja Uudenmaan sairaanhoitopiirin Picture and Archiving and Communications System) mahdollistaa kuvantamispalveluiden tehokkaan keskittämisen. Potilaasta otetut kuvat voidaan tutkia yhdessä yksikössä, vaikka kuvat olisivatkin otettu muualla.

3.3. Aluetietojärjestelmät

Suomalaisissa terveydenhuollon tietojärjestelmien integrointia koskevissa kirjoituksissa viitataan usein termiin *aluetietojärjestelmä*. Tällä termillä tarkoitetaan tietyn alueen terveydenhuollon tietojärjestelmien muodostamaa kokonaisuutta. Aluetietojärjestelmän tarkoituksena on [STM, 2003]:

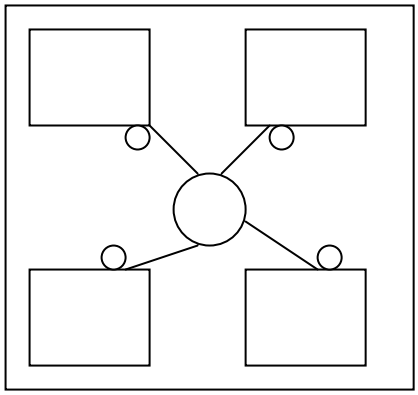
- Luoda selkeä kokonaiskuva potilaan hoitotilanteesta yli organisaatiorajojen.
- Kokonaisuuksien hallinta ja asiakkaan hoidon suunnittelun parantaminen.
- Mahdollistaa alueellinen turvallinen tiedonvälitys.
- Yhdenmukaistaa tapa, jolla tieto esitetään.

3.3.1. Tausta

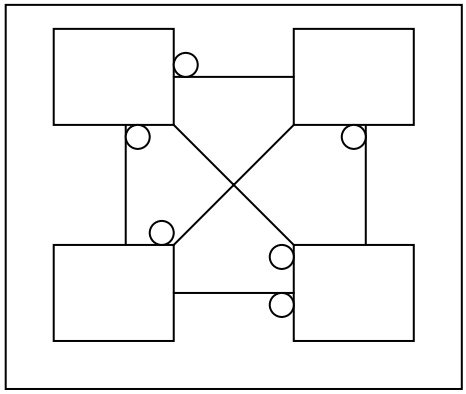
Aluetietojärjestelmiä on pilotoitu Suomessa toistaiseksi Helsingin ja Uudenmaan, Pirkanmaan ja Satakunnan hoitopiireissä. Aluetietojärjestelmien avulla käyttäjä pääsee käsiksi eri organisaatioiden perus/perinnejärjestelmiin tallennettuihin potilastietoihin asiakkaan luvalla. Tietoja ei kopioida järjestelmästä toiseen, vaan tieto luetaan viitteen avulla järjestelmästä, johon tieto on tallennettuna. Viitteet ovat tallennettuina viitetietokantaan, johon eri järjestelmät ovat yhteydessä standardienmukaisten sovittimien avulla. [Tuuri, 2003]

Tällaisen ratkaisun yksi suurimmista eduista on se, ettei järjestelmään tarvitse rakentaa lukematonta määrää kahden järjestelmän välisiä liittymiä, vaan yksi sovitin riittää jokaista liitettävää tietojärjestelmää kohti. Näin kokonaisuudesta tulee helpommin ylläpidettävä. Ennen aluetietojärjestelmämallia jokaisen kommunikoivan järjestelmän välille tarvittiin erillinen sovitin. Kuvassa 1 on esitettynä sädemallinen aluetietojärjestelmä, jonka

keskellä on viitetietokanta. Sovittimia (kuvissa pienet ympyrät) tarvitaan yksi jokaista integroitavaa järjestelmää kohden. Kuvassa 2 on neljä tietojärjestelmää, jotka on integroitu yhteen yksittäisinä projekteina ilman yhteistä suunnitelmaa. Sovittimia on tarvittu jo kuusi kappaletta. Uuden järjestelmän integrointi Kuvan 1 tapaukseen vaatisi yhden uuden sovittimen, Kuvan 2 tapauksessa neljä uutta sovitinta. [Tuuri, 2003]



Kuva 1



Kuva 2

Aluetietojärjestelmän toimiminen vaatii panostamista yhteistyöhön kaikilta osallistuvilta organisaatioilta. Tietoturvanäkökulmasta katsottuna tämä tarkoittaa yhteisten tietoturvaperiaatteiden sopimista. [Tuuri, 2003]

Järjestelmä tarjoaa käyttäjille mahdollisuuden käyttää joustavasti asiakkaiden potilastietoja riippumatta siitä, missä potilasta on aiemmin hoidettu. Samalla tehostuu yksiköidenvälinen yhteistyö ja asiakkaalle tehtävien turhien tutkimusten määrä vähenee. Asiakas hyötyy vuorostaan palvelun nopeutumisesta ja laadun paranemisesta. Kuten jo aiemmin mainittiin, kansalaisten käyttöön tulevien infopalveluiden määrä tulee todennäköisesti lisääntymään ja aluetietojärjestelmäarkkitehtuuria voitaneen hyödyntää näitä palveluja rakennettaessa. [Tuuri, 2003]

3.3.2. Tekninen toteutus

Aluetietojärjestelmä on mahdollista toteuttaa monella eri tavalla. Edellä mainittu viitetietojärjestelmään perustuva ratkaisu on eräs näistä mahdollisuuksista. Käytettyjen tietotekniikkakomponenttien tulee olla tietoturvaa tukevia valitusta toteutustavasta riippumatta. Laitteistovalintoja tehtäessä on syytä tutkia tarjolla olevia vaihtoehtoja *laitteisto-, ohjel-*

misto- ja tietoliikenneturvallisuuden kannalta. Esitetyssä viitetietojärjestelmäpohjaisessa ratkaisussa on kyse tähtiverkosta. Täten viitetietojärjestelmästä tulee kriittinen komponentti – sen mahdolliset toimintahäiriöt voivat estää kaiken tietoliikenteen verkon eri osien välillä. Kriittisten komponenttien varmistukset ovat tärkeä osa taukoamattoman palvelun tuottamista. Tämän vuoksi viitetietojärjestelmälle tulisi rakentaa varajärjestelmä, jota voidaan käyttää ongelmatilanteissa.

Yleisesti käytettyjä *laitteistoturvallisuustason* suojauksia ovat mm. palomuurit, joilla suojataan sisäverkot. *Tietoliikenneturvallisuus* pyritään usein varmistamaan erilaisin salausmenetelmin (esim. SSL) ja käyttämällä suojattuja yhteyksiä (esim. VPN).

3.3.3. Koodisto- ja sanastopalvelimet

Terveydenhuollon organisaatioissa on käytössä useita toisistaan eroavia koodistoja ja sanastoja. Eräs tunnetuimmista näistä koodistoista lienee ICD-10 tautiluokitus. Koodistot vaihtelevat käyttötarkoituksensa lisäksi myös levinneisyydeltään. Jotkin koodistot ovat kansainvälisesti hyväksyttyjä, osa vain paikallisesti käytettyjä. [Tuuri, 2003]

Koodistojen erot ovat merkittävä syy siihen, miksi tiedot tallennetaan järjestelmiin erimuotoisina. Integraatioita tehdessä nämä käsitteiden väliset erot täytyy huomioida, jotta tiedon *eheys* pystytään säilyttämään. Eräs mahdollinen ratkaisu tähän ongelmaan ovat kansalliset koodisto- ja sanastopalvelimet, jotka toimivat tulkkeina integroitavien järjestelmien välillä. Toimivat kansalliset koodisto- ja sanastopalvelimet helpottaisivat *sovittimien* toteuttamista.

4. Yhteenveto

Terveydenhuollon järjestelmäintegraatiot saattavat näyttää paperilla yksinkertaisilta, mutta käytännössä ne ovat vain harvoin sellaisia. Terveydenhuollon erityispiirteistä (kts. 2.2.) seuraa joukko tietoturvaongelmia, jotka pitää pystyä ratkaisemaan järjestelmäintegraatiota suunniteltaessa. Osa mainituista ongelmista on yhteisiä muiden alojen tietoturvaongelmien kanssa (esim. tietojen luottamuksellisuus B2B-ympäristössä). Kuitenkin on syytä huomata terveydenhuollon järjestelmissä korostuvat tiukat vaatimukset: järjestelmän on

toimittava lähes taukoamatta ja arkistoitavien tietojen suuri määrä sekä tietojen pitkät säilytysajat. Prosessiteollisuudessakin on erittäin tärkeätä, ettei prosessi katkea missään vaiheessa (esim. paperitehtaassa). Tällaisessa tehtaassa prosessin katkeaminen ei kuitenkaan useimmiten aiheuta kenellekään kuolemanvaaraa. Sairaalassa toimimaton tietojärjestelmä voi merkitä potilaan tilan heikkenemistä tai jopa kuolemaa.

Kuten edellä on tullut näytettyä, terveydenhuollon tietojärjestelmien integrointiin liittyy useita tietoturvaan liittyviä ongelmia. Näiden ongelmien voittaminen on eräs keskeisimmistä haasteista matkalla laadukkaisiin terveydenhuollon tietojärjestelmiin.

4.1. Jatkotutkimusaiheita

Alla on esitetty joitakin aiheeseen liittyviä jatkotutkimusaiheita, joita olisi ehkä vielä syytä tutkia Suomessa.

- Suostumusten käsittely. Miten suostumus tallennetaan järjestelmään? Miten asiakkaalta pyydetään suostumus?

- Järjestelmissä käytettävien termien yhdenmukaistaminen

- Aluetietojärjestelmien välinen yhteistyö?

- Tietoturva terveydenhuollon tietojärjestelmissä riskienhallinnan näkökulmasta

Lähteet

[Bemmel and Musen, 1997] van Bemmel J.H. and Musen M.A.(ed.), *Handbook of Medical Informatics*, Bohn Stafleu Van Loghum, 1997.

[Ensio ja Ruotsalainen, 2003] Ensio Antero ja Ruotsalainen Pekka, *Sähköinen asiakas- ja potilasasiakirjojen säilytyksen ja kiistämättymyyden hyvä käytäntö*, OSKE, 2003. http://www.oskenet.fi/uploads/qnmu9.pdf (25.4.2004)

[Henkilötietolaki, 1999] *Henkilötietolaki* 523/1999.

[Mäkelä, 2003] Mäkelä Niila, Effica – Erikoissairaanhoidon tietojärjestelmä. Teoksessa Nykänen Pirkko (toim.), *Terveydenhuollon tietojärjestelmät*, Tampereen yliopisto tietojenkäsittelytieteiden laitos, raportti B-2003-7, 2003.

[Kleemola] Kleemola Maija, Tietosuoja tietotekniikan käytössä. Teoksessa Saranto Kaija & Karpela Mikko (toim.), *Tietotekniikka ja tiedonhallinta sosiaali- ja terveydenhuollossa*, WSOY, 1999.

[STM, 2003] Sosiaali- ja terveysterveysministeriön muistioita 2003:18, Saumattoman palveluketjun ja sitä tukevien tietohallintaratkaisujen ohjausryhmä. Suosituksia. http://www.lskl.fi/tiedostot/folder_11/84722HdC.pdf (6.4.2004)

[STAKES], http://www.stakes.fi/oske/terminologia/sanastot/kasite.htm (6.4.2004)

[Tuuri, 2003] Tuuri Tiia, *Aluetietojärjestelmän avulla toteutettu järjestelmäintegraatio sosiaali- ja terveydenhuollossa*, Tampereen Teknillinen Yliopisto, 2003.

[Valtiohallinnon tietoturvallisuuden johtoryhmä, 2001] Valtiohallinnon tietoturvallisuuden johtoryhmä, *Valtiohallinnan lähiverkkojen tietoturvallisuussuositus*, 2001. www.vm.fi/tiedostot/pdf/fi/3378.pdf (6.5.2004)

[Vuorela, 2003] Vuorela Suvi, Perusterveydenhuollon tietojärjestelmä esimerkkinä Pegasos. Teoksessa Nykänen Pirkko (toim.), *Terveydenhuollon tietojärjestelmät*, Tampereen yliopisto tietojenkäsittelytieteiden laitos, raportti B-2003-7, 2003.

Liite I

Terveydenhuoltoon ja tietotekniikkaan liittyviä määritelmiä

- *Erikoissairaanhoito:* lääketieteen ja hammaslääketieteen erikoisaloilla tehtävä sairaanhoito.

- *Perusterveydenhuolto:* terveyskeskuksissa annettavat palvelut.

- ”*Potilaskertomus* on asiakaskertomus, joka sisältää tietoa potilaan sairauksista ja niiden hoidoista. Potilaskertomus voi sisältää erikseen sekä sairauskertomuksen että hoitokertomuksen.” [STAKES]

- *Joustava / saumaton palveluketju:* ”palveluketju, jossa asiakas ja/tai häntä koskeva tieto siirtyvät joustavasti palveluprosessista ja organisaatiosta toiseen” [STAKES]

- *Suostumus:* potilaan myöntämä yksilöity ja allekirjoitettu suostumus luovuttaa tai käyttää potilaan tietoja tiettyyn tarkoitukseen.

- *Aluetietojärjestelmä:* tietyn alueen (esim. sairaanhoitopiirin) sisäinen tietojärjestelmä, joka mahdollistaa organisaatioiden välisen yhteistyön.

- *Sovitin* ~ adapteri (eng. adapter): kahden järjestelmä välille rakennettava ohjelmisto, joka muuntaa järjestelmienvälisen tiedonsiirron sellaiseen muotoon, että vastaanottava järjestelmä ymmärtää saamansa datan.

- *Viitetietokanta:* tietokanta, johon tallennetaan potilastietojen osoitteet. Potilastiedot voidaan välittää järjestelmästä toiseen viitetietokannan avulla.

Tietoturvaan liittyviä määritelmiä

Tietoturvan pääkäsitteet [STAKES]:

Tietoturvalla tarkoitetaan niiden keinojen muodostamaa kokonaisuutta, joilla pyritään minimoimaan tietoriskejä.

Tietoriski on sellaisen tietoihin tai niiden käsittelyyn kohdistuvan tapahtuman uhka, joka toteutuessaan aiheuttaa haittaa.

Tietosuoja on tietoturvan osa-alue, jolla pyritään estämään tietojen luvaton käsittely. Terveydenhuollon tietojärjestelmien kannalta hyvin olennainen henkilörekisterilaki rajaa tietosuojan koskemaan vain henkilötietoja.

Tietoturvallisuudella viitataan taas tilaan, jossa tietoriskit ovat pienimmillään. Tulee kuitenkin huomata, että tietoriskien täydellinen eliminointi on mahdotonta.

Tietoturvallisuus vaikuttaa osaltaan merkittävästi terveydenhuollon tietojenkäsittelyssä seuraavien ominaisuuksien toteutumiseen [Bemmel and Musen, 1997]:

- Yksityisyyden säilyttäminen (privacy)

- Käsitellyn datan ja käytettyjen ohjelmien laadukkuus (quality of medical data and software)

- Tiedon ja palveluiden saatavuus (availability of data and functions).

Edellisien ominaisuuksien toteutumista voidaan mitata arvioimalla seuraavia tietoturvaperiaatteita:

- *Luottamuksellisuus* (confidentiality): Tiedot ovat ainoastaan niihin oikeutettujen käytössä.

- *Eheys* (integrity): Tieto säilyy muuttumattomana sitä käsiteltäessä ja siirrettäessä. Eheyden varmistamisen tehtävänä on taata, ettei tieto ole muuttunut tai kadonnut tahattoman tai luvattoman toimenpiteen seurauksena. Tahaton tiedon muuttuminen voi tapahtua esim. ohjelmisto- tai tiedonsiirtovirheen yhteydessä.

- *Saatavuus* (availability): Tietojärjestelmän palvelut ja tiedot ovat niihin oikeutettujen käytettävissä aina tarvittaessa.

- *Todennus* (authentication): Järjestelmässä toimivat osapuolet todentavat itsensä. Täten varmistuu se, että osapuolet ovat sitä, mitä väittävät olevansa.

- *Kiistämättömyys* (non-repudiation): Kiistämättömyys takaa sen, ettei kukaan johonkin tiettyyn tapahtumaan osallistunut voi kieltää myöhemmin osallistumistaan.

- *Pääsynvalvonta* (access control): Järjestelmään kirjautumisia valvotaan ja rajoitetaan.

Eri käyttöliittymien helppokäyttöisyyttä arvioidaan mittaamalla k*äytettävyyttä.* Laitetta, jonka käytettävyys on hyvä, on ilo käyttää ja sen käytön opettelu on vaivatonta. Kohdassa 2.2.1 käsitellään käytettävyyttä tietoturvanäkökulmasta.

Tietoturva voidaan jakaa myös erillisiin osa-alueisiin. [Valtiohallinnon tietoturvallisuuden johtoryhmä, 2001]

- *Hallinnollinen turvallisuus:* Organisaation tietoturvapolitiikan kehittäminen, ohjeistaminen ja dokumentointi.

- *Henkilöturvallisuus:* Osaaminen ja toimenkuva, koulutus, ohjeistus,

työntekijöiden valinta.

- *Fyysinen turvallisuus:* Kulunvalvonta, laitteiden suojaaminen ja varajärjestelmät.

- *Tietoliikenneturvallisuus:* Eheys, käytettävyys ja luottamuksellisuus tietoliikennenäkökulmasta. Tietoverkkojen ylläpito.

- *Laitteistoturvallisuus:* Laitteiden (mm. palvelinten) ylläpito.

- *Ohjelmistoturvallisuus:* Palvelinten ja työasemien ohjelmistojen ylläpito.

- *Tietoaineistoturvallisuus:* Tietojen turvaluokitukset, salaaminen ja arkistointi.

- *Käyttöturvallisuus:* Käyttöoikeudet ja verkon valvonta.

Terveydenhuollon potilastietoihin kohdistuvia uhkatekijöitä

Marko Napari

Terveydenhuollon potilastiedot sisältävät sensitiivistä tietoa henkilöiden identiteetistä ja elämästä. Terveydenhuollon prosessien digitalisoituminen altistaa elektroniset potilastiedot uusille uhille. Artikkelissa esitellään esimerkeillä millaisia ongelmia voi toteutua jos terveydenhuollon henkilörekistereiden tietoturva ei ole riittävällä tasolla.

Avainsanat ja -sanonnat: terveydenhuolto, elektroniset potilastiedot, henkilörekisterit, riskit ja uhat .

Sisällys

1. Johdanto

Terveydenhuollon prosesseja muutetaan siten, että potilastiedot olisivat digitaalisessa muodossa. Digitaalisuus antaa paljon mahdollisuuksia mutta siitä syntyy myös uhkia. Tässä työssä kartoitetaan millaisia tietoturvaan liittyviä uhkatilanteita voi syntyä terveydenhuollossa tapahtuneesta digitaalisesta kehityksestä. Tarkoituksena on tuoda esille havainnollisten esimerkkien kautta millaisia tilanteita vastaan terveydenhuollon tietoturvasta vastuussa olevat henkilöt joutuvat toimimaan ja miksi tämä työ on erityisen merkittävää.

2. Keskeiset käsitteet

Tässä kappaleessa käydään läpi tämän artikkelin keskeiset käsitteet.

2.1 Uhka

Uhka on tietoihin tai tietojärjestelmiin tietyltä taholta kohdistuvan vahingon tai häiriön mahdollisuus(Valtionhallinnon tietoturvakäsitteistö 2003). Uhkat voivat olla tahallisia tai tahattomia mutta ne voivat vahingoittaa järjestelmää tai tiedon luottamuksellisuus, eheys tai saatavuus voi kärsiä huomattavasti.

2.2 Haavoittuvuus

Haavoittuvuus on alttius tietoturvaa uhkaaville tekijöille(Valtionhallinnon tietoturvakäsitteistö 2003). Haavoittuvuuksia ovat heikkoudet tietojärjestelmissä, tietoturvakäytännöissä ja –proseduureissa, hallinnollisissa kontrolleissa, sisäisissä kontrolleissa, implementaatiossa tai fyysisessä toteutuksessa jos kyseisiä heikkouksia voidaan väärinkäyttää luvattomalla pääsyllä käsiksi tietoon tai työskentelyn estämiseen (Alberts et al. 2003).

Haavoittuvuudet voidaan luokitella kolmeen luokkaan (Howard 1998):

1. suunnitteluhaavoittuvuus – ohjelmistossa tai laitteistossa oleva suunnitteluvirhe, jonka vuoksi täydellisessäkin järjestelmän implementaatiossa olisi silti haavoittuvuus.
2. implementaatiohaavoittuvuus – ohjelmiston tai laitteiston implementaatiossa tapahtuneesta virheestä johtuva haavoittuvuus.
3. konfigurointihaavoittuvuus – haavoittuvuus, joka johtuu järjestelmän komponentin virheellisestä konfiguroinnista tai hallinnoinnista.

2.3 Henkilörekisteri

Henkilöstörekisterillä tarkoitetaan määrättyä käyttötarkoitusta varten laadittua henkilöstötietoja sisältävää tietojoukkoa, josta tiettyä henkilöä koskevat tiedot voidaan löytää (Tähtinen 1997).

2.4 Potilasasiakirja

Potilasasiakirjoilla tarkoitetaan potilaan hoidon järjestämisessä ja toteuttamisessa käytettäviä, laadittuja tai saatuja asiakirjoja, jotka sisältävät terveydentilaa koskevia tai muita henkilökohtaisia tietoja. Potilasasiakirjoja ovat potilasta koskevien hoito- ja tutkimustietojen lisäksi muun muassa laboratorio- ja röntgenlähetteet, tulokset ja lausunnot, erilaiset potilaspäiväkirjat, luettelot ja kortistot, atk-tallenteet sekä ääni-, filmi- ja videotallenteet. Potilasasiakirjojen tulee olla sellaisia, että ne ovat potilaan neuvonnan ja hoidon sekä näiden jatkuvuuden kannalta tarkoituksenmukaisia. (Tähtinen 1997)

3. Lainsäädäntö

Terveydenhuollon hallinnossa ja toiminnassa tarvittavien henkilörekistereiden käsittelyihin vaikuttavat useat säädökset, mm. terveydenhuollon erityislainsäädäntö, julkisuuslainsäädäntö, arkistolainsäädäntö ja tietosuojalainsäädäntö sekä lukuisat salassapitoa koskevat säännökset.

Tietosuojalainsäädäntö sisältää tietotojen turvaamisen kaikki osa-alueet kuten tietojen suojaamisen sekä luottamuksellisuuden, eheyden, saatavuuden ja käyttökelpoisuuden turvaaminen.

4. Terveydenhuollon henkilörekistereitä

Tässä kappaleessa esitellään terveyden huollon. Lisäksi tässä kappaleessa kuvataan lyhyesti millaista tietoa kyseiset rekisterit sisältävät. Terveydenhuollon henkilörekistereitä, jotka sisältävät asiakasta koskevia tietoja ovat muun muassa(Tähtinen 1997):

asiakasrekisteri

Terveydenhuollon toimintayksikön asiakasrekistereitä syntyy muun muassa tutkimuksen ja hoidon sekä siihen liittyvän palvelujen järjestämisen esimerkiksi ajanvarauksen ja voimavarojen varauksen yhteydessä. Potilasrekistereihin voidaan tallettaa ainoastaan asiakkaan hoidon ja tutkimuksen kannalta tarpeelliset tiedot.

tartuntatautirekisteri

Sairaanhoitopiirin tartuntataudin hoidosta vastaavan lääkärin tulee ylläpitää tartuntatauti-ilmoitusten tietojen perusteella alueellista tartuntatautirekisteriä.

terveydenhuollon seulontarekisterit

Kunnan järjestämien seulontojen ja joukkotarkastusten tietojen perusteella syntyneet henkilörekisterit, joita terveyskeskukset ylläpitävät.

työterveydenhuollon rekisterit

Työterveyshuoltolain mukaisten palvelujen järjestämiseksi ja toteuttamiseksi laadittuja tai saatuja asiakirjoja taikka teknisiä tallenteita, jotka sisältävät asiakkaan terveydentilaa koskevia tai muita henkilökohtaisia tietoja. Työterveydenhuollon potilasasiakirjoja ovat potilasta koskevien hoito- tai tutkimustietojen lisäksi muun muassa hoidonvarausrekisterit, laboratorio- ja röntgenlähetteet, tulokset ja lausunnot, erilaiset potilaspäiväkirjat, luettelot ja kortistot, atk-tallenteet sekä ääni-, filmi-, ja videotallenteet.

toiminnan suunnittelun, seurannan ja tilastoinnin rekisterit

Organisaation ja sen toimintayksiköiden oman toiminnan suunnittelu-, seuranta- ja tilastotarkoituksiin käytettävät rekisterit, jos niissä yksittäinen asiakas on tunnistettavissa.

ostopalvelutoiminnan rekisterit

Rekistereitä käytetään asiakkaalta perittävistä maksuista sekä asiakkaalle järjestettävistä, ulkopuolisista palveluista toimintayksikölle aiheutuvien menojen ja tulojen seurantaan, kustannusten kohdistamiseen sekä laskutuksen muodostamiseen ja valvontaan.

tutkimuksen rekisterit

Erikoissairaanhoidon omaan alaansa liittyvän yksilöidyn ja tutkimussuunnitelmaan perustuvan tieteellisen tutkimustoiminnan järjestämiseksi tarvittavat henkilörekisterit.

muut henkilörekisterit

Henkilökunnan työsuhteiden, henkilöstöhallinnon ja palkanmaksun tehtävien hoitamiseksi tarvittavat henkilöstörekisterit.

terveydenhuollon lakisääteiset valtakunnalliset henkilöstörekisterit

Valtakunnallisella asetuksella määritetyt tilasto- ja keskusrekisterit, jotka sisältävät henkilön terveydentilaa, sairautta, vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia koskevia tietoja.

STAKES:n ylläpitämät rekisterit ovat

- hoitoilmoitusrekisteri
- syntyneiden lasten rekisteri
- raskaudenkeskeyttämis- ja steriloimisrekisteri
- syöpärekisteri, jonka osana kohdunkaulasyövän ja rintasyövän seulontarekisterit
- epämuodostumarekisteri
- näkövammarekisteri

Lääkelaitosten ylläpitämät rekisterit ovat

- lääkkeiden sivuvaikutusrekisteri
- implanttirekisteri
- huumausaineseurantarekisteri

Muita valtakunnallisia rekisteitä ovat

- tartuntatautirekisteri(Kansanterveyslaitos)
- kuolemansyyrekisteri(Tilastokeskus)
- työtapaturmarekisteri(Tilastokeskus)
- työperäisten sairauksien rekisteri (Työterveyslaitos)

muut terveydenhuollon erillisrekisterit

Edellä mainittujen lisäksi on olemassa joukko valtakunnallisia, alueellisia ja paikallisia kliinisiä erillisrekistereitä. Paikallisia rekistereitä ovat: astman, diabeteksen, epilepsian laitteiden ja toimenpiteiden tietoja. Valtakunnallisia erillisrekistereitä ovat HYKS:n ja SPR:n Veripalvelun ylläpitämät erillisrekisterit.(FinOHTA 1997)

Potilastiedot kertovat siis meistä tavallisia asioita kuten pituuden, painon, verenpaineen sekä tietoja haavoista tai luunmurtumista. Samoista rekistereistä kuitenkin löytyy myös huomattavasti sensitiivisempää tietoja, joista paljastuu keitä ja millaisia me oikein olemme. Näitä tietoja ovat tiedot lisääntymiskyvystä ja raskaudenkeskeytyksistä, henkisistä ongelmista ja psykiatrisesta hoidosta, seksuaalisesta käyttäytymisestä, su-

kupuolitaudeista, HIV-statuksesta, huumausaineidenkäytöstä, fyysistä pahoinpitelystä ja periytyvistä taudeista jne.

5. Tietoturvavaatimukset ja seuraamukset

Tietoturvavaatimukset määrittelevät miten tietoa tulee suojata. Seuraavaksi käydään läpi tyypillisiä vaatimuksia asiakirjoille.

5.1 Asiakirjojen säilyminen

Asiakirjojen säilymiseen ja olemassaoloon liittyy niiden fyysinen säilyminen, käytettävyys, eheys, luotettavuus ja aitous. Käytettävyys tarkoittaa sitä, että tietojen on säilyttävä ymmärrettävinä huolimatta erilaisista konversioista, dokumentointitavoista ja ohjelmistoista. Asiakirjojen integriteetti eli eheys tulee säilyä niin tiedon tuottajan ns. perus- eli aktiivikäytön ohjelmistossa kuin sähköisessä arkistossa. Luotettavuus merkitsee, että tietojen on oltava oikeita. Arkisto itsessään ei voi tietää tietojen oikeellisuutta, joten tätä tehtävää ei voi jättää sen vastuulle. Aitous merkitsee, että tietoja ei ole asiattomasti muutettu. Aitous on dokumenttien arkistoon siirron jälkeen arkiston vastuulla. (Ensio ja Ruotsalainen 2003).

5.2 Tietojen aitous

Potilastiedot on turvattava, jotta asiattomat eivät pääse lukemaan tai muuttamaan tietoja. Tietojen muuttumisesta epäaidoiksi voi seurata samat seuraamukset kuin väärästä diagnoosista. Raatikaisen (2002) mukaan väärä tulos voi vahingoittaa potilasta. Positiivisen testin perusteella varhain aloitettu tutkimus ja hoito voi aiheuttaa enemmän ongelmia kuin hyödyttää potilasta. Terveenä itseään pitäneen henkilön psyykkinen leimaantuminen sairaaksi voi johtaa sen mukaisiin käyttäytymiseen. Väärä negatiivinen tulos testissä luo vääränlaista turvallisuuden tunnetta, koska henkilö kuitenkin myöhemmin sairastuu. Väärä positiivinen tulos taas on erityisen vaarallinen, jos sairaudella on painavat sosiaaliset seuraamukset (kuten syöpä tai HIV-infektio) tai jos positiivinen tulos johtaa välittömiin kielteisiin toimenpiteisiin asiakkaan kannalta.

5.3 Turvavaatimukset ja seuraamukset

Alberts et al.(2003) luokittelevat tyypillisimpien organisaation tietoresurssien tietoturvavaatimusten olevan:

- luottamuksellisuus – yksityisen, sensitiivisen tai henkilökohtainen tiedon näkeminen on estetty niiltä, joilla ei ole oikeuksia siihen
- eheys – tiedon autenttisuus, tarkkuus ja täydellisyys
- saatavuus – koska tai kuinka usein tiedon on oltava saatavilla tai valmiina käytettäväksi

Kun kyseisiä tiedon tietoturvan vaatimuksia on rikottu niin Alberts et al. (2003) luokittelevat viisi mahdollista seurausta:

- luottamuksellisuuden rikkoutuminen(*disclosure*) – henkilö, jolla ei ole siihen oikeuksia, näkee luottamuksellisen tiedon
- muuttuminen (*modification*)– luvaton tiedon muuttaminen
- tuhoutuminen (*destruction*)– tiedon olemassaolon tuhoutuminen; tietoa ei voida palauttaa
- menetys (*loss*)– tieto ei ole saatavilla; tieto on olemassa mutta se ei ole käytettävissä
- keskeytyminen (*interruption*)– tiedon saatavuuden rajoittaminen; keskeytyminen viittaa useimmiten palveluihin

Taulukossa 1. on esitetty tietoturvavaatimusten miten tietoturvavaatimukset ja niiden rikkoutuminen ovat yhteydessä toisiinsa.

Turvavaatimusten ja seuraamusten suhteet	
Turvavaatimus	**Seuraamus**
luottamuksellisuus	• luottamuksellisuuden rikkoutuminen
eheys	• muuttuminen
saatavuus	• tuhoutuminen • menetys • keskeytyminen

Taulukko 1. Turvavaatimusten ja niiden laiminlyönnistä aiheutuvat seuraamukset tiedolle

6. Tietoturvan pettämisestä seuraavia uhkia

Tässä kohdassa esitellään lyhyesti mistä suunnista tietoturvaongelmat voivat tulla. Uhat:

- Fyysiset ongelmat: Sähkökatkokset voivat aiheuttaa menetyksiä. Samoin vesivuodot, tulipalot, myrskyt ja muut vastaavat ilmiöt.
- Hakkerit: Hakkerit ovat henkilöitä, jotka tunkeutuvat laittomasti tietojärjestelmään. Uhkana on, että he varastavat, muuttavat tai tuhoavat järjestelmässä olevaa tietoa.
- Tyytymättömät työntekijät: Suurimmalla todennäköisyydellä tietokone sabotaasin tekijät ovat joko organisaation nykyisiä tai entisiä työntekijöitä. Sabotaasiksi luetaan laitteiston ja ohjelmiston tuhoaminen, ehdollisten pommien(logic bomb) asentaminen, jotka tuhoaisivat ohjelmia tai dataa. Muita sabotaasin muotoja ovat: tiedon syöttö väärin, järjestelmien kaataminen, tiedon poistaminen ja tiedon muuttaminen. Tämän vuoksi käyttäjätunnukset ja salasanat tulisi poistaa välittömästi kun työntekijä eroaa tai on irtisanottu.
- Varkaus: pöytäkoneet tai kannettavat tietokoneet voivat sisältää luottamuksellista tietoa, joten laitteen katoaminen voi vaarantaa tietoturvallisuuden. Tämän vuoksi on tehtävä toimia, joilla estetään vieraitten käyttäjien pääsy tietoon.
- Huolimattomuusvirheet: Loppukäyttäjät, tiedonsyöttäjät, järjestelmän valvojat ja ohjelmoijat saattavat tehdä tahattomia virheitä, joista saattaa seurata tietojärjestelmin haavoittuvuutta tai tiedon eheyden vaarantumista.
- Selailu: Käyttäjät, joilla on täydet oikeudet käyttää järjestelmää, saattavat joskus tarkastaa tietoja, joita heidän ei työn puolesta tarvitsisi, jotta saisivat tyydytettyä uteliaisuutensa. Esimerkiksi HIV-testien tulokset.

6.1 Virukset ja hakkerointi

Keskeiset turvallisuusuhkatekijät tietojärjestelmissä ovat virusohjelmien ja hakkeroinnin aiheuttamat häiriöt. Suuryrityksillä on käytössään IT-osaston jatkuvasti ylläpitämät palomuuri- ja virustorjuntaohjelmistot. Sen sijaan etenkin pienten yritysten tietojärjestelmien systemaattinen suojaus on usein yrittäjän oman aktiivisuuden ja osaamisen varassa. Julkisen sektorin organisaatioilla on käytössään viruksentorjuntaohjelmistoja, mutta useinkaan koko tietojärjestelmän systemaattiseen suojaamiseen ei ole resursseja(Ahoniemi 2003).

Sähköpostin kautta tulleet virukset voivat lähettää tietojärjestelmän sisältöä muihin sähköpostiosoitteisiin. Tällöin pahimmassa tapauksessa salassa pidettäviksi luokiteltua tietoa voisi pääty rikollisiin käsiin. Toisaalta virusohjelma tai hakkerointi voisi lamauttaa tietojärjestelmän toiminnan ja potilastietojen siirtäminen verkon välityksellä voisi olla mahdotonta.

Eräs hakkeri pääsi käsiksi Pennsylvanialaisen Drexel University College of Medicinen tietokantaan, joka sisälsi 5500 neurokirurgian tiedot. Kyseinen henkilörekisteri sisälsi potilaiden nimet, puhelinnumerot, kotiosoitteet ja tarkat tiedot sekä taudeista että hoitomenetelmistä. Järjestelmän haavoittuvuus johtui järjestelmän konfiguraatiosta, jossa sekä käyttäjätunnus että salasana pystyivät olemaan identtiset. (Null, 2003)

6.2 Tyytymättömät työntekijät

Vaikka virukset ja hakkerointi ovat merkittäviä uhkia tietoturvalle niin useimmiten suurin tietoturvauhka löytyy organisaation sisäpuolelta eikä ulkopuolelta. Organisaatioiden oma henkilöstö voi olla kiinnostunut tietojärjestelmässä olevasta tiedosta, joka ei olisi heidän käyttöoikeuksien piirissä.

6.3 Sabotaasi

Hajautetuilla palvelunestohyökkäyksissä(distributed denial of service – DDOS) rikolliset pyrkivät estämään kohdepalvelimen toiminnan kuormittamalla sitä turhilla pyynnöillä. Tämä voisi periaatteessa lamauttaa osan terveydenhuollon tietoverkosta jos internettiin kytketty palvelin on merkittävässä osassa terveydenhuollon omassa verkossa. Tällöin tiedonkulku vaikeutuisi merkittävästi ja tietoa kaipaavat eivät saisi hakemaansa.

Sabotaasin uhka voi olla myös organisaation sisällä. Joku voi päästää haitallista koodia sisältävän ohjelman tietojärjestelmään, joka vaikeuttaisi tietojärjestelmän toimintaa. Potilasta koskevien tietojen puutteellisuus saattaisi johtaa vääränlaisiin hoitotoimenpiteisiin akuuteissa tapauksissa.

6.4 Identiteetin varastaminen

Jos potilastietojen tietoturva pettää niin silloin ulkopuolinen taho voi saada selville potilastiedoista kaikki tärkeät henkilötiedot. Tämän jälkeen pahantekijä voi mahdollisesti esiintyä ja toimia rikollisesti potilaan identiteettiä käyttäen.

Jackson Memorial Hospitalin sairaalavirkailija Floridan Miamissa varasti kuudentoista Theresa-nimisen potilaan henkilötunnukset sairaalasta ja antoi ne Theresa nimiselle ystävälleen, joka avasi 200 pankki- ja luottokorttitiliä ja osti 6 henkilöautoa (Sherman 2002).

6.5 Kiristys

Rikollisen tahon pääsy potilastietoihin voi johtaa kiristykseen. Rikollinen taho voi saada selville, että potilas kärsii tai on kärsinyt jostain vaivasta, jota hän ei haluaisi julkisuuteen tietoon esimerkiksi taudin arkaluonteisuuden takia. Paljastusuhkaukset tehoavat erityisesti henkilöihin, jotka kokevat mediakuvan tai läheistensä mielikuvan tärkeäksi. Tällöin erityisesti julkisuuden henkilöiden tai päättäjien tai muiden merkittävässä asemassa olevien henkilöiden potilastiedot olisivat rikollisten tavoittelemia(Rothfelder 1992).

Terveydenhuollon tiloista varastetun tietokoneen seurauksena oli, että kaksi naista sai kiristyskirjeitä, joissa uhattiin paljastaa naisten käymät abortit (Anderson 1996).

6.6 Reseptien väärentäminen

Potilasasiakirjojen muuttaminen saattaisi kiinnostaa huumausrikoksista kiinnostuneita. Viime aikoina on harkittu siirtymistä internetin välityksellä toimitettaviin lääkereseptteihin. Lääkärien määrittämien reseptilääkkeiden määrien suurentaminen voisi olla kiinnostavaa erityisesti psyykelääkkeiden väärinkäyttäjille. Tällaisissa tapauksissa apteekissa tulisi olla mahdollisuus autentikoida resepti, jotta voitaisiin varmistaa, että resepti on aito ja että sitä ei ole missään vaiheessa muutettu laittomasti.

6.7 Potilastietojen kaupallinen käyttö

Tähän mennessä on rekisteröity useita tapauksia väärinkäytöksistä, joissa potilaan tietoja on käytetty vastoin potilaan tahtoa tai tietämystä. Näissä väärinkäytöksissä liiketoimintaa harrastavat yritykset ovat saaneet luvatta potilastietoja, joita yritykset koittavat hyödyntää liiketoiminnan kasvattamiseen.

Security Australia-lehden (1996) mukaan Yhdysvalloissa on tapahtunut potilastietojen laitonta kaupallista käyttöä, jossa pankkihenkilö lahjoi sairaalassa työskentelevän henkilön. Hoitotyöstä vastaava tarkisti pankin lainanhakijoiden terveystiedot, jotta pankkihenkilö pystyisi päättämään myönnetäänkö lainanhakijoille lainat.

Lähes samanlaisessa tapauksessa pankkihenkilö pääsi käsiksi kunnan syöpäpotilaita käsitteleviin tietoihin. Listasta hän etsi pankin asiakkaat ja peruutti välittömästi potilaiden lainat. [*Hospital Risk Management*, 1993]

Potilaan DNA tietojen päätyminen yrityksen käsiin voisi antaa yritykselle tietoa siitä, mitä potilaan terveydentilassa tulee mahdollisesti tapahtumaan. Yritys saattaisi hyvän toimitavan vastaisesti kohdistaa hiustenkasvua voimistavien tuotteiden mainontaa kaljuuntuville ihmisille tai insuliinipiikkien mainontaa henkilöille, joilla on jo diabetes tai tulee puhkeamaan diabetes.

7. Päätelmät

Terveydenhuollon potilastietoihin kohdistuvat samoja uhkia kuin muihinkin tietojärjestelmiin. Kuitenkin potilastiedot ovat henkilötiedoista tiedoista kaikkein arkaluontoisimpia ja henkilökohtaisempia. Lainsäädäntö velvoittaa henkilöstörekisterien ylläpitäjiä varmistamaan luottamuksellisuus, saatavuus ja käyttökelpoisuus. Potilastietojen tietoturvan pettämisestä voi seurata useita ongelmia, kuten tietojen käyttämistä kaupalliseen toimintaan tai potilaan identiteetin käyttämistä huijauksiin tai hoitotoimenpiteiden suorittamisen estymiseen. Tekniikoita ja käytäntöjä työn suojaamiseksi on jo olemassa, mutta avainasemassa onkin kuinka tietoturva ja tietosuoja tullaan toteuttamaan, jotta se vastaa myös tulevaisuuden muuttuviin haasteisiin.

8. Lähteet

Ahoniemi Lea, 2003, Jämsän aluekeskuksen yritysten turvallisuus- koulutus- ja neuvontatarveselvitys

Alberts Christopher J., Behrens Sandra G., Wilson William R., (2003) CPRI Toolkit: Managing Information Security in Heath Care, http://www.himss.org/CPRIToolkit/html/4.5.html viitattu 28.04.2004

Anderson R. J. (1996) Security in Clinical Information Systems, http://www.cl.cam.ac.uk/users/rja14/policy11/policy11.html viitattu 27.04.2004

Ensio Antero ja Ruotsalainen Pekka, Sähköisen asiakas- ja potilasasiakirjojen säilytyksen hyvä käytäntö. Osaavien keskusten verkoston julkaisuja 2/2003

FinOHTA, 1997, Terveydenhuollon erillisrekisterit - selvitys Suomessa ylläpidettävistä valtakunnallisista ja alueellisista potilasrekistereistä, FinOHTA raportti 3.1997

Hospital Risk Management (1993), 'RMs Need to Safeguard Computerised Patient Records to Protect Hospitals', *Hospital Risk Management*, vol. 9, pp. 16-19.

Howard, John D. & Longstaff, Thomas A. A Common Language for Computer Security Incidents (SAND98-8667). Albuquerque, NM: Sandia National Laboratories, 1998.

Leary, W. E. 1997, 'Panel Cites Poor Security on Medical Records', *New York Times Fax*, 6 March.

Null, C (2003) "Google: Net Hacker Tool du Jour," Wired News, March 4,2003 http://www.wired.com/news/infostructure/0,1377,57897,00.html viitattu 16.04.2004

Raatikainen Ari (2002) Yksityisyyden suoja työelämässä, Edita, Helsinki, s.166

Rothfelder, J. Privacy for Sale, Simon and Schuster, New York, NY

Security Australia 1996, 'Medical Records Face Hacker Risk', *Security Australia* , vol. 16, no.10, p.18.

Sherman, D.(2002), Stealing From The Sick, NBC6.net, May 21,2002

Smith Russell G. (2003), Electronic Theft of Personal Information
http://www.aic.gov.au/conferences/other/smith_russell/2003-05-etheft.pdf
viitattu 20.04.2004

Tähtinen, Heikki, 1997, Terveydenhuollon tietoturvan ja tietosuojan toteutuksen hyviä käytäntöjä, Suomen Kuntaliitto, Helsinki 1997

Valtionhallinnon tietoturvakäsitteistö, Valtionhallinnon tietoturvallisuuden johtoryhmä 4/2003

Sähköisten potilasasiakirjojen tietosuoja terveydenhuollossa

Pia Järvinen

Tämän seminaarityön tarkoituksena on koota yhteen terveydenhuollon sähköisiin potilasasiakirjoihin liittyviä tietosuojalainsäädäntöjä sekä lain rikkomusten seuraamuksia. Näkökulmana terveydenhuollon toimijoiden velvollisuudet sekä seuraamusjärjestelmä.

Avainsanat: sähköinen potilasasiakirja, tietosuoja, terveydenhuolto, lainsäädäntö

Sisällys

1. Johdanto

Potilasasiakirjat ovat viime vuosina voimakkaasti siirtyneet paperi- ja filmimuodosta sähköiseen muotoon. Paperi- ja filmimuotoiset asiakirjat tuntuivat aina olevan ”väärässä” paikassa potilaan sijaintiin nähden ja jatkuvan paikasta toiseen siirtelyn vuoksi ne hukkuvat erittäin usein. Lisäksi vielä tähän päiväänkin asti hoitohuoneissa ja -kanslioissa on notkuvia pinoja erilaisia potilaskansioita, joissa on erittäin arkaluontoisia, vain potilaan itsensä ja hänen lääkärinsä silmille varattuja tietoja. Kanslioiden jatkuva valvonta ja papereiden paikasta toiseen kulkeminen antaa uteliaille houkuttelevia ja helpostikin toteutettavia mahdollisuuksia tutkailla hänelle kuulumatonta tietoa.

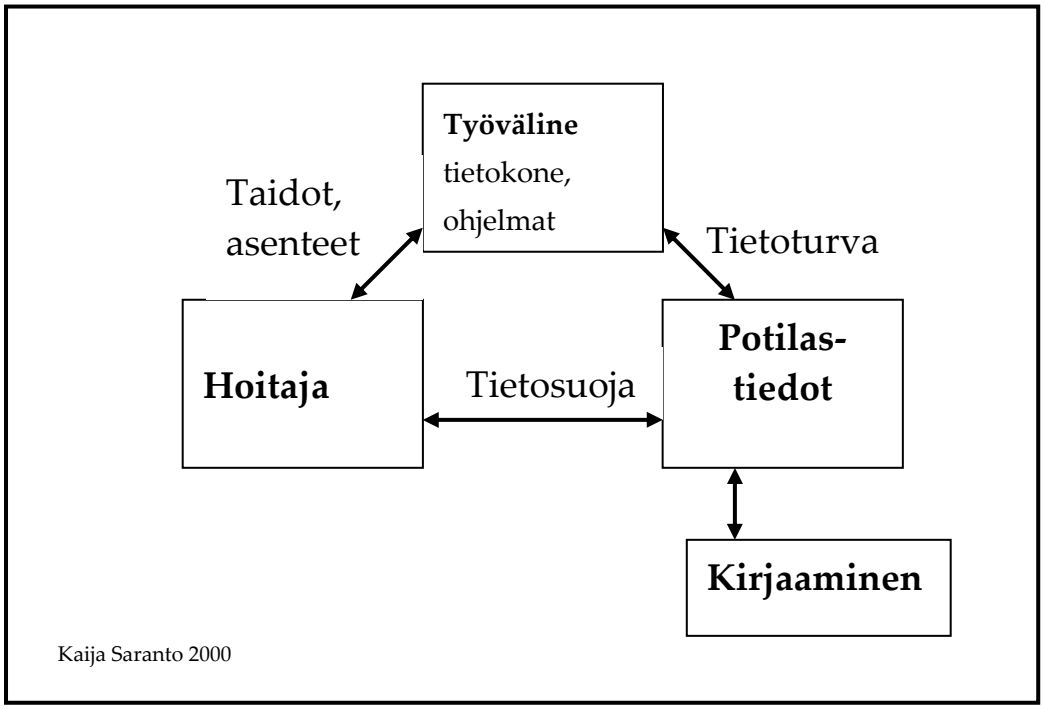
Sähköisten asiakirjojen käytön valvonta on helpompaa, lokitiedoista selviää yksityiskohtaisesti, kenen käyttäjätunnuksilla tietoja on katseltu. Toisaalta, potilasasiakirjatietojen hakeminen asiattomasti on yksinkertaisempaa juuri niiden sähköisen muodon vuoksi, jos tietoja ei ole suojattu. Jos hoitohenkilökuntaan kuuluva antaa mahdollisuuden siihen, että hänen tunnuksiaan käytetään väärin, on hän itse siitä vastuussa. Kyseenalaisen paljon tietokoneita jätetään auki työtauon ajaksi ja tilaisuus näin potilasasiakirjatietojen väärinkäyttöön mahdollistetaan. Edelleenkään ei aina ymmärretä, että naapurin vastasyntyneen sukupuolta ei ole lupa katsoa ”koneelta” tai tarkistaa minä päivänä alaikäiselle tyttärelle olikaan tehty ajanvaraus naistentautien poliklinikalle.

Käytännön vaikeuksia sähköisten potilasasiakirjojen käytössä tuo eri laitosten oma rekisterinpito. Jos potilas siirtyy laitoksesta toiseen ja hän on kykenevä hoitamaan omia asioitaan, toinen laitos voi vain hänen luvallaan hyödyntää hoidossa edellisen laitoksen potilasasiakirjoja. Potilaalla on myös oikeus antaa

asiakirjojen osittainen käyttökielto. Tätä kirjoitettaessa potilaan suostumuksen olemassaolo kulkee lähinnä paperilla sekä suullisena lupana.

2. Käsitteiden määrittelyä

Sähköisten potilasasiakirjojen tietosuoja sekä tietoturva eivät ole sama asia. Tietosuoja liittyy enemmän ihmisten (ja koneen) väliseen kanssakäymiseen sekä yksityisyyteen ja tietoturva puolestaan laitetekniikkaan ja sen avulla tehtyihin tiedon varastoinnin arkkitehtuuriratkaisuihin.



Kuva 1. Tietosuoja ja tietoturvan suhde terveydenhuollossa [Saranto, 2000]

Nykänen [2004] määrittelee tietoturvan ja –suojan seuraavasti:

Tietosuoja: Henkilötietojen käsittely turvattava ja henkilötiedot suojattava asiattomalta käsittelyltä

- tietojen valtuudettoman saannin käytön estäminen
- tietojen luottamuksellisuuden säilyttäminen

Tietoturva: Laitteistot, ohjelmistot, tietoliikenneyhteydet ja tiedot on suojattava fyysisesti, teknisesti ja toiminnallisesti.

- asiantila, jossa uhat eivät aiheuta merkittävää riskiä
- keinojen ja toimenpiteiden kokonaisuus, jolla varmistetaan turvallisuus sekä normaaleissa että poikkeustilanteissa

Tässä seminaarityössä käsitellään vain sähköisten potilasasiakirjojen tietosuoja-asioita, ei niinkään tietoturva-arkkitehtuureja. Tarkoituksena on selvittää lakisääteisiä velvollisuuksia tietosuoja-asioissa sekä sen toteutumista terveydenhuollossa.

