LAUREA AMMATTIKORKEAKOULU Uuden edellä

Sähköisten henkilötunnistusmenetelmien luotettavuus

Assola, Jukka

2011 Leppävaara

Laurea-ammattikorkeakoulu
Paikallisyksikkö

Sähköisten henkilötunnistusmenetelmien luotettavuus

Jukka Assola
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Marraskuu, 2011

Laurea-ammattikorkeakoulu Tiivistelmä

Laurea Leppävaara
Turvallisuusalan koulutusohjelma

Jukka Assola

Sähköisten henkilötunnistusmenetelmien luotettavuus

Vuosi 2011 Sivumäärä 40

Opinnäytetyön aiheena on sähköisten henkilötunnistusmenetelmien luotettavuus. Työssä keskitytään tarkastelemaan sähköistä tunnistamista ja sen luotettavuuteen vaikuttavia tekijöitä. Tarkastelun kohteena on kuusi eri tunnistusmenetelmää: sormenjälkitunnistus, kämmentunnistus, varmennekortti, mobiilitunnistus, tunnus ja salasana sekä pankkitunnukset.

Näkökulmana työssä on identiteettivarkaus, sillä erittäin suuri osa tunnistusmenetelmän luotettavuudesta koostuu sen kyvystä estää asiattomia henkilöitä pääsemästä tunnistusmenetelmän läpi. Luotettavuutta lisää myös tunnistusmenetelmän kyky minimoida vahingot identiteettivarkauden sattuessa.

Opinnäytetyössä luotiin selkeä tietopaketti eri tunnistusmenetelmistä sekä identiteettivarkaudesta. Tämän jälkeen tutustuttiin tunnistusmenetelmien luotettavuuteen vaikuttaviin ominaisuuksiin, joiden pohjalta kartoitettiin ja vertailtiin eri menetelmien luotettavuutta. Eri menetelmien heikkouksien ja vahvuuksien perusteella havaittiin kunkin menetelmän tarjoavan omanlaistaan luotettavuutta. Opinnäytetyön toteuttamisessa on käytetty identiteettivarkautta ja tunnistusmenetelmiä käsittelevää kirjallisuutta, sähköisiä lähteitä, sekä asiantuntijahaastatteluita.

Asiasanat: tunnistaminen, identiteettivarkaus, sähköiset tunnistusmenetelmät, tunnistuspalvelut, vahva tunnistaminen

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Security Management

Jukka Assola

Reliability of Electronic Person Identification Methods

Year 2011 Pages 40

The subject of this thesis is the reliability of electronic person identification methods. The thesis focuses on electronic identification and its reliability factors. There are six different identification methods to be reviewed, which are fingerprint recognition, palm recognition, certificate card, mobile ID, username and password, and access codes.

Reliability is reviewed from the perspective of identity theft, because a huge part of the reliability of identification methods consists of their ability to prevent unauthorized persons from authenticating. The reliability of the identification method is also increased by its ability to minimize the damages after an identity theft has happened.

The thesis provides a clear information package for different methods of identification and identity theft. It then investigates different properties that affect how reliable an identification method is from the perspective of identity theft. Based on these properties the reliability of different identification methods is analysed. The conclusion of this thesis is that different identification methods offer very different types of reliability. Literature on identity theft and methods of identification, electronic sources, as well as expert interviews were used to complete this thesis.

Keywords: identification, identity theft, electronic methods of identification, identification services, strong authentication

Sisällys

1 Johdanto

Monet palvelut ovat siirtyneet ja monet ovat hyvää vauhtia siirtymässä verkkoon. Esimerkkinä näistä ovat pankkipalvelut, verotietojen käsittely, tavaroiden ja palveluiden ostaminen sekä myös vähitellen erilaiset kunnan ja valtion viranomaisten toimittamat palvelut. Samaan aikaan identiteettivarkaudet lisääntyvät sekä maailmalla että kotimaassa (Korhonen 2011a). Henkilön varma tunnistaminen ja identiteetin suojaaminen alkaa olla yhä keskeisemmässä asemassa. Opinnäytetyöni aiheena on sähköisten henkilötunnistusmenetelmien luotettavuuden selvittäminen ja vertaileminen. Tarkastelen luotettavuutta identiteettivarkauden käkökulmasta, eli määrittelen tunnistusmenetelmien luotettavuuden sen mukaan, miten suuri vastustuskyky niillä on identiteettivarkauksia vastaan. Tunnistusmenetelmän luotettavuuteen vaikuttaa myös se, missä suhteessa käyttäjän oma tietoisuus ja toiminta vaikuttavat identiteettivarkauden alttiuteen. Luon havainnoistani taulukon, joka hahmottaa eri menetelmien luotettavuutta lisääviä ominaisuuksia. Teen opinnäytetyöni Fujitsu Services Oy:n tietoturva ja tunnistaminen-osaston toimeksiannosta.

2 Tutkimusprosessi

Noudatan tutkimusprosessissani tieteelliselle tutkimustyölle asetettuja yleisiä sääntöjä ja eettisiä vaatimuksia (Hirsijärvi 2004, 23). Olen kriittinen myös omia näkökulmiani kohtaan ja arvioin tutkimustyötäni sen eri vaiheissa. Pidän tärkeänä selkokielisyyttä, joten vältän monimutkaisia tapoja ilmaista asioita.

2.1 Aiheen ideointi

Lähdin liikkeelle osittain tutusta aihepiiristä. Käsitys tutkittavasta ilmiöstä, eli tunnistusmenetelmistä, oli muodostunut käytännön työn kautta ollessani työharjoittelussa Fujitsu Services Oy:llä. Työharjoittelun kautta kiinnostuin aihepiiristä ja halu syventää tietämystäni olikin vahvasti tutkimusideani taustalla. Aihepiiri on ajankohtainen paitsi itselleni, myös koko yhteiskunnalle ja täyttää kaikki hyvän aiheen kriteerit (Hirsijärvi 2004, 71).

2.2 Aiheen rajaaminen

Rajasin aiheeni rajaamisen ennakkoehtojen, eli toivotun pituuden, käytettävissä olevan lähdemateriaalin ja lukijoiden mukaan (Hirsijärvi 2004). Aiheen rajaaminen oli haastavaa sähköisten henkilötunnistusmenetelmien suuresta määrästä ja niiden ominaisuuksista johtuen. Eri tunnistusmenetelmät saattavat poiketa esimerkiksi käyttösoveltuvuuksiltaan toisistaan hyvinkin paljon, mikä tekee niiden vertailemisesta hankalaa. Toimeksiantajan toivomuksena oli tunnistusmenetelmien luotettavuuden tarkastelu ja vertailu, joten rajasin tarkasteltavista

ominaisuuksista kaiken luotettavuutta lukuunottamatta pois. Muita vertailtavia ominaisuuksia olisi voinut olla esimerkiksi hintaluokka ja käyttösoveltuvuus. Keskityin työssäni muutamaan näkyvimpään tunnistusmenetelmään. Valintakriteerinäni oli, että menetelmää on mahdollista käyttää verkkosivulle kirjautumiseen. Tarkastelemani tunnistusmenetelmät ovat sormenjälkitunnistus, kämmentunnistus, mobiilitunnistus, varmennekortti, tunnus ja salasana sekä pankkitunnukset.

2.3 Tutkimuksen tarkoitus

Tutkimuksella on aina jokin tarkoitus tai tehtävä (Hirsijärvi 2004, 128). Tutkimukseni tarkoitus on sekä kartoittava että kuvaileva. Kartoittavaan tutkimukseen voi kuulua esimerkiksi uusien näkökulmien ja ilmiöiden etsiminen, vähän tunnettujen ilmiöiden selvittäminen tai hypoteesien kehittäminen (Hirsijärvi 2004, 129). Opinnäytetyössäni tuon tunnistusmenetelmiin uutena näkökulmana identiteettivarkauden. Kuvaileva tutkimus dokumentoi ilmiöistä keskeisiä, kiinnostavia piirteitä (Hirsijärvi 2004, 130). Pyrinkin tuomaan identiteettivarkauksista kiinnostavimmat ja ajankohtaisimmat piirteet esiin.

Tutkimukseni on kvalitatiivinen tutkimus. Kvalitatiivinen tutkimus on luonteeltaan kokonaisvaltaista tiedon hankintaa ja aineisto kootaan luonnollisissa ja todellisissa tilanteissa. Tiedon keruun välineenä suositaan ihmistä esimerkiksi erilaisten paperikyselyjen sijasta (Hirsijärvi 2004, 155). Aihealue on myös itselleni melko uusi ja tulokset arvaamattomia, minkä vuoksi kvalitatiivisen tutkimuksen joustavuus soveltuu hyvin opinnäytetyölleni. Kvalitatiivisessa tutkimuksessa tutkimussuunnitelma muotoutuu tutkimuksen edetessä olosuhteiden mukaisesti (Hirsijärvi 2004, 155).

2.4 Tutkimusmenetelmät

Valitsin aineistonkeruun menetelmät sen mukaan, miten hyvin ne tukevat tutkimuksen tavoitteiden saavuttamista. Menetelminä käytin haastatteluja sekä aiheeseen liittyvien dokumenttien tarkastelua. Tavoitteenani opinnäytetyössäni oli kartoittaa tunnistusmenetelmien luotettavuuteen liittyviä ominaisuuksia sekä selvittää, miten sähköisillä tunnistusmenetelmillä tai niihin liittyvillä valinnoilla voidaan ehkäistä identiteettivarkauksia. Aineiston keräämisen oli kohdistuttava asiasta tietäviin tahoihin. Asiantuntijahaastattelu soveltui tarkoitukseen siis paremmin kuin esimerkiksi laajamittaisen kyselyn tekeminen satunnaiselle joukolle.

2.4.1 Haastattelut

Haastattelin opinnäytetyötäni varten kahta aiheen parissa työskentelevää asiantuntijaa. Haastattelujen tarkoituksena on luoda empiiristä käsitystä tunnistusmenetelmien nykytilasta ja

tukea tutkimuksessa käytettävää teoreettista materiaalia. Pääasiallisena teemana haastatteluissani on haastattelemieni asiantuntijoiden itsensä hallitsema aihealue, eli tunnistusmenetelmät, niiden ongelmat ja tulevaisuuden näkymät. Toteutin haastattelut yksilöhaastatteluina asiantuntijoiden aikatauluista johtuen. Haastattelumuotona käytin teemahaastattelua. Teemahaastattelu on lomake- ja avoimen haastattelun välimuoto (Hirsijärvi 2004, 197). Olin laatinut tutkimuksen kannalta olennaisia kysymyksiä ja lähettänyt ne haastateltaville ennen haastattelua. Näin haastateltavalla oli mahdollisuus tutustua kysymyksiin etukäteen ja pohtia niitä syvällisemmin. Haastattelun aikana kyselin aiheeseen liittyviä jatkokysymyksiä aina uuden tiedon avautuessa.

2.4.2 Dokumentit

Toisena tutkimusmenetelmänäni oli erilaisten ajankohtaisten tietolähteiden tarjoaman materiaalin tarkastelu, tiedon yhdisteleminen ja vertailu. Käytin pääasiallisena teorialähteenä työssäni lehti- ja nettiartikkeleita, sillä tietoturva-ala muuttuu ja kehittyy jatkuvasti niin nopealla tahdilla, että aiheesta löytyy vain vähän ajankohtaisia kirjoja. Mediassa identiteettivarkaudet ja tunnistaminen ovat olleet esillä aktiivisesti viime aikoina. Jotkin lähteistäni saattavat olla muutamankin vuoden vanhoja, johtuen siitä, että aiheesta ei kirjoiteta vuosittain uusia yhtä kattavia tietopaketteja. Tilastoja on vaikea löytää identiteettivarkauksiin liittyen, sillä identiteettivarkaus ei ole kriminalisoitu Suomessa (Turunen 2010).

3 Identiteetinhallinta

Identiteetinhallinta liittyy keskeisesti tunnistusmenetelmiin. Se tarkoittaa käyttäjätietokannan ja todennuksen hallintaa. Identiteetinhallinnan kautta esimerkiksi tunnistusmenetelmän hallinnoija pystyy myöntämään tai epäämään käyttöoikeuksia tunnistusmenetelmän takana oleviin palveluihin. Identiteetinhallinnassa tärkeää on käyttäjän tunnistus riittävällä varmuudella sekä käyttöoikeuksien hallinta käyttäjien roolin tai tarpeen mukaan. (Olatilu 2006.)Jokaiseen tunnistustapahtumaan liittyy aina riski, että tunnistettava henkilö ei olekaan, kuka väittää olevansa. Riittävä varmuus saavutetaan, kun riski on tilanteen kannalta tarpeeksi pieni. Identiteetin ja käyttöoikeuksien hallinta on kaikkein kriittisin väline yksityisyyden kontrolloimiseksi, mutta monelta kannalta myös kaikkein hankalin ja kallein implementoida. Identiteetinhallinta hankaloituu, kun erilaisten sovellusten ja verkkopalveluiden määrä sekä tarve kasvaa. Myös käyttäjien tiedonkäyttöä on jossain määrin monitoroitava, mistä voi jo keskisuuressa yrityksessä koitua suurikin haaste. (Axelrod 2007.)

Nykyään on melkein mahdotonta suorittaa minkäänlaista liiketoimintaa keräämättä ja varastoimatta mitään henkilökohtaisia tietoja. Yrityksillä on usein laajoja tietopankkeja tätä tietoa varten. Ihmiset ovat yleensä heikoin lenkki tiedon väärinkäyttöön liittyvissä tapauksissa. Esi-

merkiksi henkilöstön jäsenelle luovutetut oikeudet tietopankkien sisältämiin henkilökohtaisiin tietoihin tekevät hänestä melkoisen riskitekijän. Jollakin oikeudet tietoihin on kuitenkin oltava, minkä takia tämänlaiset riskit ovat vaikeasti minimoitavia. (Olatilu 2006.) Sähköinen identiteetti on käyttäjän ominaisuus, jonka avulla hänet tunnistetaan yksilönä hänen toimiessaan sähköisissä tietovälineissä (Elisa sanasto 2011).

3.1 Identiteettivarkaus

Identiteettivarkaudella tarkoitetaan toisen henkilötietojen tai muiden henkilölle ominaisten tietojen väärinkäyttöä hyötymistarkoituksessa (Cilli 2005). Myös esimerkiksi tunnuksen ja salasanan luvatonta käyttöä pidetään identiteettivarkautena (Virtuaalinen lähipoliisiryhmä 2011). Tunnus ja salasana eivät ole henkilötietoja, mutta ne ovat jokaiselle henkilölle heidän itsensä omistamaa tietoa. Toisen henkilön tunnuksen ja salasanan avulla voidaan esimerkiksi sähköisissä järjestelmissä esiintyä kyseisenä henkilönä. Opinnäytetyöni näkökulmasta identiteettivarkaus tapahtuu silloin, kun asiaton henkilö pääsee tunnistusmenetelmän läpi esiintyen toisena. Tällöin on mahdollista aiheuttaa vahinkoa identiteetin oikealle omistajalle ja vastaavasti taloudellista tai muuta hyötyä identiteetin väärinkäyttäjälle.

Identiteettivarkaudet ovat rikollisten uusi keino käyttää ihmisiä hyväkseen ja sen seuraukset voivat olla hyvinkin tuhoisat. Rikolliset kiinnittävät usein enemmän huomiota teknologioiden kehittymiseen kuin rikollisuuden estämistä suunnittelevat tahot. Ennen kuin uusi väline on ehtinyt levitä, ovat sen heikkouksien hyödyntämismahdollisuudet jo rikollisten tiedossa. Identiteettivarkaus on keino petosten tekemiseen, eikä niinkään päämäärä. Nykyään, kun asiointi hoidetaan suurelta osin tietokoneen kautta ja ihmiset tunnistetaan muutaman tuhannen sähköisen bitin perusteella, on identiteettivarkauksien uhasta tullut maailmalla jo todellinen uhka. Esimerkiksi Yhdysvalloissa identiteettivarkaustapauksia oli 635 000 vuonna 2004, kun vasta kaksi vuotta aiemmin niitä oli vain 82 094 ja neljä vuotta aiemmin vain 21 756. (Cilli 2005.) Suomessakin identiteettivarkaudet ovat yleistymässä (Korhonen 2011a).

Identiteettivarkaudet voidaan jakaa eri osiin niiden tyypin perusteella. Marjie Britz on jakanut identiteettivarkaudet kirjassaan "Computer Forensics and Cybercrime" viiteen ryhmään. Harvinaisin identiteettivarkauden muoto on identiteetin omaksuminen, joka tarkoittaa uhrin koko identiteetin anastamista itselleen kaikkine elämän osa-alueineen. Tosielämässä toisen elämän täysinäinen omaksuminen on todella vaikeaa eikä välttämättä riskin arvoista. Toinen identiteettivarkauden muoto on etenkin Yhdysvalloissa yleistynyt varastettujen identiteettitietojen käyttö työhönotto tai rajanylitystilanteissa. Tätä muotoa esiintyy yleensä laittomien siirtolaisten tai salakuljetuksen yhteydessä. Kolmantena muotona on väärän identiteetin käyttö rikosrekisteriä varten. Rikolliset saattavat käyttää toisen ihmisen identiteettiä suojellakseen itseään rikosrekisteriltä. Tämä on uhrin kannalta ikävä ja tuhoisa identiteettivarkauden

muoto, joka on myös yleistynyt Yhdysvalloissa. Neljäs muoto on virtuaalinen identiteettivarkaus, millä viitataan väärän virtuaalisen identiteetin luomiseen. Väärällä virtuaalisella identiteetillä voidaan suojella oikeaa identiteettiä esimerkiksi kiellettyjä verkkosivuja selaillessa tai kyseenalaista toimintaa harjoitettaessa esimerkiksi seurustelupalstoilla. Viides, Yhdysvalloissa yleisin ja pelätyin identiteettivarkauden muoto on suoranaisen rahallisen hyödyn tavoittelemiseen käytetty identiteettivarkaus. Varas voi esimerkiksi avata pankkitilin uhrin tiedoilla ja kirjoittaa katteettomia shekkejä tälle tilille. (Britz 2009, 117.)

Keskeinen syy identiteettivarkauksien yleistymiseen on digitaalisen tunnistamisen tarpeen kasvaminen. Tunnisteet ovat avaimia sähköisen maailman lukittuihin oviin. Yhä useammassa yhteydessä edellytetään tunnistamista ja sitä mukaan yhä useammin käytetään myös tunnistetietoja. Kun digitaalinen tunnistus tietoverkkojen yli on korvannut fyysisen tunnistamisen, myös identiteettivarkaiden mahdollisuudet ovat parantuneet. Verkko suorastaan haastaa huijaamaan identiteetillä. (Heinonen 2001, 201.)

3.1.1 Miten ja miksi se tapahtuu?

Identiteettivarkaus on erittäin salakavala uhka, joka voidaan panna täytäntöön monella tapaa. Henkilön sosiaalisen profiilin omaksumiseen tarvittavia tietoja voi saada esimerkiksi taloudellisista tiedoista, vakuutustiedoista, verotiedoista, julkisen hallinnon kanssa suoritetuista tiedonsiirroista, pankkitiedoista tai henkilökohtaisista tunnistetiedoista. Näitä tietoja on kaikkialla, ja monella ne ovat usein varastoituina koneelle. Suomessa kauppa- ja muista rekistereistä on nykyisin mahdollista selvittää esimerkiksi yritysten vastuuhenkilöiden henkilötunnukset ja kotiosoitteet. (Korhonen 2010a.)

Muita rikollisten käyttämiä keinoja ovat mm. sähköpostin sieppaaminen tai lukeminen, vakoiluohjelmat, roskapostit, tietojenkalastelusivustot sekä taskusta tai käsilaukusta varastetut identifioivat dokumentit, luottokortit, henkilötiedot, salasanat ja PIN-koodit. Sähköpostissa käytettävä protokolla on itsessään turvaton; se ei tarjoa varmuutta lähettäjän oikeasta henkilöllisyydestä eikä estä luvattomia henkilöitä lukemasta kulkumatkalla olevia viestejä. Myöskään vakoiluohjelmien estäminen ei välttämättä ole helppoa ja nojautuu paljolti käyttäjän tietouteen. Vakoiluohjelmaa voi olla erittäin vaikea havaita eikä se välttämättä anna mitään vihjettä olemassaolostaan. Edes virustorjuntaohjelmat eivät välttämättä aina tunnista vakoiluohjelmaa. Sen poistaminen saattaa olla hyvinkin monimutkaista ja vaikeaa, eivätkä automaattiset poisto-ohjelmat ole välttämättä perusteellisia. Tutkimusten mukaan yhdeksässä koneessa kymmenestä on vakoiluohjelmisto. (Cilli 2005.)

Identiteettivaras voi käyttää varastamaansa identiteettiä tai henkilökohtaisia tietoja suoralta kädeltä petoksen suorittamiseen tai pidempiaikaisen hyödyn tavoittelemiseen. Uhrin tiedoilla

voidaan esimerkiksi hankkia pääsy pornografisiin sivustoihin tai hänen tiedoillaan voidaan suorittaa kalliita ostoksia, joilla voi olla vakavatkin seuraukset. Vaikka uhri yrittäisikin vakuuttaa viattomuuttaan, saattaa se olla mahdotonta todistaa. (Cilli 2005.) Suomessa tavanomaisimpia identiteettivarkaustapauksia on pikavippien ottaminen tai puhelinliittymien avaaminen käyttäjän tiedoilla. Se ei vaadi kuin uhrin nimen ja henkilötunnuksen, joita on helppo kalastella vaikka roskalaatikosta. Henkilötunnus pysyy samana koko iän. Kun se kerran päätyy rikollisten käsiin, on identiteetti teoriassa jatkuvasti vaarassa. Petoksen uhrina perusturvallisuuden tunne saattaa kärsiä pahastikin tai mennä kokonaan, eikä varkauden jälkeen oikein voi olla enää varma, mitä tapahtuu seuraavaksi.

Identiteettivaras voi myydä kalastelemiaan henkilötietoja muille. Henkilötietojen myymiseen tarkoitetuista laittomista tietopankeista on jo todisteita. Tietopankit sisältävät kaiken tarvittavan tiedon, mitä tarvitaan toisena henkilönä esiintymiseen. Näillä tiedoilla on suuret ja jatkuvasti kasvavat markkinat. (Cilli 2005.) Myös Suomessa on uutisoitu tapauksia Suomalaisilta varastetuista käyttäjä- ja luottokorttitiedoista.