2.1. Yksityisyyden suojan historiaa

Tietosuojan ja sen sisältämän yksityisyyden tarpeen olemassaolo on dokumentoitu jo Ranskan vallankumouksen ajalta 1700-luvun lopulta. Amerikassa 1800-luvun lopulla sensaatiojournalismin lisääntyminen aikaansai Samuel D.Warrenin ja Louis D. Brandeisin kirjoittamaan aiheesta tutkielman Harvard Law-review-lehteen vuonna 1890: ”The Right to Privacy”. Artikkelin ja sen keskeisen sanoman ”right to be let alone” on sanottu vaikuttaneen merkittävällä tavalla amerikkalaiseen oikeuskäytäntöön. Sen vaikutus näkyy myös jatkuvina siihen viittauksina tietosuojakirjallisuudessa [Konstari, 1992, 9-10]

Tietokoneistuminen loi jo 1960-luvulla kiinnostusta yksityisyyden suojaamisesta. Vuonna 1972 sekä Ruotsissa (Data och intigret, SOU 1972:4) että Englannissa (Report of the Committee on Privacy) tehtiin valtiovallan toimesta selvityksiä, joista Ruotsissa se johti tietosuojalain laatimiseen. [Korhonen, 2003, 83]

OECD:n tietosuojasuosituksessa vuodelta 1981 kuvataan yleisperiaatteita henkilötietojen keräämisestä, niiden laadusta, tarvittavasta rekisteröidyn suostumuksesta sekä tarkastusoikeudesta. *Euroopan neuvoston tietosuojasopimus* samalta vuodelta määrittelee yksilöiden suojelusta sekä oikeudesta yksityisyyteen henkilötietojen automaattisessa tietojenkäsittelyssä. Sopimuksessa määritellään tietosuojan periaatteet, mutta se ei sääntele tietojen luovuttamisesta. Suomen osalta tietosuojasopimus on ollut voimassa huhtikuusta 1992 ja sen katsotaan olevan sitova kansainvälisessä oikeudessa. Henkilörekisterilaki 471/1987 ja myöhemmin Henkilötietolaki 523/1999 täyttävät sopimuksen vaatimukset. Samansisältöinen on myös *EU:n tietosuojadirektiiviksi* kutsuttu ”Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta”. Mahdollisessa ristiriitatilanteessa tietosuojasopimuksen ja direktiivin välillä sovelletaan tietosuojadirektiiviä. [Korhonen, 2003, 93-95]

2.2 Tietosuojan määritelmiä

Tietosuojaan kuuluvat kansalaisen yksityisyyden suojan ja oikeusturvan huomioon ottaminen rekisteröinnissä, tiedostojen suojaaminen luvattomalta ulkopuoliselta käytöltä sekä valtion turvallisuuden ja yhteiskunnan avoimuuden varmistaminen rekisterinpidossa, eli käsite on laajempi kuin pelkkä yksityisyyden suojan käsite. [Konstari, 1992, 13]

Perustuslain 8.1.§:n toteamus siitä, että henkilötietojen suojasta säädetään tarkemmin lailla, tarkoittaa tietosuojan perusoikeudeksi, jonka yksityiskohdista voidaan säätää lain tasolla ja laki voi sisältää rajoituksia tähän suojaan. [Korhonen, 2003, 92]

Ylipartanen [2001] näkee rekisteröidyn potilaan tietosuojan terveydenhuollossa olevan eri asia kuin pelkkä asiakirjojen salassapitovelvoite. Hänen mukaansa sen voi jaotella kolmeen osaan:

1. rekisteröityjen oikeuksien kunnioittaminen ja toteuttaminen
2. henkilötietojen hyvän käsittelytavan luominen ja toteuttaminen kaikissa henkilötietojen eri vaiheissa (mm. tukea potilassuhteen luottamuksellisuutta ja hyvä hoitokäytäntöä sekä varmistaa tietojärjestelmäinvestointien onnistuminen ja kustannustehokas toiminta)
3. rekisteröityjen sekä rekisterinpitäjien oikeusturvan varmistaminen

⇨ suojeluobjektina ovat ihmisen yksityisyyden suoja ja luottamuksellinen potilassuhde.

3. Terveydenhuollon tietosuojaan liittyvä lainsäädäntö

Terveydenhuollon tietosuoja-asioita Suomessa ei ohjaa mikään yksittäinen laki, vaan se koostuu pääsisältöisesti perustuslaista, joka turvaa oikeuden yksityiselämän suojaan *" Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla."* [Suomen perustuslaki 1999/731, 2. 10§] sekä useasta muusta laista ja ne muodostavat toisiinsa nivoutuvan vyyhdin. Perustaltaan lait pohjaavat kansainvälisiin ihmisoikeussopimuksiin sekä Euroopan unionin asetuksiin ja direktiiveihin, jotta lainsäädäntö EU:n alueella yhtenäistyisi ja potilastietojakin voitaisiin luovuttaa Suomen rajojen ulkopuolelle turvallisesti. Pääsisältönä onkin se, että jos on aihetta epäillä kohdemaan tietosuojan tasoa, asiakirjoja ei luovuteta. *"Henkilötietoja voidaan siirtää Euroopan unionin jäsenvaltioiden alueen tai Euroopan talousalueen ulkopuolelle ainoastaan, jos kyseisessä maassa taataan tietosuojan riittävä taso"* [Henkilötietolaki 523, 5. 22§]

3.1 Henkilötietolaki 22.4. 1999/523 (HetiL)

Henkilötietolakia edeltävässä Henkilörekisterilaissa 1997/471 oli luotu raamit henkilötietojen käsittelyyn, mutta 1999 voimaantullut Henkilötietolaki saattoi Suomen lainsäädännön EU:n määritysten tasolle. Tärkein muutos lienee se, että rekisterinpitäjä on informointivelvollinen pitämästään rekisteristä ja rekisteröidyllä on oikeus saada tietoja sekä vaikuttaa itseään koskeviin rekisteritietoihin (tarkastusoikeus). Henkilötietolakia sovelletaan nimenomaan potilasrekistereihin sisältyvien henkilötietojen käsittelyyn.

3.1.1 Henkilörekisteri, terveydenhuollossa potilasrekisteri

"Tässä laissa tarkoitetaan:

Henkilörekisterillä käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta." [Henkilötietolaki 523, 1. 3§, 3] Terveydenhuollossa potilasrekisteriin katsotaan kuuluviksi kaikki hoidon aikana tehdyt sekä saapuneet potilasasiakirjat sisältäen lähetteet ja lausunnot, ajanvaraustiedot, laskutustiedot. Kaikki eri teknologioilla tuotetut kuvantamistutkimukset sekä EEG- ja EKG-käyrät kuuluvat myös potilasrekisterin piiriin. [Ylipartanen, 2001, 40]

3.1.2 Rekisterinpitäjän velvollisuudet

"Tässä laissa tarkoitetaan:

rekisterinpitäjällä yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty" [Henkilötietolaki 523, 1. 3§, 4]

Terveydenhuollossa rekisterinpitäjä voi olla:

- terveyskeskus
- sairaala tai siitä erillään oleva toimintayksikkö tai muu sairaanhoitopiirin kuntayhtymän päättämä hoitovastuussa oleva kokonaisuus
- yksityinen terveydenhuollon palveluja tuottava yksikkö
- työterveyslaitos
- valtion mielisairaala
- puolustusvoimien terveydenhuolto
- vankeinhoitolaitosten terveydenhuolto
- itsenäisesti ammattiaan harjoittava terveydenhuollon ammattihenkilö

[Ylipartanen, 2001, 40-42]

Rekisterinpitäjältä edellytetään erityistä *huolellisuusvelvoitetta* rekisterinpidossa. Tulee noudattaa hyvää tietojenkäsittelytapaa ja varmistaa se, että yksityisyyden suojaa ei loukata. Sama velvollisuus on sillä, joka toimii rekisterinpitäjän lukuun, eli ostopalvelusopimuksissa on yksiselitteisesti määriteltävä, missä oikeudellisessa asemassa suhteessa rekisterinpitäjään palvelujen tuottaja toimii. Henkilötietojen käsittelyn on oltava myös *suunnitelmallista*. Rekisterin käyttötarkoitus on oltava määriteltynä sekä myös se, mistä henkilötiedot hankitaan. Mahdollinen tiedon luovuttaminen edelleen on oltava suunniteltuna. Potilasrekisterin tarkoitus on palvella potilaan neuvonnan ja hoidon suunnittelua, toteutusta ja seurantaa. Lisäksi sen tarkoituksena on mahdollistaa varmistus, että toimintaa voidaan valvoa terveydenhuollon ammattihenkilöitä koskevan lainsäädännön mukaisesti.

Käyttötarkoitussidonnaisuudella tarkoitetaan sitä, että henkilötietoja käytetään vain siihen tarkoitukseen, johon niitä on kerätty. Henkilötietoja saa käsitellä ja luovuttaa eteenpäin vain rekisteröidyn yksiselitteisesti antamalla

suostumuksella. Ylipartanen kertookin havainnollistavia esimerkkejä siitä, miten potilaan hoitoketjussa tiedonkulku eri rekisterinpitäjien välillä on ongelmallista, koska henkilötietolaissa ei ole erikseen säädetty henkilörekisterien yhdistämisestä. Eri rekistereissä olevaa tietoa voidaan pääsääntöisesti yhdistää vain rekisteröidyn kirjallisella luvalla. Lain vaatimukset täyttävän suostumuksen hankkiminen potilaan tietojen luovutukselle tai yhteiskäytölle ei ole aina yksiselitteistä. *Yhteysvaatimus* tarkoittaa sitä, rekisteröidyllä pitää olla asiallinen yhteys rekisterinpitäjän toimintaan. *Tarpeellisuusvaatimuksen* mukaan henkilötietojen käsittelyn tulee olla kyseisen tarkoituksen kannalta tarpeellisia. Virheettömyysvaatimuksen mukaan tietojen on oltava virheettömiä ja täydellisiä. Jokaisesta rekisteristä pitää olla *rekisteriseloste*, josta pitää ilmetä rekisterinpitäjän yhteystiedot, rekisterin tarkoitus, rekisterin kuvaus, minne tietoja luovutetaan sekä kuvaus rekisterin suojauksesta. [Henkilötietolaki 523, 2. 5-10§ ja Ylipartanen, 2001, 44-47 ja Kleemola, 1999, 160-164]

Rekisterinpitäjällä on *passiivinen informointivelvollisuus*, joka tarkoittaa sitä, että rekisterinpitäjän on laadittava rekisteriseloste ja pidettävä sitä jokaisen saatavilla. *Aktiivinen informointivelvoite* puolestaan tarkoittaa velvollisuutta informoida aktiivisesti ja oma-aloitteisesti rekisteröityä rekisterin sisältämistä keskeisistä seikoista sekä hänen oikeuksistaan. *Rekisteröidyn tarkastusoikeus* tarkoittaa hänen oikeuttaan saada tarkastaa itseään koskevat tiedot, ellei ole olemassa tarkastusoikeuden epäämisperustetta. [Sosiaali- ja terveyspalvelujen lainsäädäntö käytännössä, 2001]

3.1.3. Arkaluontoiset tiedot

"Arkaluonteisten henkilötietojen käsittely on kielletty. Arkaluonteisina tietoina pidetään henkilötietoja, jotka kuvaavat tai on tarkoitettu kuvaamaan:

1) rotua tai etnistä alkuperää;

2) henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista;

3) rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta;

4) henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia;

5) henkilön seksuaalista suuntautumista tai käyttäytymistä; taikka

6) henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia. " [Henkilötietolaki 523, 3. 11§]

STM:n asetuksen 7.3§:n mukaan kielto ei estä terveydenhuollon ammattihenkilöitä käsittelemästä toiminnassa saatuja arkaluontoisia tietoja, jos se on rekisteröidyn hoidon kannalta välttämätöntä, esimerkkinä tästä jehovantodistajien verensiirtokielto. Tällöinkin asiallisinta olisi merkitä hoitotahto, eikä uskontoa. Jos rekisteröity on antanut nimenomaisen suostumuksensa arkaluontoisten tietojensa käsittelyyn, estettä käsittelyyn ei ole.

Lisäksi laissa terveydenhuollon valtakunnallisista henkilörekistereistä (556/1989) sekä asetuksessa (774/1989) määritellään lakisääteiset STAKEsin ja Lääkelaitoksen tilastointi- tutkimus- suunnittelu- ja valvontakäyttöön perustetut rekisterit:

- HILMO-hoito-ilmoitusrekisteri
- syntyneiden lasten rekisteri
- lääkkeiden sivuvaikutusrekisteri
- raskauden keskeyttämis- ja sterilointirekisteri
- syöpärekisteri
- epämuodostumarekisteri

- näkövammarekisteri
- implanttirekisteri

Kyseisen lain katsotaan olevan terveydenhuollon alalla henkilötietolakia tukeva laki. [Korhonen, 2003, 126-129]

3.2. Laki potilaan asemasta ja oikeuksista 17.8. 1992/785 (PotL)

Potilaslaki yhtenäisti sirpaleista potilaan oikeuksia ja tietosuojaa koskevaa lainsäädäntöä. Lisäksi se selkeytti potilasasiakirjojen laadintaa, säilytystä ja niiden tuhoamista koskevaa ohjeistusta.

3.2.1. Potilaan oikeudet

Tiedonsaantioikeudessa määritellään potilaan oikeus saada tietoa terveydentilastaan ja eri hoitovaihtoehdoista, mutta hänellä on myös oikeus kieltäytyä näistä tiedosta. Lisäksi mikäli on ilmeistä, että selvityksen antamisesta aiheutuisi vakavaa vaaraa potilaan hengelle tai terveydelle tai jonkun muun oikeuksille, sitä ei tule antaa. Kyseeseen tulee tällöin lähinnä potilaan itsemurhavaara tai mahdollinen joutuminen psykoosiin tiedon vuoksi. Potilaan *itsemääräämisoikeudesta* ilmenee, että hoitoa on annettava yhteisymmärryksessä hänen kanssaan ja mikäli potilaan tila estää hoitotahdon saannin, on tietoa kysyttävä lähiomaiselta tai muulta läheiseltä.

Alaikäisen potilaan hoidossa on otettava huomioon *tiedonsaantioikeus ja toimivalta. "Jos alaikäinen potilas ikäänsä ja kehitystasoonsa nähden kykenee päättämään hoidostaan, hänellä on oikeus kieltää terveydentilaansa ja hoitoansa koskevien tietojen antaminen huoltajalleen tai muulle lailliselle edustajalleen."* Käytännössä ikärajaksi sovelletaan kahtatoista ikävuotta, joka on myös lapsen huollosta ja tapaamisoikeudesta annetun lain perusteluissa. 12-vuotiasta pidetään kyllin kypsänä, jotta hän pystyy osallistumaan itseään koskevaan päätöksentekoon. Jos alaikäistä pidetään kyllin kypsänä kieltämään

terveydentilansa tiedonanto huoltajilleen, on hänellä myös yksinomainen tarkastusoikeus potilasasiakirjoihinsa sekä asiakirjojen luovutusoikeus, mikäli hän ymmärtää annetun suostumuksen merkityksen. [PotL 3-9§ ja Ylipartanen 2001, 117-129]

3.2.2 Potilaan suostumus potilasasiakirjojen luovutuksesta

Suostumuksen periaatetta on käsitelty jo Nürnbergin oikeudenkäynneissä vuonna 1947, jossa luotiin käsite "informed consent". Pääsisällöltään se määrittelee, että henkilö on itsenäinen subjekti, joka tietoisena toimenpiteen luonteesta ja mahdollisista seuraamuksista kykenee antamaan harkitun, itsenäisen ja riippumattoman suostumuksen. Tätä itsemääräämisoikeutta sovelletaan myös potilaslaissa. [Ylipartanen, 2001, 70-71]

Potilaan suostumuksen määritteleminen ei ole yksiselitteinen asia. Potilaslain 13.3§:n 2 kohdassa määritellään, että tietoja voidaan luovuttaa toisen terveydenhuollon yksikölle tai ammattihenkilölle potilaan tai hänen laillisen edustajansa suullisen suostumuksen tai muuten asiayhteydestä ilmenevän suostumuksen mukaisesti. Asiayhteydestä ilmenevällä suostumuksella tarkoitetaan muuta kuin kirjallisesti tai suullisesti annettua suostumusta, jonka potilas on antanut vapaaehtoisesti tietoisena tietojen luovuttamisesta, luovutuksensaajasta, luovutettavista tiedoista sekä luovutettavien tietojen käyttötarkoituksesta ja luovuttamisen merkityksestä. Tietojen luovuttamisesta ja sen perusteesta tulee tehdä merkintä potilasasiakirjoihin

Henkilötietolain 3§:n 7 kohdassa mainitaan suostumuksella ymmärrettävän kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Kirjassa [Sosiaali- ja terveyspalvelujen lainsäädäntö käytännössä, 2001, 396] mainitaan kuitenkin, että yksiselitteisen suostumuksen vaatimus ei täyty esimerkiksi siitä

tapauksessa, jos potilaalta otetaan sairaalaan saapuessaan kirjallinen, yleinen suostumus hänen terveyttään ja hoitoaan koskevien tietojen luovuttamisesta. Potilas ei voi tietää, mihinkä tarkoitukseen hänen tietojaan tällä luvalla voidaan luovuttaa.

Jatkohoitotilanteissa potilastietoja voidaan luovuttaa jatkohoitopaikkaan potilaan vapaaehtoisen informoidun yksilöllisen suullisen suostumuksen tai asiayhteydestä muuten ilmenevän suostumuksen perusteella. Suostumuksen antaja voi olla myös hänen laillinen edustajansa, jos potilaalla itsellään ei ole edellytyksiä arvioida annettavan suostumuksen merkitystä. Informointi merkitsee sitä, että jatkohoitoon lähettävä terveydenhuollon ammattihenkilö varmistaa potilaan ymmärtävän miksi ja mitä tietoja jatkohoidossa tarvitaan. Suostumuksen antamisen jälkeen se kirjataan potilasasiakirjaan. Jos kyseessä ei ole saman sairauden jatkohoito, tarvitaan potilaan tai hänen laillisen edustajansa kirjallinen suostumus. [Ylipartanen, 2001, 72]
Potilaalla on koska tahansa oikeus muuttaa tai rajata antamiaan suostumuksia.

4. Laki terveydenhuollon ammattihenkilöistä 28.6.1994/559

Laki määrittelee yksityiskohtaisesti terveydenhuollon ammattihenkilön , joka on oikeutettu toimimaan asianomaisessa ammatissa. *Laillistettu ammattihenkilö* on saanut ammatinharjoittamisoikeuden tai ammatinharjoittamisluvan (*luvan saanut ammattihenkilö*) ja *nimikesuojatulla ammattihenkilöllä* on oikeus käyttää asetuksella säädettyä terveydenhuollon ammattihenkilön ammattinimikettä.

Myös asianomaiseen ammattiin opiskeleva henkilö voi toimia tehtävässä siten kun asetuksella säädetään. [1§, 1-2]

Näin määriteltyä ammattihenkilöä koskevat lain 16§ ja 17§ pykälät:

- velvollisuus laatia ja säilyttää potilasasiakirjat sekä pitää salassa niihin sisältyvät tiedot siten mitä on määritelty laissa potilaan oikeuksista ja asemasta PotL 1992/785

- hän ei saa sivulliselle luvatta ilmaista yksityisen tai perheen salaisuutta, josta hän asemansa tai tehtävänsä perusteella on saanut tiedon. Salassapitovelvollisuus säilyy ammatinharjoittamisen päättymisen jälkeen.

5. Laki sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilusta 22.9.2000/811 (Lex Makropilotti)

Lex Makropilotin tavoitteena on saada kokemuksia saumattoman palveluketjun järjestämisestä sekä siitä, miten tietoteknologian hyödyntämistä voidaan parantaa vastaamaan sosiaali- ja terveydenhuollon ja muun sosiaaliturvan asiakkaiden tarpeita sekä miten tietoteknologiaan käytettäviä varoja voidaan tässä toiminnassa kohdentaa tarkoituksenmukaisella tavalla.
Se säätää saumattoman palveluketjun järjestämisen alueellisesta kokeilusta sekä siihen liittyvistä omaneuvojapalveluista, palveluketjusuunnitelmasta ja viitetietokannasta. [Lex Makropilotti, 1§]

12 § momentti säätää tunnistamisesta *"Sosiaali- ja terveydenhuollon varmennetussa sähköisessä asioinnissa asiakas voidaan todentaa henkilökorttilain (829/1999) mukaisessa henkilökortissa olevalla varmenteella tai vastaavan tasoisella muulla varmenteella. Sosiaali- ja terveydenhuollon laillistettu ammattihenkilö voidaan ammattia harjoittaessaan todentaa riittävän tasoisella varmenteella. Sähköisessä asioinnissa myös sosiaali- ja terveydenhuollon organisaatio voidaan varmentaa"*

13 § momentissa säädetään sähköisestä allekirjoituksesta *"Asiakas, organisaatio tai organisaation edustaja voi 12 §:ssä tarkoitetun varmenteen avulla sähköisesti allekirjoittaa ja salata lähettämänsä asiakirjan tai muun viestin."*

22 § momentissa taas kuvataan viitetietokanta: *"Viitetietona talletetaan viitetietokantaan asiakkaan nimi, henkilötunnus, tiedon sijaintipaikka, yleisluonteinen kuvaus viitetiedon osoittamasta tiedosta, viitetiedon tallettamisaika sekä viitetietokannan toiminnan edellyttämät tekniset tiedot. "*

Lain tarkoituksen on siis käytännössä kokeilla sähköisen potilasasiakirjan, potilaan suostumuksen ja sähköisen tiedonkulun toteuttamista sosiaali- ja terveydenhuollossa yli rekisterinpitorajojen Satakunnan alueella. Myös sähköinen sosiaaliturvakortti oli kokeiltavana. Rekisteröidyllä on samat tiedonsaanti- ja korjausoikeudet kuin henkilötietolaissakin määritellään. Viitetietojen salassapito ja luovuttaminen on samoin potilaan suostumukseen perustuvaa, laissa mainitaan momentissa 23 tietojen luovuttamisesta, että luovutus ja sen peruste on kirjattava viitetietokantaan, mikäli potilas itse ei suostumusta pysty antamaan. Lain voimassaoloaikaa on jatkettu vuoteen 2005 asti korvaavalla lailla 19.12.2003/1225. Laki sisältää tarkennuksia viitetietokannan, sähköisen allekirjoituksen sekä potilaan suostumuksen määritelmiin.

6. Sähköisten potilasasiakirjojen tietosuoja

Potilasasiakirjojen laadinnasta ja rekisterinpitäjän velvoitteista säädellään tarkemmin Sosiaali- ja terveysministeriön asetuksessa 2001/99:

Terveydenhuollon toimintayksikön ja itsenäisesti ammattiaan harjoittavan terveydenhuollon ammattihenkilön tulee rekisterinpitäjänä suunnitella ja toteuttaa potilasasiakirjajärjestelmänsä siten, että sen rakenne ja tietosisältö vastaavat potilasasiakirjojen käyttötarkoitusta sekä hoitoon tai siihen liittyviin tehtäviin osallistuvien henkilöiden tehtäviä ja vastuita. Potilasasiakirjojen rakennetta ja säilytystä suunniteltaessa on muun ohella otettava huomioon tietoihin liittyvät käyttöoikeudet sekä tietojen siirtämis- ja luovuttamistarpeet.

Terveydenhuollon toimintayksikön terveydenhuollosta vastaavan johtajan tulee rekisterinpitäjän edustajana antaa kirjalliset ohjeet potilasasiakirjoihin sisältyvien tietojen käsittelystä ja menettelytavoista toimintayksikössä.

Potilasasiakirjojen käsittelyssä tulee noudattaa henkilötietolain 5 §:ssä säädettyä huolellisuusvelvoitetta siten, että potilassuhteen luottamuksellisuus ja potilaan yksityisyyden suoja turvataan.

Potilasasiakirjat tulee laatia ja säilyttää sellaisia välineitä ja menetelmiä käyttäen, että asiakirjoihin sisältyvien tietojen eheys ja käytettävyys voidaan turvata tietojen säilytysaikana." [SosT asetus 2001/99, 3§]

Potilaan hoitoon tai siihen liittyviin tehtäviin osallistuvat saavat käsitellä potilasasiakirjoja vain siinä laajuudessa kuin heidän työtehtävänsä ja vastuunsa sitä edellyttävät. Terveydenhuollon toimintayksikössä työskentelevien käyttöoikeudet potilasasiakirjoihin sisältyviin tietoihin tulee määritellä yksityiskohtaisesti.

Automaattisen tietojenkäsittelyn avulla pidettävien potilasasiakirjojen käyttöä tulee valvoa käytettävissä olevin riittävin teknisin menetelmin [SosT asetus 2001/99, 4§]

6.1. Tietosuojan toteuttaminen

Rekisterinpitäjän velvollisuuksiin kuuluu myös tietosuojan käytännön toteuttaminen, tietojen eheyden säilyttäminen sekä henkilökunnan motivointi toimimaan siten, että potilaan tietosuojaoikeus toteutuu. Tärkeätä on myös se, että jos tietoja muutetaan, muutokset ovat näkyvissä ja muuttajan henkilöllisyys saadaan tarvittaessa selville. Hyvään tiedonhallintatapaan kuuluu myös se, että tiedot ovat helposti saatavilla niille henkilöille, joille tieto asiakirjoista potilaan hoidon toteuttamiseksi kuuluu.

Tietosuojan huolellinen suunnittelu ja toteutus on osa terveydenhuollon laatujärjestelmiä. Kirjassa [Sosiaali- ja terveyspalvelujen lainsäädäntö käytännössä, 2001, 393] on määritelty rekisterinpitäjän tekniset ja organisatoriset tehtävät henkilötietojen käsittelystä seuraavasti:

- Ohjeistaa ja kouluttaa henkilökunta henkilötietojen käsittelyyn
- Antaa työntekijöille kullekin erikseen määritellyt käyttöoikeudet työtehtävien hoitamisen kannalta tarpeellisiin henkilörekisteritietoihin (erikseen tietojen katselu, lisääminen, muuttaminen ja poistaminen). Tietoja on laillista käyttää ainoastaan työtehtävän hoitamiseksi
- Poistaa työntekijän käyttöoikeudet palvelussuhteen päättyessä
- Tarkistaa työntekijän käyttöoikeudet ja antaa tarvittaessa uudet ja poista vanhat, jos työtehtävät muuttuvat
- Antaa henkilökohtaiset käyttäjätunnukset ja salasanat
- Luo menettelytavat, joiden avulla voidaan seurata tietojen käsittelyä, esim. kuka on käsitellyt tietoja ja mitä toimenpiteitä hän on suorittanut. Työyhteisössä esimerkiksi henkilökohtaisen käyttäjätunnuksen/salasanan antaminen toisen henkilön käyttöön ei ole laillista.
- Säilyttää asiakastiedot lukitussa kaapissa tai huoneessa siten, etteivät sivulliset, esim. muut asiakkaat niitä näe
- Huolehtii siitä, että tietokoneesta, jolla asiakastiedot ovat, ei ole internetyhteyttä. Jos sellainen kuitenkin on, tulee järjestelmään rakentaa niin tehokkaat suojaukset, etteivät ulkopuoliset pääse asiakastietoihin käsiksi.
- Pitää huolta siitä, että hyvän henkilötietojen käsittelytavan toteuttamiseksi annettujen säännösten, määräysten ja ohjeiden noudattamista valvotaan

Yksi tapa henkilökunnan tietosuoja-asioiden ymmärryksen lisäämiseksi on allekirjoittaa työsuhteen alkaessa tietojärjestelmien käyttäjäsitoumus, jossa yksityiskohtaisesti käydään läpi työntekijän velvollisuudet ja oikeudet sähköisten potilastietojärjestelmien käyttöön. Hoitohenkilökunnalle ei esimerkiksi ole itsestään selvää se, että edes omia tietojaan ei saa katsella ilman hoitavan lääkärin lupaa. Liitteessä 1 on yksi kirjallisen käyttäjäsitoumuksen malli [Liite 1: Tietosuoja- ja tietoturvasitoumusmalli, Ylipartanen 2001, 155-156]

6.1.1. Potilastietojen lähettäminen tietoverkossa

Potilastietojen lähettäminen salaamattomassa verkossa on yleisesti ottaen kielletty. Kuitenkin yleinen tapa on lähettää potilasasiakirjoja telefaxilla ilman salausta. Vaikka telefaxin käyttö on tietosuojamielessä epäasiallista, on katsottu kuitenkin sen tietyissä tapauksissa olevan tietosuojakriteerit täyttävä lähetystapa:

- asiakirjat salataan lähetyksen aikana
- vastaanottaja ja lähettäjä ovat molemmat tiedonsiirtoon oikeutettuja henkilöitä (kumpikaan ei ole sivullinen). Lähetyksen jälkeen on syytä varmistaa puhelimella, että tiedot on saanut oikea henkilö
- lähetyksestä tehdään potilasasiakirjaan kirjallinen merkintä
- menettelytapa on sekä ohjeistettu että sovittu eri osapuolien kesken

Suositeltavaa on, että lähetyspyynnön tekee potilaan hoidosta vastaava henkilö ja salaamattoman verkon kautta lähetetään vain kiireellisiä potilastietoja.

Vain ensimmäisen kohdan kriteeri suojaa potilaan tietosuojan toteutumisen lähettäjän mahdollisilta näppäilyvirheiltä telefaksia lähetettäessä..

Jos kaikenlainen potilaan tunnistava informaatio on poistettu asiakirjasta, sen lähettäminen salaamattoman verkon kautta on mahdollista, esim. konsultaatiotilanteissa sähköpostitse. [Ylipartanen, 2001, 74-75]

Sähköpostin salaus voidaan ottaa myös käyttöön potilasasiakirjoja lähetettäessä. Viestit voidaan salata ennen niiden lähettämistä tai ne voidaan allekirjoittaa digitaalisesti. [Nykänen 2004]

6.2. Potilasasiakirjojen säilytys ja hävitys

Sosiaali- ja terveysministeriön asetus 22§ määrittelee potilasasiakirjojen säilyttämisajat. Vastuussa oleva taho on se terveydenhuollon toimintayksikkö, missä asiakirjat ovat syntyneet ja asetus koskee asiakirjoja, jotka on laadittu 1.5.1999 tai sen jälkeen. Vaikeusastetta asetuksen toteuttamiseen tuo se, että eri asiakirjojen säilytysajat ovat erilaisia.

Potilasasiakirjojen säilyttämisajat vaihtelevat asiakirjasta riippuen:

- jatkuvakäyttöisluontoiset asiakirjat (mm. tiivistelmät, yhdistelmät, lausunnot) säilytysaika on 10 vuotta potilaan kuolemasta tai jos siitä ei ole tietoa, 100 vuotta potilaan syntymästä ja 10 vuotta hoidon päättymisestä
- tiettyyn hoitojaksoon liittyvät hoitoa tukevat asiakirjat tuhotaan 10 vuotta hoidon päättymisestä (yleisluontoisesti)
- kuvantamistutkimusten tallenteet (filmit ja digitaalimuodossa olevat) säilytetään 20 vuotta
- kaikkien 18. ja 28. päivänä syntyneitä koskevat tiedot julkisessa terveydenhuollossa sekä valtion mielisairaaloiden ja Puolustusvoimien terveydenhuollon asiakirjat säilytetään pysyvästi arkistolaitoksen 22.12.2000 antaman päätöksen mukaisesti
  [Ylipartanen, 2001, 56-57 ja 307-317]

Tiedon hävittäminen tulee tehdä salassapitovaatimusten edellyttämällä tavalla ja se koskee kaikkea potilastietoa sen muodosta riippumatta joten hävittäminen tulee olla suunniteltua. [Saranto, 1999, 172]

7. Tietosuojarikkomusten seuraamukset

Rekisterinpitäjä on Henkilötietolain 47§: mukaan velvollinen korvaamaan sen vahingon, joka on aiheutunut lain vastaisesta henkilötietojen käsittelystä. Rekisterinpitäjän vastuu on tuottamuksesta riippumatonta eli ankaraa vastuuta, mutta rekisteröidyn on todistettava häntä kohdannut vahinko sekä henkilötietojen käsittelyn syy-yhteys vahinkoon. Kuitenkin Turun HO:n tuomio 10.10.2000 on todennut, että kärsimysvahingossa todistustaakka siitä, että lainvastaisesta henkilön yksityisyyteen liittyvästä arkaluontoisen materiaalin (terveydentilatietojen) paljastamisesta ei ole aiheutunut kärsimystä on rekisterinpitäjällä. Näin ollen oletetaan, että terveydentilatietojen paljastaminen aiheuttaa kärsimystä, ellei rekisterinpitäjä toisin yksittäistapauksissa todista. [Sosiaali- ja terveyspalvelujen lainsäädäntö käytännössä, 2001, 518-519 ja Ylipartanen, 2001,142- 143]

Mediauutisten 2000 mukaan eräässä terveydenhuollon yksikössä jopa esimiesasemassa olleet henkilöt olivat lukeneet alaistensa potilastietoja. Asia paljastui omassa sisäisessä valvonnassa ja on johtanut kurinpitomenettelyihin, mm. varoituksiin.

Aamulehdessä 29.3.04 kirjoitettiin poliisimiehestä, joka oli vuosien 2001-2003 välisenä aikana tehnyt henkilökyselyjä laittomasti työtovereistaan sekä heidän perheistään peräti 7500 kappaletta. Asia tuli ilmi sisäisessä valvonnassa ja poliisimies tuomittiin henkilörekisteririkoksesta 300 euron sakkoihin.

7.1. Henkilörekisteririkos ja henkilörekisteririkkomus

Henkilörekisteririkoksen tunnusmerkit täyttyvät, jos joku tahallaan tai törkeästä huomaamattomuudesta käsittelee henkilötietoja vastoin henkilötietolain säännöksiä, jotka koskevat käyttötarkoitussidonnaisuutta, käsittelyn yleisiä edellytyksiä, henkilötietojen tarpeellisuutta ja virheettömyyttä, arkaluontoisia

tietoja, henkilötunnusta ja henkilötietojen käsittelyä erityisiä tarkoituksia varten. Lisäksi rikos on se, jos hän antaa rekisteröidylle väärän tai harhaanjohtavan tiedon estää tai yrittää estää rekisteröityä käyttämästä tarkastusoikeuttaan. Vielä rikos on siirtää henkilötietoja EU:n tai Euroopan talousalueen ulkopuolisiin valtioihin henkilötietolain luvun 5 vastaisesti. Rangaistuksena voidaan tuomita sakkoon tai enintään vuodeksi vankeuteen. Rikoslaki 38.9§.

Henkilörekisteririkkomuksen tunnusmerkit täyttyvät, jos joku laiminlyö noudattaa, mitä säädetään henkilötietojen käsittelyn tarkoitusten määrittelystä, rekisteriselosteen laatimisesta, tietojen käsittelyn informoimisesta, henkilörekisterissä olevan tiedon korjaamisesta, rekisteröidyn kielto-oikeudesta, ilmoituksen tekemisestä tietosuojavaltuutetulle. Lisäksi rikkomus on se, että antaa tietosuojaviranomaiselle henkilötietojen käsittelyä koskevassa asiassa väärän tai harhaanjohtavan tiedon tai rikkoo henkilötietojen suojaamisesta ja henkilörekisterin hävittämisestä annettuja säännöksiä ja määräyksiä. Rangaistuksena voidaan tuomita sakkoon. Henkilötietolaki 48.2§.

Yhteisenä tekijänä kummassakin on rekisteröidyn yksityisyyden suojan ja oikeuksien loukkaus tai niiden vaarantaminen [Ylipartanen, 2001,143-145]

7.2. Tietomurto

Tietomurrosta tuomitaan Rikoslain 38, 8.1§:mukaan: joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti taikka muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen tietojärjestelmän erikseen suojattuun osaan. Rikoslain 38, 8.2§:n mukaan tietomurto on myös se, joka tietojärjestelmään tai sen osaan

tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta.

Myös sattumalta onnistunut tunnusten selville saaminen on rangaistavaa, jos tarkoituksena on oikeudeton tunkeutuminen. Teon rangaistavuuden kannalta ei ole merkitystä sillä, kuinka oikean käyttäjätunnuksen hankinta on tapahtunut. Se voi olla oikealta käyttäjältä urkittu tai löydetty muistilapulta. Teko ei ole perustelujen mukaan oikeudeton, jos oikea käyttäjä on antanut oikeuden käyttää tunnustaan. Rangaistavaa se on silloin, kun tekijä tietää tunkeutuvansa järjestelmään ilman oikeutta. Tunkeutumiselta ei edellytetä mitään tarkoituksia tai suunnitelmaa henkilötietojen käytöstä, riittää, että valvontamekanismi on läpäisty. Rangaistuksena sakko tai korkeintaan vuosi vankeutta. [Raatikainen, 1999, 291]

8. Lopuksi pohdintaa

Keskeisin ongelma potilastietojen sähköisessä siirrossa tällä hetkellä (vieläkin) on se, että tiedonsiirtoa pystytään kyllä tekemään, mutta se ei täytä lain vaatimuksia. Järjestelmät eivät vielä ole niin kehittyneitä, että lain vaatimukset voitaisiin ottaa täysimääräisinä huomioon tai terveydenhuolto-organisaatio ei kykene sellaista rahoitusongelmien vuoksi hankkimaan, vaikka tarvetta turvalliseen tiedonsiirtoon olisi. Lisäksi on ymmärrettävää, että ohjelmisto- ja laitetoimittajat eivät halua tehdä yksittäisiä järjestelmää muuttavia ratkaisuja jokaiselle asiakkaalle. Ohjelmisto- ja laitetoimittajien pitäisi pystyä keskustelemaan keskenään järjestelmäintegraatioiden teknisistä ratkaisuista ja ottaa niissä huomioon tiedonsiirto ei pelkästään kansallisesti vaan myös kansainvälisesti.

Realismia on myös se, että asiakas saattaa ostaa monelta eri ohjelmisto- ja laitetoimittajalta tietojärjestelmiä joiden välinen tiedonsiirto pitää olla

tietoturvallista. Nykypäivänä sairaalamaailmassa jokaisella erikoisalalla on oma tietojärjestelmänsä, esimerkiksi anestesiayksiköillä, laboratoriolla, röntgenillä, leikkausosastolla ja kaikkien näiden tiedot liitetään sairaalan tietojärjestelmään tai sähköiseen potilasasiakirjaan. Koska kalliit laiteinvestoinnit on tehty, tietoa siirretään koska se on tarkoituksenmukaista. Tietosuojan toteuttaminen on vielä hajanaista, eikä integraatiota eri järjestelmien välillä tietosuojamielessä ole vielä tehty kattavasti.

Sähköinen potilastiedon välitys on kuitenkin potilaan hoitoa edistävää, säästytään esimerkiksi turhilta laboratorio- tai röntgentutkimuksilta. On paljon kustannustehokkaampaa välittää eteenpäin jo olemassa olevia tutkimustuloksia kuin tehdä ne uudestaan. Tämä onkin yksi perusperiaate kansallisen terveysprojektin toteuttamisessa. Potilastietojen monet eri rekisterinpitäjät aiheuttavat pohdintaa siitä, onko pirstaleinen rekisterinpito todellakin tarpeellista. Jos pienellä alueella jokainen terveydenhuollon yksikkö on oma rekisterinpitäjänsä, mitä käytännön hyötyä se tuo potilaalle? Potilas kulkee hoitopaikasta toiseen ja jos vaiva ei ole saman hoitolinjan sisällä, täyttelee hän erilaisia suostumuksia jokaisella ilmoittautumiskerralla.

Eri tietojärjestelmien yhteenintegroimattomuus tuo myös vaivaa hoitohenkilökunnalle. Käyttäjä joutuu nykyisin joka päivä käyttämään monia eri käyttöliittymiä ja jopa kymmeniä eri käyttäjätunnuksia ja salasanoja. HST-kortit (henkilön sähköinen tunnistaminen) tulevat varmastikin tulevaisuudessa helpottamaan sisään kirjautumista, mutta tällä hetkellä tuntuu täysin ymmärrettävältä, että henkilökunta turhautuu avaamaan-sulkemaan käyttöliittymiä jatkuvasti päivän aikana. Tämänhetkinen tilanne terveydenhuollossa antaa paljon mahdollisuuksia tietoturvarikoksille ja -rikkeille. Lisäksi henkilökunta tarvitsisi enemmän koulutusta tietosuoja-asioista, ei pelkästään tietojärjestelmien teknisestä käyttämisestä.

Tulevaisuuden aluetietojärjestelmien kehittyminen ja nimenomaan potilaan suostumuksen sekä oikeutettujen käyttäjien hallinta tietojärjestelmäohjelmiston avulla tuo toivottavasti selvyyttä tällä hetkellä sekavaan tilanteeseen. Tampereella 10.5.04 Terveydenhuollon ATK-päivillä näitä erilaisia ratkaisuja oli esillä ja siinä mielessä tulevaisuus näyttääkin mielestäni valoisammalta, jotta sähköinen sairauskertomus todellakin olisi koko Suomessa käytössä vuonna 2007. Pelkona on se, että koska tiedetään kansallisen terveyshankkeen ajavan tietojärjestelmäintegraatiota terveydenhuollossa, odotetaan ”jonkin instanssin” käskyttävän mitä tehdä ja sitten vasta tehdään. STAKES luo ohjeistusta ja suunnitelmia, mutta mielestäni tämän asian hoitaminen ja siinä mukana toimiminen kuuluu kaikille terveydenhuollon tietojärjestelmien kanssa toimivien asiantuntijoiden piiriin, jossa pitää ottaa huomioon lääketieteen eri erikoisalojen erityispiirteet ja heidän tietojärjestelmänsä sosiaalihuoltoa unohtamatta. Myös tietojärjestelmä- ja laitetoimittajat kuuluvat mielestäni tähän piiriin. Eurooppa yhdentyy, ihmiset kulkevat entistä vapaammin maasta toiseen ja myös sairastavat eri maissa. Potilastietojen saatavuus tietoturvallisesti myös maasta toiseen pitää ottaa huomioon.

”Sähköisessä asioinnissa voi asioijan tunnistavista rekisteröinneistä kertyvien tietojen määrä olla hyvinkin satakertainen verrattuna perinteiseen asiointiin. Jos ihminen asioi perinteisesti 50 kertaa vuodessa, sähköisessä asioinnissa kertyvien tietojen määrä on silloin 5000. Tämä merkitsee vuositasolla 250 miljardia uutta suomalaisten yksityisyyteen puuttuvaa tietoa. Henkilötietolain mukainen tietosuoja saattaa silti olla molemmissa asiointitavoissa yhtä hyvä tai huono.”

Risto Heinonen
Digitaalinen minä

LÄHTEET

[Aamulehti 29.3.2004]

[Heinonen, 2001] Risto Heinonen, *Digitaalinen minä.*
Edita Oyj, Helsinki 2001.

Henkilötietolaki 523/1999

Henkilörekisterilaki 471/1987

[Kleemola, 1999] Maija Kleemola, Tietosuoja tietotekniikan käytössä.
Teoksessa: Kaija Saranto & Mikko Korpela (toim.),
Tietotekniikka ja tiedonhallinta sosiaali- ja terveydenhuollossa
WSOY – Kirjapainoyksikkö, Porvoo 1999.

[Konstari, 1992] Timo Konstari, *Henkilörekisterilaki. Säännökset ja käytäntö.*
Lakimiesliiton Kustannus, Helsinki 1992

[Korhonen, 2003] Rauno Korhonen, *Perusrekisterit ja tietosuoja.*
Edita Publishing Oy, 2003.

Laki terveydenhuollon ammattihenkilöistä 28.6.1994/559

[Lex Makropilotti] Laki sosiaali- ja terveydenhuollon saumattoman
palveluketjun kokeilusta 22.9.2000/811

[Lohiniva-Kerkelä, 2001] Mirva Lohiniva-Kerkelä, *Terveydenhuollon juridiikka.*
Kauppakaari, Lakimiesliiton Kustannus, Helsinki 2001.

[Mediauutiset, 2000] Mediauutiset nro 11, 31.5.2000

[Nykänen 2004] Nykänen Pirkko, *Tietosuoja- ja tietoturva*, luentomoniste. Tampereen teknillinen yliopisto 2004

[PotL] Laki potilaan asemasta ja oikeuksista 17.8. 1992/785

[Raatikainen, 1999] Ari Raatikainen, *Yksityisyyden suoja työelämässä*
Oy Edita Ab, Helsinki 1999

[Saranto, 2000] Kaija Saranto. Sähköisen kirjaamisen haasteet hoitotyössä. *Sairaanhoitaja-lehti 3/2000* ***vol 73*** (2000), 37.

[Saranto, 1999] Kaija Saranto & Mikko Korpela (toim.),
Tietotekniikka ja tiedonhallinta sosiaali- ja terveydenhuollossa
WSOY – Kirjapainoyksikkö, Porvoo 1999.

[SosT asetus 2001/99] Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä 19.1.2001/99

[Sosiaali- ja terveyspalvelujen lainsäädäntö käytännössä, 2001] Jouko Narikka (toim.), *Sosiaali- ja terveyspalvelujen lainsäädäntö käytännössä.* Tietosanoma 2001, RT-Print Oy, Pieksämäki 2001

Suomen perustuslaki 1999/731

[Ylipartanen, 2001] Arto Ylipartanen, *Tietosuoja Terveydenhuollossa.*
Potilaan asema ja oikeudet henkilötietojen käsittelyssä. Tietosanoma Oy, 2001.

Liite 1: Tietosuoja- ja tietoturvasitoumusmalli

Tietosuoja- ja tietoturvasitoumusmalli

Terveydenhuollon toimintayksikön työasemien (sisältää tietoverkkoon langallisesti/langattomasti liitetyt atk-laitteet), tietoliikenneverkon ja atk-järjestelmien käyttöoikeudet annetaan vain niille, jotka ovat allekirjoittaneet tämän tietosuoja- ja tietoturvasitoumuksen. Sitoumukset arkistoidaan sovitulla tavalla keskitetysti esim. tulosyksiköittäin/vastuualueittain.

KÄYTTÄJÄSITOUMUS:

1. Salassapidosta tiedän:

- ☐ Salassapitovelvollisuudesta(asiakirjasalaisuus ja vaitiolovelvollisuus) säädetäänuseissa laeissa kuten mm.: Laki potilaan asemasta ja oikeuksista (785/92, muut. 653/2000, 13 §), Laki terveydenhuollon ammattihenkilöistä (559/1994, 17 §), Laki yksityisestä terveydenhuollosta (152/1990, 12 §), Työterveyshuoltolaki (743/78, 6 §), Laki viranomaisten toiminnan julkisuudesta (621/99, 22–23 §) ja Henkilötietolaki (523/1999, 33 §).
- ☐ Palvelussuhteentaimuuntyötehtävänaikana tai sen päätyttyä sivulliselle ei saa ilmaista työn vuoksi tietoon saatuja toimintayksikköä tai sen asiakkaita, sopimuskumppaneita tai muita yhteistyötahoja koskevia salassa pidettäviä tietoja. Tällaisia ovat mm. liike- ja ammattisalaisuudet sekä arkaluontoiset henkilötiedot, ellei julkisuuslainsäädännössä toisin määrätä.
- ☐ Hoitosuhteessa sivullisella tarkoitetaan muita kuin asianomaisessa toimintayksikössä tai sen toimeksiannosta potilaan hoitoon tai siihen liittyviin tehtäviin osallistuvia henkilöitä (PotL 13 §).
- ☐ Rekisterien katselu- tai käyttöoikeutta ei ole muihin kuin työtehtävien edellyttämiin tietoihin, esimerkiksi ei omiin eikä lähiomaisten potilastietoihin ilman hoitavan lääkärin lupaa.
- ☐ Ilmanrekisteristävastaavankirjallistalupaa ei saa luovuttaa tai siirtää salassa pidettäviä asiakastietoja tai muuta salassa pidettävää tietoa, eikä tallentaa niitä toisiin rekistereihin, työaseman kiintolevylle, levykkeelle tai muille tallennuslaitteille. Asiakastiedoilla tarkoitetaan ensisijaisesti potilastietoja.

2. Käyttäjätunnuksesta ja salasanasta tiedän:

- ☐ Työasemaa saa käyttää vain omalla käyttäjätunnuksella ja salasanalla.
- ☐ Käyttäjätunnukset ovat henkilökohtaisia. Kukin vastaa käyttäjätunnuksellaan tehdyistä merkinnöistä.
- ☐ Salasana on vaihdettava heti sen saamisen jälkeen ja myöhemmin tarvittaessa tai sovituin aikavälein.
- ☐ Käyttäjätunnus ja salasana on pidettävä muistissa. Niitä ei saa antaa muiden tietoon.
- ☐ Tietojärjestelmistäonkirjauduttavaulostai työasema on lukittava välittömästi käytön jälkeen ellei työasema ole käyttäjän valvonnassa.

3. Työaseman käytöstä tiedän:

- ☐ Työasemassasaakäyttäävaintoimintayksikön hyväksymiä ja lisensioituja ohjelmia, jotka ovat tietojenkäsittely-yksikön asentamia ja tukemia tai erillisellä tietojenkäsittely-yksikön hyväksymällä tavalla muun toimittajan asentamia ja tukemia.
- ☐ Toimintayksikönhankkimiaohjelmiaeisaa kopioida.
- ☐ Työasemaa ei saa liittää verkkoon tai siirtää luvatta.
- ☐ Samoja levykkeitä tai muita tietovälineitä ei saa käyttää työpaikalla ja sen ulkopuolella, jollei ole varmistautunut niiden viruksettomuudesta.
- ☐ Epäiltäessä työaseman olevan tietokoneviruksen saastuttama, työasemalla työskentely on lopetettava välittömästi. Tietokoneviruksista on aina ilmoitettava tietojenkäsittely-yksikköön.

155

- ☐ Työaseman käytössä on otettava huomioon tietoverkon ja palvelinlaitteiden rajoitettu kapasiteetti. Kuvia, grafiikkaa ja äänitiedostoja saa välittää verkossa tai tallentaa palvelimelle vain työtehtävien vaatiessa.
- ☐ Työasemaan talletettujen tiedostojen varmuuskopioimisesta vastaa kukin käyttäjä itse. Palvelimilla olevien tiedostojen varmistuskopiointi hoidetaan keskitetysti tai järjestelmän pääkäyttäjän toimesta.
- ☐ Työasemaa ei saa käyttää tiedostojen pysyvään säilytykseen.

4. Sähköpostin ja Internet-yhteyksien käytöstä tiedän:

- ☐ Sähköposti ja Internet-yhteydet on tarkoitettu pääsääntöisesti työtehtävien hoitoon.
- ☐ Arkaluonteisia ja muita salassa pidettäviä tietoja ei saa lähettää ulkoisen sähköpostin välityksellä.
- ☐ Virusriskin vuoksi ulkopuolelta tulevan sähköpostin liitetiedostoja ei saa avata, jos viesti tulee epämääräisestä lähteestä. Viesti on syytä hävittää.
- ☐ Sähköpostiketjukirjeitä ja muuta roskapostia ei saa lähettää eikä välittää eteenpäin, vaan ne on tuhottava.
- ☐ Internetistä ei saa kopioida ohjelmia.
- ☐ Internet/www-selaimen käytöstä kertyy loki- ja varmistustietoa, josta tietotekniikka tarvittaessa tekee yhteenvetoraportteja käyttötilanteen seuraamiseksi.
- ☐ Evästeiden (ns. cookie) asettaminen web-selaimelle tulee estää.