Varas voi hyötyä uhrin tiedoista myös aiheuttamatta suoranaista vahinkoa uhrille. Uhrilta voidaan esimerkiksi siepata ekonomisia tietoja tai hänen pankkitiliään voidaan vakoilla. Tämä ei ole todellinen identiteettivarkaus, mutta siepattua tietoa voidaan käyttää laittomana pääsykeinona uhrin yksityiseen elämään ja sitä kautta saada etulyöntiasema uhriin nähden. Henkilötietoja voidaan käyttää myös uusien luottoasemien saavuttamiseen. Uhrin tietoja voidaan käyttää hyväksi esimerkiksi uusien käyttötilien avaamiseen useissa verkkopankeissa tai takuun saamiseksi lainoille, joihin rikollisella ei muuten olisi mahdollisuutta. (Cilli 2005.) Vaikka identiteettivarkaus tässä muodossa ei olekaan niin yleinen Suomessa kuin esimerkiksi Yhdysvalloissa, on hyvin todennäköistä että se leviää myös tänne aikanaan.

Identiteettivaras voi omaksua uhrin sähköpostiosoitteen ja kalastella sitä kautta lisää tietoja tai lähettää haittaohjelmia sitä kautta. Uhrin tietoja voidaan käyttää hyväksi myös sosiaalisessa mediassa tai erilaisissa verkkopalveluissa, kuten seurustelupalstoilla. Suomessakin yleistynyt ilmiö on esimerkiksi luoda uhrin nimissä Facebook-profiili (Lehto 2011). Tästä ei välttämättä aiheudu uhrille suurta haittaa, mutta se voi olla yksityisyyden kannalta erittäin loukkaavaa. Internet ei ole ainoa ympäristö, jossa identiteettivarkauksia sattuu, mutta se on yleisin, sillä internetin henkilötietoja vaativien palveluiden käyttö on yleistynyt ja henkilötietoja on melko helppoa ja riskitöntä kalastella internetin kautta (Cilli 2005).

Vakavin uhka ovat laajat identiteettivarkaudet, joissa tavoitellaan suurta taloudellista hyötyä (Lappalainen 2011). Laajoja identiteettivarkauksia voi tapahtua esimerkiksi silloin, kun kriittisten palvelinlaitteitten tai verkkolaitteitten hallintatunnukset kaapataan vääriin käsiin ja siten vaarannetaan järjestelmän sisältämät tiedot. Järjestelmän luotettavuudesta kertovat

esimerkiksi niiden tietotekniset standardit. Tietoteknisissä standardeissa (ISO27001, PCI-DSS) määritellään vaatimuksia erilasten ympäristöjen suojaustarpeesta. Standardien mukaisesti muun muassa luottokorttitietoja sisältävä tietojärjestelmä on suojattava erityisen tarkasti kaikilta osiltansa aina kaupan kassoilta järjestelmätoimittajan konesaleihin ja palvelimiin. Hyvä esimerkki järjestelmän kassapäässä tapahtuneesta suurimittaisesta luottokorttitietoihin kohdistuneesta varkaudesta paljastui Yhdysvalloissa hiljattain, kun yli sadan hengen rikollisrinki huijasi itselleen miljoonia dollareita kopioimalla luottokortteja (Ståras 2011). Luottokorttitietoja voidaan kerätä laajamittaisesti myös esimerkiksi haittaohjelmilla (Lappalainen 2011). Luottokorttitiedot ovat jokaisen itsensä omistamaa henkilökohtaista tietoa. Luottokorttitietoja tai luottokorttia voidaan käyttää esimerkiksi ostosten tekemiseen esiintyen toisena, minkä takia sitä voidaan pitää identiteettivarkautena.

Edellä mainitut keinot ovat vain osa identiteettivarkauksien hyväksikäyttömahdollisuuksista, mutta rikollisilla on rajaton mielikuvitus. Identiteettivarkauksilla on useita muitakin haittavaikutuksia, jotka eivät välttämättä ole rahallisia. Uhri kärsii todennäköisesti myös suuria emotionaalisia vahinkoja. Uhrien täytyy todistaa, että heidän taloudellinen yksityisyytensä on rikottu, mutta mahdollisesti heidän täytyy myös taistella pitkään hyvän nimensä puolustamiseksi tai taloudellisen asemansa uudelleensavuttamiseksi. (Cilli 2005.)

3.1.2 Identiteettivarkaudet Suomessa

Suomen laki ei toistaiseksi tunne identiteettivarkautta rikosnimikkeenä, vaikka lakiin on jo jonkin aikaa pyritty saamaan muutosta. Varkaus mielletään Suomen laissa irtaimeen omaisuuteen kohdistuvaksi, joten identiteettivarkaus ei ole edes laissa tunnettu käsite. Suomen laki periaatteessa sallii esimerkiksi netissä esiintymisen toisen nimissä (Lehto 2011), vaikka oikeus onkin antanut tuomioita toisen nimellä esiintymisestä verkossa kunnianloukkauksena (Korhonen 2011b). Toisen henkilötietojen väärinkäyttö taloudellisten etujen tavoittelemiseksi on sen sijaan laissa kielletty. Identiteettivarkautta vastaavissa rikostapauksissa onkin kyse yleensä esimerkiksi väärän henkilötiedon antamisesta viranomaiselle (Rikoslaki 24.7.1998/563), petoksesta (Rikoslaki 24.8.1990/769) tai maksuvälinepetoksesta (Rikoslaki 24.8.1990/769). Jos identiteettivaras käyttää esimerkiksi uhrin ottamaa kuvaa, voi rikosnimikkeenä olla tekijänoikeusrikos tai -rikkomus (Virtuaalinen lähipoliisiryhmä 2011). Toiselle kuuluvan sähköpostiosoitteen tai käyttäjätunnuksen luvaton käyttäminen, joka myös on identiteettivarkaus, voi rikosnimikkeeltään olla esimerkiksi tietomurto tai viestintäsalaisuuden loukkaus (Virtuaalinen lähipoliisiryhmä 2011). Koska identiteettivarkautta ei ole kriminalisoitu, Suomen identiteettivarkauksista löytyy todella vähän tilastollista materiaalia. Identiteettivarkauksia epäillään Suomessa kuitenkin jo päivittäin (Lehto 2011).

Keskusrikospoliisin ylitarkastaja Sari Kajantie kertoo Tietoviikon tekemässä haastattelussa, että Suomessa poliisilla ei ole valtuuksia auttaa kaikkia identiteettivarkauden uhreja.

Suomessa identiteettivarkaustapauksia on Kajantien mukaan kolmenlaisia. Ensimmäisenä ovat tilanteet, joissa tavoitteena on mittava taloudellinen hyöty. Nämä ovat usein kansainvälisiä ja ammattimaisia tekoja, kuten massiivisia luottokorttivarkauksia tai verkkokauppatilien väärinkäyttöjä. Toinen ryhmä ovat koulukiusaamistapaukset. Tekijän tavoitteena ei ole taloudellinen hyöty, vaan vahingon aiheuttaminen toiselle henkilölle. Kolmas ja kokonaan uusi luokka ovat tapaukset, joissa todellisen henkilön nimellä ja kuvalla perustetaan väärennetty Facebook-profiili. Siellä voidaan esittää mielipiteitä, joita henkilö ei todellisuudessa lainkaan allekirjoita. Tekijä ei tavoittele taloudellista hyötyä eikä kunnianloukkauksen määritelmä täyty, mutta uhri kokee, että hänen oikeuksiaan on loukattu. (Turunen 2010). Yhteisöpalvelujen ja sosiaalisen median käytön yleistymisen myötä toisen nimissä esiintyminen onkin lisääntynyt (Lappalainen 2011).

Nykyisellään henkilötietojen varastaminen ja kerääminen on rikos vasta, kun tietoja käytetään rikolliseen tarkoitukseen. Jos jo pelkkä tietojen kerääminen olisi rikos, se ennaltaehkäisisi identiteettivarkauksia ja oikeuttaisi poliisin puuttumaan tapauksiin aikaisemmassa vaiheessa. Erityisesti sähköiset identiteettivarkaudet aiheuttavat Suomessa ongelmia, sillä ihmisille itselleen on jätetty todella suuri vastuu siitä kenelle, mihin ja millä tavalla he tietojaan antavat. (Härkönen 2009.)

3.2 Identiteetinhallinnan ongelmia

Identiteetin hallintaan ja tunnistusmenetelmiin liittyy monenlaisia ongelmia, joiden kanssa aiheen parissa työskentelevillä riittää pohdittavaa. Maailma verkottuu jatkuvasti ja verkon käyttäjistä tulee yhä liikkuvampia. Yhtenä haasteena on hallita heidän oikeuksiaan ja mahdollisuuksiaan käyttää verkon tarjoamia resursseja turvallisesti missä tahansa. Samaan aikaan resurssien hallinnan tulisi olla yksinkertaista, turvallista ja helposti auditoitavaa (Identiteetin hallinta lisää tietoturvaa 2011). Esimerkiksi identiteettivarkauksien torjuntaan tuo lisää haastetta verkon kansainvälinen luonne (Korhonen 2011b). Identiteettejä voidaan varastaa verkossa myös maiden rajojen ulkopuolelta, jolloin esimerkiksi lainsäädännölliset vaikeutuvat.

Vaikka luotettavuus identiteetin hallinnassa on usein hyvin tärkeä ominaisuus, jos ei suorastaan elinehto, niin identiteetin hallintaan ja tunnistamiseen liittyy paljon muitakin näkökulmia luotettavuuden lisäksi. Luotettavuuden lisääminen tarkoittaa lähes poikkeuksetta myös hinnan lisäämistä. Yritystoiminnassa raha on ensisijaista, joten esimerkiksi tunnistusmenetelmiä valittaessa valitaan usein se menetelmä, joka on juuri niin luotettava kuin tarpeelliseksi katsotaan. Lisäksi tunnistusmenetelmiin liittyy esimerkiksi sovellettavuus kohteen mukaan ja käytön helppous. Fujitsun tietoturva-asiantuntijan Petri Heinälän mukaan jopa imago saattaa vaikuttaa tunnistusmenetelmän valintaan (Heinälä 2010). Tunnistusmenetelmillä tai -

palveluilla saattaa esimerkiksi olla hyvä tai huono maine yksittäisten mediassa esillä olleiden tapausten perusteella.

4 Sähköiset henkilötunnistusmenetelmät

Identiteettivarkaudet ovat aina yhteydessä henkilötunnistusmenetelmiin, sillä identiteettivarkaus on periaatteessa tunnistusmenetelmän huijaamista. Tärkeimmät ja useimmat internetin palvelut ja sivustot, joita käytämme, vaativat käyttäjän tunnistamisen. Keskiverto kansalainen kirjautuu päivässä useita kertoja sähköisesti johonkin palveluun tai järjestelmään. Erilaisia käyttäjätunnuksia ja salasanoja kertyy elämänvarrella jatkuvasti lisää, niin että monet kirjoittavat niitä ylös ja varastoivat tietokoneelleen. Joku ehkä pyrkii selviytymään elämästä yhdellä ja samalla salasanalla. Kansalaisille itselleen on jätetty suuri vastuu heidän omasta tietoturvastaan, minkä takia myös identiteettivarkailla on runsaasti helppoja uhreja. Identiteettiturvaa voidaan kohentamaan huomattavasti lisäämällä omaa tietoisuuttaan, mutta myös teknisillä valinnoilla voi olla vaikutusta asiaan.

Sähköinen henkilötunnistusmenetelmä on keino tunnistaa esimerkiksi palveluun tai järjestelmään kirjautuva henkilö sähköisiä apuvälineitä käyttäen. Yleisimpiä tällaisia välineitä ovat henkilökohtainen tietokone, pankkipääte tai nykyisin myös matkapuhelin (Kännykkä käy allekirjoittamiseen 2010). Sähköisiä henkilötunnistusmenetelmiä on monenlaisia. Vertailemisen helpottamiseksi työssä tarkasteltavat tunnistusmenetelmät on rajattu niihin tunnistusmenetelmiin, joita voidaan käyttää verkkopalveluihin kirjautumiseen. Tässä työssä tutkittavia sähköisiä henkilötunnistusmenetelmiä ovat sormenjälki, kämmentunnistus, varmennekortti, mobiilitunnistus, käyttäjätunnus ja salasana sekä kertakäyttösalasanat.

4.1 Tunnistuspalvelut

Tunnistuspalvelu on eri asia kuin tunnistusmenetelmä. Vaikka tunnistuspalveluun usein liittyy jokin tietty tunnistusmenetelmä, on tunnistuspalvelu aina liiketoimintaan perustuva palvelu, jonka ideana on tarjota tunnistusmenetelmän käyttöönoton mahdollisuudet ja muut tarpeelliset puitteet, kuten palvelimet ja tunnistinlaitteet maksavan tahon käyttöön. Joissain tapauksissa palveluntarjoaja tuottaa ja hallinnoi myös tunnistamiseen tarvitut käyttäjätunnukset ja salasanat, mutta palvelussa voidaan myös hyödyntää esimerkiksi pankkien tunnistusmenetelmiä, jolloin pankit huolehtivat tunnuksista ja kertakäyttösalasanoista. (von Hintze 2010.)

Tavallinen ihminen pääsee mobiilitunnistukseen käsiksi tavallisimmin puhelinoperaattoreiden tunnistuspalvelun kautta (Tunnistautuminen mobiilivarmenteella 2011), vaikka mobiilitunnistaminen ei olekaan rajattu vain operaattoreiden tarjoamaan tunnistuspalveluun, vaan mobiilitunnistusmenetelmää voidaan käyttää monenlaisissa tilanteissa eri variaatioina (Heinälä

2010). Myös kertakäyttösalasanoihin perustuva tunnistaminen vaatii jonkun palveluntarjoajan toimittamaan salasanalistat käyttäjille. Esimerkiksi pankkitunnuksilla tehty tunnistus on pankkien tarjoama palvelu verkossa tunnistamiseen palveluja tuottaville yrityksille (Tupas-varmennepalvelu 2011). Sekä mobiilitunnistus että kertakäyttösalasanat vaativat siis palveluntarjoajan. Molempiin liittyy kuitenkin omanlaisensa tunnistusmenetelmä käyttäjän tunnistamiseen, joten tarkastelen niiden osalta tunnistuspalvelua tunnistusmenetelmänä.

Samalle tunnistusmenetelmälle voi löytyä useita eri tuotevalmistajia. Eri tunnistuspalveluilla voi usein olla samalle tunnistusmenetelmälle erilainen tuote. Esimerkiksi sormenjälkitunnistimia on ajan mittaan kehitelty monenlaisiin eri käyttötarkoituksiin ja palveluihin, esimerkkinä kannettaviin tietokoneisiin integroidut sormenjälkiskannerit. Tästä johtuen eri sormenjälkitunnistimissa saattaa olla erilainen luotettavuuden taso. Pyrin tarkastelemaan tunnistusmenetelmien luotettavuutta hyvin yleisellä tasolla.

4.2 Vahva tunnistaminen

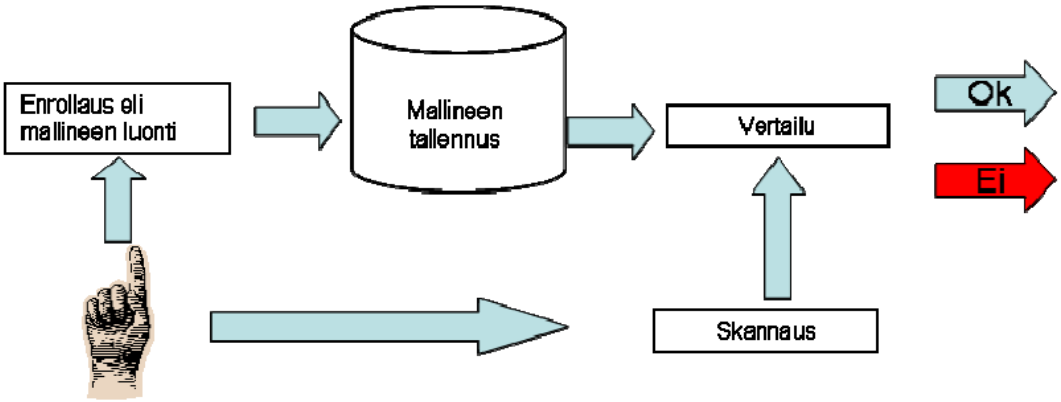
Vahva sähköinen tunnistaminen on Suomen laissa määritelty termi. Lain tarkoituksena on määritellä yhteiset pelisäännöt vahvaa sähköistä tunnistamista tarjoaville organisaatioille. Vahvalla sähköisellä tunnistamisella tarkoitetaan henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista perustuen vähintään kahteen seuraavista todentamistavoista: johonkin käyttäjän yksilöivään ominaisuuteen; johonkin, mitä käyttäjä tietää tai johonkin, mitä käyttäjällä on hallussaan (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617). Pelkkä tunnus ja salasana eivät itsessään ole vahva tunnistustapa, mutta kun käyttäjältä vaaditaan salasanan lisäksi vielä esimerkiksi sormenjälki, on kyseessä vahva tunnistaminen. Tunnistamisprosessin luotettavuutta voidaan aina lisätä yhdistelemällä eri tunnistusmenetelmiä, vaikka tunnistusprosessin nopeus ja käytännöllisyys saattaa kärsiä. (Vahva tunnistaminen 2011.)

4.3 Käyttäjän ominaisuuksiin perustuvat menetelmät

Käyttäjän yksilöiviin henkilökohtaisiin ominaisuuksiin perustuvaa tunnistusta kutsutaan tavallisemmin biometriseksi tunnistukseksi. Biometrinen tunnistus perustuu ihmisen yksilöllisten piirteiden mittaamiseen mahdollisimman tarkasti henkilön identiteetin selvittämiseksi. Biometrisessä tunnistuksessa tunniste kulkee aina käyttäjän mukana, joten hänen ei tarvitse muistaa esimerkiksi pitkiä salasanoja, kantaa mukanaan irrallisia tunnistimia tai pelätä tunnisteen hukkumista. Biometrisen tunnistamisen tekniikka ei enää ole uusi asia: Esimerkiksi sormenjälkeä on voinut käyttää salasanana jo useiden vuosien ajan. Silti biometrisen tunnistuksen läpimurtoa odotetaan vielä. Menetelmien luotettavuuden ja käyttöystävällisyyden ke-

hittymisen myötä biometrinen tunnistus voisi ainakin teoriassa tehdä sähköisestä asioinnista ja esimerkiksi kaupassakäynnistä todella helppoa. (Aukia 2005.)

Todennäköisyyksillä on suuri rooli biometrisessä tunnistamisessa. Jokainen mittaustilanne poikkeaa hieman toisestaan, vaikka mitattavana olisi sama henkilö. Haastavaa onkin asettaa virherajat sellaisiksi, että oikea käyttäjä tunnistetaan aina, mutta väärä ihminen paljastuu mittauksessa. (Aukia 2005.)



Kuva 1: Biometrisen tunnistusjärjestelmän toimintaperiaate (Liikenne ja viestintäministeriö 2005)

Biometrisessä tunnistimessa on se ongelma, että sitä ei voi vaihtaa. Kehittymättömiä biometrisiä tunnistusmenetelmiä voidaan hämätä erilaisilla valeruumiinosilla, valokuvilla tai elokuvista tutulla keinolla irrottamalla alkuperäinen ruumiinosa omistajastaan. Jos joku onnistuu biometrisen tietosi väärentämisessä, et voi enää koskaan luottaa kyseiseen tunnisteeseen. Joitain biometrisiä tunnistusmenetelmiä on myös helppo huijata: puhetta voidaan nauhoittaa, kasvoja kuvataan ja sormenjälkiä jätetään kaikkialle (Heinälä 2010). Toisaalta nykyisissä kehittyneimmissä biometrisissä tunnistusjärjestelmissä biometristä tunnistetta voi olla todella hankalaa tai jopa mahdotonta väärentää tai varastaa. Toisena ongelmana biometrisessä tunnistamisessa on, että monet kokevat biometrisen tiedon todella henkilökohtaiseksi tiedoksi. Jotkin ihmiset saattavat kokea yksityisyytensä loukatuksi, kun heidän ruumiistaan kerätään erilaista tunnistetietoa. Esimerkiksi Facebook otti käyttöön kasvojentunnistusominaisuuden, joka tunnistaa ihmisten kasvot Facebookiin ladatuista kuvista. Tämä koettiin mediassa varsin yksityisyyttä loukkaavaksi. (STT-Reuters 2011.) Biometrisen tunnistuksen helpottuessa myös yksittäisen ihmisen liikkeitä on helpompi valvoa. Siitä huolimatta biometrisen tunnistamisen luotettavuus ja siihen liittyvän teknologian kehittyminen saa tunnistusasiantuntijat uskomaan biometrisen tunnistamisen lisääntymiseen (von Hintze 2011).

Erilaisia biometrisiä tunnistusmenetelmiä löytyy todella monenlaisia ja kehitteillä on koko ajan uusia. Biometrisiä tunnistusmenetelmiä löytyy perustuen esimerkiksi sormenjäljen,

kämmenen, kasvojen, iiriksen, äänen, pituuden ja painon, kävelytyylin sekä silmänliikkeiden mittaukseen (Hyytiä 2010). Rajauskriteereinäni biometrisissä tunnistusmenetelmissä on teoreettinen mahdollisuus käyttää tunnistusmenetelmää verkkopalveluun kirjautumiseen sekä pienelle tai keskisuurelle yritykselle soveltuva hintataso. Suuresta hintaluokasta johtuen rajaan pois esimerkiksi iiristunnistuksen, vaikka sitä pidetäänkin hyvin tarkkana tunnistuskeinona (Aukia 2005). Iiristunnistusta käytetään nykypäivänä lähinnä erittäin korkean turvaluokituksen kohteissa.

4.3.1 Sormenjälki

Tunnetuin ja yleisin biometrinen tunnistusmenetelmä on sormenjälkitunnistus. Sormenjälkitunnistus vaatii sormenjälkilukijan ja tunnistusohjelmiston. Sormenjälki voidaan skannata muun muassa optiikkaan, lämpötilaan tai ultraääniteknologiaan liittyvillä antureilla. Myös tunnistusohjelmien algoritmit voivat toimia eri tavoilla valmistajasta riippuen. Yleensä ne etsivät sormenjälkilukijan tuottamasta kuvasta tyypillisiä sormenjälkeen liittyviä piirteitä ja niiden keskinäistä sijaintia. Rekisteröidessä nämä tiedot tallennetaan käyttäjän mallisormenjäljeksi ja tunnistusvaiheessa rekisteröityä sormenjälkeä verrataan tunnistautuvaan sormenjälkeen. Jos sormenjäljillä on jonkin turvallisuusrajan puitteissa riittävästi yhteisiä piirteitä, niiden katsotaan kuuluvan samalle henkilölle. Skannattu sormenjälkikuva ei koskaan ole täysin yhteensopiva käyttäjän rekisteröityessä luomaan kuvaan, sillä lukutilanteessa sormi "elää" aina jonkin verran. Sormenjälki voi ajan mittaan muuttua esimerkiksi piirteiden kulumisen tai vammautumisen takia. (Liikenne ja viestintäministeriö 2005.) Myös lukijan likaisuus tai vaurioituminen sekä sormen likaisuus tai kuivuus saattavat vaikuttaa skannatun sormenjälkikuvan laatuun ja heikentää sormenjälkitunnistuksen käyttövarmuutta (von Hintze 2010).