5. Järjestelmäkohtaisista ohjeista tiedän:

- ☐ Kunkin käyttäjän on tutustuttava toimintayksikön tietosuojaohjeisiin sekä käyttämiensä tietojärjestelmien käyttöohjeisiin ja rekistereiden rekisteriselosteisiin.
- ☐ Tietojärjestelmien käytöstä kertyy sormenjälkitietoa ja käyttöä seurataan.

6. Seuraamuksista tiedän:

- ☐ Sääntöjen ja periaatteiden rikkomisesta käyttöoikeudet tietojärjestelmiin voidaan peruuttaa. Rikkomuksista tiedotetaan aina esimiehelle. Jos kyseessä on toistuva tai vakava rikkomus, ryhdytään tapauksen edellyttämiin jatkotoimiin. Mikäli rikkomuksesta aiheutuu välittömästi tai välillisesti taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimuksiin (ks. toimintayksikön omat tietosuojaohjeet).
- ☐ Tietojen väärinkäyttö tai tahallinen ohjeiden vastainen toiminta voi johtaa muun ohella rikosoikeudellisiin seuraamuksiin.

7. Voimassa olevat käyttöoikeuteni tietojärjestelmiin (liite)

Olen lukenut ja ymmärtänyt yllä olevassa tietosuoja- ja tietoturvasitoumuksessa esitetyt periaatteet ja tutustunut toimintayksikön tietosuojaohjeisiin. Sitoudun noudattamaan niitä.

Pvm _____

Allekirjoitus ja nimen selvennys _____

Toimipaikka _____

Esimiehen allekirjoitus ja nimen selvennys _____

Liite 2

Tietosuojavaltuutetun toimisto 9.2. 2001:

SANKTIOJÄRJESTELMÄ

Henkilötietolain (523/1999) säännös, jonka rikkominen säädetty rangaistavaksi	Tekotapa	**Rangaistussäännös ja rikosnimike**	**Syyksiluettavuuden aste**	Rangaistusasteikko
6 § käsittelyn suunnittelu	Laiminlyö noudattaa, mitä henkilötietojen käsittelyn tarkoitusten määrittelystä säädetään	HetiL 48.2 § 1 kohta Henkilörekisteririkkomus	Tahallisuus tai törkeä tuottamus	Sakko
7 § käyttötarkoitussidonnaisuus	Käsittelee henkilötietoja vastoin henkilötietolain käyttötarkoitussidonnaisuutta koskevia säännöksiä	RL 38:9 1 kohta Henkilörekisteririkos	Tahallisuus tai törkeä tuottamus	Sakko – 1 v vankeutta
8 § käsittelyn yleiset edellytykset	Käsittelee henkilötietoja vastoin henkilötietolain käsittelyn yleisiä edellytyksiä koskevia säännöksiä	RL 38:9 1 kohta Henkilörekisteririkos	Tahallisuus tai törkeä tuottamus	Sakko – 1 v vankeutta

9 § tietojen tarpeellisuus ja virheettömyys	Käsittelee henkilötietoja vastoin henkilötietolain henkilötietojen tarpeellisuutta tai virheettömyyttä koskevia säännöksiä	RL 38:9 1 kohta Henkilörekisteririkos	Tahallisuus tai törkeä tuottamus	Sakko – 1 v vankeutta
10 § rekisteriseloste	Laiminlyö noudattaa, mitä rekisteriselosteen laatimisesta säädetään	HetiL 48.2 § 1kohta Henkilörekisteririkkomus	Tahallisuus tai törkeä tuottamus	Sakko
11-12 § arkaluonteiset tiedot	Käsittelee henkilötietoja vastoin henkilötietolain arkaluonteisia tietoja koskevia säännöksiä	RL 38:9 1 kohta Henkilörekisteririkos	Tahallisuus tai törkeä tuottamus	Sakko – 1 v vankeutta
13 § henkilötunnus	Käsittelee henkilötietoja vastoin henkilötietolain henkilötunnusta koskevia säännöksiä	RL 38:9 1 kohta Henkilörekisteririkos	Tahallisuus tai törkeä tuottamus	Sakko – 1 v vankeutta
14-21 § käsittely erityisiä tarkoituksia varten	Käsittelee henkilötietoja vastoin henkilötietolain henkilötietojen käsittelyä erityisiä tarkoituksia varten koskevia säännöksiä	RL 38:9 1 kohta Henkilörekisteririkos	Tahallisuus tai törkeä tuottamus	Sakko – 1 v vankeutta

22-23 § ulkomaille siirto	Siirtää henkilötietoja Euroopan unionin tai Euroopan talousalueen ulkopuolisiin valtioihin henkilötietolain 5 luvun vastaisesti	RL 38:9 3 kohta Henkilörekisteririkos	Tahallisuus tai törkeä tuottamus	Sakko – 1 v vankeutta
24-25 § informointi	Laiminlyö noudattaa, mitä informoimisesta säädetään	HetiL 48.2 § 1 kohta Henkilörekisteririkkomus	Tahallisuus tai törkeä tuottamus	Sakko
26-28 § tarkastusoikeus	Antamalla rekisteröidylle väärän tai harhaanjohtavan tiedon estää tai yrittää estää rekisteröityä käyttämästä hänelle kuuluvaa tarkastusoikeutta	RL 38:9 2 kohta Henkilörekisteririkos	Tahallisuus tai törkeä tuottamus	Sakko – 1 v vankeutta
29 § tiedon korjaaminen	Laiminlyö noudattaa, mitä henkilörekisterissä olevan tiedon korjaamisesta säädetään	HetiL 48.2 § 1 kohta Henkilörekisteririkkomus	Tahallisuus tai törkeä tuottamus	Sakko
30 § kielto-oikeus	Laiminlyö noudattaa, mitä rekisteröidyn kielto-oikeudesta säädetään	HetiL 48.2 § 1 kohta Henkilörekisteririkkomus	Tahallisuus tai törkeä tuottamus	Sakko

32 ja 34 § tietojen suojaaminen ja hävittäminen	Rikkoo henkilötietojen suojaamisesta ja henkilörekisterin hävittämisestä annettuja säännöksiä ja määräyksiä	HetiL 48.2 § 3 kohta henkilörekisteririkkomus	Tahallisuus tai törkeä tuottamus	Sakko
33 § vaitiolovelvollisuus	Ks. ko. rangaistussäännös	RL 38:1 salassapitorikos	Tahallisuus	Sakko – 1 v vankeutta
”	Ks. ko. rangaistussäännös	RL 38:2 salassapitorikkomus	Tahallisuus	Sakko
”	Ks. ko. rangaistussäännös	40:5.1 virkasalaisuuden rikkominen 40:5.2 tuottamuksellinen virkasalaisuuden rikkominen	Tahallisuus Tuottamus	Sakko – 2 v vankeutta Sakko – 6 kk vankeutta
”	Ks. ko. rangaistussäännös	Mahdollinen erityissäännös		Erityissäännöksessä määritelty

36 § ilmoitusvelvollisuus	Laiminlyö noudattaa, mitä ilmoituksen tekemisestä tietosuojavaltuutetulle säädetään	HetiL 48 § 1 mom. 2 kohta Henkilörekisteririkkomus	Tahallisuus tai törkeä tuottamus	Sakko
39 § tietosuojaviranomaisten tiedonsaanti- ja tarkastusoikeus	Antaa tietosuojaviranomaiselle henkilötietojen käsittelyä koskevassa asiassa väärän tai harhaanjohtavan tiedon	HetiL 48.2 § 2 kohta Henkilörekisteririkkomus	Tahallisuus tai törkeä tuottamus	Sakko
43 § tietosuojalautakunnan lupatoimivalta	Rikkoo tietosuojalautakunnan 43 §:n 3 momentin nojalla antamaa lainvoimaista määräystä	HetiL 48.2 § 4 kohta henkilörekisteririkkomus	Tahallisuus tai törkeä tuottamus	Sakko
	Laiminlyö noudattaa, mitä tietojen käsittelystä säädetään	HetiL 48.2 § 1 kohta Henkilörekisteririkkomus	Tahallisuus tai törkeä tuottamus	Sakko
	Ks. ko. rangaistussäännös	RL 38:8 Tietomurto (myös yritys rangaistava)	Tahallisuus	Sakko – 1 v vankeutta

Rangaistavuuden lisäedellytyksenä **henkilörekisteririkkomuksen** osalta on, että **teko vaarantaa rekisteröidyn yksityisyyden suojaa tai hänen oikeuksiaan.**

Henkilörekisteririkoksen osalta lisäedellytyksenä on, että **teko loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa.**

Esimerkki tuomioistuimen ratkaisusta:

Korkein oikeus on ratkaisussaan (3.7.1998 nro 2261) katsonut, että henkilötietojen luovuttaminen vastoin rekisteröidyn suostumusta muuhun käyttötarkoitukseen kuin siihen, mihin tiedot oli rekisteröity on tyypillisesti yksityisyyden suojan perustavoitteiden vastaista. Kyse oli henkilötietojen luovuttamisesta suoramarkkinointia varten henkilöiden tietämättä ja vastoin nimenomaista kieltoa.

XMLSec-kirjasto, digitaaliset allekirjoitukset ja salaaminen

Juha J. Kari

XMLSec on C-kielellä toteutettu ohjelmointikirjasto, joka toteuttaa joukon World Wide Web Consortiumin (W3C) antamia suosituksia. Näitä suosituksia ovat mm. XML Signature ja XML Encryption. Tässä seminaarityössä käsitellään XMLSec-kirjaston toimintoja, digitaalisia allekirjoituksia ja tiedon salaamista W3C:n antamien suositusten valossa.

Avainsanat ja -sanonnat: XMLSec, XML Signature, XML Encryption, C-ohjelmointi, ohjelmointikirjastot.

Sisällys

1. Johdanto

Tiedon salaaminen kolmannelta osapuolelta on yleinen matemaattinen ja tietojenkäsittelytieteellinen ongelma, johon on kehitetty useita erilaisia ratkaisuja. Kryptografia viittaa tieteenalaan, joka tutkii paitsi mahdollisuuksia luottamukselliseen tietojen välittämiseen myös tiedon autentikoinnin, eheyden ja kiistämättömyyden kysymyksiä.

Tässä seminaarityössä esitellään XMLSec-ohjelmointikirjaston [Sanin, 2004] toimintoja, kirjaston toiminnan kannalta oleellisia kryptografisia peruskäsitteitä sekä World Wide Web Consortiumin (W3C) julkaisemia suosituksia, joita kirjasto noudattaa. Seminaarityössä annetaan esimerkkejä digitaalisen tiedon allekirjoittamisesta ja salaamisesta.

W3C:n antamia suosituksia tämän seminaarityön aiheeseen liittyen ovat XML (extended markup language) [Bray et al., 2004], XML Signature [Bartel et al., 2002], XML Encryption [Imamura et al., 2002] ja XML Key Management Specification [Hallam-Baker, 2004], joista kerrotaan tarkemmin seuraavissa luvuissa. Aluksi käsitellään joitakin kryptografian ja tietoturvallisuuden peruskäsitteitä.

Näyttää siltä, että Internetissä ei ole yksittäistä kaikenkattavaa tietoturvaprotokollaa. Tämä johtuu mm. Internetissä käytettävien laitteiden, sovellusten ja protokollien moninaisuudesta. Seminaarityössä selvitetään, kuinka XML:n avulla toteutetut laitteistoriippumattomat kielet helpottavat erilaisten ympäristöjen välistä tiedonsiirtoa ja miten tämä liittyy tietoturvallisuuteen.

Seminaarityössä pyritään vastaamaan kysymyksiin, kuinka XMLSec tukee avoimia suosituksia, mistä osista se koostuu ja millaisiin käyttötarkoituksiin se sopii. XMLSec-kirjastolla on samalle sovellusalueelle suunnattuja kilpailijoita [Apache, 2004] [Gapxse, 2001], mutta niitä ei käsitellä tässä tutkimuksessa. Myös salausmenetelmien matemaattisen taustan käsittely rajataan tutkimuksen ulkopuolelle.

2. Kryptografia

Koska XMLSec käyttää useita salausmenetelmiä, tässä esitellään kryptografian perusteita. Kryptografiassa tarkastellaan viestiä, jonka lähettäjä haluaa välittää luottamuksellisesti vastaanottajalle. Tiedonvälitykseen liittyviä ongelmia ovat [Schneier, 1996]:

- autentikointi,
- eheys ja
- kiistämättömyys.

Ilman kryptografisia menetelmiä edellä mainittuihin ongelmiin olisi vain helposti murrettavia ratkaisuja. Hyökkääjäksi kutsutaan henkilöä, joka yrittää murtaa autentikoinnin, eheyden tai kiistämättömyyden varmistamiseen käytetyn järjestelmän.

Viestin vastaanottajan on päästävä varmuuteen viestin lähettäjän henkilöllisyydestä – tätä kutsutaan autentikoinniksi (authentication). Kryptografisesti varman autentikoinnin ansiosta hyökkääjä ei voi esiintyä toisena henkilönä.

Eheys (integrity) tarkoittaa tässä sitä, että hyökkääjä ei saa päästä muokkaamaan lähettäjältä vastaanottajalle kulkevaa dataa. Vastaanottajalla on oltava mahdollisuus eheyden varmistamiseen.

Viestin lähettäjälle ei saa antaa mahdollisuutta siihen, että hän voisi kiistää lähettäneensä viestin. Kiistämättömyys (nonrepudiation) voidaan toteuttaa tapahtumatietojen tallentamisella (audit logging), kuten pankkien tietojärjestelmissä tehdään.

3. W3C ja XML-suositukset

3.1. XML

XML:n taustalla on World Wide Web Consortiumin suositus, joka määrittelee kielen syntaksin. Myös XML Encryption ja XML Signature perustuvat W3C:n suosituksille.

XML on metakieli eli sen avulla voidaan luoda uusia kieliä. XML:n avulla luotu merkkauskieli on XML-sovellus, jolle voidaan antaa muodollisen kieliopin määrittävä rakennekuvaus (document type definition, DTD).

XML-dokumentti on hyvin muodostettu (well-formed) jos se noudattaa W3C:n määrittämää XML:n kielioppia. Validi (valid) XML-dokumentti tarkoittaa hyvinmuodostettua dokumenttia, joka noudattaa omaa rakennekuvaustaan (document type definition).

XML:n yleinen syntaksi koostuu muutamista yksinkertaisista säännöistä, jotka kuvataan kielen määrittelydokumenteissa [Bray et al., 2004]. XML-tiedostot koostuvat sisäkkäisistä elementeistä, joilla voi olla joukko attribuutteja.

3.2. XML Signature

XML Signature (XML-allekirjoitus) tarjoaa eheyden (integrity), viestin autentikoinnin (message authentication) ja allekirjoittajan autentikoinnin (signer authentication) palveluja. XML-allekirjoituksia voidaan soveltaa mihin tahansa digitaaliseen tietoon, mukaanlukien XML [Eastlake et al., 2002].

Seminaarityössä käsitellään digitaalisen tiedon allekirjoitusta ja salausta, mutta vertailun vuoksi voidaan esittää syitä, joiden perusteella käsinkirjoitettuihin allekirjoituksiin luotetaan [Zhou and Deng, 2000]:

- Allekirjoitusta on vaikea väärentää erityisesti normaalilla kirjoitusnopeudella, koska allekirjoitus on ’harjoiteltu refleksi’.
- Allekirjoitus on helposti varmistettavissa. Perinteisesti allekirjoitusta verrataan silmin toiseen aidoksi tunnettuun allekirjoitukseen.

- Allekirjoitus ei ole uudelleenkäytettävä vaan se on osa dokumenttia, johon se kirjoitettiin. Allekirjoitusta ei voi leikata ja liittää toiseen dokumenttiin.
- Allekirjoitettu dokumentti on muuntamaton (mutta rajoitetusti). Allekirjoitus varmistaa vain dokumentin yhden sivun alkuperän ja aitouden
- Allekirjoitus on osa kiistämätöntä todistetta, jota voidaan käyttää apuna erimielisyyksien sovittelussa.

Digitaalisilla allekirjoituksilla on tiettyjä etuja käsinkirjoitettuihin allekirjoituksiin nähden: digitaalinen allekirjoitus voidaan liittää nopeasti mihin tahansa binäärimuodossa olevaan tietoon ja allekirjoitettuja tietoja voidaan välittää tietoverkkojen yli.

Käsintehtyjen allekirjoitusten tapauksessa luotetaan yleisesti lähinnä alkuperäiseen allekirjoitettuun asiakirjaan, joten allekirjoitettua asiakirjaa ei voi monistaa pyytämättä allekirjoittajalta aitoa allekirjoitusta jokaiseen kopioon erikseen.

Toisaalta digitaalisen allekirjoituksen varastaminen onnistuu varastamalla käyttäjän salausavain. Kykyä käsintehtävään allekirjoitukseen ei voi suoranaisesti varastaa ellei kyse ole allekirjoituksen väärentämisestä tai ihmisen pakottamisesta tietyn paperin allekirjoittamiseen.

Digitaalisen allekirjoituksen luotettavuus vaarantuu salaisen avaimen paljastumisen myötä – siksi tarvitaan menetelmä avaimen mitätöimiseen. Mitätöinnin jälkeen tehtyjä allekirjoituksia ei tällöin pidetä pätevinä. Ennen mitätöintiä tehtyjen allekirjoitusten tulee silti pysyä voimassa. Yleensä mitätöintiin tarvitaan luotettu kolmas osapuoli, joka pitää kirjaa allekirjoitusten voimassaolosta. XMLSec-kirjasto ei kuitenkaan vastaa tähän mitätöintitarpeeseen.

XML Signature -suosituksen mukaan allekirjoitetussa XML-tiedostossa kerrotaan allekirjoitukseen käytetty algoritmi, avaintiedosto, allekirjoitettu tieto, tiivistefunktion tuloste ja varsinainen allekirjoitus. Esimerkkitiedosto havainnollistaa allekirjoitetun tiedon esitystapaa:

```
<?xml version="1.0" encoding="UTF-8"?>
<Envelope xmlns="urn:envelope">
  <Data>
    Hello, World!
  </Data>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod
        Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod
```

```
        Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="">
        <Transforms>
          <Transform
            Algorithm=
            "http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod
          Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>8iyeo+RSQJwW1S/C1ZnCL8nFzG8=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>
b5rXfKtru/efOD3NWGb3WZvW5Eiuw3IBSdE5dAOlVGcnfbXeXQ+5mrgQCuqam8w5
IWwYwDWpgKRYAlBVhSGhDm4VN9Zc8LzKGhBIKCl1b7whyaH87nzK3GLo9Oih/Lhj
KooXm4qCDkNTNYhAaonHWKCQSNytHw0/xcNzwRdB8ss=</SignatureValue>
    <KeyInfo>
      <KeyName>/home/user/newkey.pem</KeyName>
    </KeyInfo>
  </Signature>
</Envelope>
```

Esimerkissä on käytetty tiivisteen luomiseen SHA1-algoritmia, jonka XML-skeema on osoitteessa http://www.w3.org/2000/09/xmldsig#sha1. Allekirjoituksessa on käytetty RSA-algoritmia, jonka XML-skeema sijaitsee osoitteessa http://www.w3.org/2000/09/xmldsig#rsa-sha1. Allekirjoittamiseen käytetty avain on sijainnut allekirjoitushetkellä käyttäjän tietokoneella tiedostossa /home/user/newkey.pem. Digitaalinen allekirjoitus esitetään SignatureValue-elementissä.

3.3. XML Encryption

XML Encryption on W3C:n suositus salatun tiedon esittämiseen XML-dokumenttina. Salatussa XML-tiedostossa kerrotaan salaukseen käytetty algoritmi, avaintiedosto ja salattu tieto. Esimerkkitiedosto havainnollistaa salatun tiedon esitystapaa:

```
<?xml version="1.0"?>
<EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#">
  <EncryptionMethod
    Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
```

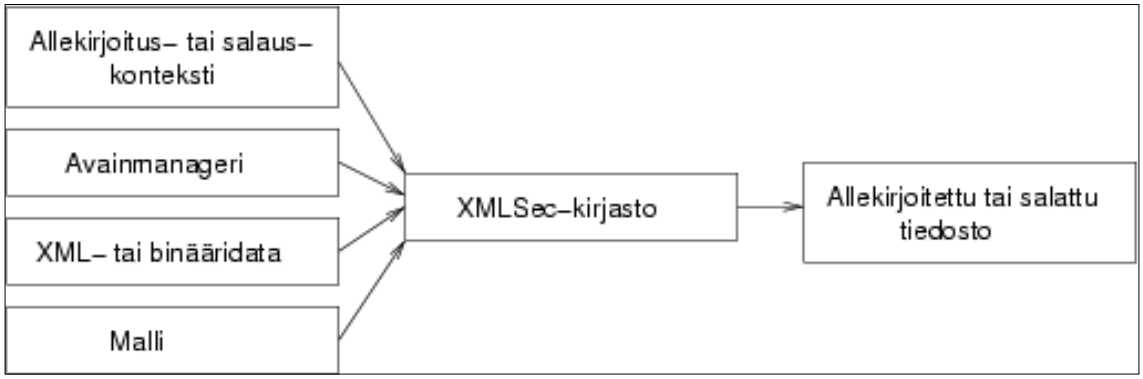
```
  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <KeyName>/home/user/newkey.pem</KeyName>
  </KeyInfo>
  <CipherData>
    <CipherValue>sOvv5lh4HzrOtevhSrKuy69X0afGDOUH</CipherValue>
  </CipherData>
</EncryptedData>
```

Tässä esimerkissä on käytetty Triple DES -algoritmia, jonka XML-skeema sijaitsee osoitteessa http://www.w3.org/2000/09/xmldsig#rsa-sha1. Salaamiseen käytetty avain on sijainnut salaushetkellä käyttäjän tietokoneella tiedostossa /home/user/newkey.pem. Salattu tieto esitetään kryptatussa muodossa CipherValue-elementissä.

4. XMLSec

XMLSec-kirjasto on C-kielellä toteutettu kryptografisia palveluita tarjoava ohjelmointikirjasto, joka vastaa autententikoinnin, eheyden ja kiistämättömyyden ongelmiin toteuttamalla seminaarityön aiemmissa luvuissa käsitellyt W3C:n suositukset. Kirjasto on modulaarinen ja laajennettavissa. Toisaalta kaikkia XMLSec-kirjaston lähdekoodin sisältämiä toimintoja ei ole pakko kääntää mukaan kirjaston binäärimuotoiseen versioon [Sanin, 2004b] – näin voidaan säästää levy- ja muistitilaa.

Kirjasto ottaa vastaan syötteenä allekirjoitus- tai salauskontekstin, XML- tai binääridataa, mallin sekä avainmanagerin, kuten Saninin kuvauksen [Sanin, 2004c] pohjalta laaditusta kuvasta 1 nähdään. Allekirjoitusoperaation tuloksena saadaan XML Signature -suosituksen mukainen allekirjoitettu XML-tiedosto (ks. Luku 3.2) ja salausoperaation tulosteena XML Encryption -suosituksen mukainen salattu XML-tiedosto (ks. Luku 3.3).



Kuva 1: XMLSec-kirjastolle annettavat syötteet ja kirjaston tuloste.

Kuvassa esitetyt XMLsec-kirjaston syötteet esiintyvät ensisijaisesti ohjelmointikontekstissa, joten kirjastoa käyttävän ohjelmoijan on osattava esittää nämä

tiedot oikeassa muodossa. XMLSecin käyttöohjeet kertovat tarkemmin oikeasta käyttötavasta.

4.1. Lisenssi

XMLSec on julkaistu MIT-lisenssillä [MIT, 2004], joten kirjastoa voidaan käyttää sekä kaupallisissa että avoimen lähdekoodin sovelluksissa. MIT-lisenssin mukaan kirjastoa saa käyttää, kopioida, muokata, yhdistää, julkaista, jakaa, alilisensoida ja myydä, jos alkuperäinen lisenssiteksti säilytetään uusissa sovelluksissa.

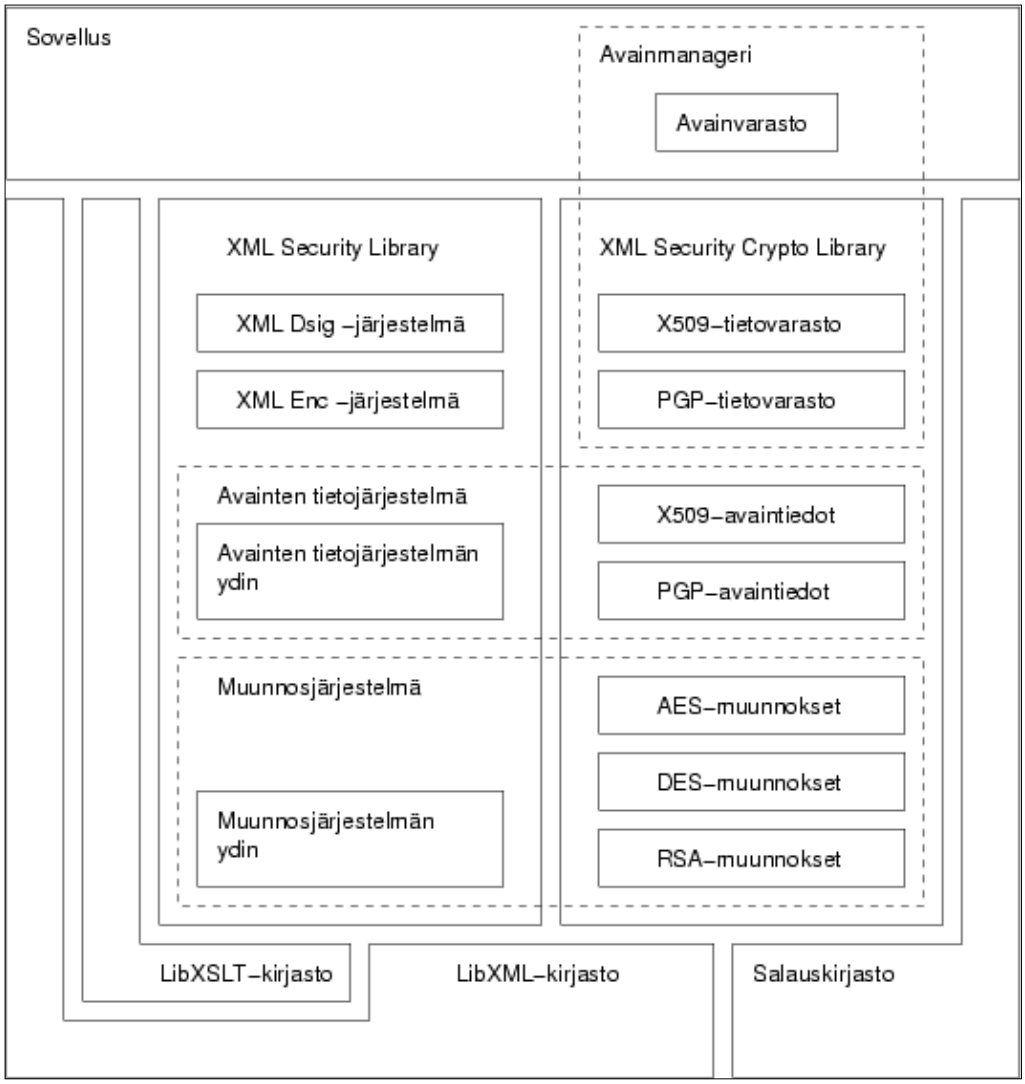
4.2. XMLSec-kirjaston perustoiminnot

XMLSec-kirjastoon kuuluvat seuraavat toiminnot :

- dokumenttien allekirjoittaminen ja salaaminen,
- dynaamisten mallien (template) luominen,
- allekirjoitusten varmistaminen ja salatun dokumentin purkaminen,
- avaimet,
- avainmanageri,
- X509-sertifikaattien käyttäminen,
- muunnokset ja muunnosketjut,
- kontekstiolioiden käyttäminen ja
- tuen lisääminen uusille salauskirjastoille.

4.3. XMLSec-kirjaston rakenne

Kuvassa 2 esitellään XMLSec-kirjaston rakenne Saninin kuvauksen pohjalta mukailtuna [Sanin, 2004d]. XMLSec-kirjasto on rakenteeltaan modulaarinen eli sovellus koostuu selkeästi erotettavista osista, joita voidaan kehittää erillään toisistaan. XMLSec voidaan jakaa kolmeen osaan: XML Security Library, XML Security Crypto Library ja apukirjastot. Kuvan yläreunassa kuvattu XMLSeciä käyttävä sovellus on neljäs osa.

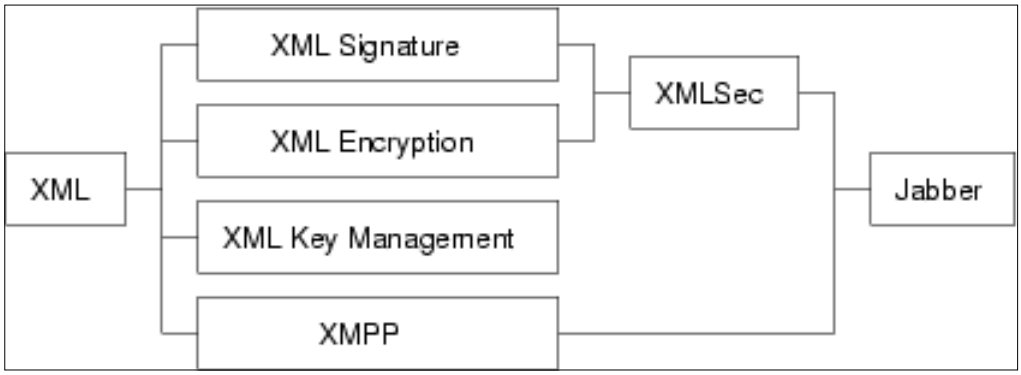


Kuva 2: XMLSec-kirjaston rakenne.

5. Jabber – esimerkki XML:n soveltamisesta

5.1. Mikä Jabber on?

Jabber on joukko avoimia XML-protokollia viestien reaaliaikaiseen vaihtoon kahden Internetissä sijaitsevan pisteen välillä [Jabber, 2004]. Protokollat luotiin laite-, käyttöliittymä- ja sovellusriippumattomien pikaviestiohjelmien (instant messaging software) käyttöön, mutta samaa arkkitehtuuria voi käyttää myös muissa verkkosovelluksissa.



Kuva 3: Jabberin riippuvuudet käytettäessä XMLSec-kirjastoa.

Jabberista on useita erilaisia toteutuksia eri ohjelmointikielillä [Jabber, 2004b]. XMLSec-kontekstiin Jabber liittyy lähinnä C-kielisten toteutustensa vuoksi. Kuten erilaisten toteutusten listasta nähdään, Jabberin suunnitteluongelmat on ratkaistu useilla tavoilla. Eräs toteutustapa Jabber-protokollien kuljettaman tiedon salaamiseen on XMLSec-kirjaston käyttäminen – tätä havainnollistetaan kuvassa 3.

5.2. Jabberin sovelluskohteita

Jabber-protokollien avulla voitaisiin esimerkiksi toteuttaa Internetin sähköpostijärjestelmä uudelleen [Hearn, 2001]. Koska Jabber tukee viestien salausta, protokollien avulla välitetty posti kulkisi automaattisesti salattuna Internetin yli. Perinteisen sähköpostin ongelmiin kuuluu myös heikosti toteutettu tuki erilaisille merkistöille. XML:n perusperiaatteisiin kuuluu tiedostossa käytettävän merkistön ilmoittaminen jokaisen dokumentin alussa, metatietojen joukossa, joten merkistöjen tulkinnassa ei voi tulla sekaannuksia lähettettäessä postia vaikkapa Aasiasta Eurooppaan.

6. Yhteenveto

Tässä seminaarityössä on esitelty XMLSec-kirjaston toimintaa, World Wide Web Consortiumin suosituksia ja annettu esimerkki näiden tekniikoiden mahdollisesta sovelluskohteesta. Koska tiedon allekirjoittaminen ja salaaminen ovat tärkeitä tietojenkäsittelytieteellisiä ongelmia, ala kehittyy jatkuvasti.

XMLSec-kirjaston avulla toteutettu Jabber-protokollajoukko tarjoaa menetelmän Internetin sähköpostijärjestelmän uudistamiseen siten, että sähköpostin välityksessä esiintyvät merkistö- ja tietoturvaongelmat vähenevät.

Viiteluettelo

[Apache, 2004] The Apache Software Foundation, *Apache XML Security*. http://xml.apache.org/security/ (tarkistettu 31.5.2004).
[Bartel et al., 2002] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia and Ed Simon, *XML-Signature Syntax and Processing*. http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/ (tarkistettu 31.5.2004).
[Bray et al., 2004] Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, Eve Maler and François Yergeau, *Extensible Markup Language (XML) 1.0 (Third Edition)*. http://www.w3.org/TR/2004/REC-xml-20040204/ (tarkistettu 31.5.2004).
[Gapxse, 2001] University of Pisa, *Gapxse*. http://gapxse.sourceforge.net/ (tarkistettu 31.5.2004).
[Hallam-Baker, 2004] Phillip Hallam-Baker (ed.), *XML Key Management Specification (XKMS 2.0)*. http://www.w3.org/TR/2004/CR-xkms2-20040405/ (tarkistettu 31.5.2004).
[Hearn, 2001] Michael Hearn, *Jabber DevZone News - Jabber Email?*. http://www.jabber.org/pipermail/jdev/2001-May/006642.html (tarkistettu 31.5.2004).
[Imamura et al., 2002] Takeshi Imamura, Blair Dillaway and Ed Simon, *XML Encryption Syntax and Processing*. http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/ (tarkistettu 31.5.2004).
[Jabber, 2004] Jabber, Inc, *Jabber Develop FAQ*. http://www.jabber.org/developer/devfaq.php (tarkistettu 31.5.2004).
[Jabber, 2004b] Jabber, Inc, *Jabber Software Libraries*. http://www.jabber.org/software/libraries.php (tarkistettu 31.5.2004).
[MIT, 2004] Open Source Initiative OSI, *The MIT Licence*. http://www.opensource.org/licenses/mit-license.html (tarkistettu 31.5.2004).
[Sanin, 2004] Aleksey Sanin, *XML Security Library*. http://www.aleksey.com/xmlsec/ (tarkistettu 31.5.2004).
[Sanin, 2004b] Aleksey Sanin, *XMLSec Frequently Asked Questions*. http://www.aleksey.com/xmlsec/faq.html (tarkistettu 31.5.2004).
[Sanin, 2004c] Aleksey Sanin, *XML Security Library Reference Manual: Signing and encrypting documents*. http://www.aleksey.com/xmlsec/api/xmlsec-notes-sign-encrypt.html (tarkistettu 31.5.2004).
[Sanin, 2004d] Aleksey Sanin, *XML Security Library Reference Manual*. http://www.aleksey.com/xmlsec/api/xmlsec-notes-structure.html (tarkistettu 31.5.2004).
[Schneier, 1996] Bruce Schneier, *Applied Cryptography*. Wiley, 1996.
[Eastlake et al., 2002] D. Eastlake, J. Reagle and D. Solo, *(Extensible Markup Language) XML-Signature Syntax and Processing*. http://www.ietf.org/rfc/rfc3275.txt (tarkistettu 31.5.2004).
[Zhou and Deng, 2000] Jianying Zhou and Robert Deng, *On the Validity of Digital Signatures*. http://www.acm.org/sigcomm/ccr/archive/2000/april00/Zhou_final2.pdf (tarkistettu 31.5.2004).

Identity management

Seppo Heikkinen
Tampere University of Technology
Institute of Communications Engineering

The proliferation of electronic identities has resulted in security and usability problems, because people have problems in managing these identities and the credentials attached to them. It is especially challenging for people to remember all the various passwords. Identity management systems try to provide solutions that could take care of these problems by managing the user identity on behalf of the user and providing means for transferring the identities seamlessly among different services. This essay considers one such system envisaged by the Liberty Alliance specifications.

Keywords: identity management, electronic identity, Liberty Alliance

Table of contents

1 Introduction

Philosophers and sociologists may have several interesting things to say about identity, but for the purposes of our discussion it is sufficient to say that an identity, and especially an electronic identity, is a collection of different kinds of attributes. These attributes can be loose or strong based on the fact how defining they are, so a strong attribute has potential of uniquely identifying a subject. To some extent they could also be called the credentials, even though strictly speaking an identity defines what an entity is and the credentials provide a certain level of assurance of this. A simple example of this is a login and a password: the login provides an identity that has meaning in some context like multiuser operating system and the password provides assurance that the subject has right to assume the particular identity. This example also shows that the identity also has a context, even though we could also speak about different roles and reflections of the core identity, which would be the sum of all the possible attributes of an entity.

Identity management is the general term for measures that are taken to create, store, modify, use and delete these identities, so it can have a rather broad scope. From the user point of view the management of identities can be seen as burdensome, because the amount of identities is increasing all the time and it can be hard to remember abstract credentials like PINs. So there is incentive to let someone else take care of the routines involved and ensure the security that otherwise might be just dependant on the fact how well you have hidden the note containing all your passwords. On the other hand, it would also be nice if this identity could be used in the most convenient way between the different types of services without involving user action. This type of seamless access is the thing that increases user satisfaction and it also reduces complexity. From the enterprise point of view there is also strong motivation to have identities managed centrally so that the changes as well as the access and authorisation policies are easily managed. This has clear cost benefits. The possibility to provide and use assured identities is also a major enabler for the electronic commerce.

On the enterprise level it is somewhat easy to resort to more proprietary solutions, like for example solutions that are based on Windows Active Directory, but when we travel across the administrative boundaries more standardised solutions are needed. This is due to environments that may have quite varied technological base.

Especially if we look bit farther into the future, when Ambient Intelligence visions with pervasive computing become reality and the user identity is used all around across heterogeneous technologies. This paper considers one potential solution, Liberty Alliance.

The paper is organised as follows. The next chapter briefly goes through some of the underlying technologies. The third chapter takes a closer look at Liberty Alliance and its specifications. Finally, a summary is presented.

2 Enabling technologies

The identity system specifications cannot define all the things themselves and it would not even be a feasible approach. For better support and wider acceptance it is useful to take advantage of the already available technology. This chapter briefly goes through a couple of such key technologies.

2.1 Digital signatures

A digital signature is, as the name implies, the electronic counterpart of the traditional signature. Its main use is to tie together some data and an identity of some entity, which is not necessarily a person. With digital signatures it is possible to assure that some piece of data really is authentic and approved by a certain entity. An implication of this is one desired property of the digital signatures, non-repudiation. This means that at some later time an entity cannot dispute the data it has signed.

The digital signatures are implemented with the help of public-key cryptography, which takes advantage of the asymmetric nature of the involved mathematical operations [1]. In such systems we have a private and a public key, which correspond to each other in such way that the data encrypted with the private key can only be opened with the relevant public key. The names of the keys imply their use: a public key can be published so everybody can encrypt data targeted only to the owner of the private key. This can work in the other direction as well: if some data is encrypted with the private key, everybody can verify with the public key that only the owner of corresponding private key could have encrypted the data. The digital signatures take advantage of this feature. Probably the best known algorithm for implementing such public-key based cryptosystem is RSA [2].

Public-key operations are mathematically rather demanding so in practise the digital signature is implemented with the help of hashes. Hash is a relatively short

digest that is calculated from the original data with the help of one-way function which ensures that the hash does not reveal anything about the original data. After the hash calculation it can be encrypted with the private key of the user. This encrypted hash forms the actual signature.

Because the usability of a detached encrypted hash in itself is not very good in the various message exchanges, there has been motivation to create standardised formats that can pack the signature and the data together or otherwise tie them together. One rather well known and widely spread de facto standard is PKCS#7 [3]. IETF calls its standardised version Cryptographic Message Syntax (CMS) [4], to which, for example, S/MIME is based on [5]. Another standard that is starting to gain popularity is XML Signature specification. It is XML based and as such is well suited for the web based services and applications [6].

2.2 PKI

Even though the digital signatures can bind data and private keys together, they really do not tell anything about the entities behind the private keys. Therefore the problem is to also find the binding between the private key and the entity. One such solution is Public Key Infrastructure (PKI) [7].

In PKI systems we need authorities that can guarantee that a certain private key is associated with a certain entity. Strictly speaking such association is made between the public key and the entity. The entity is expected to keep its private key secret. In PKI world the authorities are called Certification Authorities (CA) and they issue certificates in which they bind by their own digital signature the public key to the name of the individual or to some organisation which then may have the possibility to become a CA itself, thus creating hierarchical trust paths. Of course one can debate how accurate and relevant the naming is as well as other murky issues like those described in [8], but that's out of the scope of this paper. In the end it all boils down to the fact: Who do you trust?

The certificates need naturally a standardised format and one widely used is the X.509 specification and especially the third version of it [9]. This enables one to introduce granularity to the certificates so that a certificate can have different types of uses, e.g. one certificate is valid for email encryption whereas some other is valid for a digital signature. In other words, different types of policies may be imposed.

One important aspect of the certificates is their lifetime. Usually the certificates have a validity period, after which they have to be renewed. It is also possible that for some reason the certificate has to be revoked, i.e. it has to be invalidated. This can happen, for example, if the private key is lost or stolen or the subject of the certificate has misbehaved. In order to implement this untimely revocation, a CA can publish certificate revocation list (CRL) that lists its unexpired certificates that are not valid anymore. However, it is the responsibility of the party receiving the certificate to check the list before deciding to trust the said certificate.

2.3 HTTP

HyperText Transport Protocol (HTTP) in itself has little to do with the identity management, but being one of the core technologies of the current World Wide Web (WWW), it is worth mentioning briefly some of the properties that the identity management systems can take advantage of. Basically, HTTP is a transport protocol that just transfers data in request-response fashion between a client (e.g. browser) and a server (e.g. web server). Simply put, it has a header section that gives metainformation related to the actual data contained in the body section. The body section can also be empty, especially if the client is just requesting access to some resource. [10]

From the point of view of identity management systems an interesting property is the possibility to respond with status that indicates that the desired resource has moved to other location and give the address of the new location with a Uniform Resource Locator (URL). In normal operation client follows these instructions and tries to access the new location right away, so this redirection can be quite transparent for the actual user. URL can also contain other kind of information besides addressing appended to it [11]. Because the client uses this full URL to access the new location, the server at the new location gets the additional information as well. So this method can be used to convey information between the original and the new server without the client having to take any special actions.

HTTP is a stateless protocol, i.e. subsequent requst-response -pairs do not have any correspondence on the protocol level. There exists an extension mechanism called cookie that adds extra HTTP headers with name-value -pairs, which can be used to keep some stateful information between the different requests provided that the browser supports the extension. As a security measure those values can only be

read in the same domain that set the values. So it is possible, for example, to use this to contain the information whether a user is already logged into a specific site so that the same login information can be reused without having to ask the user to log into every single page individually. [12]

2.4 SAML

Security Assertion Markup Language (SAML) is an XML based language for conveying security related assertions. In practise this means that these assertions are statements made by a reliable party that guarantees some characteristics of an entity. The characteristics can be related to the authentication status or attributes of an entity. The values for the attributes are not defined in the specification, but means for other organisations to define them have been provided. It is also possible that these assertions grant authorisation to a resource or rather that the reliable party thinks that the entity has the right to access the resource probably based on predefined access policy. The party that receives the assertion is still responsible for enforcing the actual access control to the resources. [13]

Basically, SAML is a request-response -protocol that has two parties: relying party and asserting party or SAML authority. They exchange information, in practise XML documents, about the user party or subject. Therefore SAML authority has some information about the subject and possibly about the authentications it has made. This information can also include the identity of the subject as it is known to the SAML authority. The relying party can use the provided information to check how reliable the subject is considered to be by the authority. Of course, there must be a trusted relationship between the relying party and the SAML authority so that the statements of the SAML authority can have value. This can be achieved, for example, with the help of PKI and common trust roots. In other words, the parties have to find a common entity that they both can trust.