Sormenjälkitunnistuksessa yksityisyyden suojan kannalta hyvänä puolena on, että käyttäjä voi halutessaan antaa eri sormen eri järjestelmille. Toisena hyvänä puolena pidetään sitä, että monenlaisia sormenjälkilaitteistoja on valmistettu kaupalliseen tarkoitukseen. Eri laitevalmistajat käyttävät erilaisia algoritmeja, joten myös käytössä olevat sormenjälkimallinteet poikkeavat toisistaan. Näin ollen saman henkilön eri tietokannoissa olevat mallinteet hyvällä todennäköisyydellä poikkeavat toisistaan. (Liikenne ja viestintäministeriö 2005.)

Jotkin sormenjälkiskannerit ovat huijattavissa melko helposti (von Hintze 2010). Viime vuosikymmenellä japanilainen tutkija Tsutomu Matsumoto osoitti, että liivatemakeiseen painetulla sormenjäljellä pystyi hämäämään kaikkia silloisia sormenjälkitunnistimia (Aukia 2005). Vuonna 2010 australialaiset koululaiset taas onnistuivat ohittamaan tuntiläsnäoloa rekisteröivän tietokoneen sormenjälkilukijan nallekarkeilla. Nallekarkkien gelatiinin kapasitanssi on samaa luokkaa kuin ihmisen iholla, joten vaikka sormenjälkilukija oli tarpeeksi edistyksellinen tarkistamaan myös mitattavan materiaalin sähkönjohtavuuden, pystyttiin sitä huijaamaan nalle-

karkkiin painetulla sormenjäljellä. (Jääskeläinen 2010.) Sormenjälkiskannereihin saa hinnan myötä yhä enemmän luotettavuutta lisääviä ominaisuuksia. Jotkut skannerit esimerkiksi mittaavat myös lämpötilaa, jolloin teoriassa skanneria on vaikea huijata "kuolleella" objektilla. Huijausmenetelmät tosin kehittyvät kilvan uuden sormenjälkiteknologian myötä ja olemassa olevan laitekannan jatkuva päivitys niitä vastaan on käytännössä mahdotonta (Liikenne ja viestintäministeriö 2005).

4.3.2 Kämmentunnistus

Kämmentunnistus on sormenjälkitunnistusta hieman nuorempi tunnistusmenetelmä. Kämmen tunnistettiin aluksi skannaamalla koko kämmenen pinta sormenjäljen lailla, mikä teki siitä kuin hieman tarkemmin yksilöivän sormenjälkitunnistuksen. Nykyään kämmentunnistus on kehittynyt entisestään. Pelkän kämmenen pinnan skannaamisen sijaan kämmenestä voidaan skannata koko kämmenen verisuonikartta infrapunan avulla. Verisuonisto on kaikilla yksilöllinen, joten sitä pidetään erittäin tarkkana ja luotettavana tunnistusmenetelmänä. Suonikarttatunniste voi korvata salasanan tai muun pin-koodin esimerkiksi yhteisissä tietojärjestelmissä tai vaikkapa kulunvalvonnassa. (Karkimo 2006.)

Japanissa kämmentunnistinta käyttää jo noin puoli miljoonaa ihmistä, yleisimmin pankkiautomaatilla asioimiseen. Kämmenen verisuoniskanneri on hygieeninen, sillä infrapunalla skannatessa laitteeseen ei tarvitse periaatteessa koskea. Verisuoniston rakennetta ei voi väärentää, minkä lisäksi kämmenskanneri on erittäin tarkka tunnistin. Kämmentunnistus ei ole Suomessa vielä suuren yleisön käytössä, mutta työn alla ovat erilaiset tunnistamiseen ja tietoturvaan liittyvät komponentit, kuten kirjautuminen työasemaan ja web-sovelluksiin, älykorttipohjaiset turvatoiminnot sekä fyysisen sisäänpääsyn valvonta. (Karkimo 2006.) Fujitsun tietoturva- ja tunnistusasiantuntija Petri Heinälä uskoo, että verisuoniteknologia tulee laajentuvan tulevaisuudessa ja sille tullaan kehittämään eri käyttötarkoituksia.

4.4 Käyttäjän omaisuuteen perustuvat menetelmät

Käyttäjän omaisuuteen perustuvilla menetelmillä tarkoitetaan tunnistusmenetelmiä, jotka vaativat tunnistamiseen jonkin erillisen mukana kulkevan objektin tai tietovälineen. Varmenteena käytettävään objektiin liittyy aina varastamisen uhka, mistä syystä tämä tunnistusmenetelmä monesti yhdistetään esimerkiksi salasanaan.

4.4.1 Varmennekortti

Varmennekortilla tarkoitetaan sirullista korttia, jossa on Väestörekisterikeskuksen kansalaisvarmenne. Kansalaisvarmenne on sähköinen henkilöllisyys, joka sisältää mm. etunimen, suku-

nimen ja sähköisen asiointitunnuksen. Tällä hetkellä kansalaisvarmenne on käytössä poliisin myöntämällä sirullisella henkilökortilla. (Tunnistautuminen varmennekortilla 2010.) Varmennekortin käyttäminen tunnistautumisessa vaatii kortin lisäksi ulkoisen kortinlukijalaitteen ohjelmistoineen. Varmennekortti onkin osoittautunut erittäin epäsuosituksi tunnistuskeinoksi kaikkien sen vaatimien elementtien hankkimisen hankaluuden vuoksi (STT 2010). Varmennekortista kaavailtiin alkuperäisten suunnitelmien mukaan yleisesti käytössä olevaa vahvan tunnistamisen vaihtoehtoa esimerkiksi pankkitunnuksille, mutta palveluntarjoajat eivät ryhtyneet käyttämään sitä.

4.4.2 Mobiilitunnistus

Mobiilitunnistautuminen on tunnistautumista puhelimen sim-korttia apuna käyttäen. Mobiilivarmenteen käyttäminen vaatii mobiilitunnistuspalvelun käyttöönottamisen puhelinoperaattorilta. Mobiilivarmenne on matkapuhelimen sim-korttiin liitettävä palvelu, joka toimii sähköisenä henkilöllisyystodistuksena (Kännykkä käy allekirjoittamiseen 2010). Mobiilitunnistusta voidaan käyttää Suomessakin käyttäjän henkilöllisyyden selvittämiseen erilaisiin sähköisiin asiointipalveluihin kirjauduttaessa tai sähköisiä allekirjoituksia tehtäessä. Mobiilitunnistus vaatii siihen tarkoitetun sim-kortin ja kuukausittaisen palvelumaksun maksamisen. Mobiilitunnistuspalveluun kuuluu myös 4-8 merkkiä pitkä tunnusluku, minkä johdosta palvelu täyttää vahvalle sähköiselle tunnistamiselle laissa asetetut vaatimukset. (Tunnistautuminen mobiilivarmenteella 2011.)

Tunnistautumisprosessi alkaa käyttäjän ilmoittaessa puhelinnumeronsa asiointipalvelulle. Palvelu lähettää puhelimeen tiedon kirjautumisyrityksestä, johon käyttäjä vastaa henkilökohtaisella tunnusluvullaan. Tunnusluku ei lähde viestinä sim-kortilta mihinkään, vaikka se siltä saattaakin vaikuttaa. Viesti antaa sim-kortille erillisen varmistuksen käyttäjästä, johon simkortti reagoi lähettämällä varmistuksen asiointipalveluun. Näin asiointipalvelu varmistuu käyttäjän henkilöllisyydestä ja asiointipalvelu aukeaa käyttäjälle. (Tunnistautuminen mobiilivarmenteella 2011.) Tunnistautuminen tapahtuu salattuna ja erillään varsinaisesta asiointipalvelusta. Palveluja käytetään internetin kautta, tunnistaminen taas tehdään matkapuhelinverkossa (STT 2010). Mobiilitunnistus on vahva tunnistusmenetelmä, sillä se perustuu omistuksessa olevan sim-kortin lisäksi käyttäjän tietämään salasanaan.

Tyypillisiä mobiilivarmennuksen käyttömuotoja ovat verkkopankkipalvelut, verkkokaupat ja rahapelit sekä monet yhteiskunnan palvelut, kuten verotukseen, terveydenhoitoon ja eläke- ja sosiaalipalveluihin liittyvät palvelut. Tunnistautuminen tukee myös verkon yhteisöpalveluita ja kuluttajien välistä kaupankäyntiä verkossa. (Kännykkä käy allekirjoittamiseen 2010.) Esimerkiksi pankkitunnuksiin verrattuna mobiilitunnistuksen etuna on se, että erillisiä tunnuslukulistoja ei tarvitse kantaa mukana. Turvalliseksi järjestelmän tekee se, että siinä käyte-

tään samanaikaisesti turvallista tekstiviestiä ja internetiä. Järjestelmän kehittäjät vakuuttavat, että kahteen järjestelmään murtautuminen yhtä aikaa ei ole mahdollista (Vartia 2009).

Mobiilivarmennetta hyödyntävät myös muut palveluntarjoajat kuin puhelinoperaattorit. Mobiilivarmenteeseen liittyvällä tunnistusteknologialla voi nimittäin henkilöllisyyden tunnistamisen lisäksi myös kohta korvata maksukortin. Tunnistautuminen ja maksaminen hoidetaan vastaamalla viestiin. Kuluttaja voi liittää palveluluun minkä tahansa maksukorttinsa. Kaikille tapahtumille luodaan omat sormenjäljet, joita ei voi väärentää. (Storås 2010.) Mobiilivarmenteiden käyttö ei ole Suomessa vielä kovinkaan yleistä. Mobiilitunnistuksesta puuttuvat vielä yhtenäiset toimintamallit, sillä eri palveluntarjoaja soveltavat sitä hieman eri tavoilla. Mobiilitunnistautumisia ei myöskään ole verifioitu, niin kuin esimerkiksi Visa-korttia (von Hintze 2010). Verifiointipalvelun kautta voidaan varmistua maksutapahtuman luotettavuudesta, eli verkkokaupan ja laskutettavan summan oikeellisuudesta sekä siitä, että vain oikea käyttäjä voi tehdä ostoksia (Verified by Visa 2010).

4.5 Käyttäjän tietoon perustuvat menetelmät

Käyttäjän tietoon perustuvat tunnistusmenetelmät perustuvat siihen, että tunnistettava käyttäjä on ainoa, joka tietää tunnistukseen vaaditun tiedon, esimerkiksi käyttäjätunnuksen ja salasanan. Käyttäjän tietoon perustuvat tunnistusmenetelmät on opinnäytetyössäni rajattu käyttäjätunnukseen ja salasanaan sekä pankkitunnuksiin. Pankkitunnukset perustuvat myös johonkin, mitä käyttäjä omistaa, sillä pankkitunnusten käyttäminen vaatii pankkitunnukset sisältävän kortin, joka uusiutuu säännöllisin väliajoin.

4.5.1 Käyttäjätunnus ja salasana

Käyttäjätunnus ja salasana on yleisin tavallisen ihmisen käyttämä tunnistusmenetelmä. Vaikka tunnistusmenetelmä onkin nopea ja helppo, on se myös yksi haavoittuvimmista ja epäluotettavimmista tunnistusmenetelmistä. Salasanan luotettavuutta voidaan lisätä satunnaistamalla sitä, lisäämällä siihen isoja kirjaimia ja numeroita tai pidentämällä sitä (Salasanaohjeet 2008). Vahvakin salasana on kuitenkin melko helppoa ohittaa. Salasanan paljastumiseen ei vaadita kuin yksi vakoiluohjelma tietokoneella. Salasanojen ohittamiseen on myös netissä tarjolla ohjelmia, jotka ovat todella helppokäyttöisiä aloittelevallekin hakkerille. Monet kirjoittavat salasanan ylös ja säilövät sen esimerkiksi tietokoneelleen, missä tapauksessa on mahdotonta tietää, kuka sen on saattanut löytää. Aina salasanan turvallisuus ei ole edes pelkästä käyttäjästä kiinni, vaikka haittaohjelmia ei käyttäjän päässä olisikaan. Ei nimittäin ole varmaa, että kohdepäässä salasanamenettelyt ovat kunnossa (von Hintze 2010). Esimerkiksi Suomi24-sivustolle tehtiin vuonna 2010 tietomurto, jonka seurauksena käyttäjätunnuksia ja salasanoja joutui rikollisten käsiin (Lehto 2010). Käyttäjällä ei juuri ole mitään lain takaamaa suo-

jaa siinä tapauksessa, että palvelun tarjoaja vuotaa käyttäjän tietoja, jos kyse ei ole henkilötiedoista. Pelkän salasanan taakse siis harvoin kannattaa laittaa mitään tärkeää tietoa. Aina kun ollaan tekemisissä rahan kanssa tai tehdään toimituksia, jotka vaatisivat henkilöllisyystodistusta, ei kannata luottaa pelkkään salasanatunnistamiseen (von Hintze 2010).

4.5.2 Pankkitunnukset (kertakäyttösalasana)

Suomessa yleisin vahva tunnistamismenetelmä on pankkitunnistuksilla tehty tunnistus, josta käytetään myös nimeä TUPAS-tunnistus (Tupas-varmennepalvelu 2011). Se perustuu pankin antamaan tunnukseen ja kertakäyttöiseen salasanaan, jonka pankki on edeltä käsin jakanut käyttäjille. Tupas-tunnistuspalvelun avulla sähköisiä asiointipalveluita tarjoavan yrityksen tai yhteisön asiakas voi tunnistautua palvelussa käyttäen pankkitunnuksiaan. Pankkitunnuksilla tunnistautuminen täyttää turvallisen tunnistustapahtuman kriteerit (Tupas-tunnistuspalvelun tunnistusperiaatteet 2011). Suomen verkkopankkitunnus-järjestelmä luotiin noin 25 vuotta sitten väliaikaiseksi tunnistautumismenetelmäksi verkkopankkiin kirjautumiseen. Se on sittemmin toiminut erittäin hyvin, minkä takia väliaikainen ei ole enää hyvä termi kuvaamaan sitä. Vuosittain verkkopankkeihin kirjaudutaan noin 340 miljoonaa kertaa. (Vartia 2009.)

Tupas-palvelun osapuolten välisessä tietoliikenteessä käytetään suojattua SSL-siirtokäytäntöä, joten ulkopuoliset eivät näe tietoja eivätkä voi muuttaa niitä. Tunnistuspyynnön ja tunnisteen tiedot on suojattu tiedon eheyden turvaavalla tarkisteella, joten asiakkaalla ei ole mahdollisuutta muuttaa tietoja palveluntarjoajan tai pankin sitä havaitsematta. Sekä Tupas-palvelun tarjoava pankki että Tupas-palvelua käyttävä yritys vastaavat omien palveluidensa suojauksesta, turvallisuudesta ja säilyttämiensä tietojen oikeellisuudesta. Tunnistautuva asiakas vastaa puolestaan siitä, että pankin antamat pankkitunnukset eivät joudu ulkopuolisten haltuun. (Pankkien TUPAS-tunnistuspalvelu palveluntarjoajille 2011.) Tupas-palvelun järjestelmän turvaominaisuudet takaavat pääsynvalvonnan ja jäljitettävyyden jokaisen pankkitunnuksiin liittyvän toimenpiteen ja tehtävän osalta (Tupas-tunnistuspalvelun tunnistusperiaatteet 2011).

Noin 99 prosenttia vahvan sähköisen tunnistamisen tapahtumista tehdään Suomessa pankkitunnisteilla, loput Väestörekisterikeskuksen kansalaisvarmenteella. Ongelmana pankkitunnuksissa lieneekin niiden monopoli vahvana sähköisenä tunnistimena. Hintakilpailun puutteen vuoksi ei uuden innovointiin ole tarpeeksi pakotetta. (STT 2010.)

Fujitsun tunnistusasiantuntijan Jan von Hintzen mukaan salasanat kiertävät todellisuudessa noin parin miljoonan salasanan "kehää", mistä syystä pankkitunnusten seuraavat luvut ovat teoriassa laskettavissa. Käytännössä pankkitunnukset ovat kuitenkin melko idioottivarma tunnistusmenetelmä, jos käyttäjä pitää tunnuksensa turvassa. Myös pankkitunnuksia voitaisiin kalastella esimerkiksi huijaussivustolla, joka esittäisi olevansa pankin oma sivusto, vaikka to-

dellisuudessa on jotain ihan muuta. Tunnistuspalvelun luotettavuudesta voidaan varmistua tarkistamalla verkkosivun sertifikaatin. (von Hintze 2010.)

5 Tunnistusmenetelmien luotettavuus

Tunnistusmenetelmän luotettavuutta tarkastellaan tässä työssä identiteettivarkauden näkökulmasta eli määrittelen tunnistusmenetelmien luotettavuuden sen mukaan, miten suuri vastustuskyky niillä on identiteettivarkauksia vastaan. Tarkastelen menetelmien luotettavuutta melko yleisellä tasolla, menemättä teknisiin yksityiskohtiin.

Tunnistusmenetelmän luotettavuutta mitattaessa on ensin otettava selvää, mitkä asiat siihen vaikuttavat. Tunnistusmenetelmän luotettavuus harvoin on kovinkaan yksiselitteinen asia. Haastattelemani tunnistuspalvelujen parissa työskentelevät Fujitsun asiantuntijat ovat yhtä mieltä siitä, että tunnistusmenetelmän luotettavuuteen vaikuttaa enemmän itse tunnistusmenetelmä kuin sen käyttäjä (Heinälä 2010). Esimerkiksi salasanatunnistuksessa käyttäjällä on kuitenkin suuri vastuu salasanansa salassapidon kannalta. Jokin menetelmä voi olla luotettava vain, jos käyttäjä itse on valistunut ja huolellinen. Tunnistusmenetelmän luotettavuutta mitattaessa otan huomioon sen, missä suhteessa käyttäjän oma tietoisuus ja toiminta vaikuttavat identiteettivarkauden alttiuteen. Luotettavuus yleensä paranee käyttäjän roolin kutistuessa, esimerkiksi jos käyttäjän ei tarvitse muistaa tai kirjoitella ylös suuria määriä salasanoja. Erittäin epäluotettavaksi järjestelmän tekee, jos käyttäjä esimerkiksi unohtaa salasanansa eikä pääsekään omaan järjestelmäänsä sisälle. Koska kuitenkin tarkastelen luotettavuutta identiteettivarkauden näkökulmasta, jätän oikean käyttäjän väärän tunnistamisen tarkastelematta. Tällä tarkoitan tunnistustapahtumaa, jossa oikeaa käyttäjää ei tunnisteta oikein, eikä hän siksi pääse tunnistusmenetelmän läpi.

Fujitsun tuotekehityspäällikön Petri Heinälän mukaan tunnistusmenetelmän vahvuuteen vaikuttavat käyttäjän näkökulmasta paljolti tunnistusmenetelmän ympärillä olevat prosessit, käytännöt ja politiikat. Tunnistusmenetelmä saattaa teknisesti toimia, mutta sen ympärillä olevat asiat saattavat olla huonosti hoidettuja. Esimerkiksi rekisteröityminen on tärkeä prosessi luotettavan tunnistautumisen kannalta. (Heinälä 2010.)

Identiteettivarkausriski on riskin tapahtumisen todennäköisyys kerrottuna riskin aiheuttamilla vahingoilla. Vahinkojen suuruus riippuu tässä tapauksessa paljolti siitä, mitä järjestelmiä tai tietoja tunnistusmenetelmä suojelee. Oletusarvoisesti tarkastelussani kaikkien tunnistusmenetelmien takana on samanarvoinen kohde tai järjestelmä.

Mittaan luotettavuutta menetelmien luotettavuutta lisäävien tai heikentävien ominaisuuksien mukaan. Tarkastelemiani ominaisuuksia ovat tunnistetietojen katoamis- tai varastamismah-

dollisuus, tunnistetietojen väärennettävyys tai ohitettavuus, identiteettivarkauden huomaamattomuus sekä tunnisteen mitätöimisen vaikeus. Mittarini on jaettu ominaisuuksiin, jotka vaikuttavat kykyyn ennaltaehkäistä identiteettivarkautta, sekä ominaisuuksiin, jotka vaikuttavat kykyyn vastata identiteettivarkauteen sen sattuessa.

5.1 Kyky ennaltaehkäistä identiteettivarkaus

Tunnistusmenetelmän kyky ennaltaehkäistä identiteettivarkaus riippuu paljolti siitä, kuinka hyvin tunnistetiedot ovat suojassa. Ainoa keino, millä identiteettivaras voi päästä tunnistusmenetelmästä läpi ilman tunnistetietoja, on kokeilemalla.

5.1.1 Tunnistetietojen katoamis- tai varastamismahdollisuus

Tunnistetiedot voidaan varastaa kaikkialta, missä niitä säilytetään. Usein käyttäjä on tässäkin heikoin lenkki, mutta myös esimerkiksi tunnistetietoja säilyttäviin palvelimiin on onnistuttu murtautumaan. Sen lisäksi, että voidaanko tunnistetietoja varastaa, on olennaista kysyä onko niistä varastettaessa varkaalle mitään hyötyä. Esimerkiksi kämmentunnistuksessa tunnistetieto on vain pala koodia, millä ei ilman kättä pysty huijaamaan kämmenen lukemiseen suunniteltua skanneria.

5.1.2 Tunnistetietojen väärennettävyys/ohitettavuus

Niin kuin tutkimusmateriaaleistani kävi ilmi, myös sormenjälkitunnisteita on mahdollista väärentää tai tunnistimia huijata. Varmennekortteja voidaan kopioida erilaisilla laitteilla, mikäli niihin ei ole esimerkiksi liitetty biometristä tietoa. Fujitsun kehityspäällikön Jan von Hintzen mukaan mobiilivarmenteen voi teoriassa väärentää, mutta se voi olla erittäin vaikeaa jos ei suorastaan mahdotonta. Jos Sim-kortilla on sertifikaatti, niin väärentäminen on mahdotonta (von Hintze 2010).

Tunnistetietojen ohittamisella viittaan tunnistusmenetelmän läpäisemiseen ilman varastettua tietoa varsinaisesta varmenteesta. Tämä skenaario on yleisin pelkkään salasanatunnistukseen perustuvissa menetelmissä. Tehokkaan koneen avulla on mahdollista ohittaa heikot salasanat kokeilemalla kaikkia mahdollisia vaihtoehtoja.