SAML specifications define the protocol for exchanging assertions but the specifications also define bindings to the actual transport protocols so that the assertions can be "fitted" to them. There are also profile specifications that give guidelines how SAML is used in particular application cases, like single sign-on (SSO). The current version 1.1 of the SAML specification so far has defined bindings for using Simple Object Access Protocol (SOAP) and HTTP as transports and artifact and form profiles for web based SSO. [14]

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  MajorVersion="1"
  MinorVersion="1"
  AssertionID="buGxcG4gILg5NlocyLccDz6iXrUa"
  Issuer="www.acompany.com"
  IssueInstant="2002-06-19T17:05:37.795Z">
            <saml:Conditions NotBefore="2002-06-19T17:00:37.795Z"
              NotOnOrAfter="2002-06-19T17:10:37.795Z"/>
            <saml:AuthenticationStatement
              AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password"
              AuthenticationInstant="2002-06-19T17:05:17.706Z">
                        <saml:Subject>
                                  <saml:NameIdentifier
                                    NameQualifier=http://www.acompany.com
                                    Format="http://www.customformat.com/">
                                    uid=joe
                                  </saml:NameIdentifier>
                                  <saml:SubjectConfirmation>
                                            <saml:ConfirmationMethod>
                                              urn:oasis:names:tc:SAML:1.0:cm:artifact-01
                                            </saml:ConfirmationMethod>
                                  </saml:SubjectConfirmation>
                        </saml:Subject>
            </saml:AuthenticationStatement>
</saml:Assertion>
```

Figure 1. SAML assertion example

In the artifact profile the subject receives a small character string, artifact, from the SAML authority after the subject has authenticated itself. The subject can at later time present this artifact to the site the subject wants to access, i.e. relying party. This site then contacts the SAML authority and can request the assertions that were made based on the authentication of the subject. Figure 1 gives as an example one simple assertion [15]. The form profile has similarities with the artifact profile, but there the subject itself (or rather its browser) carries the assertion. This can be done with the help of HTML form, which contains the assertion made by the authority and which can be submitted to the destination site. Of course, it is required that the assertions are protected and this can be achieved by the digital signature of the authority. Because we are discussing about XML based protocol here, XML Signature specification is the natural choice. The transport channel should be protected as well and one can use, for example, Transport Layer Security (TLS) protocol for that. [14]

3 Liberty Alliance

This chapter goes through the identity management framework called Liberty Alliance. The specifications are quite extensive in terms of features and content so the chapter concentrates mainly on the issues that are feasible to provide today in regular web browser environment, i.e. identity federation and single sign-on.

3.1 History

Liberty Alliance Project was formed in 2001 by initiative of Sun Microsystems and the idea was to form something to compete with the Passport system introduced by Microsoft. They both aim at providing a system for managing user identities and for enabling single sign-on services. The difference was that the Passport system was much more closed and run in a centralised fashion by Microsoft whereas Liberty Alliance aimed to be an open and distributed system. [16]

3.2 Architecture

The main focus of Liberty Alliance (LA) is the network identity. Especially the term federated identity forms the core of the ideology. It means that a user is able to link several different identities originating from various different sites. This linking means that the user is able to use one single identity to authenticate itself and this authentication is sufficient to grant access to the other sites that are part of the federation, i.e. this enables single sing-on. LA terminology defines also the different parties involved in the federation procedure. Identity Provider (IdP) is the party that is responsible for taking care of the user authentication and it also provides the identity that is federated to Service Providers (SP). The federation requires that these parties have trusted relationships with each others and in practise business agreements are required as well. This group that has linked identities and have mutual business agreements can be called a circle of trust. Figure 2 shows the central components of Liberty Alliance architecture and their relations along with some of the technological choices. It is worthwhile to note that a user still has individual identities at different SPs, but they are mutually linked to the identity at the IdP and internally referenced with random identifiers. It is also possible that the user has several IdPs and it is even possible to federate between these. [17]

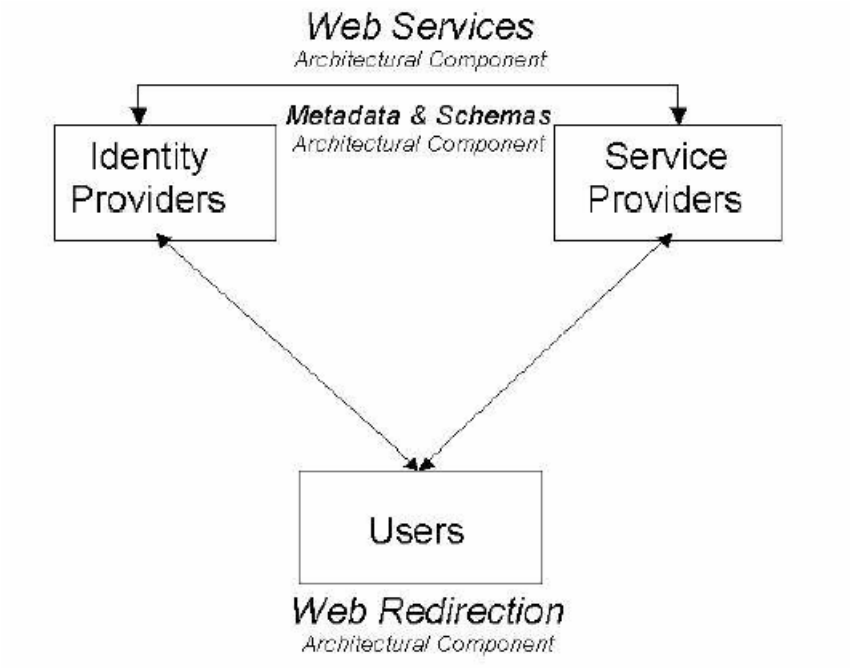


Figure 2. Liberty Alliance architecture components

3.3 Technical functionality

On practical level LA specifications make heavy use of SAML specifications and define some enhancements to the message exchanges, but basically it is about transferring different types of assertions on top of HTTP. Like SAML, LA defines profiles for different types of application environments and uses. For example, in order to implement SSO it is possible to use artifacts or HTML forms like in SAML. In addition, assertions can be transferred with direct connections using HTTP as well as SOAP. For typical web browser use the assertions can also coded bit differently: They can be appended to the URLs or included as a field of an HTML form. Figure 3 shows the flow of information in the case of SSO and artifact profile [16]. At first a user is trying to access some service provider, whose responsibility is to figure out the used identity provider. After this, the SP can give the user a page that directs her, using HTTP redirect, to the IdP site. The redirection contains a request for the IdP to send information about the user. After arriving to the IdP site the authentication state of the user is checked. At this point it could be possible to authenticate the user if it was not already done. In the next step the IdP redirects the user or rather the browser back to the SP and includes its response containing an artifact. After getting this artifact, the SP can contact the IdP and request the assertion that the given artifact references. The SP receives the relevant assertion and can then grant access to the

user. The whole arrangement may seem overly complex, but the reason is that the system tries to take advantage of the existing systems as much as possible, so that neither extra software nor plugins were needed at the user side. [18]

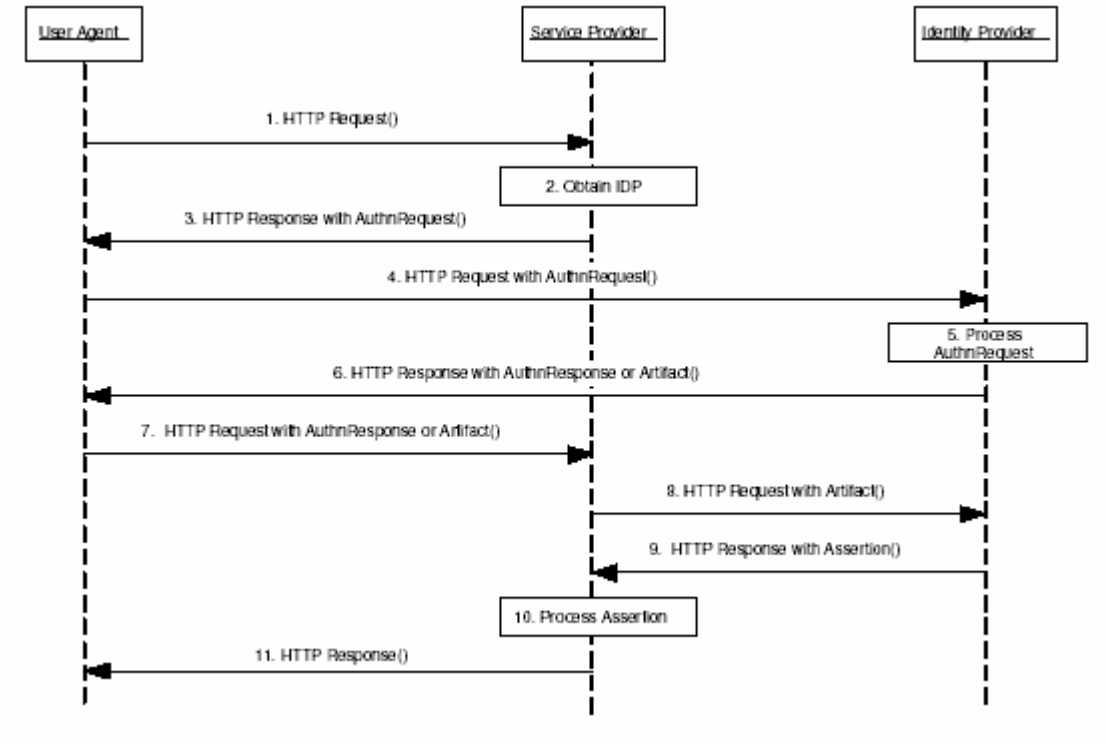


Figure 3. Liberty Alliance SSO transaction

3.4 Future directions

The previous chapters shed some light on how the single sign-on and identity federation are done according to the Liberty Alliance specifications. However, it is just part of the first phase of the specifications, even though the most dominant at the moment. At later phases the specifications are more concerned about Web Services Framework (WSF) that builds the base for making interoperable identity services and sharing permission based attributes. As the name suggests these specifications rely on emerging Web Services standards. There exists also other standards that plan on providing identity management mechanisms for Web Services and one such proposal is WS-Federation by IBM and Microsoft, but it does not seem to have any endorsement by standards bodies or bigger consortiums yet [19].

3.5 Security issues

As was seen the user browser has central role in providing LA functionality in practise. So if the browser is subverted by means like malicious software component,

there is little that can be done, but other kind of threats are addressed by specifications. According to the specifications the traffic between the parties should be protected with TLS/SSL-solutions, when it is also possible to use certificates to authenticate the parties [20] and a minimum requirement is that the server side has such certificates. The use of TLS is especially important in the case when the assertions are transferred using the user party as a conducting channel, i.e. browser is directed back and forth between the SP and the IdP.

It is good to remember that on the message level this does not necessarily provide non-repudiation and this aspect can arise especially in cases when the traffic does not go directly between two parties but uses intermediary hops or proxies. Integrity and the confidentiality of the message level can be protected with XML based security solutions like XML Signature [6] and XML Encryption [21]. The use of these techniques with SOAP is also being standardised and LA is planning on using this Web Services Security specification in its later phases [22].

In all of these techniques an important aspect is the trust between the parties, because the SP has to rely on the IdP to make the correct assessments about the users and that the received assertions are reliable. It is possible to use PKI systems for handling this, but generally it demands agreements made beforehand. PKI can provide trust at the technical level, but in the real production environments issues have to be considered from the commercial and political viewpoints as well.

Equally important with the message security is the user privacy, so the specifications have to make sure that the user has the possibility to interact with other parties without endangering her privacy. To this end, the user identifiers can be encrypted or they can be replaced by pseudonyms. It is also possible to provide total anonymity when accessing some service even though the user may be authenticated at the IdP. In this case the IdP just assures the SP that the said user is trusted. The later phases of the specification take this bit further and make it possible to inquire user every time her identity information is going to be used to provide some service. When talking about user privacy , it should be, however, noted that the IdP may have some chance to violate user privacy for example by collecting information about the sites user accesses. It might be reasonable to associate this information with phone call records, though. In this case, the use of this information would be restricted by law [23].

3.6 Microsoft Passport

Microsoft Passport is not part of Liberty Alliance specification, but it is briefly introduced here for the sake of comparison. Passport is an authentication service whose purpose is to provide SSO (even though Microsoft uses the term Single Sign-In, SSI) between different WWW sites. Nowadays it is also integrated to be part of .NET architecture. Unlike Liberty, it focuses more on centralised management, because in practise the identity of the user is stored in the Passport service, which is owned and run by Microsoft. The service can also contain profile information about the user and it is up to the user if she wishes to distribute this information to the sites participating in Passport service. It is possible that the sites themselves can store profile information about the user, because each user has unique id-number which is not the same as his real identity identifier, i.e. email address. The system does not provide the possibility to distribute this information among other sites, though.

On the technical side Passport uses many similar kind of solutions like Liberty Alliance, which is quite understandable because of the underlying WWW environment. In practise when the user selects login to Passport in a participating site, she is directed with a modified URL to the Passport page, which is personalised according to the look and feel of the original site. In this page the user writes her email address and password as her credentials. After the verification the user is granted a "ticket" that contains authentication information and is encrypted with symmetric key, which is shared between Passport and the original site. In addition, the general authentication status of the user is marked by issuing a cookie under passport.dom domain. This cookie can be checked every time the user accesses Passport site again and as such can provide authentication without a subsequent login request. In the next step the user is directed back to the original site with the generated ticket appended to the query portion of the URL. It can also contain profile information about the user, if the user has agreed to that. The original site is responsible for reading the information from the URL and generating cookies out of them, so that it can read them every time user accesses the same site. [24]

In order to take advantage of the Passport system a WWW service has to first make a contract with Microsoft. The cost of this is annually 10000 dollars and additionally Microsoft charges 1500 dollars for "testing" each of the service URL. After the contract is made, Passport generates a 3DES cipher key that is used to

encrypt the authentication and the profile data passed between the sites. It might be the initial cost or the central position of Microsoft that Passport has not received too many participating sites. Looking at www.passport.com reveals about 80 participating sites and quarter of them are Microsoft services. The intentions of Microsoft are never easy to tell, but it might be that they are more inclined to put effort for developing Web Services concepts for the identity management as they have been an active player in the field of Web Services and their next operating system is supposed to have broad support for Web Services technologies.

4 Conclusions

The amount of identities is increasing as well as the burden of managing them. This is problematic especially in the cases where the management is done by persons themselves, because it is challenging to remember rather abstract things like numbers. This paper took a brief look at systems and technologies aimed at helping to solve the issue. The main focus was especially in the Liberty Alliance specification.

These kind of systems provide useful features like identity federation that help linking different isolated identities together under the umbrella of a single identity provided by a trusted party. Therefore a user has to remember only one set of credentials that can be used for authentication purposes. A beneficial consequence of this is that single sign-on services can be provided for the user, i.e. authentication is required only once for accessing several different sites provided that these parties share relevant business agreements. It should be noted, however, that a user may still have to be aware of the individual identities, because it is possible that the user wants to defederate her identities at some point and use the service with the old identity. There is always danger that the user does not remember these identities anymore, so special care might be needed here.

One should not forget that there are also inherit risks involved with the identity management systems. Especially if one identity and credential make it possible to access several sites, this identity is a tempting target for identity theft. Therefore, the managed identity should have strong credentials, possibly involving smart card or biometric technology. The service provider ought to be informed about the used authentication method so it can decide whether some actions, like those involving paying, can be approved. It is also worth noting that the strength of authentication is also dependant on the fact how many different mechanisms are

employed. This is especially important if there is a danger of system subvertion. So a browser environment alone can be weak, but if one enhances it, for example, with authentication involving a mobile phone, the overall system can be made more secure. However, usually the more secure arrangements mean more complex usability from the user point of view and hence the users might be tempted to go for the easiest solution.

Liberty Alliance takes a holistic view on the matter and succeeds in providing rather extensive framework for the identity management. It can already provide solutions for the current application domain, i.e. web based transactions, but it also takes into account the emerging paradigms involving Web Services. This, as well its open and license free nature, are key issues when comparing it to the other kind of systems, like for example Microsoft Passport. At the moment Liberty Alliance seems to have a good momentum behind it, so it has good chances of becoming a major influencer of the identity management of the future and help us all to sort out the tangle of multiple identities.

References

[1] Stallings, W. Cryptography and network security: principles and practise, second edition. Prentice Hall, 1999

[2] RSA Laboratories. PKCS#1 v2.1: RSA Cryptography standard. 2002

[3] RSA Laboratories. PKCS#7: Cryptographic Message Syntax Standard. 1993

[4] Housley, R. RFC 2630 Cryptographic Message Syntax. 1999

[5] Ramsdell B. (ed.). RFC 2633 S/MIME Version 3 Message Specification. 1999

[6] W3C. XML-Signature Syntax and Processing. W3C Recommendations, 2002

[7] Housley R., Polk T. Planning for PKI. Wiley, 2001

[8] Ellison C., Schneier B. Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure. Computer Security Journal v16, 2000

[9] Housley R. et al. RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile. 1999

[10] Fielding R. et al. RFC 2616 Hypertext Transfer Protocol - - HTTP/1.1. 1999

[11] Berners-Lee T. et al. RFC 1738 Uniform Resource Locators (URL). 1994

[12] Kristol D., Montulli L. RFC 2965 HTTP State Management Mechanism. 2000

[13] OASIS. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1. OASIS Standard, 2003

[14] OASIS. Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1. OASIS Standard, 2003

[15] OASIS. Technical Overview of the OASIS Security Assertion Markup Language (SAML) V1.1. OASIS draft, March 2004

[16] Liberty Alliance Project. Liberty Alliance web site, http://www.projectliberty.org/ (accessed 16.5.2004)

[17] Liberty Alliance Project. Liberty ID-FF Architecture Overview version 1.2. 2003

[18] Liberty Alliance Project. Liberty ID-FF Bindings and Profiles Specification version 1.2. 2003

[19] Bajaj B. et al. Web Services Federation Language (WS-Federation). 2003

[20] Dierks T., Allen C. RFC 2246 The TLS Protocol Version 1.0. 1999

[21] W3C. XML Encryption Syntax and Processing. W3C Recommendation, 2002

[22] Liberty Alliance Project. Liberty ID-WSF Security Mechanisms Version 1.0. 2003

[23] Suomen laki. Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvassa 24.1999/565. 1999

[24] Microsoft. Microsoft .NET Passport Review Guide. 2003

Tietoturva konsernin toimintoja keskitettäessä ja standardoitaessa –asiakkaan näkökulma

Kari Kataja

Globaali, kova kilpailu ajaa yrityksiä yhä suuremmiksi konserneiksi, joissa toimintoja saatetaan sekä keskittää että standardoida. Joitakin toimintoja voidaan samalla myös ulkoistaa.

Tässä seminaarityössä tarkastellaan konsernin tietoturva-asioita toimintoja keskitettäessä. Näkökulmaksi työhön on valittu yritysasiakas, joka käyttää tuotteiden valmistuksessa sopimusvalmistusta.

Konsernin toimintojen keskittäminen voi asiakkaasta täyttää ulkoistuksen piirteitä. Näin on asianlaita erityisesti silloin, jos asiakas on pieni, paikallinen yritys ja toimittaja (sopimusvalmistaja) on suuri kansainvälinen konserni. Paikallinen asiakas ei välttämättä ole tyytyväinen tällaiseen ratkaisuun. Toisaalta, suuri kansainvälinen asiakas saattaa olla hyvin tyytyväinen toimintojen keskittämiseen, sillä tällöin esimerkiksi toimintojen auditointi helpottuu.

Toimintojen standardointi isossa konsernissa auttaa tietoturva-asioiden hallinnassa. Standardoiduilla minimikäytännöillä pystytään asiakkaalle vakuuttamaan, miten asiat konsernissa hoidetaan. Erityisen tärkeää on kysyä asiakkaan mielipide jo kehittämistoimenpiteitä suunniteltaessa.

Standardoinnin ja keskittämisen heikkoutena on se, että tietoturva keskittyy yhteen (tai harvoihin) ratkaisuihin. Mikäli ratkaisu osoittautuu vääräksi, aiheuttuu siitä ongelmia koko konsernissa. Jotta vältetään tämän riskin kasvaminen liian suureksi, tulee valittavat ratkaisut valita huolella ja seurata kyseisen osa-alueen tilanteen kehittymistä jatkuvasti.

Avainsanat ja -sanonnat: tietoturva, konserni, konsernien tietoturva.

Sisällys

1. Johdanto

Nykyisin yritykset kohtaaavat toiminnassaan yhä kovempaa kansainvälistä kilpailua. Pärjätäkseen globaaleilla markkinoilla yritykset fuusioituvat konserneiksi.

Konserniin kuulumisella saattaa olla varsin merkittäviä vaikutuksia yrityksen toimintaan ja päätöksentekoon. Konsernin keskushallinto ei välttämättä puutu kovinkaan merkittävästi paikallisien yksiköiden toimintaan. Kuitenkin Lehmannin [2002] mukaan useissa tilanteissa optimaalinen ratkaisu on ”Transnational” organisaatio, jossa sekä globaali kontrollointi että paikallinen itsenäisyys ovat korkealla tasolla. Konserneissa onkin usein saatettu päätyä keskittämään joitakin toimintoja.

Toisaalta, yritykset pyrkivät keskittymään ydinliiketoimintaansa. Tämä johtaa usein ydinliiketoimintaan kuulumattomien toimintojen ulkoistamiseen (outsourcing). Ulkoistamisella pyritään esimerkiksi kustannustehokkuuteen tai suurempaan joustavuuteen. [Pajarinen, 2001]

Tässä seminaarityössä lähtökohtana on tutkia asiakkaan näkökulmasta konsernissa tapahtuvan toimintojen keskittämisen ja standardoinnin vaikutusta tietoturvaan. Ulkoistuksen osalta esimerkkinä käytetään sopimusvalmistusta (contract manufacturing). Asiakkaalla tässä työssä tarkoitetaan yritystä, joka on ulkoistanut toimintaansa sopimusvalmistajalleen.

Tutkimuksen lähtökohtana on kirjallisuusanalyysi. Kuitenkin kirjallisuuden lisäksi työssä on käytetty hyväksi kirjoittajan omakohtaisia havaintoja kansainvälisen konsernin toiminnasta.

2. Sopimusvalmistus ja ulkoistus

2.1. Sopimusvalmistus

Sopimusvalmistuksella tarkoitetaan toimintaa, jossa yritys ulkoistaa esimerkiksi tuotteensa valmistuksen jollekin toiselle yritykselle, sopimusvalmistajalle. Sopimusvalmistus poikkeaa perinteisestä alihankinnasta siinä mielessä, että sopimusvalmistaja voi valmistaa tuotteen kokonaisuudessaan valmiiksi.

Sopimusvalmistajalla pitää olla käytössään kaikki tuotteen valmistamiseen tarvittavat tiedot. Itse valmistusprosessin lisäksi sopimusvalmistaja voi vastata myös lopputuotteiden logistiikasta ja jopa tuotteiden suunnittelusta. Tästä hyvänä esimerkkinä on Microcell, joka kehittää matkapuhelimia niin Ericssonille kuin Siemensillekin [Nikulainen, 2002].

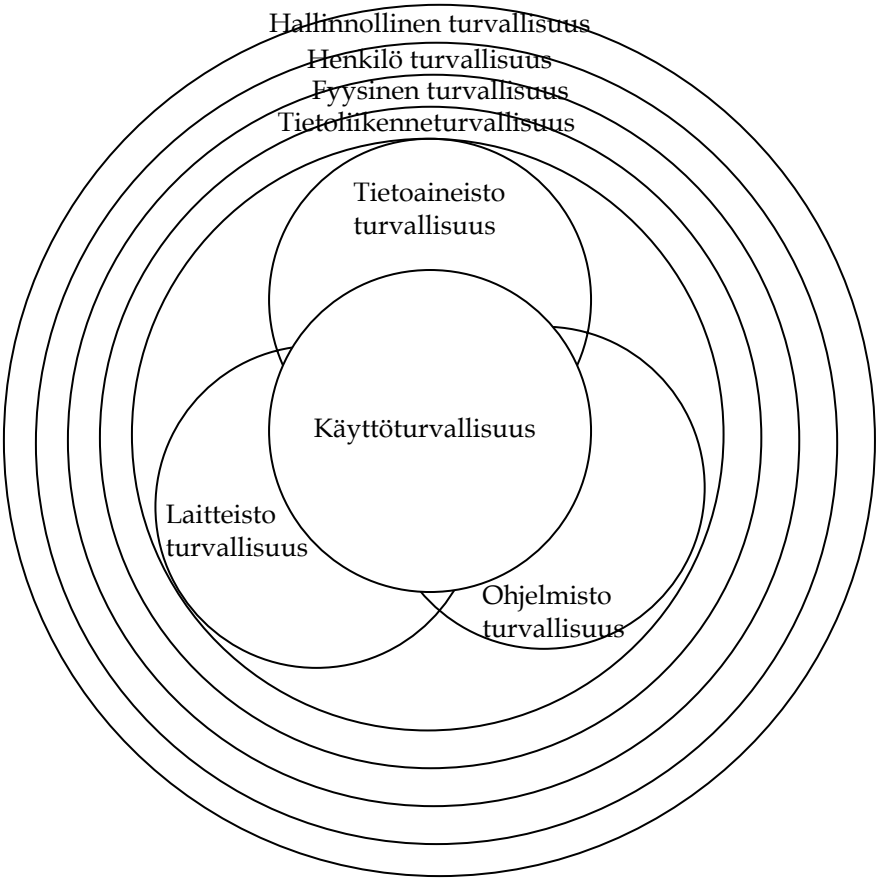
Sopimusvalmistus on yleisesti käytössä oleva toimintatapa erityisesti elektroniikan valmistuksessa. Esimerkiksi Ericsson siirsi jo vuonna 2001 matkapuhelimiensa valmistuksen sopimusvalmistajalleen [Flextronics, 2001].

Asiakkaan kannalta sopimusvalmistuksessa on siis kyse juuri ulkoistuksesta. Koska tässä yhteydessä ulkoistetaan myös kyseisen osa-alueen tietohallintoa, tulee tässä yhteydessä tarkastella myös tietoturva-asioita.

2.2. Tietoturva ulkoistuksessa

Sopimusvalmistus on siis eräs ulkoistuksen tyyppi. Ulkoistuksessa erityisen tietoturvauhan muodostaa yleisesti se, että yrityksen tietoja annetaan toiselle, ulkopuoliselle yritykselle [Kajava et al., 1996].

Hyvän lähtökohdan ulkoistamisen tietoturva-asioiden pohtimiselle antaa Valtionvarainministeriön [1999] ulkoistamisen tietoturvallisuussuositus. Tällä perusteella tietoturvallisuuden osa-alueet voidaan jakaa kahdeksaan ryhmään: hallinnollinen ja organisatorinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus. Paavilainen [1998] kuvaa tätä jakoa seuraavan kuvan (Kuva 1) mukaisesti.



Kuva 1: Tietoturvallisuuden osa-alueet. [Paavilainen, 1998]

Jokainen edellä esitetyistä osa-alueista on jo yksinäänkin varsin laaja. Tässä kohtaa rajoitutaankin tarkastelemaan vain pintapuolisesti jokaista osa-aluetta. Tavoitteena on nostaa esille nimenomaan ulkoistuksen erityispiirteitä. Yhteistä kaikille osa-alueille on se, että toimintamenettelyt pitää olla dokumentoituja.

Hallinnollisen ja organisatorisen tietoturvallisuuden tarkastelussa tulee varmistautua, että toimittajan tietoturvapolitiikka, ohjeistus yms. vastaavat asiakkaan vaatimuksia. Toimittajalla pitää olla myös suunnitelmat häiriöistä toipumiseen. Tämän lisäksi toimittajan tietoturvamenettelyt tulee voida tarvittaessa auditoida. [Valtionvarainministeriö, 1999]

Henkilöturvallisuuden kohdalta asiakas saattaa esittää henkilöstön minimivaatimuksia, joka voi pitää sisällään työntekijöille annettavan tietoturvakoulutuksen. Tämän lisäksi henkilöturvallisuuden ohjeistus ja käytännöt tulee voida tarkistaa. [Valtionvarainministeriö, 1999]

Asiakas voi myös tarkistaa toimittajan fyysisen turvallisuuden. Toimittajalla pitää siis olla esimerkiksi riittävän hyvä kulunvalvonta, hälytysjärjestelmät, paloilmaisimet jne. Asiakas saattaa haluta rajoittaa ulkopuolisien henkilöiden vierailukäyntejä. [Valtionvarainministeriö, 1999]

Samalla sopimusvalmistajalla saattaa olla asiakkaanaan kilpailevia yrityksiä. Näiden yrityksien tuotteet voidaan valmistaa samassa tehtaassa tai jopa samalla valmistuslinjalla. Tämä luo omia erityisvaatimuksiaan toiminnan järjestelyissä. Olisi suorastaan katastrofaalista jos esimerkiksi Siemensin uuden puhelinmallin protosarjan matkapuhelimet lähetettäisiin vahingossa vaikkapa Ericssonin tuotekehitykseen.

Saattaakin olla perusteltua, että kilpailevat tuotteet valmistetaan erillisissä tehdasrakennuksissa. Tällöin asiakas ei edes yritysvierailulla voisi vahingossa törmätä kilpailijan tuotteisiin.

Tietoliikenneturvallisuuden kohdalla puolestaan tulee tarkastella mm. tiedonsiirrossa käytettyjä ratkaisuita. Tietoverkkoja pitää valvoa riittävästi. Myös mahdollisia varayhteyksiä tulee harkita. [Valtionvarainministeriö 1999]

Laitteistojen turvallisuutta tarkasteltaessa asiakkaan tulisi varmistautua siitä, että toimittajan laitteistot pystyvät riittävällä varmuudella palvelemaan asiakasta. Tässä yhteydessä on hyvä sopia myös sanktioista. [Valtionvarainministeriö, 1999]

Ohjelmistoturvallisuuden kohdalla asiakaan pitäisi varmistua siitä, ettei ohjelmissa ole tietoturvaa vaarantavia osia. Ohjelmistoturvallisuuteen kuuluvat mm. virustorjunta, käyttöoikeuksien hallinta, ohjelmiston muutosproseduurit, lisenssien hallinta yms. [Valtionvarainministeriö, 1999]

Sopimusvalmistajalla kilpailevien yritysten tuotteiden tiedot ovat usein samassa tietojärjetelmässä. Erityistä tarkkuutta vaaditaankin materiaalien hallinnassa, sillä asiakasyritykset ovat saattaneet neuvotella ostosopimuksia sopimusvalmistajan puolesta.

Sopimusvalmistajan pitääkin varmistautua, ettei näitä sopimushintoja käytetä kuin kyseisen valmistajan tuotteiden valmistamisessa. Erityisen ikäviin tilanteisiin voidaan joutua, mikäli jostakin materiaalista on maailmanlaajuisesti puutetta. Tällöin asiakas saattaa auttaa sopimusvalmistajaa materiaalin hankinnassa. Olisikin asiakkaan kannalta erittäin ikävää, jos näin saatu materiaali käytettäisiinkin kilpailijan laitteissa. Ongelmien välttämiseksi esimerkiksi materiaalien koodaukseen ja ostorutiineihin kannattaa kiinnittää huomiota.

Tietoaineistoturvallisuuden kohdalla tietoaineisto pitää olla luokiteltu salassapidettävyyden mukaan ja koko tietoaineiston elinkaaren osalta pitää sopia menettelyt. Tämä pitää sisällään myös varmuuskopioinnin. [Valtionvarainministeriö, 1999]

Käyttöturvallisuudessa tavoitteena on varmistaa toiminnan jatkuvuus. Tämä pitää sisällään mm. toipumissuunnitelmat, varalaitteet, varmuuskopiointimenettelyt, lokitietojen hallinnan yms. [Valtionvarainministeriö, 1999]

3. Toimintojen keskittäminen

3.1. Ulkoistus konsernin sisälle

On mielenkiintoista pohtia, onko ulkoistamiseen liittyvä teoria sovellettavissa konsernin sisäisissä ratkaisuissa. ATK-sanakirja [2003 s. 261] määrittelee ulkoistuksen seuraavasti: ”Ulkoistus: Järjestely, jossa osa organisaation toiminnoista ja mahdollisesti resursseista, tietojenkäsittelyssä esimerkiksi käyttötoiminnot tai ohjelmistokehitys, siirretään ulkopuolisen tahon hoidettavaksi”.

Jos tarkastellaan suurta konsernia, tietohallinnon mahdollisessa keskittämisessä on havaittavissa ulkoistukselle tyypillisiä piirteitä. Konserni on voinut esimerkiksi keskittää toiminnanohjausjärjestelmät yhteen paikkaan. Tällöin konsernin atk-keskus siis tarjoaa palveluitaan eri yksiköiden käyttöön. Kirjallisuudessa tällaisestä toiminnasta on juuri käytetty termi ulkoistus konsernin sisälle (group outsourcing) [Kiiha, 2002].

Verrattaessa tilannetta edellä esitettyyn ulkoistuksen määritelmään, havaitaan, että avainkohtana on ”ulkopuolisen tahon” määritelmä. Periaatteessa konsernin pitäisi toteuttaa konsernijohdon määrittelemiä strategioita yhtenä kokonaisuutena. Kuitenkin käytännössä konsernin keskusjohto saatetaan ainakin paikallisesti kokea ulkopuolisena tahona: esimerkkinä käytetyssä toi-

minnanohjausjärjestelmien keskittämisessä paikallisilla yksiköillä ei ole välttämättä kovin suuria mahdollisuuksia vaikuttaa siihen, miten asioita hoidetaan.

3.2. Asiakas ja konsernin keskitetty tietohallinto

Konsernin keskitettyä tietohallintoa voidaan lähestyä myös asiakkaan näkökulmasta. Asiakastyytyväisyys ja asiakkaan vaatimukset ovat kuitenkin yrityksen toiminnan kannalta avainasemassa. Tarkastellaan tässä yhteydessä esimerkkinä sopimusvalmistusta tekevää yritystä.

Mikäli asiakas mieltää toimivansa maailmanluokan konsernin kanssa, konsernin atk-keskusta ei voida pitää ulkoistuksen määritelmän mukaisena ”ulkopuolisena tahona”. Itse asiassa tällaisessa ympäristössä toimintojen keskittäminen konsernin atk-keskukseen saattaa jopa helpottaa asiakkaan kanssa toimimista. Tämä johtuu siitä, että asiakkaan tarvitsee auditoida vain yhden atk-keskuksen toiminta.

Tällaisessa ympäristössä toimintojen keskittämisessä saadaan myös muita etuja. Esimerkiksi Extranet-ratkaisuissa on etu, jos asiakas voi käyttää vain yhtä konsernin keskitettyä sovellusta.

Kuitenkin, jos asiakas on tottunut toimimaan esimerkiksi vain yhden konsernin yksikön kanssa, tietojärjestelmän siirtäminen konsernin atk-keskukseen saattaa asiakkaasta näyttää juuri ulkoistuksen määritelmän mukaisesti ”ulkopuoliselta taholta”. Asiakas ei välttämättä ole tietoturvan osalta kovin tyytyväinen tähän ratkaisuun, sillä toimintamenettelyiden auditointi voi osoittautua käytännössä mahdottomaksi.

Tilannetta vaikeuttaa vielä osaltaan se, että asiakkaan paikalliset kontaktit eivät välttämättä edes itse tiedä, miten tietoturva-asiat konsernissa hoidetaan. Jos edes paikallinen tietohallinto ei ole vakuuttunut konsernin tietohallinnon tietoturvan tasosta, niin miten asiakas saataisiin vakuuttumaan tästä ? Toisaalta, ei riitä, että toimittaja tietää hallitsevansa asiat, sillä asiakkaalle pitää kyetä näyttämään asioiden olevan hallinnassa. Konsernien tapauksessa tämä saattaa osaltaan edesauttaa tietoturvaratkaisuiden standardointia.

Asiakas saattaa myös arvostaa paikallisen yksikön joustavuutta. Jos päätöksenteko tapahtuu vaikkapa toisella mantereella, saatetaan samalla menettää osa joustavuudesta. Myös mahdollisesti asiakkaan vaatimien järjestelmien pystyttäminen voi käytännössä hankaloitua, mikäli tämä edellyttää vielä kolmannen osapuolen (= konsernin tietohallinto) mukana oloa.

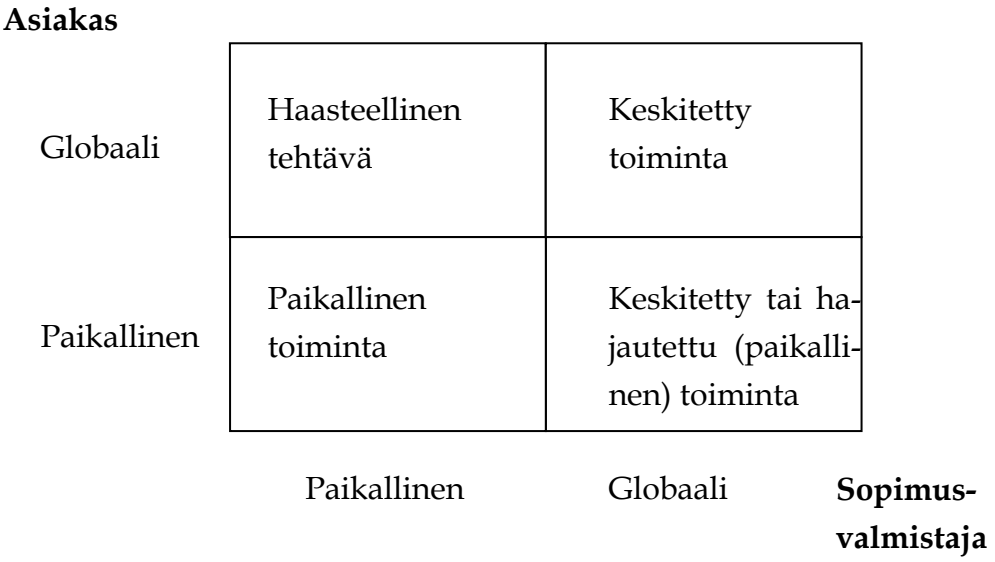
Toimintojen keskittäminen luo konserniin riskikeskittymän. Globaali asiakas voi globaalin sopimusvalmistajan kohdalla huolestua, mikäli liian suuri osa tietohallinnosta on keskitetty yhteen paikkaan. Tällöin maariski saattaa kasva merkittäväksi [Suominen, 2003]. Asiakas saattaakin haluta varmistautua, ettei

esimerkiksi luonnonmullistukset, terrori-iskut tai vaikkapa tietoliikenneyhteyksien katkeaminen heikennä liiaksi asiakkaan toimintaa.

Toimintojen keskittäminen saattaa luoda suhteellisen monimutkaisen tietoliikenneinfrastruktuurin. Tuotteiden valmistamisessa ja lähettämisessä saatetaan tarvita tietoja esimerkiksi loppukäyttäjän, asiakkaan ja konsernin tietojärjestelmistä. Mikäli yhdenkin tarvittavan yhteyden kohdalla on ongelmia, saattaa koko prosessi pysähtyä.

Muodostetaan vielä asiakkaan ja sopimusvalmistajan globaalisuuden vaikutuksia kuvaava tilanne seuraavaan nelikenttään (Kuva 2). Paikallisella sopimusvalmistajalla on haasteellinen tehtävä toteuttaa globaalin asiakkaan toiveita. Pidemmän päälle tämä tilanne saattaa olla mahdoton.

Toinen hieman epäselvä tapaus on tilanne, jossa on paikallinen asiakas ja globaali sopimusvalmistaja. Edellä esitetyn pohdinnan perusteella asiakas voisi tietoturvan osalta pitää selkeämpänä ratkaisuna hajautettua paikallista toimintaa. Kuitenkin toimintojen keskittäminen saattaa kustannustehokkuuden, ja sitä kautta halvempien hintojen, myötä olla lopulta asiakkaankin toivoma ratkaisu.



Kuva 2: Nelikenttä sopimusvalmistajan ja asiakkaan globaalisuudesta.

Mikäli sopimusvalmistaja päätyy ulkoistamaan toimintojaan johonkin ulkopuoliseen yritykseen, tämä ei periaatteessa lisää ainakaan Suomen lainsäädännön mukaan asiakkaan taloudellista riskiä. Sopimusvalmistaja siis vastaa edelleen ulkoistetustakin toiminnasta [Kiiha 2002].

Kuitenkin aina kun asiakkaan tietoihin pääsee käsiksi joku uusi taho, riski siihen, että tietojen luottamuksellisuus vaarantuu kasvaa. Joissakin tilanteissa

konserni saattaa ulkoistaa toimintojaan myös yhteisomistuksessa olevalla yritykselle (joint venture outsourcing) [Kiiha 2002].

Toimintojen keskittämisen vaikutus asiakaan tyytyväisyyteen ei siis ole lainkaan itsestään selvä. Tästä syystä olisikin perusteltua keskustella jo muutoksen suunnitteluvaiheessa ainakin tärkeimpien asiakkaiden kanssa.

Myös eri maiden lainsäädännöt saattavat aiheuttaa ylimääräisiä haasteita tietojärjestelmiä keskitettäessä. Esimerkiksi henkilöstöhallinnon kohdalla tietosuojalakien vaatimukset siitä, mitä tietoa pitää ja mitä ei saa työntekijöistä kerätä, vaihtelevat maittain.

3.3. Ulkoistuksen teoria ja konsernin keskitetty tietohallinto

Tässä työssä esitetyssä sopimusvalmistuksen tapauksessa on ulkoistuksen teorian soveltaminen konsernin keskitettyyn tietohallintoon varsin perusteltua. Tämä johtuu siitä, että asiakas soveltaa konserniin ulkoistuksen teorian mukaisia vaatimuksia, jolloin myös konsernin sisällä vastaavat vaatimukset tulee täyttää.

Ulkoistusta käsittelevässä kirjallisuudessa korostetaan sopimuksien merkitystä [Kiiha, 2002 ja Pajarinen, 2001]. Tässä kohtaa konsernin sisällä tapahtuva toimintojen keskittäminen eroaa merkittävästi tilanteesta, jossa ulkoistus tapahtuu konsernin ulkopuoliseen yritykseen.

Toki konsernin sisälläkin asioista tulisi sopia huolellisesti etukäteen. Kuitenkin, koska kyse on samasta yrityksestä, ei esimerkiksi sovittujen asioiden rikkomisesta voida langettaa sopimussakkoja. Yrityksen sisällä tietysti voidaan siirtää rahaa paikasta toiseen, mutta käytännössä tämä ei ole tehokasta ohjausta.

Samoin konsernissa yhdessä sovitut päätökset voidaan purkaa nopeasti, mikäli keskushallinto näin päättää. Paikalliset yksiköt ovatkin hyvin pitkälti konsernin keskushallinnon armoilla.

4. Tietoturvan standardointi konsernissa

4.1. Standardointi ja riski

Tietoturvaan liittyvien asioiden standardoinnissa ovat toisaalta vastakkain standardoinnin tuoma varmuus tietysti tietoturvatasosta ja toisaalta riski siitä mitä tapahtuu jos valittu standarditietoturvataso ei olekaan riittävän vahva.

Tilannetta voidaan verrata sijoitustoimintaan: hajauttamalla sijoitukset useampiin sijoituskohteisiin saadaan epäonnistuneen sijoituksen riskiä pienennettyä. Toisaalta jo Mark Twain toteaa kuuluisassa lauseessaan ”Put all your

eggs in the one basket and -WATCH THAT BASKET". Tämä sama ongelma on havaittavissa myös toimintojen keskittämisessä.

Mikäli konserni päätyy standardoimaan tietoturvaratkaisuitaan, tulee valittujen ratkaisuiden toimivuutta siis tarkkailla jatkuvasti. Tarvittaessa myös valittuja ratkaisuita tulee pystyä päivittämään ripeästi, mikäli tietoturvassa havaitaan puutteita.

Ylipäätään standardoinnissa konsernin keskusjohdolla on merkittävä rooli. Globaalissa yrityksessä valittavien ratkaisuiden kohdalla pitää erityisesti ottaa huomioon tuotteiden ja palveluiden saatavuus eripuolilla maailmaa. Paikallisilla yksiköillä saattaa tilanteesta riippuen olla tarvetta saada paikallista tukea, koulutusta yms. Standardointia pohdittaessa tulisikin tehdä riskianalyysi, jossa selvitetään systemaattisesti riskikohteet, riskien todennäköisyys, riskien vakavuus ja niistä aiheutuvat seurannaisvaikutukset [Suominen, 2003].

Minkäli konserni on standardoinut jonkun ratkaisun, yksiköiden saattaa olla erittäin vaikeata saada lupa hankkia muita kuin standardiratkaisuita. Joissakin tilanteissa tämän kuitenkin pitää olla mahdollista. Näin on asian laita ainakin silloin, jos asiakas ehdottomasti vaatii jotakin tiettyä ratkaisua.

4.2. Ohjelmistot

Konsernin keskushallinto saattaa määritellä hyvinkin tarkasti käytettävät ohjelmistoratkaisut. Paikalliset yksiköt eivät välttämättä pysty vaikuttamaan näihin ratkaisuihin millään tavalla. Esimerkiksi käyttöjärjestelmien, palvelimien ohjelmistojen, sähköpostijärjestelmien ja toiminnanohjausjärjestelmien kohdalla ovat ratkaisut isoissa konserneissa mittavia, eikä niitä lähdetä kovin helposti muuttamaan.

Periaatteessa konserni voisi asettaa esimerkiksi virustorjunnalle vain tietyt minimivaatimukset, jotka käytettävien järjestelmien tulee täyttää. Kuitenkin käytännössä on vaikeata vakuuttaa jonkin paikallisen, sinällään hyvin toimivan, virustorjunnan luotettavuus esimerkiksi Amerikassa sijaitsevalle keskushallinnolle. Itse asiassa paikallisen toimittajan virustorjuntaohjelmisto voisi palvella kyseistä yksikköä jopa paremmin kuin konsernin vastaava standardiratkaisu, sillä tukipalvelut saattaisivat olla selkästi paremmat.

Juuri virustorjunnan standardoinnissa merkittäväksi riskiksi muodostuu tilanne, jossa käytössä oleva ohjelmisto ei jostain syystä havaitsekaan jotain virusta. Tällöin koko konsernin verkko saattaa saastua ennenkuin tilanne havaitaan. Toinen potentiaalinen uhko on virheellisen virustorjuntaohjelmiston päivityksen aiheuttamat ongelmat. On mahdollista, että virustorjuntaohjelman ongelmat vaikeuttavat (tai jopa estävät) tietokoneen normaalin käytön.

Osaltaan ohjelmistojen standardoinnissa lähtökohtana on kustannustehokkuus. Ohjelmistojen hankita-, ylläpito- ja käyttökustannukset yleensä laskevat, jos ohjelmistoja hankitaan enemmän.

4.3. Laitteistot

Konserni on saattanut neuvotella puitesopimukset, joita tulisi käyttää laitteistoita hankittaessa. Tietoturvan ja riskin kannalta vain tiettyjen laitteistoiden käyttämisellä saattaa olla vaikutuksia.

Esimerkiksi palomuurien standardointi kasvattaa konsernin haavoittuvuuden riskiä. Jos kyseisestä palomuurista löytyy tietoturva-aukko, kaikki konsernin palomuurit kohtaavat saman ongelman.

Toisaalta, laitteiston standardointi takaa tietyn minimitoiminnan kaikissa konsernin osissa. Samalla konsernin sisälle kumuloituu tieto-taitoa kyseisestä laitteesta. Myös laitteiden rikkoutumiseen varautuminen helpottuu, kun voidaan sopia varalaitteiden varastoinnista.

4.4. Menettelytavat

Konserni on saattanut ohjeistaa tiettyjä tietoturvaan liittyviä menettelytapoja. Esimerkiksi salasanojen minimipituudet ja vaihtojaksot on saatettu määritellä keskitetysti.

Tiettyjen minimimenettelyiden määrittely keskitetysti on perusteltua. Tällöin asiakkaalle on helppo kertoa, että näin konsernissa asiat on hoidettu. Tarvittaessa paikallisesti voidaan tietysti soveltaa omia, vielä tiukempia menettelyohjeita.

Myös paikalliset konsernin asiakkaat saattavat olla kiinnostuneita konserninlaajuisista standardi menettelyistä ja –ratkaisuista. Tämä johtuu siitä, että tietoturva-aukko vaikkapa toisella mantereella luo potentiaalisen uhan konsernin muihinkin osiin.

Asiakkaalla saattaa myös olla omia menettelytapavaatimuksia. Näiden vaatimuksien toteuttaminen saattaa osoittautua vaikeaksi ja kalliiksi. Tästä syystä kaikki asiakkaan tietojenkäsittelyyn (ml. tietoturvaan) liittyvät vaatimukset on syytä käydä läpi jo sopimusneuvotteluiden aikana.

Joissakin tilanteissa asiakkaalla saattaa vaatimuksena olla esimerkiksi jonkin tietyn teknologian käyttäminen. Sopimusvalmistajaehdokkaalla saattaa kuitenkin olla jo käytössä jokin käyttökelpoinen kilpailevan teknologian ratkaisu. Tällöin saattaisi olla molempien osapuolien etu siirtyä käyttämään sopimusvalmistajan tarjoamaa ratkaisua. Näin meneteltäessä sopimusvalmistaja pystyisi todennäköisesti toimimaan kustannustehokkaammin.

Kuitenkin, mikäli asiakas vaatii määrittelemänsä teknologian käyttämistä, tulee sopimusvalmistajan sopeutua tähän, sillä muutoin tilaukset menevät

jollekin kilpailijalle. Tärkeätä on kuitenkin organsiaatiossa keskustella kyseisen osa-alueen asiantuntijoiden kanssa vaaditun teknologian kustannusvaikutuksista, jotta ne voidaan ottaa huomioon tarjouksen hinnoittelussa.

Menettelytapojen standardointi helpottaa myös yrityksen sisäistä toimintaa. Esimerkiksi eri tehtaiden välinen kommunikaatio helpottuu ja väärinymmärrysten todennäköisyys pienenee, kun koko konsernissa käytetään samoja menettelytapoja. Tarvittaessa jopa henkilöiden siirtyminen tehtaiden välillä helpottuu.

Pelkkä yhteisistä menettelytavoista sopiminen ei vielä riitä, vaan niiden noudattamista kannattaa konsernin sisällä valvoa. Sisäisessä valvonnassa menetelminä käytetään sisäistä tarkkailua ja sisäistä tarkastusta. [Pirnes et al., 2000]

Mahdolliset poikkeamat on parempi havaita sisäisessä valvonnassa kuin asiakkaan tekemässä toimittaja-auditoinnissa. Yrityksen toimintaympäristöstä riippuen saattaa olla perusteltua jo alunperin käyttää englanninkielistä ohjeistusta. Saattaa myös olla, että osa ohjeista joudutaan tekemään sekä englanniksi että paikallisella kielellä. Mikäli yrityksellä on kansainvälisiä asiakkaita, englanninkieliset toimintaohjeet osaltaan helpottavat menettelytapojen selittämistä.

5. Päätelmät

Konsernin sisäisestä toimintojen keskittämistä voidaan joiltakin osin lähestyä ulkoistamisen kannalta. Merkittävä ero normaalin ulkoistamiseen on kuitenkin se, että konsernin tapauksessa kyse on samasta yrityksestä, jolloin sopimukset ovat juridisesti erityyppisiä. Sopimussakot eivät oikein toimi ja tarvittaessa konsernin keskushallinto voi muuttaa jo sovittuja asioita hyvin nopeasti.

Tilanteesta riippuen asiakas voi kokea konsernin toimintojen keskittämisen tietoturvan kannalta joko positiivisina tai negatiivisena asiana. Todennäköisesti globaali asiakas on tyytyväisempi toimintojen keskittämisestä. Vastaavasti paikallinen asiakas saattaisi mieluummin toimia paikallisen organisaation kanssa.

Tietoturvan standardointi kasvattaa riskiä, mikäli valinta on kohdistunut "väärään" teknologiaan. Standardoinnin yhteydessä tuleekin huolellisesti valita käytettävät teknologiat ja jatkuvasti tarkkailla kyseisen osa-alueen tietoturvan kehittymistä.