5.2 Kyky vastata identiteettivarkauteen

Kyvyllä vastata identiteettivarkauteen tarkoitan tunnistusmenetelmään liittyviä toimenpiteitä, joita voidaan suorittaa vahinkojen minimoimiseksi identiteettivarkauden sattuessa.

5.2.1 Identiteettivarkauden huomaamattomuus

Identiteettivarkauden sattuessa on hyvin mahdollista, että kohteeksi joutunut ei edes tiedä hänen henkilökohtaisten tietojensa joutuneen vääriin käsiin. Esimerkiksi tietomurrot ja sähköpostilla tai vakoiluohjelmilla suoritetut kalastelut ovat yleensä erittäin hyvin naamioitu juuri siksi, että uhri ei tiedä hänen tietojensa vaarantuneen. Näin varas voi rauhassa käyttää uhrin tietoja hyödykseen ilman, että uhri vaihtaa tietojaan tai ilmoittaa kenellekään. Joskus tunnistetietojen häviäminen voidaan huomata. Esimerkiksi kiinteän varmennekortin häviämisen huomaa melko nopeasti, kun korttia ei enää tarvittaessa näy missään.

5.2.2 Tunnisteen mitätöiminen

Identiteettivarkauden sattuessa on tärkeää pystyä mitätöimään vaarantunut tunniste, jottei identiteettivaras pysty enää käyttämään sitä hyödykseen. Jos tunnistamiseen liittyy jokin tunnistuspalvelu, on sulkupalvelun kautta yleensä melko vaivatonta mitätöidä vaarantuneet tunnisteet. Mutta esimerkiksi jos identiteettivaras kaappaa käyttäjätilin sivustolta, joka ei kerää käyttäjistä mitään henkilöä tunnistavaa tietoa, ja vaihtaa uhrin salasanan, on melko mahdotonta todistaa kenellekään olleensa tilin alkuperäinen luoja. Myös biologisten tunnisteiden osalta on hyvä miettiä, voiko tunniste joutua pysyvästi vääriin käsiin. Pysyvästi vääriin käsiin joutumisella tarkoitan tilannetta, jossa varas voi pysyvästi tai pitkäaikaisesti hyväksikäyttää uhrin tunnistetietoja niiden muuttumattomuuden takia. Ihmisen biologiset ominaisuudet ovat yleensä melko pysyviä.

5.3 Menetelmien heikkoudet ja vahvuudet

Tunnistusmenetelmiä vertaillessa on huomioitava käyttötarve. Esimerkiksi yksin kulunvalvontaan tarkoitettua menetelmää on turhaa verrata verkkopalveluun kirjautumiseen käytettävään menetelmään. Tarkastelen työssäni tunnistusmenetelmiä, joita on mahdollista käyttää verkkopalveluun kirjautumiseen.

Alla olevassa taulukossa on esitetty yhteenveto eri menetelmien heikkouksista ja vahvuuksista, jotka myös toimivat perusteluina tunnistusmenetelmien riskikartoituksen tuloksille. Taulukkoon on listattu vain luotettavuuden kannalta olennaiset heikkoudet ja vahvuudet.

	Vahvuudet	Heikkoudet
Sormenjälki	+ melko tarkka tunnistamaan oikean henkilön sormen + kulkee aina mukana + eri tunnistamistilanteissa voidaan käyttää eri sormia, mikä lisää luotettavuutta	- sormenjälki on mahdollista väärentää tai ohittaa - jätämme sormenjälkemme kaikkeen, mihin koskemme - sormenjälkeä ei pystytä vaihtamaan
Kämmentunnistus	+ todella tarkka tunnistamaan oikean henkilön + käytännössä väärentämätön	- kämmenen verisuonikarttaa ei pystytä vaihtamaan
Varmennekortti	+ helppo mitätöidä + ei vaadi henkilökohtaista tietoa	- mahdollista varastaa tai väärentää tarkoitukseen sopivilla laitteilla
Mobiilitunistus	+ todella vaikeaa väärentää + ei häviä huomaamatta + helppo mitätöidä	- riippuvainen sim-kortista
Tunnus & salasana	+ ei vaadi henkilökohtaista tietoa	- suhteellisen helppo selvittää tai murtaa - luotettavuus riippuu paljolti käyttäjästä itsestään - joutuu helposti huomaamatta vääriin käsiin
Pankkitunnukset	+ erittäin vaikea ohittaa ilman tunnuskortin tietoja + helppo mitätöidä + ei vaadi henkilökohtaista tietoa	- voidaan varastaa tai kopioida huomaamatta

Taulukko 1: Menetelmien heikkoudet ja vahvuudet

5.4 Tunnistusmenetelmien riskikartoitus

Seuraava taulukko hahmottaa eri tunnistusmenetelmien luotettavuutta lisääviä ominaisuuksia identiteettivarkauteen liittyen. Riskin suuruus on mitattu asteikolla yhdestä kolmeen. Näin yleisellä tasolla tehdyssä tutkimuksessa suurempi asteikko saattaisi johtaa epätarkkoihin tai perustelemattomiin tuloksiin. Taulukon kautta on helpompi hahmottaa eri tunnistusmenetelmien suhdetta toisiinsa.

	Sormenjälki	Kämmentunnistus	Varmennekortti	Mobiilitunnistus	Tunnus ja salasana	Pankkitunnukset
Tunnistetietojen katoamismahdollisuus/ varastamismahdollisuus	1	1	2	2	2	2
Tunnistetietojen väärennettävyys/ ohitettavuus	2	1	2	1	3	1
Varkauden huomaamattomuus	2	1	2	1	3	2
Mitätöinnin vaikeus	3	3	1	1	2	1

Taulukko 2: Tunnistusmenetelmien riskikartoitus identiteettivarkauden näkökulmasta

Riski	
Olematon/pieni	1
Keskisuuri	2
Suuri	3

5.5 Tulosten arviointi

Tuloksista voidaan havaita eri tunnistustyyppiin perustuvien tunnistusmenetelmien heikkoudet ja vahvuudet. Biometriset tunnistusmenetelmät ovat luotettavia tunnistamaan oikean henkilön, mutta ovat silti vielä hieman arveluttavia siitä syystä, että niihin on luovutettava omaan kehoon liittyvää muuttumatonta tietoa. Ulkoiseen esineeseen perustuvat tunnistusmenetelmät ovat yleisesti melko luotettavia, vaikka tunniste voi hukkua tai se voidaan varastaa. Salasanaan tai salasanoihin perustuvien tunnistusmenetelmien luotettavuus taas on todella riippuvainen käyttäjän omasta huolellisuudesta.

Jos menetelmien luotettavuutta tarkastellaan raa'asti sen mukaan, miten pieni niiden yhteenlaskettu kokonaisriski on, niin luotettavimmat menetelmät ovat mobiilitunnistus, pankkitunnukset sekä kämmentunnistus. Jos käyttäjän olisi valittava mahdollisimman luotettava tunnistusmenetelmä suojaamaan hänen identiteettiään, olisi hänen taulukon mukaan kannattavaa valita yksi näistä kolmesta. Sekä mobiilitunnistus että pankkitunnukset ovat luokiteltu vahvoiksi tunnistusmenetelmiksi, mikä selittää niiden suhteellista riskittömyyttä.

Vertailun tarkoituksena ei kuitenkaan ollut määrittää, mikä menetelmistä on yksiselitteisesti luotettavin, vaan hahmottaa eri menetelmien eroavaisuuksia ja suhdetta toisiinsa. Eri menetelmät tarjoavat erilaista luotettavuutta ja myös esimerkiksi menetelmän hinta sekä soveltuvuus kohteeseen ovat hyvin tärkeitä tekijöitä. Jotkin tilanteet vaativat kovat turvaluokan tunnistusta, kun taas jollekin epäolennaiselle foorumille kirjautumiseen ei ole mitään järkeä käyttää muuta kuin salasanaa. Tunnuksen ja salasanan ei välttämättä tarvitse sisältää mitään henkilöivää tietoa, mikä tekee siitä luotettavan menetelmän silloin, kun palvelu ei vaadi henkilötietojen tai rahan käsittelemistä. Toisin sanoen parhaita kenkiä ei tarvita roskien viemiseen.

6 Yhteenveto ja johtopäätökset

Modernin informaatioyhteiskunnan siirtyessä yhä enemmän kohti sähköisen tiedonsiirron ja sosiaalisen median maailmaa, sähköisen identiteetin merkitys kasvaa. Rahansiirrot ja ostoksetkin ovat jo suurilta osin sähköisiä toimenpiteitä. Siinä missä ennen oltiin huolissaan kiinteästä omaisuudesta, ollaan nykyään yhä enemmän huolissaan sähköisen identiteetin turvallisuudesta. Asiattoman henkilön kirjautuminen omalle käyttäjätilille tuntuisi melkein yhtä ikävältä kuin oman asunnon ryöstäminenkin. Siksi on olennaista tarkastella sähköisen suojamuurimme pitävyyttä. Onnistuneeseen identiteettivarkauteen liittyy aina jonkin tunnistamismenetelmän puuttuminen tai pettäminen. Jopa tapauksissa, joissa identiteettivaras luo uhrin nimiin profiilin satunnaiselle verkkosivulle, on kyseessä verkkosivun rekisteröitymisvaiheessa tehtävän tunnistuksen pettäminen. Tunnistamiselle olisi käyttöä paikoissa, joissa emme edes tiedä sitä kaivattavan.

Sain kuulla opinnäytetyötäni tehdessäni pariin otteeseen, että tunnistusmenetelmiä ei oikein voi verrata keskenään, sillä ne ovat niin erilaisia eri tilanteisiin soveltuen. Olikin mielenkiintoista havaita, miten tarkastelemillani tunnistusmenetelmätyypeillä on omanlaistansa luotettavuutta. Vaikka tunnistusmenetelmien luotettavuuden tarve on kasvussa identiteettivarkauksien lisääntymisen myötä, en usko, että yksikään tunnistusmenetelmä tulee nousemaan ylitse muiden kaikkialla, missä tunnistusta tarvitaan. Tunnistusmenetelmien valinnanvara on enemmänkin rikkaus, josta pitää vain osata ottaa mahdollisimman suuri hyöty irti.

6.1 Oma arviointi

Omaa työskentelyäni arvioiden sanoisin, että opinnäytetyöni olisi kaivannut hieman enemmän omistautumista. Suurimpana ongelmana opinnäytetyössäni oli suunnitelman mukaisessa aikataulussa pysyminen. Aikaa tutkimuksen tekemiseen olisi voinut uhrata rajattomasti, mutta ajankäytön tehottomuudesta johtuen aika loppui lopulta kesken. Haastattelujen kannalta oli olennaista tietää, minkälaista tietoa haastateltavilta tarvittiin. Siksi oli vaikea arvioida, minkälaista asiantuntemusta omaavia asiantuntijoita olisi työn kannalta ollut tarpeen haastatella, ennen kuin raportti oli melkein jo valmis. Myös työn rakenteen ja sisällön suunnitteleminen oli haastavaa, sillä tunnistusmenetelmien luotettavuuden selvittäminen ei ole kovin yksiselitteinen tai yksinkertainen prosessi.

Yksi opinnäytetyöni tavoitteista oli avartaa omaa sekä lukijan käsitystä tunnistusmenetelmistä ja identiteettivarkauksista. Tutkimusprosessi oli haastava, sillä aihealue oli vielä itselleni suhteellisen uusi. Aiheeseen oli todella mielenkiintoista perehtyä, mutta jouduin monesti tarkastelemaan tekemääni työtä kriittisesti ja muuttamaan näkökulmaani uuden tiedon myötä. Olen kuitenkin tyytyväinen sekä opinnäytetyöni valmistumiseen että lopputulokseen.