Jotta asiakas pystyy vakuuttumaan globaalin sopimusvalmistajansa tietoturvaratkaisuista, tulee konsernista käytännössä löytyä ainakin jonkin tason minivaatimukset. Käytännössä saattaa olla vaikeata vakuuttaa asiakasta ilman menettelyiden (ja joissakin tapauksissa myös käytettävien ohjelmistojen) standardointia.

Tyytyväisen asiakkaan tulee olla yrityksen toiminnan perusajatus. Sopimusvalmistuksessa asiakas on erityisen kiinnostunut tietoturvasta, sillä sopimusvalmistajalla on käytössä huomattavan paljon luottamuksellista tietoa.

Asiakas pitää pystyä vakuuttamaan siitä, että tietoturva on kunnossa. Niinpä myös toimintoja kehitettäessä tulee asiakas aina pitää mielessä. Tarvittaessa asiakkaan kanssa tulee keskustella jo muutoksien suunnitteluvaiheessa.

6. Viiteluettelo

[Atk-sanakirja, 2003] *Atk-sanakirja*. Talentum, Helsinki, 2003.

[Flextronics, 2001] Flextronics Press Release 26.1.2001, *Flextronics to manage Ericsson's mobile phone operations.* http://www.flextronics.com/News/PressReleases/PressReleases01/20010126SJA.pdf. Noudettu 20.2.2004

[Kajava et al., 1996] Jorma Kajava, Sami J.P. Heikkinen, Paavo Jurvelin, Tero Viiru ja Päivi Parviainen, *Tietojenkäsittelyn ulkoistaminen ja tietoturva.* Oulun yliopisto, Working papers series **B 42**. Oulu, 1996.

[Kiiha, 2002] Jaakko Kiiha, *Yritystoiminnan ulkoistaminen ja sopimusvastuu*. Grummerus Kirjapaino Oy, Saarijärvi, 2002.

[Lehmann, 2000] Hans Lehmann, The Design of Information Systems for the International Firm: Grounded Theory of Some Critical Issues. In: Prashant C. Plavian, Shailendra C. Jain Plavian and Edward M Roche (eds.), *Global Information Techonology and Electronics Commerse, Issues for the New Millennium*. Ivy League Publishing, Marietta 2002, 370 – 392.

[Nikulainen, 2002] Kalevi Nikulainen, Microcell valmistamaan Siemens-puhelimia. Digitoday 19.11.2002. http://www.digitoday.fi/showPage.php?page_id=12&news_id=20330. Noudettu 20.2.2004.

[Paavilainen, 1998] Juhani Paavilainen, *Tietoturva*. Grummerus Kirjapaino Oy, Jyväskylä, 1998.

[Pajarinen 2001] Mika Pajarinen, *Ulkoistaa vai ei – outsoursing teollisuudessa*. Elinkeinoelämän tutkimuslaitos, sarja **B 181**. Taloustieto Oy, Helsinki, 2001.

[Pirnes et al., 2000] Jari Pirnes, Anssi Sahlman, Jorma Kajava, *Tietoturva ja sisäinen valvonta*. Oulun yliopisto, Working papers series **B 62**. Oulu, 2000.

[Suominen, 2003] Arto Suominen, *Riskienhallinta*. WSOY, Helsinki, 2003.

[Valtionvarainministeriö, 1999] *Valtionhallinnon tietohallintotoimintojen ulkoistamisen tietoturvasuositus*. Valtiovarainministeriö, hallinnon kehittämisosasto. Helsinkin, 1999. Saatavana myös osoiteesta: http://www.vm.fi/tiedostot/pdf/fi/3405.pdf.

Peruskäyttäjän tietoturva

Anne Kunnari

Tämä seminaarityö käsittelee peruskäyttäjän tietoturvaa erityisesti kotiympäristössä. Tutkimuksessa tarkastellaan sitä, miten peruskäyttäjä asennoituu tietoturvaan ja minkälaista informaatiota peruskäyttäjälle on tarjolla. Seminaarityö käsittelee myös sitä, miten taidoiltaan vaatimaton peruskäyttäjä osaa tunnistaa tietoturvariskit ja toimia niiden pienentämiseksi.

Avainsanat ja -sanonnat: tietoturva, peruskäyttäjä.

1. Johdanto

Tietotekniikan käytön lisääntyminen ja yleistyminen kokonaisuudessaan on tuonut tietokoneiden ja verkkopalvelujen käyttäjiksi lukemattomia uusia noviisikäyttäjäryhmiä. Työpaikkojen ja koulujen tarjoamien tietoteknisten mahdollisuuksien lisäksi myös kotikäyttö on lisääntynyt. Kotikoneista ja nopeista Internet –yhteyksistä on tullut edullisempia, ja yhä useampi julkinen tai kaupallinen palvelu löytyy helposti verkkoyhteyden avulla. Tilastokeskuksen mukaan vuoden 2002 keväällä tietokonetta oli voinut käyttää jossain 75 prosenttia sekä miehistä, että naisista (Tilastokeskus, 2002). Tämä paikka on voinut olla koti, työ, oppilaitos tai jokin muu kohde. Internet –verkkoon pääsy kotikoneelta oli sen sijaan tietokoneen käyttömahdollisuutta alhaisempi, ja vain nuorimpiin ikäryhmiin kuuluvista merkittävällä osalla oli verkkoyhteys kotonaan. Kaiken kaikkiaan mahdollisuus päästä verkkoon jostain oli noin kahdella kolmanneksella 10 – 74 –vuotiaista. Useimmiten verkkoyhteyttä ja sähköpostia pääsivät käyttämään 15 – 19 –vuotiaat ja toisaalta yli 60 –vuotiaat eivät juurikaan päässeet verkkoyhteyttä käyttämään. (Tilastokeskus)

Näin ollen siis tietokoneen ja Internetin varsinaisia käyttäjiä löytyy kaikista ikäluokista, kuitenkin painottuen nuoriin ja työssäkäyviin aikuisiin. Erityisesti Internet –palvelujen käytön lisääntyminen johtaa siihen, että tietoturvariskit kasvavat ja entistä useampi käyttäjä joutuu hankkimaan tietoa tietoturvasta ja yksityisyyden suojasta verkkoyhteyttä käyttäessään. Tutkimuksessani keskityn siihen, miten suomalaisen peruskäyttäjän tietämys ja asenteet tietoturvakysymyksiä kohtaan vastaavat todellista tilannetta. Selvitän, millaista informaatiota julkiset ja kaupalliset organisaatiot välittävät tietoturvasta tavalliselle peruskäyttäjälle, ja miten käyttäjän hyödyntää tätä tietoa omassa toiminnassaan.

Tutkimusmotivaatio on myös osittain lähtöisin omasta käyttökokemuksesta. Roskapostit, vakoiluohjelmat ja virukset tuottavat päänvaivaa jo edistyneellekin käyttäjälle; kysymykseksi siis jää, miten peruskäyttäjä selviää kyseisistä ongelmista. Ratkaisuiksi tarjotaan palomuureja, monimutkaisia salasanoja, koneen suojaamista ulkopuolisilta käyttäjiltä, sekä erilaisia virustorjuntaohjelmistoja. Liittymäoperaattorit myyvät kuukausihinnoiteltuja tietoturvapalveluja, ja vakuuttavat niiden välttämättömyyttä. Kuinka peruskäyttäjä voi onnistuneesti arvioida tietoturvariskejä ja valita oikeat

ratkaisut omalle kotikoneelleen? Millaista tietoa peruskäyttäjälle on tarjolla tietoturvasta?

2. Lähtökohdat aiheesta

Tilastokeskus teetti vuosina 1996, 1999 ja 2002 haastattelututkimuksen suomalaisten suhtautumisesta tietoyhteiskunnan palveluihin ja tietosuojaan (Tilastokeskus, 2002). Tutkimuksessa kävi ilmi, että vaikka suomalaiset eivät ole erityisen huolestuneita tietosuojan toteutumisesta nykyaikaisessa yhteiskunnassa, on juuri tämä huolestuneisuus kasvanut vuosien 1996 ja 1999 välillä. Aikaisemmin tietosuojaan hyvinkin vakaasti luottaneen nuorison keskuudessa huolestuneisuus oli lisääntynyt, ja toisaalta yli 50 –vuotiaiden (aikaisemmin huolestuneimman ryhmän) luottamus tietosuojaan oli kasvanut. Tämä osoittaa sen, että käsitykset tietosuojasta ja tietoyhteiskunnasta ovat vielä muotoutumassa ja että tietoyhteiskunnan kehitys ei ole vielä asennetasolla saavuttanut vakaata tilaa suomalaisten keskuudessa.

Suomalainen peruskäyttäjä siis käyttää entistä enemmän tietokonetta ja Internet –palveluja. Toisaalta luottamus Internet –palvelujen turvallisuuteen on lisääntynyt. Viruksista ja tietoturvauhkista puhutaan, mutta vain harva kotikoneen peruskäyttäjä pystyy ymmärtämään näiden asioiden käytännön sisällön. Erilaiset oppaat kehottavat toimimaan tietyillä tavoilla, suullinen tieto välittyy käyttäjältä toiselle ja erilaiset käsitykset sekoittuvat. Ihmiset ovat huolestuneita, mutta ovatko he huolestuneita oikealla tavalla, oikeista asioista?

3. Peruskäyttäjän tietoturva kotikoneella

3.1. Käyttäjävalvonta

Yritysmaailmassa käyttäjävalvonta on yksi tärkeimmistä tietoturvan ylläpidon tavoista, mutta kotikoneen käyttöön ei useinkaan ajatella liittyvän varsinaisia tietoturvauhkia. Perheenjäsenet käyttävät konetta kukin omiin tarkoituksiinsa; lataavat ohjelmia ja luovat tiedostoja, vierailevat verkkopalveluissa omilla salasanoillaan ja tallentavat erilaisia dokumentteja koneelle. Tällaisessa tilanteessa ei kuvitella, että koneen käyttöä tulisi erityisesti valvoa tai ohjeistaa. Luonnollisestikin valvonnan tarve ja oikea toteuttamistapa riippuu perheen koostumuksesta. Esimerkiksi lapsiperheessä vanhempien tulisi olla tietoisia lapsen tekemisistä.

Microsoft ohjeistaa lapsiperheiden vanhempia tarkkaan suojaamaan jälkikasvuaan sopimattomalta aineistolta tietokonetta käytettäessä. Käytännössä tähän löytyy selvät ohjeet, mutta monessa perheessä lapset ja nuoret käyttävät tietokonetta ja Internetiä sujuvammin kuin vanhempansa. Lapsille kehotetaan määrittelemään omat, valvotut käyttäjätilinsä, neuvotaan, miten lapsen nettikäyttäytymistä voi seurata ja määritellään erilaisia rajoituksia, joita voi käyttää lapsen valvonnassa.

Äärimmäisten ohjeistusten mukaan käyttäjävalvonta tulisi viedä niin pitkälle, että jokaisella perheenjäsenellä on oma, henkilökohtainen koneensa. Tämän toteutuminen käytännössä tuntuu kuitenkin aika epätodennäköiseltä ja jopa ylireagoinnilta tietoturvauhkiin. Käyttäjän oma toiminta on kuitenkin peruslähtökohta onnistuneelle tai vastaavasti epäonnistuneelle tietoturvalle, minkä vuoksi ensisijainen ratkaisu tietoturvaongelmiin onkin oikeanlaisen tiedon välittäminen.

3.2. Virusten torjunta

Petteri Järvisen mukaan ”Tietoturva on 20 % tekniikkaa ja 80 % psykologiaa”. Tällä hän viittaa siihen, että käyttäjät odottavat erilaisten tietoturvaohjelmistojen ratkaisevan kaikki nykyiset ja tulevat tietoturvaongelmat, todellisen tilanteen ollessa ihan toisenlainen. Tietoturva onkin nähtävä kaiken kaikkiaan yleisluontoisena ongelmana, johon vaikuttavat ratkaisevasti teknisten näkökulmien lisäksi myös käyttäjän tietämys ja toiminta.

Erilaiset tietokonevirukset ovat tietoturvauhkista kenties näyttävimmin esillä mediassa. Kotikoneen suojaamiseksi näiltä haitallisilta ohjelmilta tarjotaan sekä erillisiä tietoturvaohjelmistoja, että operaattorin tarjoamia kokonaisvaltaisia tietoturvapalveluja. Kotikäyttäjän voi kuitenkin olla vaikeaa tunnistaa tarvetta ohjelmistoille. Myös asennus- ja päivitystoiminnot voivat olla ylivoimaisen vaikeita tietokoneen peruskäyttäjälle. Esimerkkinä mainittakoon Symantecin tarjoama virustorjuntaohjelmisto Norton Anti-Virus, jonka käyttäjiä opastetaan uusimaan vanhentunut tilaus puhelinpalvelun kautta. Palvelua on kuitenkin saatavilla ainoastaan ruotsiksi ja englanniksi. Tilauksen uusiminen tätä kautta siis vaatii jo merkittävää kielitaitoa ja alan sanaston tuntemusta.

4. Peruskäyttäjän tietoturva Internet -palveluissa

4.1. Sähköposti

Peruskäyttäjä valitsee itselleen usein jonkin yleisimmistä ja ilmaisista Internet –sähköposteista. Harva sähköpostin käyttäjä kuitenkaan tuntee tekniikkaa, jolla postin kulku varmistetaan. Silti käyttäjä useinkin luottaa sähköpostiin kuten tavalliseen kirjepostiin. Webmailin etu on siinä, että käyttäjä voi lukea postinsa mistä tahansa verkkoyhteyden ulottuvilta. Peruskäyttäjän yleisimmät sähköpostiin liittyvät ongelmat ovat yleensä seuraavanlaisia: ohjelma ei anna kuittausta viestin vastaanottamisesta, viesti lähtee väärälle vastaanottajalle tai osoite on virheellinen. Kuitenkin sähköpostia käytetään erittäin henkilökohtaisten ja luottamuksellisten asioiden välittämiseen. Sen välittömyyden ja helppouden vuoksi myös yhteydenottokynnys madaltuu. Sähköpostilla lähestytään tahoja ja käsitellään asioita, joihin esimerkiksi puhelinyhteydellä ei olla valmiita. Tämän lisäksi roskapostitulva ja epämääräiset liitetiedostot aiheuttavat ongelmia lähestulkoon jokaiselle sähköpostia käyttävälle.

Internet –sähköpostia käytettäessä on huomioitava koneen muut käyttäjät. Julkista päätettä käytettäessä on huomioitava asetukset, joilla osoite ja salasana saadaan tallennettua seuraavaa istuntoa varten. Näistä asetuksista täytyy kuitenkin olla tietoinen ja niitä tulee osata muokata, jotta tietoturva säilyisi. Samoni välimuistin asetukset on syytä tuntea. Oman uhkansa sähköpostin käyttöön tuovat liitetiedostot, roskaposti, virukset ja huonot salasanat. Perheen sisällä sähköpostin pitäminen yksityisenä voi olla vaikeaa, sillä useat sähköpostiohjelmat (esimerkiksi Hotmail) käyttävät unohtuneen salasanan lähettämisessä henkilökohtaista varmistuskysymystä, jonka vastaus edellyttää ainoastaan käyttäjän perusteellista tuntemista.

Peruskäyttäjä voi ajatella, että oma sähköpostikansio ei sisällä mitään erityisiä salaisuuksia, eikä tämän vuoksi vaivaudu esimerkiksi suojaamaan salasanaansa muilta. Internet –sähköpostin käyttö henkilökohtaisena viestivälineenä toimii, mutta yritys – tai työasioiden hoidossa on syytä käyttää toisenlaista postipalvelua.

4.2. Pankkipalvelut

Sähköisten pankkipalvelujen käyttö arveluttaa peruskäyttäjää kenties eniten. Toisaalta reaalimaailman pankkipalveluiden maksullisuus ja varsinaisen kassapalvelun hitaus ajavat yhä useampia käyttäjiä verkkopankkien asiakkaiksi. Pankkiasioiden hoitaminen kotikoneelta on paitsi nopeaa ja käytännöllistä, myös edullista. Kuitenkin juuri tämä käyttömukavuus voi johtaa käyttäjän huolimattomaan toimintaan. Kaiken kaikkiaan mistä tahansa maksuvälineestä tulee turvaton, jos sen käyttöä ei toteuteta huolellisesti (Järvinen, 2002, s. 215).

Osuuspankin verkkopalvelun käyttö vaatii käyttäjätunnuksen ja salasanan, sekä kertakäyttöisiä palvelun avainlukuja sisältävän avainlukulistan. Vaihtoehtoisesti sisäänkirjautumisen voi suorittaa sähköistä henkilökorttia käyttäen, mikä vaatii koneelta erillisen tietokoneeseen asennetun lukulaitteen. Näin ollen kotikäyttäjälle tavallisempi tapa on tunnuslukujen käyttö tunnistautumisessa. Käyttäjätunnus on numerosarja, joka sisältää 6 lukua. Salasanaksi vaaditaan nelinumeroinen luku, jonka säännöllisestä vaihtamisesta ei muistuteta. Palvelu muistuttaa käytön lopettamisesta uloskirjautumisen kautta ja huomauttaa sivuhistorian tyhjentämisestä käytön jälkeen. Käyttäjälle on tarjottu myös linkki, jossa on yksityiskohtaiset ohjeet näiden tehtävien suorittamiseksi. Etusivulta löytyvässä uutisartikkelissa käsitellään lisäksi pankkipalveluihin liittyvää tietoturvaa.

Osuuspankin verkkopalvelussa varoitetaan tunnuslukujen ja pin –koodien antamisesta muille henkilöille ja tiedotetaan lyhyesti yleisimmistä Internet –palvelujen käyttöön liittyvistä tietoturvariskeistä. Palvelua käyttävän on siis syytä säilyttää avainluvut erillään muista tunnuksista, jotta tehokas suojautuminen on mahdollista. Lisäksi salasanan vaihto ajoittain on tarpeellista. Kummastakaan seikasta ei käyttäjälle muistuteta, mikä olisi ehdottoman tarpeellista verkkopankin asiakkaille. Palvelun tietoturvaominaisuudet jäävät hämäräksi, eikä käyttäjän oman toiminnan tärkeyttä hyvän tietoturvallisuuden säilyttämisessä korosteta tarpeeksi.

Aktia Säästöpankin verkkosivuilla Internet –pankin käyttöön käyttäjää opastetaan etusivun verkkomanuaalissa. Pankin käyttäjä saa 8 numeroisen käyttäjätunnuksen ja voi tämän jälkeen itse määritellä 6-8 merkkiä pitkän salasanan, joka voi sisältää kirjaimia, numeroita tai muita merkkejä. Lisäksi

kaikki pankissa tehtävät toimeksiannot vahvistetaan 88 lukua sisältävällä avainlukukortilla, jonka lukuja käytetään satunnaisessa järjestyksessä. Palvelu myös katkaisee itse yhteyden, jos sitä ei käytetä 15 minuuttiin. Aktian verkkopankki muistuttaa käyttäjää vaihtamaan salasanansa kuukauden välein. Palvelun esittelyssä korostetaan tietoturvan eri näkökulmia, ja selvitetään tarkasti, mitä käyttäjä voi itse tehdä tietoturvan parantamiseksi.

Aktian palvelun käyttäjä saa tietoa salasanojen ja tunnusten hallinnasta ja oikeanlaisesta käytöstä, käytetystä yhteysmenettelystä ja salaustekniikasta, oman ja muiden kotikonetta käyttävien toiminnasta tietoturvan hyväksi, toiminnasta esimerkiksi salasanan unohtuessa sekä selaimen ja välimuistin asetuksista. Ohjeistus on mielestäni tarpeellinen ja helppokäyttöinen, ja se korostaa käyttäjän oman toiminnan merkitystä. Pankkipalvelun verkkokäyttö on luonnollisesti asia, jonka käyttäjät haluavat turvata. Oikeanlainen tiedon jakaminen auttaa tässä mielestäni enemmän, kuin asiaton pelottelu tietoturva-aukoilla. Tässä Aktian verkkopalvelu on mielestäni onnistunut parhaiten verrattuna tässä tarkasteltuihin muihin verkkopankkeihin.

Nordean Solo –palvelussa käyttäjän tunnus on 6 merkkiä pitkä ja salasana sisältää 4 merkkiä. Yhteys katkaistaan myös 15 minuutin käyttäjähiljaisuuden jälkeen. Käytön lopettamisen jälkeen sivuhistorian tyhjentämisestä muistutetaan, mutta samalla ruudulla näkyy omituiselta vaikuttava ilmoitus ”yhteysnumerosi oli xxxxxxxx”. Etusivun linkistä ”Tietoturvaohjeita pähkinänkuoressa” käyttäjälle aukeaa tietoisku tietoturvasta. Tässä keskitytään kuitenkin yleisiin tietoturvaohjeisiin ja niihinkin teknisellä otteella. Esittelyssä ei siis kuvata juurikaan sitä, miten käyttäjän tulisi toimia, jotta tietoturvariskit pysyisivät mahdollisimman pieninä. Salasanan vaihtamisesta mainitaan, mutta muutoin esittely käsittelee hyvin abstrakteja tietoturva-asioita. Peruskäyttäjän kaipaamat konkreettiset ohjeet jäävät puuttumaan.

4.3. Verkkokauppa

Verkkokaupassa ja sen sovelluksissa ostajan ja myyjän välisen luottamuksen saavuttaminen vaikeutuu. Asiakkaan henkilöllisyyden tai maksun todentaminen on kriittistä, samoin kuin se, että tilaaja saa tuotteen, josta on maksanut. Verkkokaupan maksukäytännöt voivat tuntua peruskäyttäjästä pelottavilta, kun konkreettista yhteyttä myyjään ei ole (Järvinen, 2002, s. 364).

Verkkokauppa osoitteessa www.verkkokauppa.com on laaja sähköinen kauppa, jonka tuotevalikoimassa ovat mm. atk- laitteet ja tarvikkeet. Sisäänkirjautumisen yhteydessä käyttäjälle tarjotaan linkkiä ”Lisätietoa tietoturvapolitiikastamme”. Tämä ei kuitenkaan anna peruskäyttäjälle minkäänlaista informaatiota varsinaisesta tietoturvan tilasta. Tilaus- ja tilinhallinnan kerrotaan olevan toteutettu 128 –bittisellä salauksella ja käyttäjälle vakuutetaan että kaikki hänen antamansa tiedot siirtyvät yritykselle salattuina. Käyttäjän tunnuksina ovat sähköpostiosoite ja salasana. Muuta tietoa tämän verkkokaupan tietoturvasta ei käyttäjälle anneta.

Ruoka.net –osoitteessa toimiva kodin- ja elintarvikkeiden verkkokauppa tarjoaa etusivullaan linkin Tietoyhteiskunnan Kehittämiskeskuksen sivuille. Sivuilta löytyy sähköisen kaupan opas peruskäyttäjälle. Ohjeistus on pitkä ja raskas luettava. Oppaassa kerrotaan, miten käyttäjä voi minimoida ostotapahtuman riskit. Ruokaostoksia voi halutessaan suorittaa suojatulla yhteydellä etusivun linkin kautta. Valinta ei kuitenkaan aiheuta palvelussa mitään havaittavaa muutosta, joten käyttäjän luottamus ei toimenpiteen myötä lisäänny.

Anttilan verkkokauppa netAnttila.com ei vaivaa käyttäjiä tietoturva-asioilla. Ainoastaan sivuston info-osuudesta löytyy kysymyksiä ja vastauksia, joissa käsitellään myös tietoturva-asioita. Anttila vastaa käyttävänsä SSL- tekniikkaa ja muistuttaa käyttäjää sivuhistorian tyhjentämisestä. Lisäksi muistutetaan siitä, että jokainen asiakas vastaa tunnuksillaan tehdyistä tilauksista. Käyttäjälle ei tarjota edes linkkiä yleisiin tietoturvaoppaisiin, ja koko aihe sivuutetaan kevyesti.

5. Peruskäyttäjän tietämys ja asenteet

Peruskäyttäjän tietämys tietoturvasta vaihtelee kovasti käyttäjän taustasta riippuen. Työn ja koulutuksen merkitys näkyy selvästi, samoin kuin eri ikäluokkien erot. Valmiin kotikonepaketin - ja mahdollisesti valmiiksi asennetun tietoturvaohjelmiston - käyttäjä ei useinkaan tunnista tietoturvan ongelmakohtia itse. Huolestuneisuus tietoturvakysymyksistä on Tilastokeskuksen mukaan yleisesti laskenut (Tilastokeskus, 2002). Toisaalta käyttäjät voivat olla ylihuolestuneita siihen pisteeseen asti, etteivät uskalla avata sähköpostiaan. Toisaalta taas liika mukavuus ja luottamus ohjelmistoihin saa aikaan varomatonta käyttäytymistä. Neutraalia ja asiallista suhtautumista edesauttava informaation jakelu ei näytä onnistuneen. Peruskäyttäjän osaaminen ja asennoituminen tietoturvakysymyksiin ei ole kohdallaan.

Seuraavassa tarkastellaan, millaista informaatiota tietoturvasta on tarjolla peruskäyttäjälle.

6. Saatavilla oleva tieto ja sen ongelmat

6.1. Julkinen sektori

Valtiovarainministeriö julkaisee Asiointiopas.fi –sivustolla tietoturvaohjeistuksia hallinnon verkkopalveluihin. Sivusto kehottaa käyttäjiä mm. tutustumaan tietoturvasäädöksiin, käyttämään virustorjuntaohjelmistoja ja salattua yhteyttä. Pelkästään nämä ohjeet saavat taitotasoltaan vaatimattoman peruskäyttäjän ymmälleen. Tietoyhteiskunnan kehittämiskeskuksen sivuilla tarjotaan lisäohjeistusta taitamattomalle käyttäjälle. Ohjeissa annetaan hyvin yleispäteviä ohjeita tietoturvasta. Käyttäjää neuvotaan olemaan tarkkana puheidensa suhteen ja käyttämään muita kuin kokonaan kirjaimista koostuvia salasanoja (Tieke, 2004).

Kotikoneen käytöstä Asiointioppaassa mainitaan varmuuskopioiden teko, sekä virustorjuntaohjelmien ja palomuurin käyttö. Näistä ei kuitenkaan anneta lisätietoa, eikä käyttäjää opasteta lainkaan eteenpäin. Torjuntaohjelmat ja palomuurit on siis osattava hankkia ja asentaa itse, jos käytettävissä ei ole tietotekniikan taitajaa. Tiedon ongelmana ei ole siis sen vähyys tai puutteellisuus, vaan varsinaisten toimintaohjeiden puuttuminen. Käyttäjää voidaan neuvoa ”pitämään huoli selaimen asetuksista”, mutta tämän tarkoitus jää varmasti hämäräksi useammalle peruskäyttäjälle. Oppaan käyttäjälle tarjotaan mahdollisuus lähettää palautetta oppaan tekijöille, mutta seminaarityötä kirjoitettaessa linkki oli viallinen, eikä käyttäjä voi siis esittää kysymyksiä. Tarjolla ei myöskään ole linkkejä muihin tietoturva-artikkeleihin tai ohjeistuksiin ja kokonaisuudessaan tämä Valtiovarainministeriön julkaisema ohjeistus on hyvin vaatimaton.

Viestintäviraston sivusto (www.ficora.fi) on sisällöltään selvästi teknisempi ja yksityiskohtaisempi. Sivusto antaa tietoa Suomen tietoturvalainsäädännöstä, raportoi tuoreimmat virukset ja muut tietoturvauhkat, sekä antaa ohjeita keskeisimpien tietoturvauhkien torjumiseen. Ohjeissa käsitellään myös esimerkiksi palomuuriohjelmiston asentamista kotikoneeseen, mutta itse tekstiosuus jää raa’an tekniseksi ja käyttäjä ohjataan lopulta tietoiskuun palomuureista tai ohjelmistovalmistajien ulkomaisille www –sivuille. Ideana tämä yksityiskohtaisiin käyttäjätapauksiin perustuva ohjeistus on toimiva,

mutta peruskäyttäjälle sivusto ei tarjoa minkäänlaista apua. Edistyneempikin käyttäjä joutuu tutkimaan ohjeita perusteellisesti, jotta asiasisältö selkenee.

6.2. Uutisjulkaisut

Digitoday – verkkojulkaisu käsittelee tietoturvaa laajasti asiantuntijatasolla. Uutisoinneista löytyy ajankohtaisia aiheita miltä tahansa tietoturvan alueelta. Raportit ovat kattavia ja asiapitoisia, ja näin ollen tiedonhakijalla tulee olla ainakin perustiedot tietoturvasta. Data –osuudesta löytyy kuitenkin myös ohjeita vaatimattomammille peruskäyttäjille. Ohjeissa neuvotaan esimerkiksi kotikoneen ja Internet –yhteyden turvallisempaan käyttöön.

Sektori.com –tietotekniikan uutispalvelu välittää myös tietoturvauutisia verkkokäyttäjille. Tarjolla on tuoreita uutisointeja tietoturvasta, ja käyttäjillä on mahdollisuus keskustella ja kommentoida aiheita. Tämäkään palvelu ei tarjoa erityisen suurta hyötyä perustaitoiselle kotikäyttäjälle, sillä oletusarvoisena palvelun käyttäjäkunta on IT-alan ammattilaisia tai taitotasoltaan osaavia harrastelijoita.

6.3. Kaupalliset organisaatiot

Kaupallisten organisaatioiden tietopaketteja löytyy Internetistä runsaasti. Jokainen palvelun- tai ohjelmistontarjoaja korostaa juuri niitä tietoturvaongelmia, joiden ratkaisuihin omia ohjelmistoja myydään. Tietoturvaohjelmistojen ja käyttäjän ohjeiden lisäksi myydään tietoturvakoulutusta yritysten lisäksi yksityishenkilöille. Järvinen ottaa kirjassaan kantaa tähän värittyneeseen tiedonvälitykseen. ”Pelko on hyvä myyntivaltti”, hän kirjoittaa viitaten torjuntaohjelmistoja tuottavien yritysten taipumukseen uutisoida näyttävästi ja jopa liioitellen tietokonevirusten haittavaikutuksia oman myyntinsä edistämiseksi (Järvinen, s. 29).

6.3.1. Tietoturvaohjelmistojen tarjoajat

Symantec tarjoaa sivuillaan kotikäyttäjälle informaatiota tuotteistaan, tukipalveluistaa ja yleisen tason tietoturvasta. Kotikäyttöön tarkoitettuja tuotteita ovat Norton AntiVirus –ohjelmisto ja sen eri versiot, Personal Firewall sekä viestintä- ja ongelmanratkaisutyökalut. Symantec tarjoaa myös mahdollisuuden selvittää kotikoneen tietoturvan taso verkkosivuilta löytyvällä testillä. Erilaiset käyttäjien kysymykset saavat myös sivustolla vastauksia.

Luonnollisesti jokaiseen ongelmaan on tarjolla jokin Symantecin tuote. Tälläkin sivustolla varsinainen tietoaines jää vähäiseksi, ja sivusto on suunniteltu tuotteiden myymistä – ei niinkään tietoturvan edistämistä – tukevaksi. Käyttäjälle tarjotaan tuotteita, mutta niiden varsinaisista taustoista jää hyvin hämärä käsitys.

F-secure tarjoaa kotikäyttäjälle AntiVirus –ohjelmistoja ja palomuureja. Tuoteinformaatio on annettu englanniksi, ja käyttäjälle ei suoranaisesti selviä mitä tuotetta käytetään mihinkin tarkoitukseen. Sivuilla kerrotaan myös tuoreimmista virusuhkista ja neuvotaan erilaisissa tietoturvatoimenpiteissä, esimerkiksi virusten poistamisessa. Tälläkin sivustolla hyvä tietoturva yhdistetään lähes suoraan F-Securen tarjoamiin tuotteisiin, eikä yleispätevää informaatiota juurikaan löydy. Kaupalliset tarkoitukset sivusto toki täyttää, mutta yleisempää tietoa hakeva käyttäjä ei löydä haluamaansa.

Elisan kotisivujen tietoturvaosiossa käyttäjää ohjeistetaan alustavasti yleisemmällä tasolla. Tietoturvan perusperiaatteet mainitaan ja käyttäjälle tarjotaan linkki myös Tietoturvaopas. fi – manuaaliin. Itse Elisa tarjoaa asiakkaalleen sähköpostin käsittelyyn, virustorjuntaan ja palomuureihin liittyviä ratkaisuja. Elisa Kotipostin Virusturva ja Roskapostinsuodatin käsittelevät saapuvan postin ja F-Securen tuottama palomuuripalvelu tarjoaa yhdistetyn palomuurin ja virustorjunnan.

Elisan tietoturvapalvelut voi ostaa suoraan verkosta, jolloin käyttäjä voi laskea vastuun tietoturvasta Elisan harteille. Palvelua tarjotaan aloitusmaksulla 8,24 euroa, jonka jälkeen kotikäyttäjän kuukausimaksu on 5,89 euroa. Tämä ratkaisu voi tuntua helpolta käyttäjästä, joka ei halua vaivata itseään tietoturvakysymyksillä. Kuitenkaan Elisa ei tarjoa tarkempaa tietoa siitä, mitä tämän rahan vastineeksi saa. Esimerkiksi sähköpostin suodattamisen periaatteita ja mahdollisista vastuukysymyksistä tietoturvaongelmien sattuessa ei käyttäjälle kerrota. Vastaavia kuukausiveloitettuja tietoturvapalveluita tarjoavat myös Sonera, DNA ja Welho. Kaikki nämä ovat ominaisuuksiltaan lähes toisiaan vastaavia ja sisältävät siis myös samat informaationpuutteesta johtuvat ongelmat kuin Elisan tietoturvapalvelu.

6.3.2. Käyttäjän ohjeet

Microsoft tarjoaa suomenkielisillä sivuillaan yleisempää tietoa kotikäyttäjän tietoturvasta. Artikkeleissa mainitaan erityisesti Windowsin tietoturvaominaisuudet, mutta keskitytään kuitenkin yleisen tason ohjeisiin, mikä on käyttäjän kannalta toivottavaa. Tarjolla on yksityiskohtaista tietoa kotikoneen ja Internetin käytöstä sekä perustietoturvasta. Esimerkiksi palomuuritekniikoista on perusteellinen selitys taitamattomallekin käyttäjälle. Käyttäjä pääsee tietoturvaoppaasta myös suoraan tietoturvatuotteiden valmistajien sivuille. Tämä tietoturvaohjeistus on hyvä peruspaketti käyttäjälle, jonka tietoturvaosaaminen on alkutekijöissään.

”Turvallisesti nettiin – Kansalliset tietoturvatalkoot” –otsikolla ilmestynyt verkko-opas käsittää perustietoa ja ohjeita käyttäjälle. Opas on suunniteltu sekä julkisten, että kaupallisten organisaatioiden yhteistyöllä ja mukana on mm. ohjelmistotalo Computer Associates Finland, Eduskunnan Liikenne- ja Viestintävaliokunta, sekä useita muita viestintä- ja teleliikenteen yrityksiä sekä yhteisöjä. Opas aloittaa käyttäjän ohjeistuksen ruohonjuuritasolta ja kertoo yksityiskohtaisesti perustiedot Internetin kautta syntyvistä tietoturvaongelmista ja niiden käsittelystä. Käyttäjä voi myös esittää sivuilla kysymyksiä tietoturvasta, ja vastaukset tuntuvat helppotajuisilta ja asiallisilta. Tässä oppaassa on pystytty keskittymään itse ongelmiin yleisellä tasolla, eikä kaupallista ohjelmistotarjontaa ole korostettu mitenkään. Oppaaseen tutustuminen on hyödyllistä kenelle tahansa kotikäyttäjälle, ja siitä löytyy perustietojen lisäksi yhteystietoja ongelmatilanteen varalle.

6.3.3. Tietoturvakoulutus

Tieturi Oy tarjoaa tietoturvakoulutusta lähinnä yrityksille. Osana Tieturin Tietoturvan kehittämisohjelmaa yritys järjestää Käyttäjän tietoturvaa käsitteleviä koulutuksia. Nämä koulutukset ovat kuitenkin yrityskohtaisia, ja jälleen peruskäyttäjän tietoturvatietämys nojaa työnantajan harteilla.

Tamperelainen Contrasec tarjoaa sivuillaan tietoturvakurssia ”tavallisille loppukäyttäjille”. Kurssin kestoa ei suoranaisesti mainita, mutta sivuilta selviää että kyseessä on 1-2 päivää kestävä koulutus. Kurssin sisällön teemat käsittelevät aiheita yleisestä tietoturvasta www-selailuun ja edelleen salasanoihin. Kurssin hinta on 350 euroa + alv 22%. Kurssin tavoitteena on, että: ” Kurssilaiset oppivat käyttämään PC:tä turvallisesti ja ymmärtävät, mitä

tietoturva PC-ympäristössä merkitsee". Tällaisiin koulutustilaisuuksiin osallistuminen vaatii käytännössä sen, että käyttäjän työnantaja järjestää kyseisen mahdollisuuden, vaikkakaan yksityishenkilöiden osallistumista ei varsinaisesti ole rajoitettu.

6.4. Käyttäjien keskustelut

Käyttäjien keskusteluja seurattaessa kotikoneen tietoturvan ongelmallisimmat kohteet liittyvät juuri virustorjuntaohjelmiin. Suomi24.fi – keskustelufoorumissa käyttäjät voivat keskustella ajankohtaisista tietoturva-aiheista, ja tällä hetkellä ongelmalliset tilanteet sivuavat erilaisia viruksia ja niiden torjuntaa. Käyttäjien keskusteluja leimaa se, että näitä foorumeja käyttävät jakautuvat selkeästi kahdeksi ryhmäksi: perustaitoisiin käyttäjiin, joilla on ongelma sekä osaavimpiin käyttäjiin, jotka käyttävät kanavaa neuvoakseen kanssakeskustelijoita (suomi24).

Osoitteessa www.virustorjunta.net toimii foorumi, jonka rekisteröityneet käyttäjät voivat lukea artikkeleita ja keskustella tietoturvasta. Käyttäjälle tarjotaan näin kattavaa kokemuspohjaista tietoa, melkeinpä tietoturvan aiheesta kuin aiheesta. Tämä kanava on suunnattu kuitenkin lähinnä asiantunteville käyttäjille, joiden tietotaso on selvästi normaalia kotikäyttäjää korkeampi. Sivustolla on asiallisia artikkeleita ja paljon ajankohtaista tietoa nykyhetken tietoturvatilanteesta.

Erään käyttäjän henkilökohtaisella sivustolla (osoitteessa www.markusjansson.net) on pureuduttu kotikoneen käyttäjän tietoturvaan lähtien alkeista. Tämän harrastelijan sivulta löytyy informaatiota salauksista, viruksista, tietoturva-aukoista ja oman toiminnan tärkeydestä. Sivun pääsisältö on se, että käyttäjän tulee pitää huolta omasta yksityisyydestään. Tähän tähtääviä toimenpiteitä ohjeistetaan kädestä pitäen, ja sivusto on helppotajuinen jopa peruskäyttäjälle. Kuitenkin tämänkaltaisten tietolähteiden kohdalla herää kysymys tekijän asiantuntemuksesta ja motiiveista. Sivuilta löytyy esimerkiksi useita linkkejä erilaisiin testeihin ja tiedostojen latauksiin. Näiden lähempi tarkastelu ei kuitenkaan varovaista käyttäjää houkuta. Toisaalta sivusto tarjoaa runsaasti asiallista tietoa ja linkkejä esimerkiksi viestintäviraston sivustolle. Ilmeisesti käyttäjän tarkoitus on sittenkin levittää tietoa yksityisyyden suojasta tietoverkkojen maailmassa. Valitettavasti tätäkään sivustoa ei peruskäyttäjän ole helppoa löytää.

Käyttäjien omilla palstoilla liikkuu paljon hyödyllistä tietoa tietoturvasta. Ongelmana on lähinnä se, miten tottumaton käyttäjä löytää näille palstoille. Toisaalta tiedonlähteet keskustelufoorumeilla ovat hyvinkin epävarmoja, ja ohjeista voi olla vaikeaa tai jopa mahdotonta poimia ne, joita todella kannattaa noudattaa. Erinomaisena kanavana nämä foorumit toimivat silloin, kun käyttäjällä on kysymyksiä tai ongelmia, joihin ei muualta saa vastausta. Osaavammat käyttäjät ovat erittäin halukkaita kommentoimaan ongelmia, joita kotikonetta käyttävä voi kohdata. Monet löytävät avun ongelmiinsa juuri tämän tiedonlähteen kautta, mutta perustasoinen käyttäjä vaatii apua jo löytääkseen näille foorumeille.

7. Yhteenveto

Peruskäyttäjän tietotekninen osaaminen, ja erityisesti tietoturvaosaaminen, liittyy kiinteästi henkilön työnkuvaan. Lähes jokainen työympäristö painii tietoturvasäädösten ja –ongelmien kanssa, ja siten kulunvalvonta, käyttäjien tunnistaminen ja tietoturvan ohjeistukset ovat entistä useamman työntekijän arkipäivää. Työssään tietoturvakäytäntöjen kanssa toimivat ovat siis luonnollisesti paremmin informoituja kuin tietokonetta ainoastaan kotiympäristössään käyttävät.

Peruskäyttäjälle tarjottava tieto on lähteestä riippuen sekalaista. Viruksista puhutaan ja niiden avaamisesta varoitetaan, mutta tieto varsinaisista toimenpiteistä kotikoneella on kiven alla. Viralliset sähköiset esitteet antavat toki informaatiota, mutta käyttäjän on osattava etsittävä nämä sähköiset neuvonannot.

Kotikoneen ja Internetin käytössä peruskäyttäjä kohtaa monia tietoturvakysymyksiä, mutta tuskin lainkaan vastauksia. Monet palveluista sivuuttavat tietoturvaominaisuudet täysin, ja näin käyttäjälle voi syntyä illuusio siitä, että palvelu on turvallinen käyttää. Mukavuudenhaluinen käyttäjä ei myöskään usko tarvitsevansa erityistä suojaa ulkopuolisilta hyökkäyksiltä. Juuri tämä usko hyvästä tietoturvasta saa käyttäjän toimimaan varomattomasti. Julkisten tahojen kannanotot tietoturvaan ovat usein heikosti saatavilla ja niiden asiasisältö voi olla vanhentunutta. Kaupalliset organisaatiot taas mielellään liioittelevat itselleen ja omalle myynnilleen edullisia tietoturvauhkia. Tarjolla on ohjelmistoja ja kokonaisia kuukausihinnoiteltuja tietoturvaratkaisuja. Tässäkin tilanteessa käyttäjän on osattava asennusprosessi ja mahdollisesti vielä huolehdittava vastuukysymyksistä kaupatun järjestelmän pettäessä.

Käyttäjien keskeinen tiedonvälitys, esimerkiksi keskustelufoorumien kautta, on kanavana käyttökelpoinen, mutta senkään tietämykseen ei voi sinisilmäisesti luottaa. Näin ollen peruskäyttäjä on kotikoneen tietoturvaongelmissa varsin yksin. Helppona ratkaisuna monet pitävät laitevalmistajien valmiita tietoturvaohjelmistoja, jotka päivittävät itse itsensä. Ongelmakenttä on kuitenkin laajempi, sillä harva huomio oman toimintansa tärkeyttä tietoturvan ylläpidossa.

Tietotekniikan käyttö lisääntyy edelleen ja tietämys tietoturvakysymyksistä laahaa perässä. Mielestäni jokaiseen kotiin olisi hyödyllistä jakaa asiallista informaatiota käyttäjän oman toiminnan merkityksestä tietoturvan parantamisessa. Tämä informaatio olisi hyvä saada luotettavasta lähteestä, ja informaation tulisi puhutella juuri perustaidot hallitsevia kotikoneen käyttäjiä. Tällä tavoin mahdollisuudet väärinkäytöksiin vähenisivät ja käyttäjän luottamus tietotekniikkaan ja sen käyttöön kasvaisi.

Viiteluettelo

Aktia.fi

Asiointiopas.fi - Käyttäjän opas hallinnon verkkopalveluihin
http://www.asiointiopas.fi/asiointiopas/suomi/tietoturva_verkossa/?device=text

Contrasec -tietoturvakoulutus
http://www.contrasec.fi/1801/1801.html

DigiToday - Mitä on spyware?
http://www.digitoday.fi/showPage.php?page_id=14&news_id=22726

Elisa.fi - Internetin käyttäjän tietoturva
http://www.elisa.fi/index.cfm?t=1&o=127.00

F-Securen suomalainen kotisivu
http://support.f-secure.com/fin/home/index.shtml

Järvinen, Petteri: Tietoturva ja yksityisyys, Jyväskylä 2002, (muutoksia ja lisäyksiä kirjan tietoihin)
http://www.pjoy.fi/kirjat/tietoturva/

markusjansson.net - miksi yksityisyydestään kannattaa pitää huolta
http://www.markusjansson.net/fwhybother.html

Microsoft - Tietoturva kotikäyttäjille
http://www.microsoft.com/finland/security/kotikayttaja/7steps.asp

Microsoftin opas vanhemmille
http://www.microsoft.com/finland/security/childrenonline/

Netanttila
http://www.netanttila.com

Nettikaista - Tietoturva
http://www.nettikaista.fi/tietoturva

Nordean verkkopankki
http://www.nordea.fi

Osuuspankin verkkopalvelu
http://www.osuuspankki.fi

Sektori.com - IE:ssä vakava tietoturva-aukko
http://sektori.com/uutiset/2939/online

Suomi24.fi – käyttäjien keskustelufoorumi
http://keskustelu.suomi24.fi/show.fcgi?category=108&conference=1500000000000007

Tietoturva Internetissä - käyttäjän tietoturva
http://keskus.hut.fi/opetus/s38118/s99/htyo/64/salasanat.shtml

Tietoturva ja virukset
http://appro.mit.jyu.fi/2004/kevat/tyovaline/luennot/luento9/
Tietoyhteiskunnan kehittämiskeskus, sähköisen kaupan opas
http://www.tieke.fi/kauppa/ostoksilla
Tieturi Oy
http://www.tieturi.fi
Tilastokeskus - suomalaiset tietoyhteiskunnassa
http://www.tilastokeskus.fi/tk/yr/tietoyhteiskunta/suomalaiset.html
Turvallisesti nettiin – kansalliset tietoturvatalkoot
http://www.tietoturvaopas.fi
Verkkokauppa
http://www.verkkokauppa.com/
Virustorjunta.net - keskustelufoorumi virustorjunnasta ja tietoturvasta
http://www.virustorjunta.net/modules.php?name=Forums
Symantecin suomalainen kotisivu
http://www.symantec.fi/

Roskaposti ja sen torjunta

Susanne Anttila

Roskapostissa on kyse tietoturvaongelmasta. Ongelmaa ei aluksi ymmärretty vakavaksi, eikä sen analysointiin käytetty resursseja. Vasta viime vuosina, ongelman paisuttua, on tehty laskelmia, miten paljon ihmisten työaikaa ja kaistan leveyttä roskaposti tuhlaa. Ratkaisun löytämiseksi roskapostista pitää tietää miten, miksi, ketä ja kenelle sitä lähetetään. Tämän jälkeen on ratkaistava, miten roskapostia voidaan torjua. Erilaisia torjuntakeinoja on kehitetty ja kehitetään edelleen.

Avainsanat ja -sanonnat: roskaposti, spam.
CR-luokka: H.4.3 Sähköposti

Sisällys

1. Johdanto

Roskaposti käsitteenä on laaja. Yleisimmin roskapostiksi luetaan sellainen sähköposti, jota vastaanottaja ei ole halunnut saada (ks. esim. [Sorkin, 2004]). Roskaposti on jokapäiväinen ongelma niiden kohdalla, joiden sähköpostiosoite on ollut kohtuullisen aktiivisessa ja julkisessa käytössä. Roskapostia on alettu tutkia vasta viime vuosina ongelman nuoruudesta johtuen. Aiheen tutkimusta löytyy niin etiikan tutkimuksesta kuin tilastotieteestä.

Ongelmaa on lähestytty ohjelmallisesti kehittämällä erilaisia suodatintoimintoja perustuen merkkijonojen täsmäyksestä koneoppimisen menetelmiin. Erilaisista menetelmistä löytyy jonkin verran vertailevia tutkimuksia.

1.1. Mikä on roskapostia

Spamhaus [Spamhaus, 2004] määrittelee englanninkielisen roskapostin käsitteen UBE (Unsolicited Bulk Email) seuraavasti: pyytämätön (Unsolicited) tarkoittaa, että vastaanottaja ei ole antanut todistettavissa olevaa lupaa viestin lähettämiseen. Roska (Bulk) tarkoittaa, että viesti on lähetetty osana suurta samankaltaisten viestien joukkoa.

Käsite UCE (Unsolicited Commercial E-Mail) puolestaan käytetään [Järvinen, 2000], kun tarkoitetaan sähköpostilla saapuvaa, usein arveluttavaa aikuisviihteeseen liittyvää, mainontaa, jossa kustannukset jäävät sattumanvaraisesti valitulle vastaanottajalle. Käyttäjän lisäkustannus verkon käytön kuukausimaksuna arvioitiin vuonna 2000 olevan noin 2 dollaria. London Internet Exchange:n (LINX) ehdotus roskapostin nimeksi on Unsolicited Bulk Materia (UBM).

Varsinaiselle sähköpostille on mm. François Pinard ehdottanut nimitystä Ham erotuksena roskapostille käytetystä Spam-nimityksestä. Spam on laajempi käsitteenä kuin UBE tai UCE. Spamhaus selittää sanan Spam sähköiseksi viestiksi, jossa viestin vastaanottaja ja viestin sisältö eivät liity kiinteästi yhteen eli viesti voisi olla kenelle tahansa lähetetty. Viestin lähettämiselle ei ole todistettavasti annettu lupaa ja sekä viestin lähettäminen että vastaanottaminen ovat lähettäjän hyväksi. Spam-nimityksellä voidaan tarkoittaa roskapostin lisäksi myös pieniä aukeavia selain-ikkunoita. Nimitys Spam tulee eräästä Monthy Python –sketsistä, jossa tarjoilijalta kysyttiin paikan ruokalistaa ja tarjoilija luetteli monenmoiset yhdistelmät Spam:iä (SPieced hAM tai Shoulder Pork and hAM) ja jotain muuta. Tästä sketsistä oletettavasti innostuneena eräs MUSH:iin (multi-user shared hallucination) osallistunut pelaaja teki makron, joka kirjoitti toistuvastsi sanan SPAM ruudulle haitaten toisten
pelaajien osallistumista [Sorkin, 2001]. Spam itsessään on Hormel Foods Corporationin valmistama lihasäilykemerkki.

Yerazunis [2003] määrittää roskapostin olevan matalantason DoS (Denial of Service)-hyökkäys: inhimillisen ajan, kaistan ja levytilan tuhlausta. DoS-hyökkäyksen tarkoituksena on ylikuormittaa laitteisto ja/tai ohjelmisto. Roskapostaaja tukkii sähköpostipalvelimen

lähettämällä niin paljon sähköposteja, ettei palvelin pysty enää tallentamaan uusia viestejä. Palveluntarjoajan näkökulmasta roskapostin näköinen viesti voi paljastua oikeaksi DoS-hyökkäykseksi. Palveluntarjoajalla tosin ei välttämättä ole infrastruktuuria, jolla voidaan tutkia roskapostittajia ja saada heidät kiinni.

Sähköposteja on monenlaisia ja roskan määrittely on jokaiselle henkilökohtainen asia. Toiset määrittävät, että ketjukirjeet eivät ole roskapostia, mutta toisten mielestä ketjukirjeet ehdottomasti ovat roskapostia [Sorkin, 2001]. Roskapostin sisältö voi kaupallisten 'tiedotteiden' lisäksi olla myös mm. poliittista tai uskonnollista.

Sähköpostin voi määritellä myös massapostituksen kautta eli jos sama viesti on lähetetty esim. yli 50 ihmiselle, se lasketaan roskaksi. Itse viestin muuntelu, esim. suodatinohjelmien huijaaminen, indikoi kyseessä olevan roskapostin.

1.2. Miksi roskapostitutkimus on tärkeää

Roskapostin osuus kaikesta sähköpostiliikenteestä on kasvanut kasvamistaan. Roskapostin torjunta 'käsin', eli poistamalla saapuneiden sähköpostin joukosta roskapostit itse, on helppoa, jos roskapostia tulee vain muutama päivässä. Vuoden 2003 kesän lopussa ongelma paisui aivan eri mittakaavaan, sillä roskapostittajat ottivat lähettämisen avuksi virusten jättämät takaportit ja vastaanottajalle alkoi tulla kymmeniä, jopa satoja roskaposteja päivässä.

Roskapostin ja oikean postin saapumisen todennäköisyys alkaa liikkua samoissa lukemissa, jollei jopa roskapostin todennäköisyys ole jo suurempi (liite 1) [Brightmail, 2004]. MessageLabs tilastoi tämän vuoden 2004 huhtikuussa 841,4 miljoonaa viestiä ja saivat roskapostin osuudeksi 67,6 % [MessageLabs, 2004].

2. Taustaa

Tutkimme seuraavaksi, miten roskaposti on sitten päästetty paisumaan nykyisen kaltaiseksi ongelmaksi ja mihin suuntaan kehitys näyttäisi menevän?

Roskapostin sanotaan syntyneen Laurence Carterin ja Martha Siegelin 12.4.1994 yli 6000 keskusteluryhmään lähettämästä ilmoituksesta, jossa he tarjosivat lainopillisia palveluitaan [Järvinen, 2000]. He ovat kirjoittaneet myös oppaita muille, miten Internetiä voitaisiin hyödyntää kaupallisesti (Canter ja Siegel, 1995], [Siegel, 1997]). Tätä ennen, jo vuonna 1978, DEC:n (Digital Equipment Corporation) markkinoija yritti lähettää kaikkiin Yhdysvaltojen länsirannikon ARPAnetin (Advanced Research Project Agency) eli Internetin edeltäjän osoitteisiin sähköpostimainoksen tietokonejärjestelmistä. Silloisista ohjelmista johtuen osa osoitteista ei mahtunut vastaanottaja-kentään, joten ne vyöryivät itse viestiosuuteen [Templeton, 2004].

Vuoden 1995 keväällä Jeff Slaton, liikanimeltään Spam King, alkoi kerätä sähköpostiosoitteita, postituslistojen ja keskusteluryhmien nimiä. Hän laittoi saman vuoden heinäkuussa mainoksen atomipommisuunnitelmien myynnistä [Gauthoronet ja Drouard, 2001].

Keväällä 1996 Sanford Wallacen perustama Cyber Promotions tuli markkinoille. Yritys lähetti AOL:n (American OnLine) asiakkaille mainoksen. Asiakkaiden valitettua saamastaan roskapostista AOL antoi heille mahdollisuuden valita, haluavatko he jatkossa Cyber Promotionsin sähköposteja vaiko ei. Tämän seurauksena Wallace haastoi AOL:n oikeuteen saman vuoden syyskuussa, jonka hän voitti ensimmäisessä oikeusasteessa, mutta toinen oikeusaste kumosi päätöksen. Cyber Promotions lopetti toimintansa seuraavan vuoden syksyllä. [Gauthoronet ja Drouard, 2001]

Oikeus on alkanut laskea kustannuksia, joita roskapostaajat joutuvat maksamaan tekemästään haitasta. Jo vuonna 1998 [Edwards and Waelde, 2000] arvioitiin, että roskaposti maksaa englannissa 5 miljardia puntaa vuodessa. Palveluntarjoajille oikeuden päätöksen mukaan [Edwards and Waelde, 2000] maksaa 0,078 senttiä viestiltä. Täten 130 miljoonan viestin lähettämisestä tuli 400.000 dollarin lasku (ED Va No 97-1652-A, 12/10/98). Toisessa oikeusjutussa arvioitiin että roskaposti hidasti postien välitystä minuuteista kolmeksi päiväksi (Compuserve Inc v. Cyber Promotions Inc No C2-96-1070 SD Ohio 24/10/96). Roskapostiongelman syyllisiä eivät tosin ole roskapostittajat tai palveluntarjoajat, vaan se, että roskapostittaminen valitettavasti kannattaa ja on hyvä markkinointitapa.

Uusia muotoja roskapostista tulee Yerazuniksen [2004] kokemusten mukaan yhdestä kolmeen kuukaudessa, joten torjuntakeinojen pitää mukautua jatkuvasti uuteen.

2.1. Miksi ja kenelle roskapostia lähetetään

Ernest ja Young arvoivat, että jopa 14 % amerikkalaisista roskapostin saaneista vierailee mainostetuilla www-sivuilla [Järvinen, 2000]. Jos vain muutama ihminen reagoi roskaan, niin roskaa lähetetään yhä suuremmalle joukolle, jotta reagoivien määrä lisääntyisi. Eli kärjistäen: Niin kauan kuin yksikin vastaa, miljoonat kärsivät.

Yerazunis [2003] määrittelee tyypillisen roskapostilähetyksen sisältävän noin miljoona postitusta ja maksavan n. 250 - 500 dollaria. Vastaussuhde on 0,0001. Tavallinen mainosposti maksaa lähettäjälle noin 25 c /mainos, ja vastaussuhde on 0,05. Tasoitettu kustannus yhteen sähköiseen roskapostiin on 2,5 c ja mainospostivastaukseen noin 5 dollaria. Pitäisi pystyä suodattamaan vähintään 99.5 % roskapostista, jotta roskapostittaminen ei enää kannattaisi. Vastaanottajan kustannus poistoon olisi 2 c/mainos ja 5.15 dollaria tunnilta eli kaiken kaikkiaan 28000 dollaria. Roskapostittajan tehokkuus on oma voitto jaettuna uhrin kustannuksella eli noin 10 %. Tähän ei moni muu mainostusmuoto yllä.

Roskapostin lähettäjän ei tarvitse muuta kuin saada käsiinsä massoittain toimivia sähköpostiosoitteita. Robottiohjelmat (ks. esim. http://www.contentsmartz.com/) hakevat osoitteita verkossa näkyvistä www-sivuista. Osoitteita myydään, kuinka muutenkaan, roskapostissa; "57 miljoonaa osoitetta 99 dollarilla". Ihmisiä myös huijataan antamaan osoitteita mm. kilpailuilla, joissa pitää muodostaa 'joukkue' antamalla sähköpostiosoitteita ja edelleen nämä henkilöt lisäävät vastaavasti osoitteitta saatuaan luotettavan oloisen ilmoituksen osallistumisestaan 'kisaan' tai tarjoamalla tiettyjä etuuksia, kuten ilmaisia elektronisia kirjoja luettavaksi.

2.2. Kuka roskapostia lähettää

Taustan selvittäminen on tärkeää, sillä ilman taustaa on vaikea miettiä keinoja torjuntaan. Roskapostissa on menossa samankaltainen kilpajuoksu kahden osapuolen välillä kuin virustorjunnassakin.

Roskapostin lähettäjän ilmoittamaa verkkosivua voi analysoida selvittämällä, kuka sen on tehnyt. Tosin aina ei pystytä selvittämään, kenen tekemä sivu on kyseessä. Todellisen lähettäjän selvittäminen voi olla kohtalaisen vaikeaa. Domain-nimen haltijan selvittäminen on helpompaa. Jos vaivaa haluaa nähdä, voi pyytää lisätietoa mainostetusta tuotteesta (ns. social engineering -menetelmä). Rahavirtoja seuraamalla syyllinen aina löytyy. Edellyttää, että rahavirtaa on mahdollista seurata. Esim. Nigerian huijauskirjeissä tämä ei ole tyypillisesti mahdollista.

Roskapostittajien ei välttämättä tarvitse selvittää missä vastaanottaja on, vaikka hän mainostaisikin vain lähialueen asiakkaille tuotteita. Tyypillisiä lähialueen tuotteita ovat mm. vakuutukset ja suuret tavarat, joiden liikuttaminen kauas maksaa liikaa. Kauas lähetettäviä tuotteita ovat lääkkeet, diplomit ja lehdet. Koko maailmanlaajuisesti on helppo markkinoida tuotteita, joita ei tarvitse edes lähettää eli www-sivuja, ohjelmia ja erilaisia huijauksia. Roskapostin lähettäjänkin pitää ajatella lopullisia kustannuksia.

2.3. Miten roskapostia lähetetään

Yhä useampi roskaposti tulee sellaisesta tietokoneesta, jossa on laajakaistayhteys päällä yötä päivää, ja johon roskapostaaja on päässyt käsiksi. Roskapostaaja yrittää väärentää jotakin osaa viestin kulkureitistä, jotta roskapostaajaa ei pystyttäisi selvittämään. Tätä vastaan on suunniteltu MTA Mark, joka tutkii onko MTA (Message Transfer Agent) oikeassa IP-osoitteessa. MTA:t välittävät viestit käyttäjien sähköpostilaatikoihin (User Agent). [Sergeant 2004].

Jos organisaatio ei ole suojannut postipalvelinta siten, etteivät muut kuin omasta verkosta tulevat viestit välity eteenpäin, voivat muut käyttää palvelinta omien viestien välittämiseen (ns. releointi). Tällöin roskapostittajan viestit näyttävät tulevan omasta palvelimesta.

3. Torjuntakeinot

Tavallisen käyttäjän yksinkertaisin torjuntakeino on olla julkaisematta osoitettaan missään. Tämä ei ole aukoton keino, sillä jotkut roskapostittajat arvaavat osoitteet generoimalla palvelinpäätteen eteen satunnaisia merkkijonoja. Ne osoitteet, jotka eivät palauta 'ei olemassa' -viestiä, selviävät oikeiksi osoitteiksi ja tulevat saamaan roskaa hyvin nopeasti ja paljon.

Jos osoite pitää julkaista, yksinkertaisina keinoina on julkaista muoto, josta osoite päätellään, esim. etunimi.sukunimi@uta.fi, tai lisätä osoitteen joukkoon ylimääräistä, kuten Maija.Mehilainen.poistatama@uta.fi. Mahdollisesti voit piilottaa osoitteet JavaScriptin avulla, jolloin sivua lukeva roskapostaajan ohjelma ei pysty koodista osotetta tunnistamaan, mutta sivulla osoite näkyy selkokeilisenä. Selaimille tai käyttäjille, jotka eivät tue JavaScriptiä, voi osoitteet piilottaa käyttämällä kuvaa. Lomakkeiden käyttö, jossa osoite on tallessa palvelin puolen skriptissä (ks. esim. http://innerpeace.org/escrambler.shtml) tai CGI-sovelluksessa, joka prosessoi lomakkeen, ei itse lomakkeessa.

Williems [2004] mainitsee edellisten lisäksi yleistymässä olevat WebBugit, eli skriptit kuvia sisältävissä roskaposteissa. Tällaisen kuvan lataaminen automaattisesti sähköpostiohjelman toimesta kertoo roskapostaajalle saajan osoitteen olevan aktiivisessa käytössä ja käyttäjän lukevan roskapostejaan.

3.1. Ohjelmallinen torjunta

Roskapostin estossa eivät algoritmit ole niin tärkeitä kuin harjoitusmateriaali, jonka pohjalta algoritmit toimivat, sillä roskaposti muuttuu ajan myötä eikä kaikille tule samanlaista oikeaa sähköpostia. Roskapostia voi tutkia helposti käyttämällä hyväksi olemassa olevia arkistoja. Yksi tällainen on SpamArchive (http://www.spamarchive.org/), jonka tietokannassa on n. neljännesmiljoona roskapostiviestiä ja mm. Microsoft kerää tilastoaineistoa vapaaehtoisesti käyttäjiltään.

Erityyppiset suotimet ovat käytössä jo monissa ohjelmissa. Suotimet voivat perustua useampaan tapaan selvittää roskaposti. Ohjelmat yleensä tarkkailevat viestin eri osia, kuten lähettäjä-, otsikko-, maa- ja lähetysaikakenttiä. Roskapostit, joiden ainoana sisältönä on jokin liite, vaikka kuva, jota ei voida suoraan ohjelmallisesti lukea, torjutaan näiden kenttien perusteella. Asiaa vaikeuttaa sähköpostin vapaa rakenne sisällön suhteen, sillä sen suhteen ei ole olemassa strukturoituja tutkittavia kenttiä.

Viestin sisällön sanat ovat silloin hyvä indikaattori, jos muu posti ei todennäköisesti sisällä roskapostissa käytettyjä sanoja. Esimerkiksi "to unsubscribe" tai "buy * online now" voivat olla tällaisia ominaisuuksia, jotka kannattaa erottaa muusta tekstistä analyysiin mukaan.

Graham [2003a] listaa viisi hyvän tilastoon perustuvan torjuntaohjelman ominaisuutta: (1) Ohjelman on oltava erittäin tehokas, sillä jo yksinkertainenkin tilastosuodatinkin tunnistaa 99 % roskasta. (2) Hyvät ohjelmat luokittelevat vain todella harvoin oikeat viestit roskaksi (ns. false positive). (3) Ohjelmien on pystyttävä oppimaan ja mukautumaan, sillä roskapostittajien toiminta muuttuu. (4) Käyttäjällä pitää olla valta päättää itse, mikä on roskaa; Jokaisen sähköpostin laatikon sisältö on joka tapauksessa erilainen. (5) Ohjelmien huijaaminen on oltava vaikeaa.

Ohjelmallisessa torjuntaan liittyvät listat, lähettäjätietojen selvittäminen, muodon ja sisällön analysointi ja linkkien seuraaminen. Monet ohjelmat toimivat iteratiivisesti, analysoiden uutta varsinaista ja roskaksi määriteltyä sähköpostia. Tämän vuoksi käyttäjä määrittää postinsa kahteen joukkoon: roskaan ja oikeaan postiin esim. painamalla painiketta postia poistaessaan tai siirtäessään kansioon.

3.1.1. Listat

Perinteisesti esto on tehty erityisten listojen avulla joko lähettäjien tai viestin sisältämien sanojen perusteella.

Isot organisaatiot käyttävät sulkulistoja eli tietyistä osoitteista ei vastaanoteta ollenkaan postia organisaation sisälle. Sulkulistojen tarkkuus saattaa vaihdella 0 – 60 %, ja vääriä hälytyksiä tulee n.10 % [Graham 2003b]. Tyypillinen tapa tämän kaltaiseen estoon on käyttää listaa tunnetuista roskapostilähettäjien domain-osoitteista. Warsaw [2003] esittää lähettäjän joutumista automaattiselle mustalle listalle, jos lähetyksiä tulee 300 esim. 6 tunnin sisällä.

Mustien listojen lisäksi on ns. valkoisia listoja, joille pääsee, jos ehdottomasti ei ole roskapostittaja. Käyttäjien omat valkoiset listat muodostuvat luotettavaksi todetuista osoitteista, jotka löytyvät omasta osoitekirjasta. Kun osoite on valkoisella listalla, ei sisältöä lähdetä edes analysoimaan. Usein käyttäjä voi määritellä esim. että hän vastaanottaa *vain* osoitekirjassa olevista osoitteista tulevia sähköposteja.

Yhdysvalloissa suoramarkkinointialan etujärjestö E-MPS (http://www.e-mps.org) on tarjonnut vuodesta 2000 alkaen palvelua, johon sähköpostin käyttäjät voivat ilmoittaa osoitteensa, jos eivät halua roskapostia. Tällainen toiminta käyttäjän kannalta on arveluttavaa, sillä hän käytännössä kertoo markkinoijille osoitteensa toimivan.

3.1.2. Lähetyskenttien analyysi

Erilliset torjuntaohjelmat auttavat käyttäjää selvittämään todellisen lähettäjän paljastamalla piilotetut X-kentät. Oikean lähetysosoitteen selvittäminen vaatii header-tietojen analysoinnin. Header-tietoja ovat lähettäjän nimi, domain, aikavyöhyke, sähköpostin koko, vastaanottajien lukumäärä, flags, sähköposti-client ja MIME (Multipurpose Internet Mail Extensions) -tyyppi. Jos selviää, että lähettäjä-kenttä on väärennetty, roskapostiohjelman ei yleensä tarvitse enempää tarkastaa.

Helenius [2004] tarjoaa yhdeksi vaihtoehdoksi sähköpostien jakamisen alueisiin. Tietyn alueen tai verkoston sisältä, tai muutoin luetettavaksi määritellyltä lähettäjätaholta tuleva sähköposti käsiteltäisiin eri tavoin kuin muualta tuleva sähköposti.

Lähetysaika voi paljastaa ns. aikahyppäyksen, jolloin roskapostittajan viestit tulevat ennen merkittyä lähetysaikaa. Tarkoituksena roskapostittajalla on kenties ollut kiertää aikatarkastusta, sillä monet roskapostittajat lähettävät yölliseen aikaan roskapostinsa.

IP-osoitteiden ja nimien vastaavuuden tarkistuksen tarjoaa esim. Sam Spade (http://samspade.org/ssw), joka mahdollistaa myös nimipalvelukyselyt, pakettien reittien selvittämisen ja sähköpostin toiminnan analysoinnin.

3.1.3. Muotoanalyysi

Ennen sisällön analyysia kannattaa tehdä ennakkosiivous koskien sähköpostin ulkoisia muotoiluja.

Useat roskapostit sisältävät HTML-tekstiä, ja vieläpä erikoisia elementtejä siitä. Tällaisia elementtejä saattavat olla tekstiväritys samalla värillä kuin tausta, eli halutaan hämätä ohjelmia, jotka tekevät sisältötekstistä analyysia huomioimatta sitä tosiseikkaa, että oikean tekstin näköinen osa ei edes näy käyttäjälle. Samalla periaatteella lisätään sanoja erottamaan kommentti-määritteitä tyyliin

vi<!-- aa12 -->agra

Näistä pääsee eroon helposti jos sähköpostiohjelma poistaa html-määritteet ennen sisältöanalyysiä.

Muotoon liittyy myös sen analyysi, miten vastaanottaja ja lähettäjä yleensä käyttäytyvät. Jos vastaanottaja ei ole koskaan esiintynyt cc-listassa joltain lähettäjältä, voi se olla epäilyttävä piirre. Samoin, jos vastaanottaja ei koskaan vastaa jostain osoitteesta tulleeseen viestiin, tai jos lähettäjä on aiemmin lähettänyt vastaanottajalle vain kerran kuussa postia ja yhtäkkiä lähetystiheys nousee päivittäiseksi.

Hotmailin tekemä analyysi 2 miljoonan huhti-kesäkuussa 2003 lähetetyistä viesteistä [Hulten 2004] tuotti mielenkiintoisen tilaston siitä, että käyttäjien roskaposteiksi määritellyistä viesteistä peräti 90.8 % käytti US-ASCII –merkistöä. Tosin tätä merkistöä käytti myös oikeiksi postiksi määritetyistä viesteistä 60.31 %. Toiseksi suosituin merkistö roskapostissa oli ANSI Latin –merkistö, jota käytti 7.52 % roskasta ja 29.18 % oikeasta postista. Roskapostittajien suosiossa ei näyttänyt olevan Suomessa ehkä yleisemmin käytetty ISO Latin –merkistö, jonka osuus Hotmailin aineiston roskapostista oli vain 0.31 %, tosin oikeasta postista osuus oli vain 1.41 %, mutta suhdeluku on silti murskaava. Voidaan päätellä, että roskaposti on selkeästi suunnattu englanninkieliseen väestöön.

3.1.4. Sisältöanalyysi

Sähköpostin sisältö ratkaisee sen, onko se vastaanottajasta roskaa vaiko ei. Käyttäjä pystyy sanomaan sen nopeasti, ehkä jo pelkkää otsikkoa katsomalla, mutta ohjelma tähän ei toistaiseksi pysty.

Käyttäjä tai organisaatio on voinut käyttää yksinkertaisinta sisältöanalyysin torjuntatapaa listaamalla sanat, jotka määrittävät tilastollisesti roskan. Yksinkertainen läpikäynti ja täsmäysten lukumäärä antavat tietyn 'roska-arvon'.

Ohjelmia voidaan hämätä liittämällä viestiin HTML-tekstin lisäksi MIME-osio, johon sijoitetaan esim. sanakirjoista sanoja. Tällöin viestin roskapostiksi tunnistamisen todennäköisyys pienenee. Tätä vaikutusta voidaan ehkäistä valitsemalla kaikkien sanojen tarkastelun sijaan esimerkiksi 10…20 merkitsevintä kohtaa eli sanaa, sanontoja, isoilla kirjaimilla kirjoitettuja sanoja, dollari- yms. merkkejä, pisteitä jne. Tällöin jäävät kiinni myös ne roskapostit, joissa on alussa jonkinlainen elämäntarina ennen tyypillistä roskapostitekstiä.

Sana-analyysi vaikeutuu, kun roskapostittajat sijoittavat viestiin mukaan JavaScriptiä. Jälleen suodatinohjelman pitää etukäteen hoitaa koodin purku ennen varsinaista sisältöanalyysiä.

Tyypillinen keino sana-analyysin vaikeuttamiseksi on sijoittaa sanojen väliin yksinkertaisesti tyhjää tilaa tai muita merkkejä vastaamaan kirjaimia, esim. M 0 N E Y, F*R+UNE tai 1nve/st. Nämä piirteet on helpohkoa tunnistaa roskapostille tyypillisiksi, kun tiedetään, että erikoisia merkkejä ja yhden kirjaimen 'sanoja' on harvemmin tavallisessa sähköpostissa.

Sisällölle annetaan todennäköisyyksiä sen perusteella, mikä on sisällössä esiintyvien roskaposti-indikaattoreiden, kuten sanojen tai kuvalinkkien, suhde muuhun sisältöön. Tätä sisältötodennäköisyyksiä hämätään laittamalla satunnaisesti generoituja sanoja tekstin sekaan. Suodattaminen on vaikeaa, kun ei ole tällöin minkään näköistä vertailupohjaa, eikä 'uudissanoista' tule olemaan hyötyä muihin viesteihin. Ohjelmien pitäisikin ottaa huomioon esiintymisen useus, eli jättävät tilastoimatta harvoin esiintyvät sanat, vaikka niitä olisikin vain roskapostiviesteissä. Haaste roskapostittajille olisi valita sanoja, joiden perusteella viesti päätellään heti oikeaksi viestiksi. Näitä voisivat olla esim. vastaanottajalle tuttujen ihmisten nimet. Hankalaksi tällaisten sanojen laittamisen tekee se, etteivät roskapostittajat tiedä, minkälaista postia ihmisillä on – varsinkin kun jokaisella on erityyppisiä viestejä.

Mielenkiintoisen skenaarion tarjoaa kokeiluasteella oleva Gmail (https://gmail.google.com/), jossa käyttäjä saa käyttöönsä erittäin paljon (1 Gt) tallennustilaa muihin sähköpostilaatikoihin verrattuna. Vastineeksi käyttäjä antaa

Gmailille oikeuden lukea ohjelmallisesti sähköpostinsa ja laittaa joukkoon mainoksia liittyen viestin sisältöön. Toisin sanoen, käyttäjä sallii roskan sijoittamisen tavallisten sähkö-

postiensa *sekaan*. Mikä torjuntaohjelma voisi näitä enää poistaa? Toisaalta, jos Gmail pystyy tutkimaan ihmisten sähköposteja, niin se pystyy myös laatimaan vastaavia keinoja analysoida sisältöä roskapostittajille kuin nyt roskapostin vastustajilla on. Näin saadaan massoittain dataa tilastoanalyyseihin siitä, miten pystyttäisiin luokittelemaan roska tavalliseksi postiksi.

3.1.5. Linkit

Roskapostissa saattaa muut kentät olla laillisen näköisiä, ja sisältönä ainoastaan linkki johonkin URL-osoitteeseen. Lähettäjä saattaa yrittää piilottautua muuttamalla selkeän URL-osoitteensa hex tai octal-muotoiseksi numerosarjaksi, kuten http://776363167/index.html. Tähän ongelmaan mm. Abuse.net tarjoaa palvelun, jonka kautta numeron saa muutettua IP-numeroksi ja muuta lisätietoa roskapostittajista. Abuse välittää myös valituksia roskapostista lähettäjätaholle.

Ohjelmallisesti voidaan tutkia onko osoite roskapostittajan vai oikea. Tunnetut roskapostittajan osoitteet löytyvät mustilta listoilta. Jos osoite on tuore, niin sivulle voidaan suorittaa vastaava sisältöanalyysi kuin roskapostillekin.

Toinen indikaattori siitä, että linkki vie roskaa sisältävälle sivulle, on se, että palvelimella kestää vastaaminen. Tämä johtuu siitä, että vastaavat roskapostiohjelmat niistä miljoonista osoitteista, johon linkki on lähetetty, ovat käymässä samassa osoitteessa.

3.1.6. Bayesialainen algoritmi

Useat suodattimet perustuvat Bayesialaiseen teoriaan. Mm. Microsoft käyttää Bayesilaista koneoppimisen lähestymistapaa vuonna 1997 aloittamassaan roskapostitorjunnassa [Goodman, 2003]. Bayesialainen tilastoanalyysi perustuu oletukseen, jonka mukaan epävarmuutta voidaan käsitellä klassisella tilastoanalyysillä. Lähestymistapa perustuu hahmontunnistusongelmaan ja oletukseen, että päätösongelma on esitettävissä todennäköisyyksien termein ja että kaikki vaadittava todennäköisyys tunnetaan [Duda and Hart, 1973].

Tuleva posti on joko roskaa ($p0$) tai oikeaa postia ($p1$). Nämä ovat satunnaisia muuttujia, sillä etukäteen ei voida tietää, kumpaa tuleva sähköposti on. Näiden todennäköisyydet ovat $P(p0)$ ja $P(p1)$, eli ns. a priori –todennäköisyys, kun muuta tietoa ei ole saatavissa. Tämä ei riitä, vaan tarvitaan enemmän informaatiota. Otetaan käyttöön kirjain k, joka määrittää todennäköisyyden roskapostin ja varsinaisen sähköpostin suhteen ehdollisessa todennäköisyydessä:

$P(k \mid p0)$ ja $P(k \mid p1)$. Ehdollisen todennäköisyyden käsite perustuu siihen, että todennäköisyys lasketaan käytettävissä olevan tiedon perusteella. Ehdollinen todennäköisyys $P(k \mid p0)$ tarkoittaa, että kun tunnetaan tietty ominaisuus (k). Esimerkiksi jos sähköpostissa on ominaisuutena sanan *money* esiintyminen, niin $P(k \mid p0)$ kertoo todennäköisyyden sille, että

sähköposti on roskapostia. Vastaavasti P(k | p1) kertoo todennäköisyyden sille, että sanan *money* sisältämä sähköposti ei ole roskaa.

Bayesin kaava perustuu Posteriori-todennäköisyyteen, eli tietty olettamus on tosi silloin, kun aineisto on otettu huomioon. Bayesin sääntö voidaan kirjoittaa muotoon

$$P(p_j \mid k) = \frac{p(k \mid p_j)P(p_j)}{p(k)}, \text{ jossa}$$

$$p(k) = \sum_{j=0}^{1} p(k \mid p_j)P(p_j).$$

Bayesin päätössääntö on: päätä p0, jos P(k | p0) > P(k | p1), muutoin p1. Bayesin säännön avulla voidaan arvioida päättelyn oikeellisuus, sillä se on ottanut huomioon olemassa olevan ennakkotiedon (olettamuksen) ja varsinaisen aineiston.

Bayesiläisyys rakentaa muuttujien todennäköisyysjakaumille P(a,…,x) mallin. Mallin rakentamisessa valitaan se, joka maksimoi posteriori-todennäköisyyden. Mallia sovelletaan kerätyn tiedon analysointiin ja ennustamiseen. Ongelmana on se, miten päivittää olettamus, kun roskaposti muuttuu jatkuvasti. Bayesiläisyyden etuna on mahdollisuus yhdistää priori-jakaumien kautta asiantuntijatietämys ja optimaalisten parametrien löytäminen ilman iteratiivisia oppimisprosesseja. Tilastollista aineistoakaan ei tarvita paljoa.

Bayes-verkot ovat laadullisia suunnattuja syklittömiä graafeja (DAG), eli mistään verkon solmuista ei ole polkua takaisin ko. solmuun ja verkon kaarilla on suunta. Bayesverkoissa solmut edustavat satunnaismuuttujia ja kaaret riippuvuutta solmujen välillä. Jokaiseen solmupisteeseen liittyy ehdollinen todennäköisyysjakauma.

Naiivi Bayes-malli on yksi Bayes-verkon muutos. Naiivi Bayesin sääntö oppii, kun sijoitetaan jokaisen viestin ominaisuus, eli sana tai sanonnat, joko roskaposti- tai oikea posti -joukkoon. Kun lasketaan miten usein jokin tietty ominaisuus on roskapostin joukossa, ja miten usein oikean postin joukossa, niin saadaan todennäköisyydet. CRM114 [Yerazunis 2003] käyttää Naiivia Bayesialaista luokittelijaa ja on geneerinen suodatinkieli. Kieli perustuu sään-

nöllisten ilmaisujen täsmäykseen. Muita Bayes-verkon muunnoksia ovat esim. päätösverkko, noisy-or-malli ja dynaaminen malli.

Suosittu suodatinohjelma SpamAssassin sisältää erilaisia roskapostin havainnoivia tekniikoita, mm. Bayes-suodattimen, joka kerää tietoa pisterajan ylittävistä viesteistä. Muita tekniikoita ovat mm. HTML-määritteiden lukumäärä ja header-tietojen yksityiskohdat. Pistearvo 5 tarkoittaa, että on suurin todennäköisyys sille, että viesti on roskaa. SpamAssassin myös analysoi lähetys- (header) ja tekstiosaa ja sisältää geneettisen algoritmin. Geneettinen algoritmi testaa onko tarkkuus tarpeeksi hyvä, ellei, kehitetään tuloksia ja testataan uudelleen kunnes saadaan tarkkuudelle esim. yli 99 % lukema ja voidaan tulostaa

lopullinen arvo. Ohjelmalla on useita kymmeniä miljoonia käyttäjiä, joiden mukana on myös palveluntarjoajatahoja.

3.2. Muut torjuntakeinot

Torjuntakeinoja on myös muita, kuten lainsäädännölliset keinot ja roskapostin lähettäjän pakottaminen toiminnan lopettamiseen erilaisin keinoin, kuten verkkosivun sulkeminen.

Lait antavat palveluntarjoajille mahdollisuuden suodattaa, mutta harvoin estävät itse lähetystä. Vaikutus tällä hetkellä lienee se, ettei roskapostittajilla ole välttämättä resursseja oikeustaisteluun, ainakaan, jos vastassa ovat suuret toimijat, kuten AOL, Earthlink, Yahoo! ja MSN. Tavoitteena onkin nostaa roskapostittajien kustannuksia niin, ettei toiminta enää kannattaisi [Praed 2004]. Roskapostittajilla on tapana olla yhteyksissä toisiinsa, eli jos seurataan rahavirtaa ja saadaan kiinni yksi henkilö, hänen kauttaan saadaan kiinni toinen, esim. lähde, josta sähköpostiosoitelista on peräisin.

Suomessa on säädetty 1.7.1999 laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta. Euroopan unionilla on Distance Selling Directive (97/7/EC, OJ NoL 144/19), jonka mukaisesti kuluttajilla on oikeus olla saamatta sähkö-, tai muutakaan postia, jota hän ei ole pyytänyt ja jota hän selkeästi ei olisi halunnut. Direktiiviä tarkennettiin kahdella lisäyksellä: Directive on Distance Marketing of Financial Services (1998) ja Electronic Commerce Directive (2000). Vuonna 2002 säädettiin sähköisen viestinnän tietosuojadirektiivi, jonka 13 artiklassa kielletään lähettämästä ilman lupaa sähköpostia suoramarkkinointitarkoituksessa. Sähköpostiksi direktiivissä määritellään "yleisessä viestintäverkossa lähetettävää teksti-, puhe-, ääni- tai kuvaviestiä, joka voidaan tallentaa verkkoon tai vastaanottajan päätteelle, kunnes vastaanottaja on vastaanottanut sen." [EU, 2002].

Roskapostin torjuntaa miettimään on perustettu järjestö The Coalition Against Unsolicited Commercial Email (CAUCE, http://www.cauce.org), jonka tehtävänä on saada verkon käyttäjät liittoutumaan roskapostittajia vastaan.

Yhdysvalloissa eri osavaltiot ovat laatineet omia roskapostin vastaisia lakeja, mutta roskapostittajat pyrkivät valittamaan näistä perustuslain vastaisina. Esimerkkinä on Washingtonin osavaltion 10.3.1998 säätämä laki, jonka mukaisesti ei saa lähettää sähköpostia, jota vastaanottaja ei ole halunnut, tai laittaa vääriä lähettäjä- ja vastausosoitetietoja. Kaliforniassa Californian Internet Consumer Protection Act teki tammikuussa 1999 esityksen, jonka mukaisesti palveluntarjoajalla olisi oikeus haastaa lähettäjätaho oikeuteen ja vaatia 50 dollarin maksu jokaiselta viestiltä, mutta enintään kuitenkin 25000 dollaria päivässä. Tämä ehdotus kumottiin perustuslain vastaisena kesällä 2000. Goldstonen [1998] mielestä palveluntarjoajan tekemä viestin suodatus ei ole vapaan puheoikeuden vastaista, sillä palveluntarjoajat ovat yksityisiä toimijoita eivätkä osavaltion elimiä. Maksullisuuden saaminen roskaposteihin poistaisi roskapostin kannattavuuden, mutta toteuttaminen toistaiseksi on vaikeaa.

Internetin yhteisöt ovat yleisesti sitä mieltä, etteivät lait auta, vaan jokaisen on toimittava omin strategioin, käyttämällä suodatinohjelmia, mustia listoja ja ohjelmia, jotka rajoittavat lähetettyjen sähköpostien kopiointimäärää. Pegasus Mail on määritellyt, että yli 50 vastaanottajalle lähetetty sähköposti on jo massapostitusta.

Palveluntarjoajien tehokkain torjuntakeino on tehdä asiakkaan kanssa sopimus, jonka mukaan asiakas on oikeus irtisanoa jos tämä lähettää roskapostia. Kuluttajalle on tarjolla myös ns. opt-in/out –järjestelmä, jonka mukaan hän määrittää itse haluamansa sähköpostit.

4. Yhteenveto

Tulevaisuuden arvioni on se, että sähköpostiviestejä luetaan yhä enemmän puhelimen kautta ja monesti puhelimen käyttö maksaa enemmän kuin sähköpostin lukeminen tietokoneelta. Palveluntarjoajat saattavat ottaa kohta tosissaan asiakkaidensa tarpeet. Jos esim. rajoitetaan sähköpostimäärä 300 viestii kuukaudessa, ei tavalliselle käyttäjälle koidu ongelmia, mutta roskapostittajalle koituu.

Tapoja ohjelmalliseen torjutaan tulevaisuudessa löytyy päätöspuista, jotka vähentäisivät sääntömäärää. Erilaiset sääntöjä yhdistävät algoritmit, kuten sääntösolmuista muodostuvat neuroverkot, voivat olla tulevaisuuden menetelmä. Haittana neuroverkoissa tosin on hidas oppimisprosessi. Jos käyttäjälle tulee kohtuutonta haittaa eli esim. postien lukeminen hidastuu, ei käyttäjä tule käyttämään tällaista järjestelmää. Yerazunis [2004] on tullut siihen tulokseen, että Bayesia parempi keino on Markovin malli, joka saadaan helposti Bayesilaisesta mallista muutamalla sanojen vertailu useiden sanojen vertailuksi ja muuttamalla painoja siten, että kauemmin olleet ominaisuudet saavat suuremman painon. Painotus vaihtelee myös sanojen yhteismäärän mukaan: 2^{2N}, jossa N on sanojen lukumäärä. Yksi sana saa painotuksen 1, kaksi sanaa painotuksen 4, kolme sanaa 16 jne.

Yerazunis esittää myös rokotusjärjestelmää, jolla lähettäjä, joka huomaa saaneensa roskapostin suodattimen läpi, lähettää tästä tiedon toisille järjestelmässä oleville, jolloin he voivat suojautua vastaavaa roskaa vastaan. Pitkä lause. Käyttäjät ovat saaneet tavallaan rokotuksen uudenlaista roskaa vastaan.

Vielä nykyään suomalaiset ovat voineet aika helposti poistaa roskat laatikosta, sillä ainakin omakohtaisesten kokemusten perusteella suurin osa oikeasta postista tulee suomen kielellä ja roska englanniksi. Valitettavasti roskaajat ovat huomanneet kielimuurin ja kääntävät roskaviestit automaattisesti sille kielelle, mistä vastaanottajan sähköpostiosoite on peräisin. Esimerkiksi suomalaisen päätteen osoitteeseen käännetään roskaposti suomeksi. Emme voi siis tuudittautua kielivähemmistön harvalukuisuuteen. Koneet ovat tässä suhteessa valitettavasti yhä tehokkaampia ja nopeampia kielenkääntäjiä.

Suodattimien arviointi on vaikeampaa kuin luulisi: Mitä voidaan käyttää mittoina? Käytetäänkö esimerkiksi prosenttilukuja seulan läpäisseestä roskasta (miss rate) vai roskaksi määritellystä oikeasta postista (false positive rate)?

Sähköpostin julkinen luonne mahdollistaa roskapostaamisen, mutta vaatimuksia autetikoinnista ja lähettäjäkenttien lisämääreistä on esitetty [Sergeant, 2004].

Viiteluettelo

[Brightmail, 2004]. Brightmail, Spam Statistics. Saatavilla http://www.brightmail.com/spamstats.html (12.5.2004).

[Canter ja Siegel, 1995]. Laurence A. Canter ja Martha S. Siegel, *How to Make a Fortune on the Information Superhighway: Everyone's Guerrilla Guide to Marketing on the Internet and Other On-Line Services*. HarperCollins, 1995.

[Duda and Hart, 1973]. Duda Richard O. and Hart Peter E., *Pattern Classification and Scene Analysis*. John Wiley & Sons, 1973.

[Edwards and Waelde, 2000]. Lilian Edwards and Charlotte Waelde, *Law and the Internet. A Framework for Electronic Commerce*. Hart Publishing, 2000.

[EU, 2002]. Euroopan Unioni, direktiivi 2002/58/EY. *Virallinen lehti*. Nro L 201, (31.7.2002), 0037-0047. Saatavilla myös http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=fi&numdoc=32002L0058&model=guichett (12.5.2004).

[Gauthronet ja Drouard, 2001]. Serge Gauthronet ja Etienne Drouard, Unsolicited Commercial Communications and Data Protection. Saatavilla http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamstudy_en.pdf (12.5.2004).

[Goldstone, 1998]. David J. Goldstone, *A Funny Thing Happened on The Way To The Cyber Forum: Public v. Private in Cyberspace Speech*. University of Colorado Law Review. **69**, 1 (1998).

[Goodman, 2003]. Joshua Goodman, Spam Filtering: From the Lab to the Real World. In: *Spam Conference 2003*.

[Graham, 2003a]. Paul Graham, The future of spam. In: *Computer Security Journal*. **19** (Jan. 2003), 1-5. Saatavilla osiltaan myös: http://paulgraham.com/wfks.html.

[Graham, 2003b]. Paul Graham, Better Bayesian Spam Filtering. In: *Spam Conference 2003*.

[Grossman, 1997]. Grossman W., *Make. Money. Fast.* SPAMMIN SYNNYSTÄ NET.WARS NYUP,1997.

[Helenius, 2004]. Marko Helenius, *Why Does E-mail Fail?*. In: U.E. Gattiker (ed.), *EICAR 2004 Conference*.

[Hulten, 2004]. Geoff Hulten, Filtering Junk Mail on a Global Scale. In: *Spam Conference 2004*.

[Järvinen, 2000]. Järvinen Pertti, *Sinulle on sähköpostia*. Teknolit Oy, 2000.

[MessageLabs, 2004]. MessageLabs April Monthly Report, How effective is current legislation?
Saatavilla http://www.messagelabs.com/intelligence/reports/monthlies/april04/default.asp (26.5.2004).

[Praed, 2004]. Jon Praed, Latest Trends in the Legal Fight Against Spammers. In: *Spam Conference 2004*.

[Sergeant, 2004]. Pete Sergeant, Closing loopholes: MTA Mark and SPF. In: *Virus Bulletin Spam supplement*. May 2004, S2-S3.

[Siegel, 1997]. Martha Siegel, *How to Make a Fortune on the Internet*. HarperCollins, 1997.

[Spamhaus, 2004]. The Definition of Spam. Saatavilla http://www.spamhaus.org/definition.html (5.4.2004)

[Sorkin, 2001]. David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*. U.S.F. Law Review. **35** (2001). Saatavilla http://www.spamlaws.com/articles/usf.pdf (12.5.2004).

[Templeton, 2004]. Brad Templeton, Reaction to the DEC Spam of 1978. Saatavilla http://www.templetons.com/brad/spamreact.html (26.5.2004).

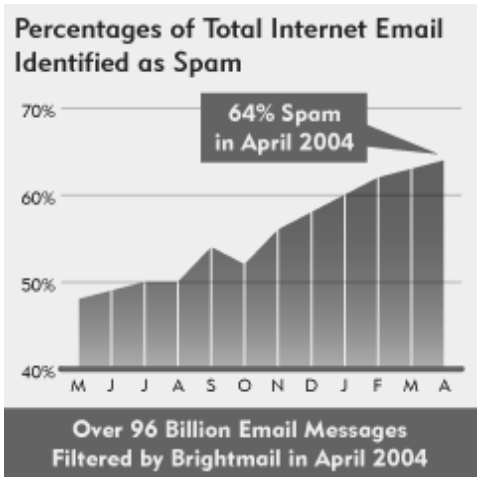
[Warsaw, 2003]. Barry Warsaw, Anti-Spam Techiques at Python.org. In: *Spam Conference 2003*.

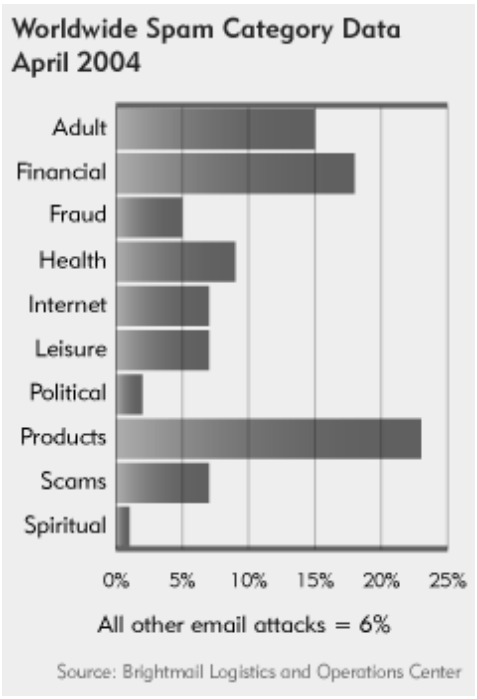
[Willems, 2004]. Eddy Willems, Editorial: Your own Anti-Spam Stragety!. In: *Eicar News*. **11**, 1 (Feb. 2004).

[Yerazunis, 2003]. Yerazunis Bill, Sparse Binary Polynomial Hash Message Filtering and The CRM114 Discriminator. In: *Spam Conference 2003*.

[Yerazunis, 2004]. Yerazunis Bill, The Plateau at 99.9% Accuracy, and How to Get Past It. In: *Spam Conference 2004*.

Brightmailin roskapostitilastoja





TETRA-verkon tietoturva

Tommi Rautiainen

Viranomaiset ovat aina tarvinneet työssään erilaisia viestintäratkaisuja kuin siviilit. Tämä johtuu siitä että viranomaisten työ eroaa luonteeltaan huomattavasti siviilien työstä, ja viranomaisilla on työn luonteesta johtuen usein tarve useamman henkilön yhtäaikaiseen viestintään. Viranomaisten viestintäratkaisut ovat kuitenkin olleet vielä viime vuosikymmenelle asti huomattavan puutteellisia nykyaikaisen viestinnän tarpeet huomioon ottaen.

Viime vuosikymmenellä näihin ongelmiin kuitenkin tuli ratkaisu uuden digitaalisen, erityisesti viranomaisille tarkoitetun matkapuhelinstandardin muodossa. Tämän standardin nimi on TETRA ja se kehitettiin Eurooppalaisen yhteistyön seurauksena.

TETRA-standardin mukaisessa verkossa on viranomaisilla mahdollisuus turvattuun yhtäaikaiseen viestintään. Enää ei viranomaisten puheluiden salakuuntelu ole mahdollista, ja nykyisin viestintä toimii myös viranomaisryhmien välillä jopa yli valtioiden rajojen.

Juuri tietoturvan huomioiminen TETRA-standardia kehitettäessä on noussut standardin suureksi eroksi verrattaessa esimerkiksi GSM-järjestelmään. Tässä tutkielmassa kuvaan TETRA-verkon tieturvaan liittyviä seikkoja. Nämä seikat ovat TETRA-verkon algoritmit, tietoturvauhat ja vastatoimet. Tässä tutkielmassa esittelen myös TETRA-standardiin perustuvan viranomaisverkon, VIRVE:n toimintaa ja mahdollisuuksia.

Tutkielmastani selviää myös se, että TETRA-verkon tietoturvaominaisuuksista eivät sen kehittäjät ole kovinkaan halukkaita julkisesti kertomaan. Ehkä TETRA-verkon hyvä maine tietoturvan suhteen on osittain seurausta myös tästä seikasta. Tutkielmassani jääkin lopussa muutamia kysymyksiä ratkaisematta TETRA-verkon tietoturvaa koskien. Ehkäpä pääsen joskus työn puolesta löytämään ratkaisut näihin kysymyksiin, ainakin toivon niin.

Avainsanat ja -sanonnat: TETRA, VIRVE, tietoturva

Sisällys

1. Johdanto

Vielä joitain vuosia sitten oli mahdollista skannerilla kuunnella poliisien keskusteluja, ja sivullisia sekä joskus jopa lehdistön edustajia saattoi tästä johtuen eksyä rikosten tapahtumapaikoille ennen poliiseja. Toisaalta salakuuntelu saattoi pahimmassa tapauksessa pitää myös rikolliset askeleen poliisia edellä. LA-puhelimen kantama oli lyhyt ja täten maan laajuisten operaatioiden suorittaminen käytössä olevien laitteiden avulla oli melkein mahdotonta. GSM-puhelimen käyttö oli tietysti eräs ratkaisu, mutta sen käyttö rajoitti keskustelut vain kahden henkilön välisiksi.

Salakuuntelun lisäksi toinen suuri ongelma oli yhteisten standardien puuttuminen. Suomessa viranomaisilla oli käytössä useita erilaisia järjestelmiä, ja sama päti myös muihin Euroopan valtioihin. Yhteisten standardien puuttuminen haittasi siis eri viranomaisryhmittymien yhteistoimintaa sekä Suomen sisällä, että kansainvälisesti.

Asia huolestutti myös Euroopan unionia ja tästä johtuen alettiin suunnitella uutta kansainvälistä viranomaisverkkostandardia. Tämän standardin kehitystyö etenikin ajan kuluessa, ja standardin nimeksi tuli TETRA. Oli siis onnistuttu luomaan uusi kansainvälinen digitaalinen matkapuhelinverkkostandardi viranomaiskäyttöön. Suomi oli TETRA-standardin hyödyntämisessä edelläkävijän asemassa VIRVE- ja HelenNet -verkoillaan.

Eräs TETRA-standardin parhaista ominaisuuksista on, että johtuen verkon kriittisestä roolista viranomaiskäytössä, on standardia kehitettäessä erityisesti otettu kehitystyön kohteeksi hyvän tietoturvan saavuttaminen. Salakuuntelun estämisen lisäksi liittyy TETRA-verkon tietoturvaan monia muitakin seikkoja.

Tässä tutkielmassa käsitellään TETRA-verkon tietoturvaa. Suomen kansalaisena oli aiheeseen helppo valita myös VIRVE-verkon ja HelenNet-verkon näkökulmat molempien edustaessa TETRA-verkon eteen Suomessa tehtyä pioneerityötä ja parasta mahdollista TETRA-teknologiaa. Seuraavassa esittelen kaksi ensin mainittua ja HelenNet-verkosta on kerrottu tutkimukseni luvussa 9.

1.1. Johdatus VIRVE-verkkoon

VIRVE on nimitys Suomessa käytettävälle TETRA-verkon standardin mukaiselle viranomaisverkolle. VIRVE-verkon nimi on lyhenne ”viranomais”- ja ”verkko” -sanoista. VIRVE on kaikkien Suomen viranomaisten yhteinen verkko. [Kotilainen, 2004a, ss. 18]

VIRVE-verkon suunnitteluun ja käyttöönottoon johtanut kehitystyö alkoi jo 1980-luvulla. Kehitystyö alkoi kun vallitsevat viranomaisverkkoratkaisut todettiin Suomen viranomaisten käyttöön riittämättömiksi. VIRVE-verkon kehitystyön kantavina voimina olivat pitkään Suomen sisäasiainministeriö ja liikenneministeriö. Myös Sonera oli kehitystyössä mukana. VIRVE-verkon omistus siirtyi Sisäministeriön projektiorganisaatiolta Suomen Erillisverkot Oy:lle 1.1.2004. Suomen Erillisverkot Oy on nykyisin kokonaan valtion omistuksessa. [Kottila, 2004, ss. 20]

VIRVE-verkon suurin käyttäjäkunta on sosiaali- ja terveystoimi 30 prosentin osuudellaan. Seuraavina käytön määrässä tulevat pelastus ja väestönsuojelu, joiden osuus on 20 prosenttia. Poliisin osuus on 15 prosenttia. Raja- ja merivartioston osuus verkosta on kahdeksan prosenttia. Tullin osuus verkosta on neljä prosenttia. Muita VIRVE-verkon käyttäjiä ovat muun muassa energialaitokset, Ilmatieteen laitos, Ilmailuhallinto, liikennelaitokset, Metsähallitus, Tielaitos, turvallisuuspalvelut, vesilaitokset ja Yleisradio. [Kotilainen, 2004a, ss. 18]

Ennen kaikki nämä organisaatiot rakensivat itse omat verkkonsa, ja kustannukset olivat melko suuret verrattuna VIRVE-verkon aiheuttamiin kustannuksiin. VIRVE-verkon sisälle on toteutettu jokaiselle käyttäjäviranomaiselle omia virtuaali- eli näennäisverkkoja. Näennäisverkot mahdollistavat sen että viranomaiset eivät häiritse vahingossa toisiaan. VIRVE-verkon kautta on tarvittaessa kuitenkin mahdollisuus saada yhteys myös toiseen viranomaiseen. [Kotilainen, 2004a, ss. 18-19]

TETRA-verkon standardin mukaisesti VIRVE-verkkokin toimii 380-400 megahertsin taajuusalueella. Suomessa tämä taajuus vapautui 12-kanavaisilta puheliikenteen radiolinkeiltä vuonna 1999. VIRVE-verkon taajuusalue on itsessään jaettu 25 kilohertsin välein. Tämä tarkoittaa käytännössä sitä, että verkko on jaettu kahdeksan kertaa tiuhempaan kuin GSM-verkko. VIRVE-verkon lisäksi Suomessa on toinenkin TETRA-verkko: Helsingin Energian oma HelenNet-verkko. [Kotilainen, 2004a, ss. 18-19]

1.2. Johdatus TETRA-verkkoon

Euroopan yhdentyminen on luonut tarpeen viranomaisverkkostandardille. Käytännössä tämä tarve syntyi, kun Schengen-sopimuksessa sovittiin että allekirjoittajamaiden viranomaisten on voitava kommunikoida riippumatta sijaintipaikastaan, ja että tulevissa viranomaisverkoissa kommunikoinnin täytyy olla mahdollista tapahtua yli rajojen. [Vesanen, 2003]

Tähän asti kuitenkin viranomaisverkot ovat Euroopassa olleet kansallisten vaatimusten mukaisia, mutta eivät yhteensopivia muiden maiden järjestelmien kanssa. Schengen sopimuksen täytäntöönpanoa valvovan elimen mukaan viranomaisverkkojen täytyy kuitenkin perustua avoimeen, eurooppalaiseen standardiin ja olla yhteensopivia keskenään. Tällä hetkellä ainoa Schengen-sopimuksen täyttävä viranomaisverkkostandardi on TETRA (TErrestrial Trunked Radio). TETRA on ETSI:n (European Telecommunications Standards Institute) [ETSI] julkaisema avoin digitaalinen radiopuhelinstandardi, jonka valmistelu käytiin jo 1980-luvun loppupuolella. Avoimen standardoinnin hyötynä on että laitteita voi tuottaa moni valmistaja, jolloin teknologian tuottaminen ei ajaudu yksiin käsiin, ja näin voidaan taata parempi kilpailu ja laatu. [Vesanen, 2003]

1.3. Tutkimuksen lähtökohdat

Tässä tutkimukseksi olen lähtökohdakseni valinnut tutkia TETRA-verkon tietoturvaa ja sen suomalaista toteutusta, VIRVE-verkkoa. Tarkoituksenani on eri lähteiden tietoja yhdistelemällä selvittää tutkimuksessani TETRA-verkon ja VIRVE-verkon ominaisuudet, toiminta, uhat ja salaus. Tämän lisäksi perehdyn tutkimuksessani lyhyesti verkossa käytettäviin päätelaitteisiin ja HelenNetiin, joka on toinen suomalainen TETRA-verkko VIRVE-verkon lisäksi.

2. TETRA-verkot

Vuonna 1990 ETSI pyysi ehdotuksia TETRA–teknologiaksi, ja annettujen ehdotusten pohjalta sitten valittiin TETRA-teknologia vuonna 1991. Standardointityö teknologialle valmistui vuonna 1995, ja vuoden 1994 joulukuussa perustettiin TETRA Memorandum of Understanding (MoU), jossa on nykyään lähes 100 jäsentä [Vesanen, 2003]

2.1. Ominaisuudet

Yksi fyysinen TETRA-verkko voidaan jakaa useisiin virtuaaliverkkoihin, joissa kukin käyttäjäryhmä pystyy käyttämään omaa osuuttaan verkosta ikään kuin koko verkko olisi heidän käytössään. Tällainen järjestelmä takaa kunkin organisaation sisäisen virtuaaliverkon ja eri virtuaaliverkkojen välisen turvallisuuden. Täten organisaatioiden välinen kommunikaatio voidaan toteuttaa helposti, kun käyttäjäryhmien virtuaaliverkot ovat fyysisesti samassa verkossa. [Vesanen, 2003]

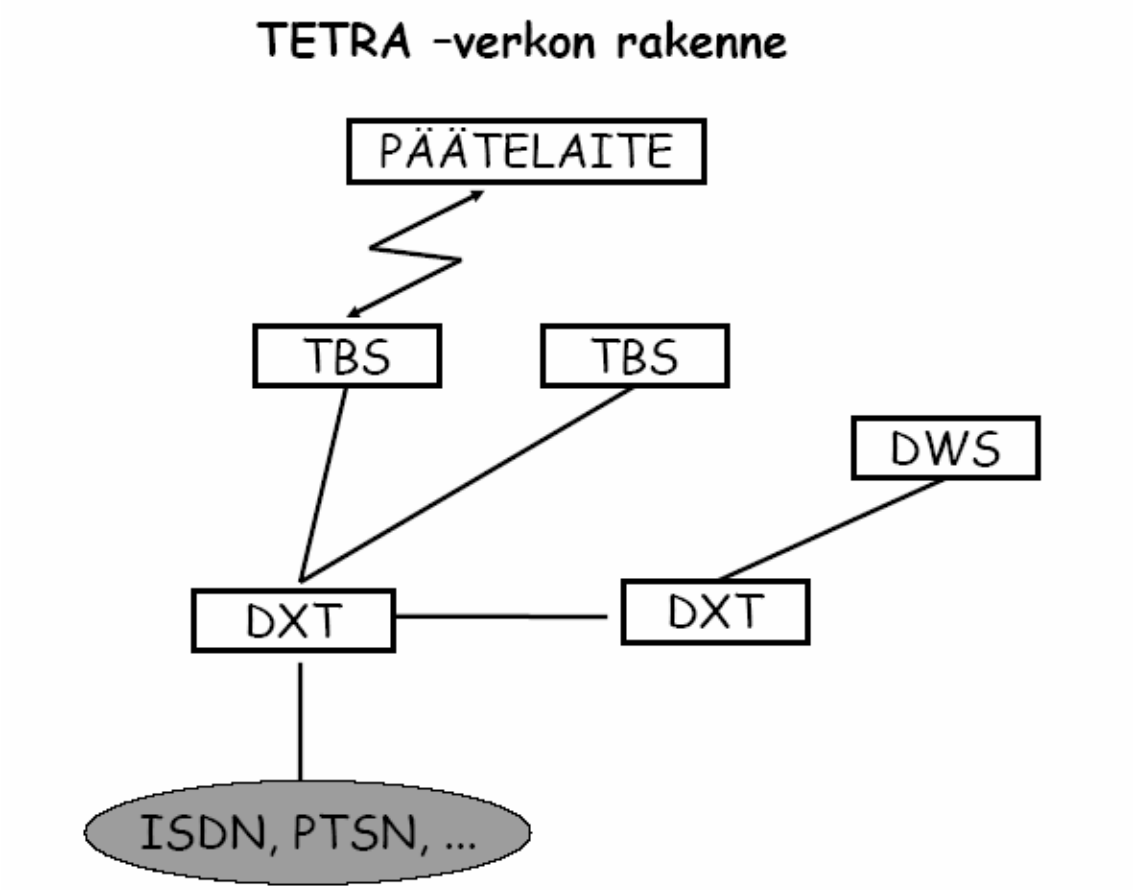
Puhelut on TETRA-verkossa priorisoitu asteikolla 0-10 ja korkeimman prioriteetin puheluja ovat hätäpuhelut. Hätäpuheluille varataan aina resursseja riippumatta muun liikenteen määrästä. Siinä tapauksessa että hätäpuhelua soitettaessa resurssit ovat varattuja, puretaan alhaisimman prioriteetin puheluja hätäpuhelun tieltä. [Vesanen, 2003]

Solunvaihto tapahtuu TETRA-verkossa siten että solunvaihdon tekee päätelaite. TDMA-kanavointi on TETRA-verkossa toteutettu niin että kanavaa kohden on neljä aikaväliä ja aikavälin maksiminopeus on 7,2 kilobittiä sekunnissa. TETRA-verkko tukee myös piiri-ja pakettikytkentäistä liikennettä. [Vesanen, 2003]

Rakenteeltaan TETRA-verkko muistuttaa suuresti GSM-verkkoa (Kuva 1.). TBS tarkoittaa TETRA-verkossa tukiasemaa eli TETRA Base Stationia. DXT tarkoittaa TETRA-verkossa keskusta eli Digital eXchange for TETRA. Tukiasemakontrollereja TETRA-verkossa ei ole vaan tukiasemat on kytketty suoraan keskuksiin. DWS eli Dispatcher Workstation taas on viranomaisverkoille tyypillinen osa. [Vesanen, 2003]

Dispatcher tarkoittaa TETRA-verkossa toiminnanjohtajaa. Dispatcher jakaa kentällä toimivalle henkilöstölle tehtävät, seuraa annettujen tehtävien suoritusta ja kenttätilanteen kehitystä, voi kontrolloida verkon viestiliikennettä, voi osittain hallita verkkoa ja voi liittyä mukaan käynnissä oleviin ryhmä- tai yksilöpuheluihin. [Vesanen, 2003]

Muita TETRA-verkon ominaisuuksia ovat muun muassa häirinnän havaitseminen ja viranomaisten pääsy verkkoon. Häirinnän havaitseminen (jamming detection) on toteutettu TETRA-verkossa siten, että radiosignaaleja tarkkaillaan koko ajan, ja jos järjestelmä havaitsee tarkoituksellista radioliikenteen häirintää, annetaan varoitus ja pyritään siirtämään liikennettä häiriintymättömille taajuuksille. Viranomaisten pääsy verkkoon on toteutettu LII-rajapinnan (Lawful Interception Interface) kautta. [Vesanen, 2003]



Kuva 1. Tetra-verkon rakenne [Vesanen, 2003].

3. TETRA -verkon tietoturva

TETRA-verkon salaus- ja autentikointimekanismit muistuttavat GSM-verkossa käytettäviä mekanismeja. Parannuksena GSM-verkkoon TETRASSA on kuitenkin kaksisuuntainen autentikaatio, minkä lisäksi algoritmit ovat vapaasti valittavissa ja avaintenhallinta on parempi. Suorassa päätelaitteiden välisessä yhteydessä tarvitaan tukiasemaa päätelaitteiden tunnistamiseksi yhteyden aikana. [Vesanen, 2003]

3.1. Autentikaatioavaimen luonti

TETRA-verkossa tunnistamiseen käytettävä avain K on 128-bittinen ja avaimen luontitapa sallii käyttäjän, päätelaitteen tai molempien tunnistamisen. Avaimen luontiin on kolme erilaista tapaa. [Vesanen, 2003]

Ensimmäinen tapa on että avain johdetaan autentikaatiokoodista AC. Tässä tavassa käyttäjä syöttää AC:n, joka konvertoidaan avaimeksi K. Joko avain K tai AC on verkon autentikointikeskuksen tiedossa. Tässä tavassa tunnistetaan käyttäjä, mutta ei päätelaitetta. [Vesanen, 2003]

Toinen tapa on että johdetaan avain käyttäjän autentikaatioavaimesta UAK (User Authentication Key). UAK on satunnainen 128-bittinen luku, joka on SIM–kortilla päätelaitteessa ja verkon autentikointikeskuksella. Tässä tavassa tunnistetaan päätelaite, mutta ei käyttäjää. [Vesanen, 2003]

Kolmas tapa autentikaatioavaimen luontiin on että avain johdetaan sekä AC:stä että UAK:sta. Tässä tavassa lasketaan avain K AC:n ja UAK:n yhdistelmästä, ja täten tunnistetaan sekä käyttäjä että päätelaite. Avain K on verkon käytössä. [Vesanen, 2003]

3.2. Autentikaatio

Autentikaatio tapahtuu TETRA-verkossa molemminpuolisen haaste-vastaus–menettelyn kautta. Täten siis päätelaite autentikoidaan verkkoon, ja verkko autentikoidaan myös päätelaitteelle. Tämä on huomattava parannus verrattuna esimerkiksi GSM-verkkoon, jossa autentikointi tapahtuu autentikoimalla päätelaite verkolle, mutta verkkoa ei autentikoida päätelaitteelle. Täten siis GSM-verkon teoreettisena uhkana oleva tukiaseman väärentäminen ei ole mahdollinen uhka TETRA-verkossa.

TETRA-verkon Autentikaatio perustuu K–avaimen tuntemiseen. Kummassakin autentikaation osassa luodaan puolet ilmatien salausavaimesta, ja autentikaation jälkeen ilmatien salausavain DCK on valmis. [Vesanen, 2003]

Vieraassa verkossa TETRA-verkon autentikaatio voi tapahtua kolmella tavalla. Ensimmäinen tapa on lähettää autentikaatioavain K kotiverkosta vierailuverkkoon. Tämä tapa ei kuitenkaan ole suositeltava. Toinen tapa on välittää autentikointivektoreita kotiverkosta vierailuverkkoon. Tämä tapa on turvallinen, mutta se voi olla hieman tehoton. Kolmas tapa on välittää kotiverkosta istuntoautentikaatioavain vierailuverkkoon. Tätä tapaa käytetään toistuvasti autentikaatioon. Tässä tavassa ei paljasteta alkuperäistä autentikaatioavainta ja tämä tapa on tehokas, koska autentikaatioavain tarvitsee tässä tavassa siirtää vain kerran. [Vesanen, 2003]

3.3. Salausmekanismit

TETRA-verkossa käytetään kahta erilaista salausmekanismia. Ensimmäinen salausmekanismi on ilmatiensalaus, jota käytetään salaamaan puhelimen ja tukiaseman välinen liikenne, ja tätä salausmekanismia käytetään suurimmassa osassa liikennettä. [Vesanen, 2003]

Toinen mekanismi on päästä-päähän –salaus, jota käytetään kaikkein suurinta turvallisuutta vaativissa tilanteissa koko järjestelmän läpi puhelimesta puhelimeen. Päästä-päähän –salaus voidaan toteuttaa monilla tavoilla standardin puitteissa. Päästä-päähän –salauksen salausfunktiot E1 – E4 ovat Vesasen [2003] mukaan ”musta laatikko” –periaatteella määriteltyjä ja operaattori voi itse valita ne. Vesasen luennoista ei kuitenkaan käy tarkemmin ilmi mitä ”musta laatikko” tarkoittaa ja miten mainitut salausfunktiot toimivat.

3.4. Salausavaimet

TETRA-verkon salausavaimia käytetään ilmatien salaukseen. Salausavaimia on yhteensä neljä erilaista. DCK-avain (Derived Cipher Key) luodaan autentikaation yhteydessä, ja sen avulla tapahtuu yhden käyttäjän ja tukiaseman välinen salaus. [Vesanen, 2003]

CCK-avaimen (Common Cipher Key) luo keskus, joka jakaa avaimen DCK:lla salattuna kaikille saman sijaintialueen käyttäjille. CCK-avainta on tehokasta käyttää ryhmäpuheluiden salaukseen yhdellä sijaintialueella. [Vesanen, 2003]

Myös GCK-avaimen (Group Cipher Key) luo keskus, joka jakaa avaimen ryhmälle. Avainta käytetään jonkin tietyn ryhmän ryhmäpuhelun salaukseen. GCK-avain salakirjoitetaan sijaintialueen sisällä CCK-avaimella jonka tuloksena syntyy MGCK-avain (Modified Group Cipher Key). [Vesanen, 2003]

SCK-avain (Static Cipher Key) on ennalta määrätty avain, joka on voimassa kunnes korvataan uudella. Tätä avainta voidaan käyttää ilman etukäteen tehtävää autentikaatiota. TETRA -standardi tukee 32 erilaisen SCK:n käyttöä ja ensisijaisesti SCK-avainta käytetään laitteelta laitteelle tapahtuvien DMO-puhelujen salaukseen. [Vesanen, 2003]

Avaimenjakomekanismina TETRA-verkossa on OTAR (Over The Air Re-keying). OTAR mahdollistaa turvallisen CCK-, GCK- ja SCK–päivityksen ilmateitse. TETRA-verkossa on myös olemassa vastaava mekanismi päästä-päähän salausavaimille. [Vesanen, 2003]

4. TETRA-verkon algoritmit

Vesasen [2003] luentojen mukaan TETRA-verkossa kaikki algoritmit ovat operaattorin valittavissa, mutta TETRA-standardi kuitenkin suosittelee joitakin algoritmeja. Ilmatien salaukseen on neljä suositusta ja päästä-päähän salaukseen yksi. Autentikointi –ja avaimenluontialgoritmiksi on myös yksi suositus.

Ensimmäinen suositus Vesasen [2003] luentojen mukaan on TEA2:sen ja TEA3:sen yhteiskäyttö. Nämä ovat Wessenaar-sopimuksen kontrolloimia (”Restricted Export”). Toinen suositus on TEA1:sen ja TEA2:sen yhteiskäyttö. Nämä ovat vapaasti vietävissä (”Readily Exportable”). Kolmas suositus on TEA1:sen, TEA3:sen ja TEA4:sen yhteiskäyttö. Tätä valvoo ETSI. Neljäs suositus on TEA3:sen käyttö. Tätä taas valvoo Hollannin poliisi.

Päästä-päähän salaukseen suositellaan Sveitsiläistä IDEA-salausalgoritmia. Autentikointi –ja avamenluontialgorimeille ei ole vientirajoituksia, ja niille on olemassa vain yksi suositus, TAA1 joka koostuu joukosta algoritmeja. Valitettavasti Vesasen [2003] luennoissa ja missään muissakaan käyttämissäni lähteissä ei mainita tämän enempää TETRA-verkkoon liittyvistä algoritmeista, joten en pysty kuvailemaan tarkemmin niiden toimintaperiaatteita.

5. Vaatimuksia viranomaisverkoille

Viranomaisverkoille on asetettu joitakin perusvaatimuksia. Tällainen vaatimus on muun muassa että verkon pitää pystyä takaamaan tehokas kommunikointi kaikissa tilanteissa, ja täten verkon pitää olla erityisen luotettava ja kattava. [Vesanen, 2003]

Viranomaisverkon kattavuusalueen pitääkin olla lähes koko maa, ja kaikkien viranomaisten olisi järkevää käyttää samaa infrastruktuuria. Samassa fyysisessä infrastruktuurissa tulisi olla kullekin viranomaisorganisaatiolle oma virtuaaliverkko. [Vesanen, 2003]

Viranomaisten on myös toimittava ryhmänä, ja verkon on tuettava ryhmäpuheluita, mutta tämän lisäksi verkon on tuettava myös kiireellisiä hätäsanomia. Verkon on taattava myös turvallinen kommunikointi ja salakuuntelu on ehdottomasti estettävä. [Vesanen, 2003]

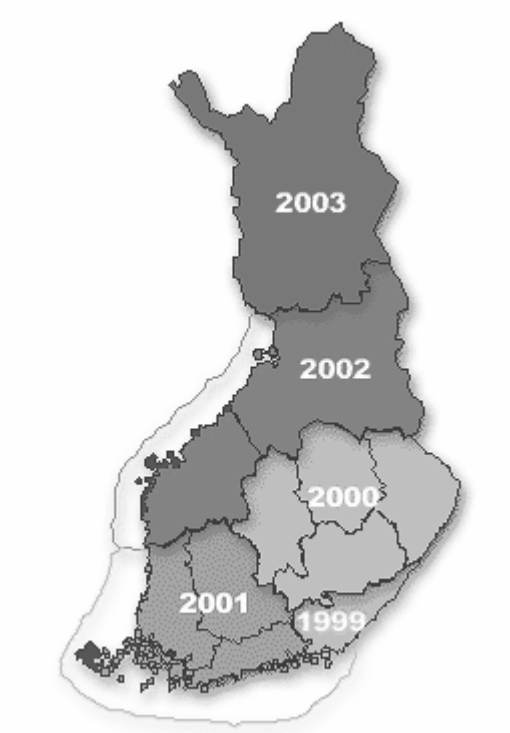
6. VIRVE-verkko

VIRVE on Suomeen rakennettu viranomaiskäyttöön tarkoitettu radioverkko, jota on rakennettu Suomessa vuodesta 1998 asti ja tällä hetkellä verkko kattaa suurin piirtein koko Suomen alueen (Kuva 2.). [VIRVE]

VIRVE-verkko on ensimmäinen TETRA-standardille perustuva maanlaajuinen viranomaisverkko koko maailmassa ja se on myös suurin tällä hetkellä käytössä olevista TETRA-verkoista. [VIRVE]

VIRVE-verkossa on useita parannuksia aikaisempiin järjestelmiin verrattuna. VIRVE-verkko on muun muassa nykyisiä järjestelmiä nopeampi, monikäyttöisempi ja paremmin salattu. VIRVE-verkko helpottaa myös eri viranomaistahojen yhteistyötä ja mahdollistaa monien erilaisten kokoonpanojen luomisen joustavasti, mutta silti ydinjärjestelmää muuttamatta. [VIRVE]

VIRVE-verkon kiinteä osuus käsittää viisitoista keskusta, joista kaksi on solmukeskuksia ja tukiasemia on tähän mennessä rakennettu yli 1200. [VIRVE]



Kuva 2. VIRVE-verkko Suomessa [VIRVE].

7. VIRVE-verkon palvelut

VIRVE-verkko on tehnyt mahdolliseksi monia uudenlaisia palveluita joita ei aiemmissa erillisverkoissa ole nähty. Uudet palvelut tehostavat viranomaisten toimintaa parantaen samalla myös käyttäjien turvallisuutta ja toimintaedellytyksiä erityistilanteissa. VIRVE-verkossa on tällä hetkellä neljä erilaista peruspalvelua jotka ovat käytettävissä kaikilta VIRVE-verkon päätelaitteilta käyttöoikeusluokituksesta riippuen. VIRVE-verkon palvelut ovat ryhmäpuhelu, suojattu yksilöpuhelu, hätäkutsu ja suorakanavatoiminne. [VIRVE]

Ryhmäliikenteessä ryhmäpuhelupalvelu muistuttaa avointa kanavaa ja käyttäjä voi valita mihin ryhmäpuheluun haluaa osallistua. Sama käyttäjä voi kuulua samanaikaisesti moneen eri puheryhmään ja käyttäjä voi myös selata listaa, josta hän voi valita haluamansa ryhmän ja määritellä ryhmille erilaisia prioriteetteja siten, että hän kuulee aina tärkeimmäksi määriteltyä puheluryhmää. Puheryhmän toiminta-alueeksi voidaan valita koko verkko tai verkon osa täysin käyttäjien kulloisistakin tarpeista riippuen eikä puheryhmää ole mahdollista kuunnella sille määritellyn alueen ulkopuolella. Verkkoon voidaan myös luoda uusia puheryhmiä ja nämä ryhmät ohjelmoidaan päätelaitteisiin automaattisesti langattoman yhteyden avulla. [VIRVE]

Suojatussa yksilöpuhelussa puhelu voi olla kahden päätelaitteen välinen, hätäkeskuksen ja päätelaitteen välinen tai kahden hätäkeskuksen välinen. Suojatussa yksilöpuhelussa käyttäjä voi ottaa puheluyhteyden yleiseen puhelinverkkoon tai puhelinvaihteen alanumeroihin samalla tavoin kuin tavallisesta matkapuhelimesta. Keskus ei yksilöpuheluita pysty kuuntelemaan. [VIRVE]

Hätäkutsu suoritetaan painamalla päätelaitteen hätäpainiketta ja tämän seurauksena puhelulle muodostuu korkein tärkeysluokitus ja puhelu voi myös keskeyttää muut puhelut tarvitsemaansa kanavakaistaa varten. Hätäkutsun oletuskohteena voi olla esimerkiksi hätäkeskus tai toinen käyttäjä ja oletuskohde voidaan ohjelmoida päätelaitteelle etukäteen. [VIRVE]

Suorakanavatoiminne mahdollistaa päätelaitteiden väliset yhteydet käyttäen suoraa, verkkoon kuulumatonta kanavaa ja tällainen yhteys voidaan muodostaa myös verkkoyhteyden puuttuessa. [VIRVE]

Edellä mainittujen neljän palvelun lisäksi on myös olemassa erityinen hälytyspalvelu, jonka sisäasiain ministeriö ja hätäkeskuslaitos tarjoavat turvallisuusviranomaisten käyttöön. Hälytyspalvelusta ilmestyi VIRVE:n kotisivuilla tiedote 30.8.2002. Hälytyspalvelu on palveluista uusin ja se on otettu käyttöön täydentämään entisiä palveluja. Hälytyspalvelu käyttää Digitan ula-verkkoja, jotka ovat ensisijaisia kriisiajan viestintäverkkoja. Tällä pyritään suureen luotettavuuteen. Hälytyspalvelu perustuu DARC-teknologiaan. Hälytyspalvelun sanomat liikkuvat reaaliajassa ja hälytyspalvelun kautta on mahdollista lähettää myös ryhmäkutsuja. [VIRVE]

8. VIRVE-verkon datapalvelut

VIRVE-verkossa on neljä erilaista pääasiallista datapalvelua. Nämä datapalvelut ovat lyhytsanomat, statusviestit, automaattipaikannus ja pakettidata & WAP. [VIRVE]

Lyhytsanomien avulla voidaan antaa nopeasti ja joustavasti lyhyet tilanneilmoitukset verkossa oleviin päätelaitteisiin, ja täten pystytään säästämään aikaa ja verkkokapasiteettia. Päätelaitteesta lähetettynä lyhytsanoman enimmäispituus on 128 merkkiä ja käyttöpaikalta lähetettynä lyhytsanoman enimmäispituus on 256 merkkiä. [VIRVE]

Statusviestien avulla voidaan hoitaa rutiini-ilmoitukset käyttäjien ja hätäkeskuksen välillä ja käyttäjä voi ilmoittaa statuksensa yksinkertaisesti yhden näppäimen avulla. Tällaisia statusilmoituksia ovat esimerkiksi ”TEHTÄVÄ”, ”PAIKALLA”, ”TAUKO” ja ”VAPAA”. Keskus vastaanottaa statusviestit viivästyksettä, eikä puheluyhteyden muodostamista täten tarvita. [VIRVE]

Automaattipaikannus tarkoittaa käytännössä käyttäjän sijainnin ja kohteen näkymistä GPS-paikannuksen avulla hätäkeskukselle, ryhmän jäsenille ja käyttäjälle itselleen. Automaattipaikannus voidaan tehdä myös tukiasemien perusteella, jolloin päivystäjä pystyy näkemään puhujan sijainnin tukiaseman tarkkuudella, mutta tämä ei ole yhtä tarkka tapa, kuin GPS-paikannus. [VIRVE]

VIRVE-verkko tukee pakettidataa ja WAP:ia tarjoten GPRS-tyyppisen tiedonsiirtomahdollisuuden koko verkon alueella. Tiedonsiirron nopeus VIRVE-verkossa on TETRA-verkon maksimi eli enintään 7,2 kilobittiä sekunnissa. [VIRVE]

9. HelenNet

HelenNet-verkko on Helsingin Energian oma verkko, ja perustuu samaan TETRA-teknologiaan kuin VIRVE-verkkokin. HelenNet-verkko on itse asiassa ensimmäinen maailmassa käyttöön otettu TETRA-verkko ja se otettiin käyttöön jo vuonna 1997. Verkon kehitys tapahtui yhdessä Nokia Networksin kanssa ja Helsingin Energialla on tällä hetkellä verkossa 300 päätelaitetta. [Kotilainen, 2004b, ss. 27]

Verkossa käytetyt taajuudet vaihtelevat VIRVE-verkosta poiketen 410 ja 430 megahertsin välillä. Helsingin Energian tarjoaa nykyisin HelenNet-liittymiä muillekin organisaatiolle ja yrityksille, koska verkon suuri kapasiteetti tämän mahdollistaa. Koska jokainen organisaatio saa HelenNetissäkin oman sisäisen virtuaaliverkkonsa, eivät organisaation sisäiset asiat tässäkään verkossa leviä vahingossa verkon kautta muihin organisaatioihin. [Kotilainen, 2004b, ss. 27]

Helsingin kaupungin liikennelaitos on HelenNetin suurin asiakasorganisaatio tällä hetkellä ja liikennelaitoksella onkin raitiovaunuissa ja linja-autoissa yhteensä jopa 650 HelenNet-verkkoon kytkettyä päätelaitetta. Liikennelaitoksen lisäksi toinen suuri asiakasryhmä ovat erilaiset vartiointiliikkeet ja yhteensä HelenNetin verkkoa käyttääkin noin sata organisaatiota. HelenNetissä on monia samoja palveluja, kuin VIRVE-verkossa, mutta myös HelenNetin datapalvelut ovat olleet käyttökelpoisia. Muun muassa Helsingin Eko-Viikin aurinkoenergiatalo käyttää HelenNetin datapalveluja kerätäkseen ja siirtääkseen analysoitavaksi mittalaitteista ja sääasemilta saadut tiedot. [Kotilainen, 2004b, ss. 27]

10. Uhat

Kuten kaikkiin muihinkin järjestelmiin, on tietysti myös TETRA-verkkoon murtautuminen mahdollista. Koska TETRA-verkon tietoturvapuutteista ei ollut saatavilla kirjallista lähdeaineistoa, on niitä tässä tutkielmassa pohdittu teoreettisen pohdinnan keinoin. Tässä pohdinnassa olivat hyvänä apuna myös Tietoturvallisuuden erityiskysymyksiä –seminaarissa [Seminaari, 2004] käydyt keskustelut.

Luultavasti suurimpina motiiveina TETRA-verkkoon murtautumiselle on rikollisten tekemä viranomaisten liikkeiden tarkkailu ja toisaalta yksityisiin TETRA-verkon käyttäjäorganisaatioihin kohdistuva liikesalaisuuksien urkinta. Varsinaisessa TETRA-verkossa on murtautujalle saatavilla lähinnä meneillä olevia tapahtumia koskevia keskusteluja ja informaatiota, mutta TETRA-verkon datapalveluihin tehty murto voi mahdollistaa merkittävienkin tutkimustulosten joutumisen vääriin käsiin.

Seuraavassa esittelen joitakin tapauksia joissa TETRA-verkossa kulkeva tieto saattaa joutua vääriin käsiin tai tiedon yhtenäisyys saattaa muuten joutua kyseenalaiseksi.

10.1. Operaattorin verkko

TETRA-verkossa ilmarajapinta päätelaitteen ja tukiaseman (TBS) välillä on hyvin suojattu. Tukiaseman ja keskuksen (DXT) välisen linkin salaus saattaa kuitenkin olla heikompi. Jos hakkeri onnistuu murtautumaan tukiaseman ja keskuksen väliseen linkkiin, saa hän mahdollisuuden salakuunnella verkon puheluita reaaliaikaisesti. Linkkiin murtautumisen onnistuminen on kuitenkin verkko-kohtaista, eli murtautuminen onnistuu vain, jos yhteyden muodostaneet tahot eivät käytä päästä-päähän –salausta yhteytensä salaamiseksi. Päästä-päähän salauksella salatun TETRA-verkon yhteyden kuunteleminen murtautumalla linkkiin on käytännössä mahdotonta.

10.2. Internet

TETRA-verkkoon on teoriassa mahdollista murtautua myös, jos verkon keskukseen kuuluva tietokone on kytketty Internetiin. Tällöin hakkerilla on mahdollisuus murtautua Internetistä käsin tietokoneelle, ja murretulta tietokoneelta salakuunnella tai manipuloida verkkoa.

10.3. Sisäiset uhat

Erotetut tai muuten vihamieliset ja epärehelliset viranomaiset, tietoliikenneasentajat ja muut työntekijät saattavat muodostaa suuren riskitekijän TETRA-verkolle, sillä heillä on yleensä melko rajoittamaton pääsy työssään käyttämiinsä TETRA-verkon osiin. Edellä mainitun kaltaisilla henkilöillä on mahdollisuus aiheuttaa haittaa työnantajalleen, yrityksensä asiakkaille ja työtovereilleen. Mahdollisia haittoja ovat muun muassa puheluiden salakuunteleminen, puheluiden nauhoittaminen, puheluiden salakuuntelun mahdollistaminen jollekin kolmannelle osapuolelle ja verkossa liikkuvan datan väärentäminen.

10.4. Sosiaalinen hakkerointi

TETRA-verkkoon saattaa olla mahdollista päästä käsiksi myös sosiaalisen hakkeroinnin keinoin. Käytännössä tämä tarkoittaa murtautumista työyhteisöön ihmisten luottamusta hyväksikäyttäen ja erilaisiin rooleihin tekeytymistä. Eräs tyypillinen rooli, jonka sosiaalinen murtautuja saattaa ottaa, on asennusmiehen rooli. Asennusmiehen valtuuksilla varustetun murtautujan on mahdollista hankkia käsiinsä tarvittava materiaali verkkoon murtautumisen suorittamiseksi. Sosiaalinen hakkeri pyrkii yleensä pääsemään tavoitteisiinsa keskustelun keinoin, eli kyselemällä uhriltaan erilaisia asioita ja taivuttelemalla uhria kertomaan tärkeitä tietoja. Taitavimmat sosiaaliset hakkerit osaavat hankkia uhreiltaan informaatiota keskustelussa manipulaation ja erilaisten kyselytekniikoiden avulla niin, että uhri ei välttämättä edes tajua kertoneensa mitään merkittävää.

Kun sosiaalinen hakkeri pääsee verkkoon käsiksi, pyrkii hän luultavimmin hankkimaan verkosta kaikkea mahdollista käyttäjillä olevaa tietämystä, ja käyttämään tietämystä joko verkon käyttäjien kiristämiseksi, kaupankäynnin välineenä tai muuten omaksi hyödykseen.

10.5. Passiiviset uhat

TETRA-verkkoa koskevat myös muutamat perinteiset passiiviset uhat. Tällaisia uhkia ovat muun muassa tekniset viat, yhteensopivuusongelmat, huonosti tehdyt kytkennät ja muut inhimilliset ongelmat. Luonnonilmiöt ovat myös eräs seikka jota ei tulisi jättää huomiotta. Erilaiset rakennus– ja huoltotyöt verkon tukiasemien, ja muiden verkon keskusten ympäristöissä saattavat myös muodostaa varteenotettavan passiivisen uhan tarjoten kolmannelle osapuolelle mahdollisuuden päästä käsiksi verkkoon.

Joidenkin VIRVE verkon-kotisivujen [VIRVE] keskustelupalstan kirjoitusten mukaan VIRVE-verkkoa Suomessa vaivaavat yhä monet verkon huonosta peitteestä johtuvat ongelmat. Ilmeisesti verkko ei kata kunnolla edes koko Helsingin aluetta, joten katvealueet saattavat häiritä viranomaisia työssään.

10.6. Kanavien ylikuormittuminen

Kanavien ylikuormittuminen on aiemmin ollut tyypillinen uhka viranomaisverkoissa. Tämä sama uhka on olemassa myös TETRA-verkossa. Jatkuvalla verkon kehitystyöllä on ylikuormittumisen riskiä kuitenkin pystytty pienentämään [Kottila, 2004, ss. 20], ja TETRA-verkossa verkon kapasiteetti pystytään käyttämään lähes kokonaan hyödyksi. Tästä johtuen kanavien ylikuormittuminen ei aiheuta suurta uhkaa TETRA-verkon toiminnalle, vaan ongelmia tulee vasta siinä tapauksessa, että kaikki verkon kanavat ovat täynnä, ja verkon kapasiteetti on riittämätön mahdollistamaan kaikki tarpeelliset yhteydet. Tähän ongelmaan on saatu osittainen ratkaisu priorisoinnin avulla, eli TETRA-verkossa pystytään takaamaan aina tärkeimpien puheluiden läpipääsy ylikuormittumistilanteissakin.

10.7. Muut uhat

Myös salauksen murtaminen, häirintä ja D-DoS-palvelunestohyökkäykset ovat teoreettisia TETRA-verkkoon kohdistuvia uhkia, mutta näitä uhkia en pysty analysoimaan sen tarkemmin, koska en ole onnistunut saamaan käsiini mitään materiaalia näitä uhkia koskien.

10.8. Vastatoimet

Monia esittelemiäni teoreettisia uhkia vastaan pystytään taistelemaan kouluttamalla henkilöstöä asiaankuuluvalla tavalla, ja esimerkiksi kehittämällä kriisisuunnitelma jossa etukäteen suunnitellaan toiminta erilaisissa kriisitilanteissa.

Operaattorin verkkoon tapahtuvaa murtautumista vastaan pystytään parhaiten toimimaan käyttämällä verkossa aina tarvittaessa päästä-päähän –salausta.

Internetistä tapahtuvien murtautumisten riskiä voidaan pienentää asianmukaisten palomuuriohjelmistojen käytön avulla. Internetistä tapahtuvat murtautumiset voidaan estää myös kokonaan, jos TETRA-verkon keskuksen koneita ei kytketä lainkaan Internet-verkkoon.

Sisäisiä uhkia vastaan voidaan taistella parhaiten niin, että pyritään karsimaan ihmisiä jo työhönottovaiheessa, jolloin uhkatilannetta ei pääse syntymään. Mahdollisessa irtisanomistilanteessa voidaan myös pyrkiä vähentämään epärehelliseksi todetun irtisanottavan henkilöstön jäsenen oikeuksia päästä irtisanomisaikana käsiksi tärkeisiin dokumentteihin ja järjestelmiin. Irtisanomistilanteessa kannattaa myös pitää muu henkilöstö ajan tasalla väärinkäsitysten välttämiseksi ja verkon turvaamiseksi, mutta hienovaraisuus irtisanottua kohtaan olisi silti suotavaa eli on pyrittävä informoimaan vain niitä henkilöitä, joihin epärehelliseksi todettu irtisanottava saattaisi ottaa yhteyttä päästäkseen käsiksi verkkoon.

Sosiaalista hakkerointia vastaan pystytään taistelemaan henkilöstön koulutuksella. Pääasiassa tämä tarkoittaa sitä että kerrotaan henkilöstölle sosiaalisen hakkeroinnin uhkat, toimintatavat ja vastatoimenpiteet.

Erilaisiin luonnonilmiöiden vaikutuksesta seuraaviin poikkeustilanteisiin on melko hankalaa varautua etukäteen, mutta luultavasti joitakin yleisiä vaaratilanteita pystytään kuitenkin simuloimaan etukäteen, ja kouluttamaan henkilöstöä toimimaan kyseisenkaltaisissa tilanteissa.

TETRA-verkon ylikuormittumista vastaan pystytään toimimaan parhaiten lisäämällä verkon kapasiteettia erilaisten laitteisto- ja ohjelmistoratkaisujen avulla. TETRA-verkon standardin alaisten verkkojen kehitystyö jatkuu yhä, ja luultavasti parempia ratkaisuja verkon ylikuormittumisongelmiin kehitellään tälläkin hetkellä.

11. Päätelaitteet

VIRVE-verkkoa suunnitellessa päätettiin, ettei päätelaitteita ja logistiikkaa kilpailuteta keskitetysti, vaan jokaisen viranomaisen tai muun yksikön tulee kilpailuttaa päätelaitehankintansa oman organisaationsa hankinnoista annettujen määräysten mukaisesti. [VIRVE]

Päätelaitteita TETRA-verkkoon on saatavilla monelta eri valmistajalta, ja moniin erilaisiin käyttötarkoituksiin. Päävastuu päätelaitteiden VIRVE-yhteensopivuudesta on jätetty niitä hankkiville viranomaisille itselleen. [VIRVE]

11.1. Nokia

Nokialla on valmistuksessa tällä hetkellä kolmea erilaista TETRA-päätelaitetta. Nämä ovat THR850, THR880 ja TMR880. Näistä THR-mallit muistuttavat pitkälti muutaman vuoden takaisia GSM-puhelimia, kun taas TMR-malli on ajoneuvoradio. [NOKIA]

Pienikokoisin ja eniten matkapuhelimia ulkonäöltään muistuttava malli on THR850 (Kuva 3.). THR850:n ulkonäössä on yhdennäköisyyttä Nokian taannoisen 6150 GSM-puhelimen kanssa. THR850 painaa 196 grammaa, sen mitat ovat 137 * 53 * 36 millimetriä, ja se tarjoaa enimmillään 4,5 tuntia puheaikaa ja 28 tuntia valmiusaikaa. THR850-puhelimen teholuokka on 4L. [NOKIA]

Kuva 3. THR850 [NOKIA].

11.2. Motorola

Motorola valmistaa tällä hetkellä viittä erilaista päätelaitetta. Motorolan päätelaitteet ovat MTH800, MTH650, MTH500, MTP700 ja MTM700. Näistä MTH800, MTH650, MTH500 ja MTP700 muistuttavat enemmän matkapuhelimia, kun taas MTM700 on erityisesti suunniteltu moottoripyörään kiinnitettäväksi. [MOTOROLA]

Motorola mainostaa sivuillaan erityisesti mallia MTH800 (Kuva 4.), joka tulee markkinoille vuoden 2004 toisella puoliskolla. MTH800 painaa käyttökunnossa 228 - 239 grammaa, on mitoiltaan 141 * 55 * 32 millimetriä, tarjoaa enimmillään 3 tuntia puheaikaa ja 20 tuntia valmiusaikaa. [MOTOROLA]

Kuva 4. MTH800 [MOTOROLA].

12. Yhteenveto

TETRA-verkko kehittyy kokoajan kovaa vauhtia ja onkin arvioitu että verkon käyttäjäkunta kasvaa tulevaisuudessa ehkä jopa miljooniin käyttäjiin joista suurin osa on siviilejä [Vesanen, 2003]. TETRA-verkko on GSM-verkkoon verrattuna nuori verkko ja luultavasti tulevaisuudessa TETRA-verkon tietoturvauhkien pohdinta ja käytännön esimerkit tulevat muokkaamaan verkon julkista kuvaa nykyisestä. Myös TETRA-verkon käyttötarkoitukset saattavat muuttua tulevaisuudessa ja verkon lopullinen rooli niin viranomais-, kuin siviilikäytössä saattaa sekin muuttua alun perin kaavaillusta.

12.1. Tutkimustulokset

TETRA-verkko on langattomaksi verkoksi melko turvallinen valittujen salausmenetelmien ja algoritmien suhteen. Tietoturva on huomioitu jo TETRA-verkkoa kehitettäessä hyvin, ja ilmeisesti verkon tietoturvallisuutta parannellaan kokoajan. Tutkimuksessani mukana olleita tekstejä tarkemmat TETRA-aiheiset kirjoitukset ja spesifikaatiot eivät ilmeisestikään ole tavallisten ihmisten saatavilla. Harmikseni huomasin tutkimustani tehdessä, ettei ETSI tai VIRVE ollut julkaissut sivuillaan mitään merkittävää materiaalia verkon turvallisuudesta, ja muutenkin tarkka selvitys verkon ominaisuuksista ja teknologiasta puuttui kyseisiltä sivuilta. Tämän vuoksi TETRA-verkon uhkien kartoitus osoittautui melko hankalaksi tehtäväksi.

VIRVE-verkon kotisivuilta [VIRVE] jäi kuitenkin mieleeni kotisivujen keskustelupalstalla mainittu 10W pyyhkäisygeneraattori, jolla kirjoittajan mukaan olisi mahdollista saada koko VIRVE-verkko toimimattomaksi. Tämä ilmeisesti on pelkkää VIRVE-käyttäjän spekulaatiota, mutta olisi tietysti mielenkiintoista tietää onko huhulla myös todellisuusperää.

TETRA-aiheisten kirjoitusten vähyydestä johtuen minulle heräsi kysymys onko TETRA-verkon tietoturvan suhteen mahdollisesti tehty jotain suunnitteluvirheitä joista halutaan vaieta, vai onko julkisten tietojen niukkuus tarkoituksellista jostain muusta syystä. Jos on olemassa pienikin epäily, että tiedoista olisi haittaa väärissä käsissä, saatetaan tiedot jättää julkaisematta. On myös mahdollista että esimerkiksi ETSI:n sivulla on tietoa saatavilla, mutta se on julkaistu sellaisessa muodossa, ettei siihen sivuilla olevalla haulla pääse helposti käsiksi.

Vaikka VIRVE-verkko onkin ollut suosittu Suomessa, on ilmeisesti TETRA-verkko kansainvälisesti jäänyt julkisuudelta syrjään. Tämä selittäisi sen, miksi verkkosivuilta ei löydy paljoakaan tutkimustietoja ja spekulaatiota TETRA-verkon tietoturvauhkia koskien. Toinen syy saattaa olla, että verkkoa pidetään yleisesti turvallisena, ja tätä mielikuvaa ei haluta kyseenalaista kertomalla, että verkolla olisi olemassa edes teoreettisia tietoturvauhkia. Jos verkko nousisi kansainvälisesti julkisuuteen, saattaisi verkkoa koskevia tutkimuksiakin ilmestyä enemmän.

Mielestäni TETRA-verkko on tutkimuskohteena erittäin mielenkiintoinen, mutta päästäkseni käsiksi verkkoa koskeviin tarkempiin tietoihin tulisi minun ilmeisesti olla töissä TETRA-verkon teknologiaa hyödyntävässä tai sitä kehittävässä yrityksessä. Toivonkin että pystyisin tulevaisuudessa työn puolesta tai muuten tutkimaan TETRA-verkkoa lisää, jolloin saisin vastaukset minua askarruttamaan jääneisiin TETRA-verkon turvallisuutta koskeviin kysymyksiin.

12.2. Tulevaisuuden näkymiä

Tällä hetkellä VIRVE-verkon ja TETRA-verkkojen tulevaisuus näyttää valoisalta. Valtio myönsi VIRVE-verkon toimiluvan Suomen erillisverkoille tammikuussa 2004 ja eri puolilla maailmaa on valmistumassa useita TETRA-teknologiaan perustuvia verkkoja. TETRA-verkko on Vaaliston [2004, ss. 4] artikkelin mukaan toiminnassa jo 55 eri maassa. Valtakunnallisia viranomaisverkkohankkeita on Vaaliston [2004, ss. 4] artikkelin mukaan tällä hetkellä perusteilla Euroopan lisäksi muun muassa Lähi-itään ja Aasiaan. VIRVE-verkko on myös saanut kehuja muun muassa liikenne- ja viestintäministeri Leena Luhtaselta. Hän kuvaa Karhun [2004, ss. 9] artikkelin

mukaan verkkoa menestystarinaksi. Viimeisimpiä TETRA-verkon tilaajia on Ruotsi, joka Vaaliston [2004, ss. 4] artikkelin mukaan on päättänyt tilata verkon Nokia Networksilta.

Turvallisuus-lehden [Kotilainen, 2004a, ss. 18] mukaan on arvioitu että ensi vuonna VIRVE-verkossa olisi päätelaitteita, eli pääasiassa käsipuhelimia noin 50.000 kappaletta, ja että käyttäjiä verkolla olisi noin 100.000 henkeä.

Tulevaisuudessa TETRA-verkko luultavasti tulee kattamaan suuren osan eurooppalaisista valtiosta. Koska TETRA-verkko on rakennettu älykkäästi, on se mahdollista päivittää ilman suuria muutostöitä, ja tämän vuoksi verkko luultavammin tulee nykyiselläänkin olemaan melko pitkäikäinen. Luultavasti Suomessakin vähenevät tulevaisuudessa VIRVE-verkon kotisivuilta löytyvien kuuluvuusvalitusten kaltaiset kannanotot, kun VIRVE-verkon tukiasemia erityisesti pääkaupunkiseudulla lisätään. Uskon, että verkon avulla pystytään tulevaisuudessa lisäämään yhä paremmin Suomen ja Euroopan maiden turvallisuutta ja viranomaisten välinen yhteistyö tulee tulevaisuudessa kasvamaan TETRA-verkon ansiosta sekä valtioiden sisällä että niiden rajojen ulkopuolella.

12.3. Lähteiden arviointi

Lähteitä oli saatavilla tutkimustani varten melko vähän, mutta käyttämäni lähteet osoittautuivat hyviksi. Turvallisuus-lehden numeroista sain ajankohtaisia näkökulmia aihepiiriin. IT-viikon numeroista löysin muutaman TETRA-verkkoa käsittelevän artikkelin. VIRVE-verkon kotisivuilta löytyi perustietoa VIRVE-verkosta [VIRVE]. Aluksi uskoin että ETSI:n kotisivut [ETSI] tulisivat olemaan tutkimukseni merkittävin lähde, mutta ETSI:in sivuilta en löytänyt aiheesta merkittävää informaatiota. TETRA-verkon teknistä tietoa löysin eniten tietoa Ari Vesasen luentomateriaalista [Vesanen, 2003]. Nokian [NOKIA] ja Motorolan [MOTOROLA] kotisivut toimivat pätevinä lähteinä päätelaitteiden tietojen etsimiseen.

Viiteluettelo

[ETSI] European Telecommunications Standards Institute
http://www.etsi.org
[Viitattu 24.4.2004]

[Karhu, 2004] Tuomas Karhu – Luhtanen pitää Virveä menestyksenä *Itviikko* (4.3.2004), ss. 9.

[Kotilainen, 2004a] Lauri Kotilainen – Virve yhdisti viranomaisten radioverkot. *Turvallisuus* (1/2004), ss. 18-19.

[Kotilainen, 2004b] Lauri Kotilainen - HelenNet tarjoaa liittymiä pääkaupungissa. *Turvallisuus* (2/2004), ss. 27.

[Kottila, 2004] Jouko Kottila – Suomalainen sisu synnytti Virven. *Turvallisuus* (1/2004), ss. 20.

[MOTOROLA] Motorolan TETRA-päätelaitteet
http://www.motorola.com/cgiss/emea/tetra/
[Viitattu 24.4.2004]

[NOKIA] Nokian TETRA-päätelaitteet
http://www.nokia.fi/puhelimet/tetra/
[Viitattu 24.4.2004]

[Seminaari, 2004] Seminaari – Tietoturvallisuuden erityiskysymyksiä, Tampereen Yliopisto, kevät 2004.

[Vaalisto, 2004] Heidi Vaalisto – Nokia parantaa asemia tetra-kamppailussa *Itviikko* (15.4.2004), ss. 4.

[Vesanen, 2003] Ari Vesanen, Langattoman tietoliikenteen tietoturva, luentomateriaali. Oulun yliopisto, kevät 2003.
http://www.tol.oulu.fi/%7Eavesanen/Langaton_TT/luennot/
[Viitattu 24.4.2004]

[VIRVE] VIRVE-verkon suomalainen kotisivu
http://www.virve.com/
[Viitattu 24.4.2004]

Muuta luettavaa

[TETRAMOU] http://www.tetramou.com/

[TETRASEC] Gert Roelofsen: “Security issues for TETRA Networks”
http://www.tetramou.com/resources/files/tetra_implem_sec.doc

Spyware eli vakoiluohjelmat

Jari Kautiala

Tiivistelmä

Spyware eli vakoiluohjelma on ohjelmakoodi, joka usein käyttäjän tietämättä lähettää ennalta määrättyyn paikkaan tietoja käyttäjästä, käyttäjän ympäristöstä tai käyttäjän organisaatiosta. Tämä voi mahdollistaa tietojen luvattoman luovutuksen sekä käytön jopa rikolliseen toimintaan esimerkiksi taloudellisin intressein. Tällä tekniikalla on mahdollista saada myös käyttäjän käyttäjätunnus-salasana pareja, pankkitietoja ja –tunnuksia kuin myös tilastollista dataa tai ohjelmistojen virhetapauksia. *Spyware* ohjelmien käyttöä voidaan myös pitää tietyissä tilanteissa oikeutettuna. Seminaarityössä käsitellään vakoiluohjelmien määrittelyn, sijoittumisen haitallisen ohjelmakoodin alajoukkoon, tekniikan lisäksi myös näiden oikeutukseen ja pohdintaan missä tilanteissa *spyware* ohjelmien käyttö on hyväksyttävämpää, kyse on kuitenkin miten lainsäädäntö tähän suhtautuu ja miten sen pitäisi suhtautua.

Avainsanat ja –sanonnat: spyware, sniffer, vakoiluohjelma, hijacker, adware

SISÄLLYSLUETTELO

1 Johdanto

Tietotekniikan huima kehitys ja sen verkottuneiden käyttäjien massiivinen lisääntyminen viime vuosina on tuonut alalle mukanaan myös ei-toivottuja ilmiöitä. Näistä jokapäiväisiä esimerkkejä ovat tietojärjestelmiin tunkeutujat ja virukset, jotka haittaavat tai jopa vahingoittavat järjestelmien suunniteltua käyttöä. Tämän teknisen aikakauden sairaus, tietokonevirus, on nykypäivänä monimuotoinen ja tehokas.

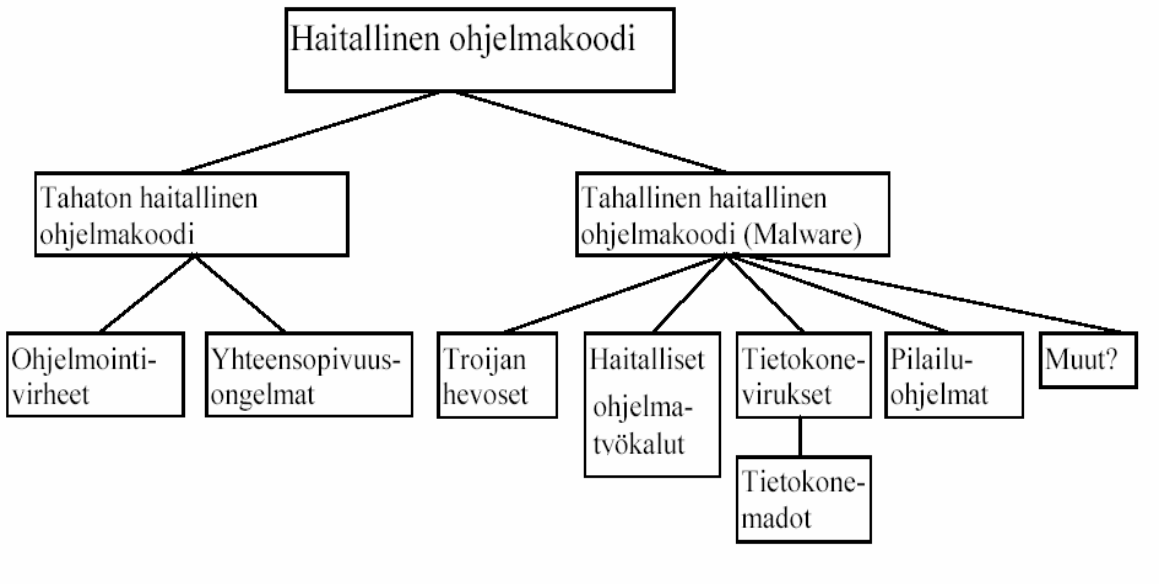
Historiansa alussa viruksilla ja muilla tahallisesti haitallisella ohjelmakoodilla oli primäärisenä tehtävänään levitä ja sekundäärisenä mahdollisesti aiheuttaa haittaa järjestelmälle, yksittäiselle tietokoneelle tai sen käyttäjälle. Ehkä historian tunnetuimpia matoja oli Robert Tappan Morrisin marraskuussa 1988 Unix-ympäristöön kirjoittama ohjelmakoodi. Sen tarkoituksena oli kokeilla toimivatko hänen SMTP protokollan tietoturva-aukkoa hyödyntävä ohjelmansa käytännössä. Tulos oli katastrofi vaikka hänen perimmäisenä tarkoituksenaan ei ollut aiheuttaa haittaa. Hän oli vain utelias [JÄRVINEN, 1990].

Viime aikoina esimerkiksi sähköisen kaupankäynnin lisääntyessä on myös sähköisen tiedon varastamisen mahdollisuus kasvanut. Tämä uhka voi tarkoittaa myös tavallista kuluttajaa, joka käyttäessään sähköisiä pankkipalveluita voi menettää tilitietojaan. On myös mahdollista että pyrkiessäsi siirtymään verkkopankkiin, oikotietä tai kirjanmerkkiä pankin sivulle onkin selaimessa tietämättäsi muutettu ja joudut näköissivulle jolloin on mahdollista menettää käyttäjätunnuksen ja salasanan lisäksi myös käyttämättömiä kertakäyttöisiä tunnuslukuja, kuten mediassa viime aikoina on uhkakuvina maalailtu. Sähköisten lääkereseptien yleistyessä on mahdollisuus reseptien joutumisella vääriin käsiin. Ehkä nämä tässä yhteydessä kuvitteelliset esimerkit ovat kuitenkin ainakin oman mielikuvitukseni lievimmästä päästä.

Seminaarityössäni pyrin käsittelemään *spyware*-ohjelmia ja niiden toimintatapoja läpileikkaavasti yleisellä tasolla sekä muutaman esimerkkitapauksen valossa joihin tarkemmin tutustutaan. *Spyware*-ohjelmien olemassa oloon on varmaan useitakin syitä joista osa saattaa olla tietyssä perspektiivissä jopa näennäisesti puolusteltavaa. Pyrin hahmottamaan tätä oikeutusta eri argumentein sekä analyyttisesti pohdiskelemaan onko *spyware*-ohjelmille oikeasti paikkaa tässä universumissa.

1.1 Mikä on haitaksi ?

Haitalliseksi ohjelmakoodiksi luokitellaan ohjelmakoodi joka on vastoin järjestelmän määrityksiä tai tarkoitettua toimintaa. Haitallinen ohjelmakoodi voidaan jakaa tahalliseen ja tahattomaan [HELENIUS, 2004]



Yllä olevan kategorisoinnin avulla voidaan hahmottaa haitallisen ohjelmakoodin kehityksen motiivit. Tahaton haitallinen ohjelmakoodi voidaan tässä yhteydessä luokitella lähes hyväksyttäväksi tai ainakin hyväksyttävämmäksi koska se ei ole ollut kehityksen suoranainen tarkoitus. Tosin haitallinen ohjelmakoodi ehkä on

voinut olla tiedostettu uhka jo ohjelmistoprojektin alkuvaiheessa esimerkiksi huonon ohjelmistokehitysprosessin, muun laatukriteerin tai yksinkertaisesti puuttuvan kompetenssin aiheuttamana. Kategorisoinnin toinen polku on tahallisesti haitallinen ohjelmakoodi jossa tahallisuuden kehityksen motiivi on tietoinen. Tähän kategoriaan luokitellaan haitalliset ohjelmat kuten esimerkiksi virukset ja Troijan hevoset. Kategorisointi näillä perusteilla on ehkä hieman ontuva mutta puolusteltava. Kategorisointiin kohdistuu aina luonnollista ja puolusteltavaa kritiikkiä kuten jo Aristoteles aikoinaan huomasi. Luonto on yksi, mitäpä sitä jakamaan. Tässä seminaarityössä keskitytään haitallisten ohjelmatyökalujen (engl. *Malicious software kit*) tarkasteluun ja siinä tarkemmin *spyware*-ohjelmiin. Nämä samoin kuin esimerkiksi Troijan hevoset eivät täytä perinteisen virusten tunnusmerkkejä (rekursiivisesti leviävä, resurssien luvaton käyttö). Myös Troijan hevonen voi sisältää *spyware* toiminallisuutta. Näistä käytetään lyhennettä RAT, *Remote Access Tool/Trojan horse*.

1.2 Spyware

Spyware- eli vakoiluohjelma tarkoittaa ohjelmaa tai tiedostoa, jonka tarkoituksena on tarkkailla sinua ja toimintaasi tai organisaatiotasi sekä välittää näistä tietoa käyttäen Internet-yhteyttäsi sinun tietämättä. Tarkkailun kohteena ovat esimerkiksi mitä tiedostoja ajat koneessasi, millä sivuilla käyt Internetissä, tietoja käyttöympäristöstä, tavoista käyttää tiettyä ohjelmaa, periaatteessa mitä tahansa ohjelmallisesti saatavaa tietoa sinusta ja koneestasi. Tarkkailusta saatujen tietojen avulla voidaan mahdollisesti luoda käyttäytymisestäsi profiilia ja käyttää sitä johonkin tiettyyn tarkoitukseen kuten mainontaan (*adware*). Seuranta voi myös liittyä jonkin ohjelman suorittamisen käyttötapausten seurantaan tai ohjelman suorituksen aikana ilmenneen ongelman raportointiin tai käytön tilastollisten profiilien muodostamiseen.

Mielenkiintoista sinänsä on että *spyware* voi olla myös täysin laillista. Tämä on mahdollista, koska esimerkiksi viittaukset käyttäjien seurantaan voivat olla piilotettu esimerkiksi pitkän ”Terms of usage” listan joukkoon. Web-sivuilla tietoja käyttäjästä voidaan välittää eteenpäin myös käyttäen evästeitä, *cookies*. Evästeitä ei yleisesti ottaen kuitenkaan voi suorittaa käyttäjän tietämättä ja ne voi helposti estää selaimen asetuksissa, tosin toiminnallisuudesta tinkien. Evästeiden lisäksi *spyware* on suuri uhkatekijä yksityisyydelle tietoverkoissa.

Vakoiluohjelma on mikä tahansa sovellus, joka hyödyntää taustalla (ns. "taustakanavalla") käyttäjän Internet-yhteyttä ilman että käyttäjät ovat siitä tietoisia tai antaneet siihen lupaa. Ennen Internetin taustakanavan huomaamattoman käytön aloittamista pitää edeltää toden mukainen huomautus aiotusta käytöstä ja tämän jälkeen ennen käytön aloittamisesta pitää seurata selkeä ja informatiivinen kysely aiotusta käytöstä. Ohjelmisto, joka ei täytä edellä mainittuja elementtejä ja kommunikoi Internettiin syyllistyy informaatiovarkauteen ja ohjelmistosta voidaan käyttää termiä vakoiluohjelma. Tämä Steve Gibsonin vapaasti suomentamani määritelmä *spyware*-ohjelmista mielestäni kuvaa kattavasti miten käyttäjää pitäisi informoida ohjelman dataliikenteestä ulospäin. Tässä on myös moraalinen rajaus miten ohjelmistotalojen pitäisi suhtautua ohjelmien käyttäjiin eli maksaviin asiakkaisiin. [GIBSON]

1.3 Tekniikka

1.3.1 Tartunta

Spyware voi tartuttua ympäristöönsä kolmella eri tavalla.

Käyttäjä asentaa tai tuo muuten ympäristöönsä ohjelman joka sisältää *spyware*n. Paikallinen käyttäjä suorittaa operaation joka asentaa kaupallisen tai ilmaisen ohjelman, suorittaa Internetissä esimerkiksi ActiveX-kontrollin tai Java-ohjelman, avaa dokumentin, joka sisältää makron tai yksikertaisesti suorittaa haitallisen

ohjelmatyökalun. Ohjelmakoodi voi olla myös sähköpostiviestin liitteenä. Suurin osa tartunnoista tapahtuu käyttäjän tietämättä mutta käyttäjä voi myös olla tietoinen siitä että kyseinen ohjelmakoodi lähettää dataa käyttäjästä eteenpäin. Osan näistä hyökkäyksistä voi ehkäistä esimerkiksi ympäristön tietoturvallisemmilla asetuksilla tai etsintäohjelmilla.

Tahallinen asentaminen eli tietoinen tartuttaminen. Henkilö, jolla on riittävät käyttäjäoikeudet, voi tahallisesti asentaa ohjelman tietäen että se sisältää *spywaren*. Esimerkiksi joku perheenjäsenistä voi ostaa kaupallisen *spyware*-ohjelman vain uteliaisuuttaan tarkkaillakseen muiden perheenjäsenten tietokoneen käyttöä. Tämänkaltainen toiminta on ainakin Suomessa kriminalisoitu. Tässä kuvattuja hyökkäyksiä vastaan voi olla mahdoton suojautua muulla kuin koneen fyysisellä eristämisellä.

Järjestelmän ulkoinen tunkeutuminen eli etäkäyttö. Järjestelmään voidaan riittävin edellytyksin tunkeutua myös ulkopuolelta. Erilaiset etäkäyttötekniikat joista perinteisiä ovat esimerkiksi RPC (RemoteProcedureCall), Telnet, RemoteShell (RSH) mahdollistavat järjestelmässä ulkoisten operaatioiden suorittamisen ja murentavat näin ollen tietoturvaa. Näitä tekniikoita kuitenkin ainakin yritysmaailmassa tietoisesti vältetään jopa yrityksen sisäisessä verkossa. Riittävällä turvallisuusohjeistuksella, sen valvonnalla, turvallisella järjestelmäinfrastruktuurilla sekä järjestelmä- ja palveluntoimittajilla ennalta ehkäistään ulkopuolinen tunkeutuminen.

1.3.2 Tartunnan jälkitoimet

Internetistä on saatavilla runsaasti etsintäohjelmia jotka tunnistavat vakoiluohjelmia. Osa näistä on kaupallisia ja osa *freeware* ohjelmia. Esimerkkejä tunnetuista etsintä ohjelmista ovat SpyBot Search&Destroy, PestPatrol ja SpySweeper. Nämä ovat nopeita ja etsivät tuntemiaan vakoiluohjelmia niille tyypillisistä kohdista. Ongelmana tässä on kuten tunnettujen virusten

etsintäohjelmilla, että ne eivät löydä kuin tuntemiaan vakoiluohjelmia eivätkä aina sisällä heuristista etsintäominaisuutta. Tällä tarkoitetaan että etsintäohjelma osaisi tunnistaa haittaohjelmalle tyypillisiä piirteitä sekä toimia ja osaisi näiden perusteella luokitella ohjelman haitalliseksi, verrattuna siihen että etsintäohjelma tunnistaa joukon haittaohjelmia ja tätä joukkoa tarvitsee ylläpitää ja päivittää. Näin ollen vakoiluohjelman löytäminen ja poisto ei ole aina helppoa. Lisäksi esimerkiksi kaupallisten ohjelmien laajenteet saattavat sisältää *spyware*ksi luokiteltavaa ohjelmakoodia. Näiden kaupallisten ohjelmien osien poistamisessa tarvitsee käyttää erityistä harkintaa [PCMAG, 2003].

1.3.3 Mitä voidaan seurata

Näppäimistölyöntien lisäksi vakoiluohjelma voi myös nauhoittaa tai seurata Internet-puhelua tai mitä tahansa muuta verkkoon lähtevää tai tulevaa datavirtaa, kaapata kuvia näytöstäsi, seurata tulostusta, verkkostatistiikkaa, leikepöytää, ikkunointia, sovelluksia, käyttää web-kameraasi eli periaatteessa mitä tahansa mitä ohjelmallisesti voi käytössä olevilla käyttöoikeuksilla tehdä. Kerätty tieto voidaan välittää ennalta määrättyyn paikkaan. Ohjelmakoodi voi tutkia tiedostojärjestelmäsi tiedostojen sisältöä verkkolevyilläkin eli hyvin arkaluontoista materiaalia voi päästä leviämään ulkopuolisten tietoon. Tosin tämä edellyttää, että ohjelma osaa etsiä oikeaa tietoa oikeasta paikasta.

1.3.4 Esimerkkejä spywareista

Kaupallisia esimerkkejä näistä tuotteista ovat ISpyNow ja NetObserve Keylogger. ISpyNow on vieläpä tarpeeksi pieni sähköpostin liitteenä lähetettäväksi. ISpyNow tuotteesta on saatavilla myös etäkäyttötuote: SpyAnywhere. Ohjelmalla voi tarkkailla lähes kaikkea mitä verkossa olevalla työasemalla operoidaan, kunhan siihen on riittävät edellytykset. Sillä voi jopa tallettaa sähköpostiviestien sisällöt luettavaksi jälkikäteen.

1.4 Moraalisesti hyväksyttävää ?

Kaupallisia vakoiluohjelmia on ollut jo jonkin aikaa, mutta suuren yleisön tietoisuuteen nämä tulivat viimeistään vuonna 2001, jolloin FBI tutki herra Nicodemo Scarfoa uhkapelin sekä laittoman lainanantojen ja perinnän johdosta. FBI asensi Scarfon tietokoneeseen kotietsintäluvan perusteella ohjelman, joka tallensi ja lähetti Internetitse Scarfon koneellaan tekemiä näppäimistösekvenssejä. Näiden näppäimistösekvenssien analyysin avulla FBI onnistui saamaan salasanan Scarfon kryptattuun tietokoneeseen ja näin saamaan todisteita häntä vastaan. Tästä käytetään termiä *key logging*. Juttu aiheutti kohua yksityisyyden loukkaamisen takia etenkin ennakkotapauksen muodossa mutta myös siksi että lehdistö raportoi FBIn olevan kehittämässä ”Magic Lantern - maaginen lyhty” nimistä vakoiluohjelmaa. Ohjelma pystytään asentamaan epäilyn koneelle etänä esimerkiksi sähköpostin liitteenä. Ohjelmaa käytettäisiin samoin kuin edellä [CRS, 2003].

Yrityksien sisällä on usein tarvetta seurata käyttäjien koneiden tilaa käyttäjän tietämättä. Esimerkiksi käytettyjen ohjelmistojen lisenssien kuormitusta voidaan tarkkailla jotta optimi lisenssien määrä saavutetaan. Yrityksen tietojärjestelmähallinto voi myös tarvittaessa tarkkailla muitakin käyttäjien tekemiä toimenpiteitä tai koneiden tilaa. Myös suoritettavia prosesseja voidaan hajauttaa suoritukseen käyttäjän koneelle ilman että hän tätä välttämättä huomaa. Tällöin ei mielestäni kuitenkaan ole kyse laittomasta resurssien käyttöönotosta sillä yritys omistaa kaikki edellä mainitut resurssit ja yrityksen tietojärjestelmä politiikassa saattaa jopa olla tästä maininta. Lainsäädäntö ja julkinen valta seuraa tekniikan edistymistä mutta kulkee usein hieman jäljessä kuten viime vuosina käydystä keskusteluista yrityksien sähköpostin kautta tulleista yksityisviesteistäkin voidaan johtaa. Mielestäni lainsäädännöllisiä linjanvetoja yksityisyyteen tässä yhteydessä kaivataan. Oma mielipiteeni on, että yritykset voisivat tarkkailla tietojärjestelmissään olevien työasemien tilaa tilastollisessa ja kuormituksellisessa mielessä, mutta varsinaiseen yksittäisen työntekijän

datasisältöön ei pitäisi oikeuksien ulottua. Sallisin kuitenkin järjestelmät ja tekniikat, joilla dataa tarjotaan tietoisesti näkyville.

Internetin ja tietotekniikan käyttäjät luottavat liikaa ympäröivään maailmaan. Jos WWW-sivulla, mailissa tai ohjelmassa pyydetään painamaan nappia niin käyttäjä painaa. Miksi ? Koska napit on tehty painettavaksi, ovet avattaviksi eikä kyseenalaistamista näiden toiminnallisuuksien kohdalla ole ollut aiemmin tapana tehdä. Uskon kuitenkin että on kasvamassa uusi valveutuneempi sukupolvi, joka suhtautuu varovaisemmin ja valveutuneemmin uusiin teknisiin vaaroihin ja omalta osaltaan vie kehitystä turvallisempaan suuntaan käyttäytymisellään. Toivottavasti myös, että ohjelmistojen valmistajat huomaavat käyttäytymismuutoksen, reagoivat siihen ja edesauttavat omalta osaltaan turvallisemman tietoyhteiskunnan kehitystä. Uskon myös että tietoturvallisemmat käyttöjärjestelmät ja –ympäristöt yleistyvät sillä muuten nyky-yhteiskunnalla ei ole mahdollisuuksia kasvaa avoimeksi tietoyhteiskunnaksi ja taantuma parasiittiekonomiaksi on valmis. [GÖRLING, 2004]

LÄHDELUETTELO

[CRS, 2003] Marcia S. Smith, “Internet Privacy: Overview and Pending Legistlation”, Congressional Research Service report for Congress, Order code RL31408, Updated February 6 2003

[GIBSON] Steve Gibson, Gibson Research Corp., http://grc.com/oo/spyware.htm

[TECHTARGET] Lowell Thing, TechTargetNetwork, http://searchcrm.techtarget.com

[HELENIUS, 2003] Marko Helenius, “Threats Caused by Computer Viruses and Other Malicious Code to Computer Systems”, Presentation paper in CESSDA Expert Seminar, Sept. 1-2.2000, Tampere, Finland, http://www.fsd.uta.fi/CESSDA2000/

[GÖRLING, 2004] Stefan Görling, ”An introduction to the parasite economy”, Presentation paper in EICAR 2004

[JÄRVINEN, 1990] Petteri Järvinen, “Tietokonevirukset”, WSOY, 1990

[PCMAG, 2003] Cade Metz, “Spyware—It's lurking on your machine”, article and spyware remover surveillance report, PCMagazine, Aprill 22 2003, http://www.pcmag.com/article2/0,1759,992435,00.asp

General factoring attacks on RSA cryptosystem

Hautamäki Kalle

Tampereen yliopisto
Tietojenkäsittelytieteiden laitos
Seminaari
Tietoturvallisuus
14.7.2004

Tampereen yliopisto
Tietojenkäsittelytieteiden laitos
Seminaari
Hautamäki Kalle: General factoring attacks on RSA cryptosystem
Tietoturvallisuus, 13 sivua
Syyskuu 2004

Tiivistelmä

Algorithms for finding the prime factors of large composite integers are important because widespread use of public key cryptosystem whose security depends on the difficulty of factoring integers. In recent years there has been increase of limit of factoring, due Moore's law and algorithmic improvements. Fastest known factoring algorithm for large integer is General Number Field Sieve. I will discuss possibility of factoring 1024-bit RSA key using General Number Field Sieve and what are factoring limitations.

Sisällys

1 Introduction

In this paper I will show the fastest know factoring algorithm and try to analyze its asymptotic runtime. Then I will discuss its parallel complexity. RSA is most common public key cryptosystem. RSA with 1024-bit moduli is widely used in SSL, PGP, XMLsec, digital signature, etc. It has been considered to be too difficult to factor. Even if some one breaks single 1024-bit RSA modulus, that do not change much. It is more important to determine how hard it is to factor 1024-bit RSA key. Can it be done in couple of months using hardware that costs 10000€? We can always replace RSA key with the bigger key, replacing 1024 with 2048 and replacing 2048 with 4096. Huge keys become cumbersome when using PDA which has small processor and not so much memory. With bigger keys, operations like generating keys, encrypting messages and decrypting messages will take more time and memory.

Table 1.1 will show how long it will take to generate different RSA keys. Program used to generate keys was OpenSSL 0.9.6b. the CPU used was Intel Celeron 466.582 MHz, 927.79 Bogomips.

Table 1.1: Time it took to generate RSA keys of different size

Key size	time
512	0m0.218s
1024	0m0.649s
2048	0m2.170s
4096	0m34.209s
8192	10m7.785s

I start by demonstrating the idea of RSA cryptosystem.

Let $N = pq$ be the product of two large primes of the same size. The lengths of p and q is $n/2$ bits. (The length of n is usually 1024 bits) ($n/2$ bits each. For N is $n = 1024$ bits). Let d and e be two integers satisfying $ed \equiv 1 \mod (\emptyset(N))$, so that there exist an integer k,such that $ed = k\emptyset(N) + 1$, where $\emptyset(N)$ is Euler's phi-function. N is relatively prime to $\emptyset(N)$ and if p and q are primes then $\emptyset(N) = (p-1)(q-1)$.

e is called the encryption exponent, and d the decryption exponent. The public key is the pair $\langle N, e\rangle$, and the pair $\langle N, d\rangle$ is called the secret key.

When encrypting integer message m, message's owner have to have a public key of recipient. Message is encrypted as $E = m^e$ mod N. The resulting E can be decrypted by computing $D = E^d$ mod N.

Therefor $D \equiv E^d \equiv (m^e)^d = m^{ed} = m^{k\emptyset(N)+1} = (m^{\emptyset(N)})^k m \equiv m(\text{mod } n)$. It follows from the fact $ed \equiv 1$ mod $\emptyset(N)$, and from Fermat's and Euler's theorems that $D = m$.

Security of RSA is based on the hope that encryption function is one way, that it will be computationally hard to decrypt a ciphertext. The trapdoor that allows the decryption of the ciphertext is knowledge of factorization $N = pq$ so that $\emptyset(N) = (p-1)(q-1)$ can be computed. From $\emptyset(N)$ one can easily compute e and d.

2 Factoring attacks on the RSA cryptosystem

There are two classes of algorithms to determine factors of integer N. The first class includes modern factoring algorithms. The second class includes old factoring algorithms which are useless when factoring large integers.

In the second class there are factoring algorithms like trial division and Pollard's Rho method[1]. Trial division algorithm tries to divide n with one prime at time. Since smallest prime divisor can be $\sqrt{N}$ at most, the running time of the algorithm is $O(\sqrt{N})$.

Pollard's Rho method:

Set $x = 2$ and $y = x^2 + 1$

1. $g = \gcd(x - y, N)$
2. If $1 < g < N$, stop: g is proper factor
3. If $g = 1$, replace x by $x^2 + 1$ and y by $y = (y^2 + 1)^2 + 1$ and repeat.
4. If $g = N$: Factor not found

The running time of Pollard's Rho method is $O(\sqrt[4]{p})$ where p is the smallest prime divisor.

The first class includes *the multiple polynomial quadratic sieve*(MPQS), *the general number field sieve*(GNFS) and many others. MPQS and GNFS are fastest known factoring algorithms. Their running time is subexponential. The class of algorithms $L(a, b)$ is the class of algorithms whose running time for input n is

$$O(e^{(b+O(1))(\log n)^a(\log\log n)^{1-a}}) \tag{2.1}$$

They are based on the idea of finding integers u and v such that $u^2 \equiv v^2 \pmod{N}$ and such that $u \neq v \pmod{N}$ gives half change of $\gcd(u - v, N) \neq 1$ being a factor of N.

[1] Paul Garrett, Making, breaking codes an introduction to cryptology. p.389

2.1 Dixon's method

The MPQS algorithm is based on Dixon's method. MPQS is an improvement on Dixon's-method and it uses the same kind of factor base, smoothness value, finding dependencies among vectors over $\mathbb{Z}/2\mathbb{Z}$. MPQS also tries find subset V. GNFS is based on the ideas of MPQS and Dixon's method. It is relevant to show the basic idea of Dixon's method.

When factoring N using Dixon's method, we must first create factor base $F = \{p_1, p_2, ..., p_m\}$. Then we generate random integers r_i. This is done usually by $\lfloor\sqrt{N}\rfloor + k$, where $k = 1, 2, ...$ Integer r_i must fulfill the condition of $f(r_i) \equiv r_i^2 \pmod{N}$ is smooth over F. When m integers $p_1, p_2, ..., p_m$ have been found, we can start finding subset V of integers with the property

$$\prod_{r_i \in V} f(r_i) = p_1^{2e_1} p_2^{2e_2} p_3^{2e_3} \cdots p_m^{2e_m} = (p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}) \tag{2.2}$$

with $e_i \geq 0$. From

$$u = \prod_{r_i \in V} r_i \text{ and } v = p_1^{e_1} p_2^{e_2} \cdots p_m^{2e_m} \tag{2.3}$$

it follows that

$$u^2 = \prod_{r_i \in V} r_i^2 \equiv \prod_{r_i \in V} f(r_i) \equiv v^2 \pmod{N} \tag{2.4}$$

We have found our $u^2 \equiv v^2 \pmod{N}$, which hopefully fulfill the condition is $1 < \gcd(u - v, N) < N$ and gives proper factor of N. The runtime is

$$O(e^{(c+O(1))\sqrt{\ln n}\sqrt{\ln \ln n}}) \tag{2.5}$$

for Dixon's method.

2.2 Number field sieve

GNFS represents a substantial step toward polynomial time algorithm. Improvements come from realization that polynomials of Dixon's method and MPQS do not necessarily need to be quadratic. Polynomials that are higher degree could perhaps produce more smooth values than quadratics. Another improvements comes from realization that rings, besides $\mathbb{Z}$, that have smoothness imposed on them would more likely contain more smooth values. If natural mapping could exist between them and $\mathbb{Z}/n\mathbb{Z}$, then it would be possible to get difference of squares.

First we choose degrees d_1 and d_2 of monic polynomials $f_1(x)$ and $f_2(x)$, respectively and an integer $m \in \mathbb{Z}$, that $f(m) = 0 \pmod N$. Polynomial $f(x)$ should be irreducible in $\mathbb{Z}$. Degree d should be a small odd number.

Let α be a complex root of $f(x)$ and let ring $\mathbb{Z}[\alpha]$ include all polynomial expressions in α with integer coefficients. Since $f(\alpha) = 0$ and $f(m) \equiv 0 \pmod N$ we can replace every instance of α with m mod N so that we get ring homomorphism $\phi : \mathbb{Z}[\alpha] \to \mathbb{Z}_N$ of the form $\phi : \sum a_i \alpha^i \to \sum a_i m^i$.

The goal of the algorithm is to find u and v so such that

$$u^2 = (\phi_1(\gamma_1))^2 = \phi_1 \left(\prod_{(a,b) \in S} (a - b\alpha_1) \right) = \phi_2 \left(\prod_{(a,b) \in S} (a - b\alpha_2) \right) = (\phi_2(\gamma_2))^2 = v^2 \tag{2.6}$$

where α_1 and α_2 are roots of polynomials f_1 and f_2, and ϕ_1 and ϕ_2 are ring homomorphisms originated by polynomials. Define S to be a limited set of prime ideal (a, b)-pairs. Finding S we will work with the norm of the number. Define further $F(a, b) = b^d f(a/b)$, where d is degree of f. Now the norm is $N(a - b\alpha) = F(a, b)$. Every prime ideal is Y_i-smooth, where every factor p_i of γ_i is $p_i \leq Y_i$.

In order to construct two squares we must be sure that each factor appears on even time. This will be done by creating matrix where we insert the relations of pairs (a, b), where $F(a, b)$ is Y-smooth. Relations are rows of matrix and columns are the factor base elements. Then the matrix will be filled with the powers of the divisors of the norm. From matrix we find linear dependency modulo 2. There should be at least as many relations as there are members in factor base that we are sure that linear dependency can be found. We then have γ_1^2 and γ_2^2. Last step is extract square root of γ_i^2 to get γ_i.

Running time of GNFS is $L_N[1/3, (64/9)^{1/3}]$, according to Lenstra, Tromer, Shamir, Kortsmit, Dodson, Hughes and Leyland[2]. Running time of GNFS can also be written as

$$O(e^{(1.923+O(1))(\log N)^{1/3}(\log \log N)^{1-1/3}}) \tag{2.7}$$

In table 2.1 there is estimate of factoring efforts of GNFS. 768-bit and 1024-bit data are estimate based on 512-bit data. Total time means number of arithmetic operations.[3]

[2] Lenstra, Tromer, Shamir, Kortsmit, Dodson, Hughes, Leyland: Factoring estimates for a 1024-bit RSA modulus

[3] Robert D. Silverman, An analysis of Shamir's factoring device

Table 2.1: Estimate effort that GNFS will take to factor RSA modulo

modulo size	Total time	Factor base	Matrix memory
428	$5.5 * 10^{17}$	600K	128M
465	$2.5 * 10^{18}$	1.2M	825M
512	$1.7 * 10^{19}$	3M	2G
768	$1.1 * 10^{23}$	240M	160G
1024	$1.3 * 10^{26}$	7.5G	10Tbytes

2.3 Quantum computing

Only know factorization algorithm that has polynomial running time is Shor's quantum factoring algorithm[4]. Algorithm can work only on quantum computer. Even if quantum computer can factor integer in polynomial time there is no proof that it is powerful enough to solve NP-complete problems. While we are waiting to quantum computer to actualize, it is worth of effort to try finding polynomial time factorization algorithm on classical computer.

2.4 Parallelization of GNFS

To form maximum parallel GNFS we must first understand implementation of some steps in the algorithm, like sieving and matrix step. Sieving and matrix eats most of the running time of GNFS. Therefore their maximum parallelization defines maximum parallelization of the GNFS

2.4.1 polynomial step

Finding two polynomials with good characteristics. Goodness is determined by number of smooth values it produces for given smoothness bound. This step can be done in parallel. Choosing good polynomials will decrease running time of sieve and matrix step.

[4] Peter W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer

2.4.2 sieving step

In sieving step algorithm will try to find ideal (a, b)-pairs. Sieving takes most computer time in GNFS. For smoothness bounds y_r (rational factor base) and y_a (algebraic factor base) and sieving regions size S and the sieving effort is dominated by the number of times primes and prime and root pairs hit the sieving region. This value is approximately[5]

$$S(\log\log(y_r) + (\log\log(y_a)) \tag{2.8}$$

Sieving process can be parallelize easily. Sieving processors can run independently each will sieve $a + bm$ and the norm $a - b\alpha$ and sends found relation to central computer. The size of factor base for 1024 bit moduli is about 10^9, so finding one relation takes lot of memory. Adi Shamir and Eran Tromer estimated that 1024-bit sieving takes about 170GB of RAM memory. Since that amount of memory is not sufficiently common (there should be millions of computers doing sieving simultaneously) it is not possible to factor 1024-bit moduli with traditional PC.

Tromer and Shamir introduced TWIRL[6] (The Weizman Institute Relation Locator) device. TWIRL implements sieving step of GNFS. To complete sieving step in 1 year, 194 clusters of TWIRL devices need to be used. Estimated cost is a few dozen million US dollars. TWIRL is still theoretical device.

2.4.3 matrix step

The relations are inserted into a matrix from which linear dependency is found using Gaussian elimination modulo 2 to vectors consisting exponents. If N is large there may be problems in run-time and storage. If matrix possessed additional properties of being symmetric, positive-defined and sparse, then the Lanczos method can be employed. If $a + bm = 65$ then column entry for matrix using rational factor base $2, 3, 5, 7, 11, 13, 17$ would be $65 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot 13^1 \cdot 17^0$

$$(0, 0, 1, 0, 0, 1, 0)$$

[5] Lenstra, Tromer, Shamir, Kortsmit, Dodson, Hughes, Leyland: Factoring estimates for a 1024-bit RSA modulus

[6] Adi Shamir, Eran Tromer, Factoring Large Numbers with the TWIRL Device, proc. Crypto 2003, LNCS 2729, 1-26, Springer-Verlag, 2003

Binary matrix size for 1024-bit moduli is $D * D$, where $D \approx 10^9$. Matrix step is usually done in single supercomputer. Matrix size grows when factor base and number of relations grows. With 1024-bit modulus, size of matrix is too enormous and single computer memory wont be enough. Parallel version of matrix step requires processors to communicate frequently and this would increase too much the actual running time of factoring program when we take account the bandwidth. To compute 1024-bit matrix step one needs thousands of interconnected Crays and still it takes years.

Bernstein proposed hardware solution to matrix problem. Let A be bit matrix consisting of $D = L(\beta)$ columns such that each column contains $L(0)$ non zero entries. Let $w(A)$ be total number of non zero entries in A, it follows that $w(A) = L(\beta) \cdot L(0) = L(\beta)$. One matrix-by-vector multiplication can be done in $O(w(A) = L(\beta)$ operations, the matrix can be completed in $L(\beta)^2 = L(2\beta)$ operations. Bernstein's "matrix-by-vector multiplication using mesh sort" uses mesh of $m * m$ processors to compute matrix in $L(\frac{3\beta}{2})$ operations[7].Optimistically estimated, from 1024-bit factorization linear dependency can be found in matrix within a few hours by device that costs 5,000€.

2.4.4 Square root step

Algorithm finds, from linear dependency, two square algebraic numbers. The square roots can be computed using serial program. This step compared to sieve and matrix step wont take long.

[7] Lenstra, Shamir, Tomlinson, Tromer: Analysis of Bernstein's Factoring circuit

3 CONCLUSIONS

I do not have enough knowledge of GNFS algorithm that I could estimate its maximum parallel processor time and work. But it is clear that 1024-bit RSA is not as secure as generally assumed. Some government or company, with sufficient amount of money to build TWIRL and Bernstein's devices, can factor 1024-bit keys in couple of months. It would be good idea to replace 1024 key with 2048 key (or 4096-bit key) or make sure that 1024-bit key life time is very short.

Table 3.1 demonstrate development of factorization. Information is taken from http://www.rsasecurity.com/ home page

Table 3.1: Factorization of RSA-155 and RSA-160 using GNFS

RSA challenge	512-bit RSA-155	530-bit RSA-160
Sieving step	year 1999	year 2002
Time	3.7 months	18 days
Relations	124′722′179	323′778′082
computers	8000 MIPS	32 R12000 and 72 Alpha EV67
Matrix step	year 1999	year 2003
size	6699191 rows and 671133 columns	5037191 columns
time	1.5 months	148 hours
computers	224 CPU hours	25 R12000 CPU's

Social engineering

Vesa Huotari
University of Tampere
Department of Computer Sciences

Social engineering in computer security refers to exploitation of human weaknesses in order to gain unauthorized access to computer systems. Computer criminals have a vast number of different techniques which can be used to manipulate human behavior. Countermeasures focus on training and proper implementation of all parts of computer security. This paper presents the methods of social engineering and how to resist social engineering.

Keywords: social engineering, computer crime, information security, computer security.

1 Introduction

Information systems are vulnerable to various threats: computer viruses, worms, loss of data due to power failures and other malfunctions. Organizations and individuals are more aware about these dangers and countermeasures like firewalls and virus protection are being used.

Usually we assume that computer system related attacks come via network in form of a virus or a hacker attack. We often forgot that it is a human behind these attacks and the ways of violating computer security are not limited to utilization of computer systems. The final target might be a computer system but instead of hacking computers and networks, criminals may hack people.

Purpose of this paper is to emphasize that social engineering risks should be taken seriously. This paper does not especially address the industrial espionage and spying issues more than in general level. First we define what social engineering is. Next we discuss different social engineering methods. Finally the countermeasures for social engineering are presented.

1.1 Definition

According to Harl (1997), social engineering is the art and science of getting people to comply with your wishes. It is a valid and wide definition but we want to be more precise:

> Social engineering refers to human to human interaction technologies that are used for obtaining information that will allow him/her to gain unauthorized access to a valued system or enables gaining other information that he/she is not authorized. Social engineering is not limited to pure human to human communication, but could utilize all modern technology in order to make the others behave with desired manner.

Social engineering is a human to human interaction and communication. It is not necessarily face to face communication because the attacker might use different carrier

technologies like telephone, SMS, IRC, fax, email etc. All communication devices and technologies may be utilized by attackers.

2 Measures and risk areas

This chapter presents common methods of social engineering and some risk areas.

2.1 First step: background checking

Attacker may do extensive background check of the target organization and individuals. If the attacker knows many details about the target it is much easier to contact people and to fabricate lies. Background checking may include checking the names of personnel from web-site, looking information from phonebook and information available from the Internet. Especially SME's (Small, Medium Enterprises) tend to publish names of employees and other contact information. Large organizations (enterprises, governments and research organizations) participate to different events that leave traces to the Internet. This information might, for example, include conference participation, names of the preventatives, presentations, partnerships and subcontractors. Attackers may also use spam email to collect email addresses and personnel information for attacking purposes.

Attacker may also monitor behavior patterns of personnel. This may be long-term surveillance with different equipment (camera, video, audio equipment) or wandering around facilities in order to spot useful information.

A point worth mentioning is that a car license plate reveals information about the owner since everybody may ask from the registration authority the get name and the address of the owner. No questions are asked from the attacker, at least in Finland. Next we discuss about dumpster diving which may be part of background checking, but also provides enough information for direct attack.

2.2 Dumpster diving

From the early days of hackers, the dumpsters have provided information for people trying to discover vulnerabilities and useful information about certain company or system. Various types of information may be valuable for attackers, for example, company contact information, phonebooks, memos, reports, organization charts, even

passwords and anything that reveals information about the target. Information gathered from dumpsters can be utilized, for example, for contacting persons, creating genuine looking papers, responses and orders. Stealing the identity of employee is a threat too. Personnel cards are often put into dumpsters and distributed to different persons in vast numbers. Especially if cards are put into dumpsters, it is possible that someone omits identity printed into card. The attacker may also be interested about company procedures: hiring new people, security policies, working shifts, holidays etc.

It must be noted that the dumpsters are freely available to everybody – if an item is left to dumpster the ownership is lost.

2.3 Guessing

Even surface analysis/background checking might reveal enough information for the attacker to guess the user password. This is valid, of course, if the user has very poor password like a pet name, birthday or something similar. A vast number of passwords may lead users to use easy to remember passwords, which helps attackers guessing passwords.

2.4 Shoulder surfing and eavesdropping

Passwords typed by the keyboard are the most common method of identifying a person. The password is something that only the user should know. A keyboard or a numpad is used in various systems, not only computer systems: doors, bank automats and cell phones use similar input methods. The problem is that keyboard is visible – when typing the username and the password, someone may monitor the process and use this information later on to log on into the system.

Another common tactic (Jones, 2004) of the social engineer with physical access to a facility is an attempt to gather more information about the company through eavesdropping. This could be carried out just hanging around company or with technical equipment.

Traveling personnel are vulnerable for shoulder surfing since laptop computers and other mobile computers like PDA's (Personal Digital Assistant) are operated outside

organization premises and often in a public place. Personnel working with laptops during a train trip or a flight trip can be easily spied by a person in viewing distance and angle. There have been cases when important corporate information has been copied by rivaling company representative sitting behind in the train. Opportunity makes a thief.

Theft of a physical computer can compromise the security of information and even give user information about corporate systems which may cause more damage.

2.5 Persuasion and plain asking

Kevin Mitnick is perhaps the most well know computer criminal who used social engineering. He has defined the main idea of social engineering (Lemos, 2000): "*You try to make an emotional connection with the person on the other side to create a sense of trust*," he said. "*That is the whole idea: to create a sense of trust and then exploiting it*."

Persuasion is the basic social engineering method – simple and effective. Being convincing and the ability to lie are personal traits that can be trained. Sometimes persuasion is not needed if target of the attacker is unsuspicious: Just asking might be enough to gain information. Persuasion, in social engineering attacks, usually involves some lying in order to get the counterpart to comply. Usually deception needs certain impersonation (for example Arthurs. 2001). Following the roles among others might serve the purposes of the attacker:

- **Repairman, janitor or other support staff.** Men coming with repairman equipment and clothing request to enter the premises in order to check air conditioning – how many could suspect them?
- **IT Support, helpdes**k. Someone calls pretending being a person from the helpdesk and requests your password in order to check/fix something.
- **Fellow Employee / helpless user**. A sharp dressed man introduces himself as a new person, chats a bit and asks how to access the customer database.
- **Manager/authority**. An urgent sounding man calls you and demands the remote access to the corporate network.

- **Trusted third party**. After gaining the trust, in one way or the other, the attacker may use the trust as a tool for getting information.

The role of the attackers may vary a lot, depending on the attacker's motivation, skills, results of background checking, etc. In addition to roles, there are different methods to influence behavior of the people and guide behavior of the target into desired direction. , For example, some tricks that the attacker might use to persuade people are:

- **Flattery and liking**. We usually like people who like us. Expression of liking and small flattery might blur just enough the target for a social engineering attack. Opposite sex might have a greater change of succeeding in this kind of attack?
- **Reciprocation and deceptive relationships** (Gragg, 2002). If someone gives us something we are willing to return the favor. This is related to building relationships. We are more willing to like people who have similar interest that we have. It could be having a common enemy, the same hobby or knowledge. Once the trust is gained the attacker may be able to ask information or exchange it.
- **Pleading to common sense, moral and commitment**. We aim to be practical while working, especially under heavy workload and hurry. We are willing to save time of our own and others time as well. Attacker pleading to common sense using phrases like "It will save money and time" has decent changes of influencing targets decisions.
- **Authority and pushing.** Taking responsibility is a difficult task for most of us. Standing against our superiors is also very difficult. The attacker might pretend to be an authority and try to threaten the target with cause of damage and losses without desired actions. "I really need to get access to this information or we will lose big sales". "Do you really want to take the responsibility?"
- **Diffusion of responsibility** is one trick that attacker might try. If the target feels that responsibility is shared, he/she might feel safe to do as the attacker wants.
- **Overloading** (Gragg. 2002). If we receive a lot of information very quickly we might absorb information rather than evaluate it.

- **Bribing and teasing**. The recent survey made for the Infosecurity Europe trade show (BBC, 2004) proposed that 37% of the respondents were willing to tell their password for chocolate and additional 34% after teasing that their password has something to do with a pet or a child's name. However, it was not reported if people really gave their real passwords.
- **Tailgating and following** personnel can provide access to secure areas without providing identification. While exiting the locked computer laboratory, how many of us ask from the person going in the same door opening what is his/hers business or identity?

Persuasion is easier if a target is under the influence of alcohol or drugs. Parties, social events and other occasions where alcohol is present offer natural environment for the attacker to ask information and persuade with the help of alcohol.

2.6 Reverse social engineering

Reverse social engineering refers to methods how attacker tries to switch roles so that the target makes the contact to attacker. The attacker usually solves problems or assists the user but at the same time gathers information from the target. According to Allen (2001) a typical reverse social engineering attack involves three parts:

Sabotage - After gaining simple access the attacker either corrupts the workstation or gives it an appearance of being corrupted. The user of the system discovers the problem and tries to seek help.

Marketing - In order to ensure the user calls the attacker, the attacker must advertise. The attacker can do this by either leaving their business cards around the target's office and/or by placing their contact number on the error message itself.

Support - Finally, the attacker will assist with the problem, ensuring that the user remains unsuspicious while the attacker obtains the information required.

Reverse social engineering is a difficult task to carry out but can be totally invisible since the target is happy about getting the problem solved and does not suspect being attacked since target contacted the attacker and not the other way round.

2.7 Personnel risks and social engineering

This chapter presents the issues that are related to a company's regular personnel or support staff.

2.7.1 Regular personnel

Personnel are often background checked by authorities and evaluated with different psychological methods by a specialized company. These methods may reveal extreme ends of personnel, but it is difficult to spot someone who might turn into a mole or malicious attacker later on.

When people feel than they are treated badly (for example, fired from the company), they might do things what they would not normally do. Perhaps they do damage, steal equipment or information or turn into moles. Often fired people are escorted outside facilities and their computer accounts are terminated right after firing. Is it just about being careful or a statement of mistrust to an ex-employee?

2.7.2 Summer trainees

Summer vacation time is a risk for companies. Most of the regular employees are away and usually some summer trainees are managing the routines. From the social engineering point of view this is a great opportunity for all kind of attacks. Summer trainees are not probably willing to disturb regular staff that is enjoying vacation and they might trust their own instincts too lightly. Summer trainees usually have access to computer systems and mobile or fixed phones are available which mean that they have access and are accessible for attackers. It is possible that summer trainees do not know practices and personnel of organization very well or at all. Do not forget that a summer trainee could be the attacker.

2.7.3 Support personnel

Janitors, cleaning personnel and security personnel are examples of certain types of personnel that have a wide access to the organization facilities. Physical security mechanisms do not protect from people that are entitled to access the facilities. Moreover, they might be able to access the facilities during out of the office hours, when there is no one else around.

Offices are often loaded with papers containing confidential information. A good practice would be to store all working papers and documents into an appropriate, locked place in order to avoid having them stolen, photocopied or photographed.

Another risk factor is that passwords are changed quite often. This is actually a security measure but may cause people to write passwords onto plain paper since remembering passwords is difficult. It is not rare to have password notes close to the monitor or the keyboard. Anyone having access to facilities has also access to this information and to corporate systems. Support personnel and visitors should not be able to see passwords or other confidential material.

2.8 Carrier technology

Like discussed in the introduction chapter, the attackers might use different technology and communication devices.

2.8.1 Telephone

Telephone offers distance for the attacker – he/she does not have to compromise security by face to face communication. Telephone, like any other electronic media, offers possibility to communicate globally from anywhere to anywhere. They also hide the physical appearance and the other attributes of an attacker. Attacker may use different background effects and sounds with telephone in order to support the story he/she is telling.

2.8.2 Fax, email, web pages

Faking email address is easy; there are services around the Web meant for this purpose. Receiving formal looking email can deceive the recipient. Email is also popular way of delivering trojan horses and other malware (malicious software). Email pages can also be deceitful. For example, a link in email that moves to official looking web page asking the user to input a username and a password in order to take a part to a corporate lottery can lead the unsuspecting target to loose identity to attackers.

2.8.3 Instant messaging, IRC

There have been cases (CERT, 2002) where IRC and instant messaging systems have been used to lure a user into downloading malicious software. Instant messaging systems and IRC are tools for fast communication. Unfortunately, attackers may use them as well.

2.9 Homes – enabling access to corporate systems

Using corporate and home systems has also become independent about the location. We are used to distance working via VPN or with mobile and handheld devices. Home environment is considered as a secure and a private place. For computer criminals home systems are an interesting gateway to corporate systems since home computers are vulnerable to all types of social engineering attacks and what is more important, the physical security mechanisms are often limited to locked doors and windows. Often different people visit homes (sales men, different representatives, janitors etc.) but we maybe rarely think that our computer security might be threatened.

3 Countermeasures

Computer security can be divided into different layers. Figure 1 illustrates the different parts of computer security according to Paavilainen (1998). Without going into details of every layer, we can say that social engineering is used to find and to utilize weaknesses from almost every layer of computer security.

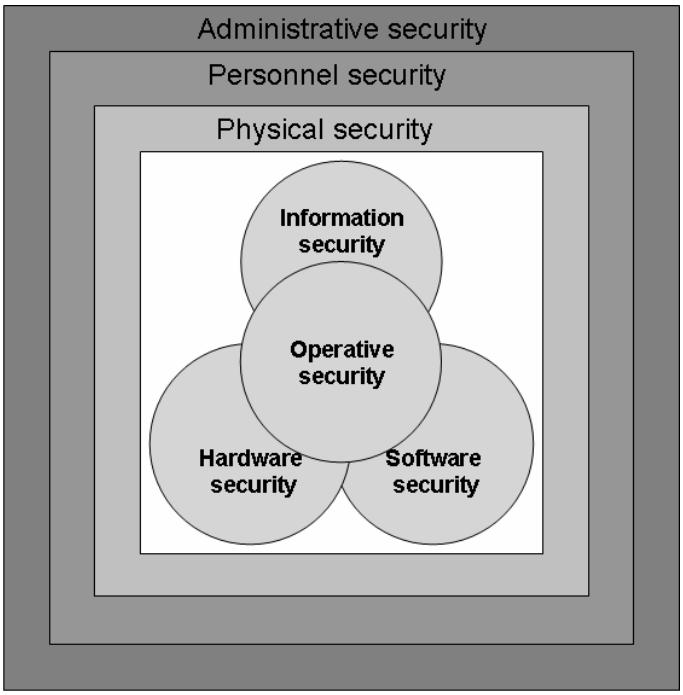


Figure 1. Layers of computer security

Social engineering aims at influencing human behavior and decisions. All layers of computer security must be effectively implemented and operational in order to have a strong defense against social engineering attacks.

3.1 Layers of computer security and defense

The very first thing is that the **administrative security** layer, or more precisely, the security policy must address the threat of social engineering. Because social engineering is about hacking people, the training and awareness of personnel is most important. Well trained staff has better changes identifying attempts to violate security. Regular personnel, summer trainees and traveling personnel should be trained to resist social engineering.

Personnel security should ensure that people are aware of their privileges and responsibilities. Moreover, people should understand the importance of computer security. Furthermore, personnel managers and people responsible for choosing the personnel for organization should be aware of possibility of moles and deceitful people.

Physical security should prevent unauthorized people accessing the premises and ensure that valuable information is not lost. It is a good practice that all guests and visitors are escorted and not allowed to wander around. Visitor badges should always be collected back.

Information security should ensure that attackers are not given even pieces of information that might be used for social engineering attacks. Personnel information available from different channels should be limited to minimum. Papers containing information should not be left to regular dumpsters but destroyed instead.

Operative security should, at least, define the measures that are taken after a social engineering attack and preferable, the measures that are taken if social engineering is going on.

Software and hardware security may provide means for identifying attacks that come from a network. Emails and attachments can and should be scanned before reaching the target since attackers may try to use Trojan horses or other malicious software against the target organization.

3.2 Technology and resisting social engineering

Using smart cards for identifying the users is improvement for a password and username –based authentication. Biometric identification also makes it difficult for attackers to steal the identification and the identity. Biometric identification could be used with door entries, computer devices and for other identity checking.

Surveillance equipment like cameras and motion detecting systems may prevent or help resolving social engineering attacks. This is, of course, true only if targets can suspect or notice the attack. Telephone systems enable us to see the callers' phone numbers, which helps identifying the caller.

3.3 Basic set of rules for individuals how to resist social engineering

Following are basic rules for individuals (For example NIST, 2000) how to avoid some social engineering attempts and how to act when being under social engineering attack.

- Never give your password to anyone for any reason. Verify the identity of all callers.
- Don't give out information about other employees (names, positions, etc.).
- Never type commands into the computer when someone tells you to unless you know exactly what the results of the commands are.
- Don't give out the dial-in phone numbers to any computer system unless they are valid users.
- Never answer questions from telephone surveys. Tell the caller that employees do not participate in telephone surveys from vendors.

Table 1: Tips on social engineering

If being under social engineering attack, the following procedure (For example, NIST, 2000) might be used to reveal and get attacker caught. Procedure is meant for resisting telephone based social engineering but might be modified according to the carrier technology used by the attacker.

- If the number of the caller is available on Caller ID write the number down.
- Take detailed notes of the conversation.
- Try to reverse social engineer the caller.
- Get them to talk about themselves.
- Act as if you believe their story.
- Promise to provide them with the information they seek.
- Ask them to hold or call back.

Table 2: How to react when being under social engineering attack

3.4 Auditing

Auditing and testing personnel skills and security measures is needed. According to Jones (2004) auditing social engineering defense may consist of the following parts:

- **Intelligence gathering phase**. This basically means checking how much information is available about the target organization from the Internet, newsgroups etc.

- **Physical entry phase**. Attackers must not be able to entry facilities. Impersonation, using company dress code, fake ID's grant access should be audited.
- **Shoulder surfing and eavesdropping**. This part may be performed if physical entry phase succeeds.
- **Telephone and e-mail based auditing**. In this phase the personnel "helpfulness" to provide confidential information via phone

Auditing helps identifying problem areas and revising security policies. It also reminds the personnel about threats of social engineering.

4 Conclusions

Humans are often the weak link in computer security. Computer criminals and other parties (competitors, intelligence agencies) understand this and use it against organizations and individuals. Wide variety of methods makes identifying social engineering attack difficult. We might never know that information was stolen or that we revealed something valuable to third party. Organizations are willing to invest heavily in technology but scarcely on humans.

Proper implementation of all parts of computer helps to solve many problems but still training is the key element resisting social engineering. Very worrying is that training and employee awareness is not a high priority: "*Only 29% of organizations list employee awareness and training as a top area of information security spending compared with 83% of organizations that list technology as their top information security spending area"*. (Ernst & Young 2003)

Organizations should recognize the threat and start reinforcing their defenses against these attacks. Information and the confidentiality of information may be the most valuable item for organization. If the information is lost, it is possible that organization never recover from that. For the future work: social engineering offers opportunities for researchers since the topic itself has not been very deeply researched yet.

5 References

Allen, Malcolm. 2001. The Use of 'Social Engineering' as a means of Violating Computer Systems. Online article (accessed 23.4.2004) http://www.sans.org/rr/papers/index.php?id=529

Arthurs, Wendy. A Proactive Defense to Social Engineering. 2001. Online article (accessed 5.5.2004). http://www.sans.org/rr/papers/index.php?id=511

BBC News. 2004. Passwords revealed by sweet deal. Online article (accessed 23.4.2004). http://news.bbc.co.uk/1/hi/technology/3639679.stm

CERT Incident Note IN-2002-03. Social Engineering Attacks via IRC and Instant Messaging. http://www.cert.org/incident_notes/IN-2002-03.html

Ernst & Young. 2003. GLOBAL INFORMATION SECURITY SURVEY 2003

Gragg, David. 2002. A Multi-Level Defense Against Social Engineering. Online article (accessed 5.5.2004). www.sans.org/rr/papers/51/920.pdf

Harl. 1997. People Hacking: The Psychology of Social Engineering (Accessed 23.4.2004). http://cybercrimes.net/Property/Hacking/Social%20Engineering/PsychSocEng/PsySocEng.html

Jones, Chris. SANS Institute 2004, Social Engineering: Understanding and Auditing. Online article (Accessed 23.4.2004).
www.giac.org/practical/GSEC/Chris_Jones_GSEC.pdf

Lemos, Robert. 2000. Mitnick teaches 'social engineering'. Online article (accessed 23.4.2004). http://zdnet.com.com/2100-11-522261.html?legacy=zdnn

Nelson, Rick. Methods of Hacking: Social Engineering. Online article (accessed 5.5.2004).
http://zeth.kodslav.org/security/dokumentation/dokumentation/soceng/socialeng.html

NIST. 2000. Social Engineering Checklist: Tips on how to deal with Social Engineering! (Online article accessed. 23.4.2004)
http://csrc.nist.gov/organizations/fissea/presentations/2000/engineer-check.doc

Paavilainen, Juhani. 1998. Tietoturva. Painopaikka. ISBN: 951-762-647-9