Tunnistusteknologia ja eri menetelmät muuttuvat ja kehittyvät niin nopeaa tahtia, että aiheesta voisi mielestäni tehdä runsaasti jatkotutkimusta. Esimerkiksi jo pelkästään erilaisia sormenjälkiteknologioita löytyy niin monia, että niitä voisi tarkastella ja vertailla syvällisemmin. Myös tunnistuspalveluita ja niihin liittyviä eri elementtejä, kuten asiakaslähtöisyyttä tai tunnistuspalvelun valintaperusteita voisi tarkastella lähemmin.

6.2 Toimeksiantajan arviointi

Opinnäytetyön toimeksiantaja Fujitsu Services Oy oli tyytyväinen siihen, että opinnäytetyö korostaa identiteetinhallinnan merkitystä koko yhteiskunnan kannalta. Sähköiset palvelut ovat nykyisin elintärkeä osa yhteiskunnan toimintaa ja Fujitsunkin asiakaskunnassa niiden tärkeys tunnustetaan poikkeuksetta. Identiteetin väärinkäyttö pääsee median otsikoihin hyvin näkyvästi, eikä alalla toimivien yritysten kannata IT-palveluita toimittaessaan juurikaan ottaa tarpeettomia riskejä. Tähän vaikutetaan tehokkailla tunnistamismenetelmillä ja jatkuvalla tuotekehittelyllä. Kilpajuoksu yhä parempien tunnistamismenetelmien kehittäjien ja vastaavasti laittomien keinojen hyödyntäjien välillä on jatkuva, kuten raportissa on tuotu esille. Tehtävästä suoriuduttiin kokonaisuudessaan mallikkaasti.

Lähteet

Aukia, J. 2005. Biometrinen tunnistus, Tietokone 5/2005, sivu 18.

Axelrod, W. 2007. Information Systems Control –lehti, Volume 2, Identity and Access Management. Sivut 56-57.

Britz, M. 2009. Computer Forensics and Cybercrime. Second Edition. New Jersey: Pearson Education.

Cilli, C. 2005. Information Systems Control –lehti, Volume 6, Identity Theft: A New Frontier for Hackers and Cybercrime. Sivut 39-42.

Elisa sanasto 2011. IT-alan sanasto. Viitattu 14.10.2011.
http://sanasto.elisa.fi/showWord.cfm?id=1194&languageId=1

Heinonen, R. 2001. Digitaalinen minä. Helsinki: Edita Oyj.

Hirsijärvi, S., Remes, P. & Sajavaara, P. 2004. Tutki ja kirjoita. 10., osin uudistettu laitos. Helsinki: Tammi.

Hyytiä, T. 2010. Sormenjälki on historiaa, nyt tunnistetaan silmänliikkeitä. Tietoviikko. Viitattu 17.10.2011.
http://www.mikropc.net/kaikki_uutiset/sormenjalki+on+historiaa+nyt+tunnistetaan+silmanliikkeita/a531927

Härkönen, R. 2009. ID-varkaus halutaan kriminalisoida. Turun Sanomat. Viitattu 26.1.2011

Identiteetin hallinta lisää tietoturvaa 2011. Viitattu 11.10.2011.
http://direxon.fi/index.php?id=36

Jääskeläinen, O. 2010. Koululaiset huijasivat sormenjälkilukijoita nallekarkeilla. MikroPC. Viitattu 17.10.2011.
http://www.mikropc.net/kaikki_uutiset/koululaiset+huijasivat+sormenjalkilukijoita+nallekarkeilla/a525889

Karkimo, A. 2006. Kämmentunnistus skannaa verisuonet. Viitattu 24.8.2011.
http://www.tietokone.fi/uutiset/2006/kammentunnistus_skannaa_verisuonet

Korhonen S. 2011a. Identiteettivarkaudet yleistyvät Suomessa. Viitattu 9.2.2011.
http://www.tietoviikko.fi/kaikki_uutiset/article568392.ece?s=u&wtm=tt-26012011

Korhonen, S. 2011b. Identiteettivarkaudet uhkaavat yhä useampia. Tietoviikko. Viitattu 26.1.2011

Kännykkä käy allekirjoittamiseen 2010. Markkinointi ja mainonta. Viitattu 26.1.2011.
http://www.marmai.fi/uutiset/article540500.ece

Laki vahvaasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617,

Lappalainen, E. 2011. Identiteettivarkauden uhri on suojaton. Helsingin Sanomat 27.1.2011.

Lehto, T. 2010 Tietomurto Suomi24-sivustolle. Tietokone. Viitattu 17.10.2011.
http://www.tietokone.fi/uutiset/tietomurto_suomi24_sivustolle_vaihda_heti_salasanasi

Lehto T. 2011 Identiteettivarkauksia epäillään Suomessa jo päivittäin. Viitattu 16.8.2011.
http://www.tietokone.fi/uutiset/netissa_saa_riehua_toisen_nimissa_muutosta_luvataan_lakiin

Liikenne ja viestintäministeriö 2005. Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja. Viitattu 17.10.2011.
http://www.lvm.fi/fileserver/80_2005.pdf

Olatilu, O. 2006 Information Systems Control -lehti, Volume 6, Identity Theft and Corporations' Due Diligence. Sivut 27-28

Pankkien TUPAS-tunnistuspalvelu palveluntarjoajille 2011. Finanssialan keskusliiton sivut. Viitattu 18.10.2011.
http://www.fkl.fi/teemasivut/sahkoinen_asiointi/Dokumentit/Tupas-varmennepalvelu_v23c.pdf

Virtuaalinen lähipoliisiryhmä 2011. Nettirikosten pohdintaa. Viitattu 14.10.2011.
http://www.poliisi.fi/poliisi/helsinki/home.nsf/files/Nettirikosten%20pohdintaa/$file/Nettirikosten%20pohdintaa.pdf

Rikoslaki 24.7.1998/563.

Rikoslaki 24.8.1990/769.

Salasanaohjeet 2008. Sangen osuuskunnan kotisivut. Viitattu 17.10.
http://www.sange.fi/help-password

Tupas-varmennepalvelu 2011. Finanssialan keskusliiton sivut. Viitattu 17.10.2011.
http://www.fkl.fi/teemasivut/sahkoinen_asiointi/tupas/Sivut/default.aspx

Turunen J. 2010 Identiteettivarkaus on hankala asia poliisille. Viitattu 9.2.2011.
http://www.tietoviikko.fi/kaikki_uutiset/article506039.ece?s=l&wtm=tietoviikko/-24092010

Turunen J. 2010 Tietoviikko, Identiteettivarkaus on hankala asia poliisille. Viitattu 26.1.2011
http://www.tietoviikko.fi/kaikki_uutiset/article506039.ece

Storås, N. 2010 Tekstiviesti käy kohta pankkikortista, Tietoviikko. Viitattu 26.1.2011
http://www.tietoviikko.fi/kaikki_uutiset/tekstiviesti+kay+kohta+pankkikortista/a546610

Storås, N. 2011 Yli sadan hengen rikollisringin epäillään kopioineen luottokortteja ja huijanneen miljoonia, Tietoviikko. Viitattu 14.10.2011.
http://www.tietoviikko.fi/kaikki_uutiset/yli+sadan+hengen+rikollisringin+epaillaan+kopioineen+luottokortteja+ja+huijanneen+miljoonia/a700260?s=u&wtm=tivi-10102011

STT-Reuters 2011 Bloomberg: Facebookin kasvojentunnistus syynätään, Iltalehti. Viitattu 18.8.2011
http://www.iltalehti.fi/digi/2011060813861178_du.shtml

STT 2010. Henkilöllisyyden tunnistus kännykällä alkaa. Iltalehti. Viitattu 26. 1.2011

Tunnistautuminen varmennekortilla 2010. Viitattu 24.8.2011.
http://www.suomi.fi/suomifi/suomi/asioi_verkossa/sahkoinen_tunnistus_ja_allekirjoitus/tunnistautuminen_varmennekortilla/index.html

Tunnistautuminen mobiilivarmenteella 2011. Viitattu 24.8.2011.
http://www.suomi.fi/suomifi/suomi/asioi_verkossa/sahkoinen_tunnistus_ja_allekirjoitus/tunnistautuminen_mobiilivarmenteella/index.html

Tupas-tunnistuspalvelun tunnistusperiaatteet 2011. Finanssialan keskusliiton sivut. Viitattu 18.10.2011.
http://www.fkl.fi/teemasivut/sahkoinen_asiointi/Dokumentit/Tupas-tunnnistusperiaatteet_v20b.pdf

Vahva tunnistaminen 2011. Helsingin kaupungin ATK sivusto. Viitattu 14.10.2011. http://www.helsinki.fi/atk/lehdet/103/Vahva%20tunnistaminen.html

Vartia, A. 2009 Tämä järjestelmä korvaa pian verkkopankin. Kauppalehti. Viitattu 26.1.2010 http://www.kauppalehti.fi/5/i/talous/uutiset/etusivu/uutinen.jsp?oid=2009/05/22263&ext=rss

Verified by Visa 2010. Luottokunnan verkkosivut. Viitattu 1.11.2011. http://www.luottokunta.fi/fi/kortit_ja_setelit/visa/verified_by_visa

Julkaisemattomat lähteet:

von Hintze, J. 2010. Kehityspäällikön haastattelu 22.12.2010. Liite 1. Fujitsu Services Oy. Helsinki.

Heinälä, P. 2010. Tuotekehityspäällikön haastattelu 20.12.2010. Liite 2. Fujitsu Services Oy. Helsinki.

Kuvaluettelo

Taulukot

Liite 1: Yhteenveto Jan von Hintzen haastattelusta 22.12.2010

Kumpi on yleensä tärkeämmässä roolissa tunnistautumisen luotettavuuden kannalta, käyttäjä vai menetelmä?	Tunnistautuminen koostuu kolmesta eri asiasta jotka ovat jotain mitä tiedät (esim. salasana), jotain mitä olet (esim. sormenjälki) ja jotain mitä sinulla on (esim. kännykkä). Tämän periaatteen mukaan sanoisin että menetelmä on käyttäjää varmempi, koska käyttäjä voi jakaa salasanansa jollekin muulle mutta samaa hän ei voi tehdä biometrisessä tunnistautumisessa.
Mistä elementeistä tunnistusmenetelmän luotettavuus koostuu?	Kolmesta edellä mainitusta. Luotettavuus kasvaa, kun tunnistautumistapoja yhdistellään toisiinsa. 2/3 tunnistautumistavasta riittää vahvaan tunnistukseen.
Mitä vahvuuksia biometrisillä tunnistusmenetelmillä on muihin tunnistusmenetelmiin nähden?	Biometristä tunnistetta ei voida jakaa yhtä helposti kuin muita tunnisteita. Jotkin biometriset tunnistusmenetelmät (esim. sormenjälki) ovat kuitenkin huijattavissa suht helposti. Myös niiden käyttövarmuus ei ole aina ideaalinen, esimerkiksi kuivat kädet, likaiset sormet ja likainen lukija saattavat vaikuttaa tunnistusvarmuuteen.
Mitä tulevaisuuden näkymiä biometrisillä tunnistusmenetelmillä on?	Niiden käyttö tulee lisääntymään ja ne tulevat toimimaan yleisesti ottaen hyvinä tunnistautumismenetelminä. Iso ongelma on kuitenkin käyttäjän ajatus siitä, että esimerkiksi sormenjäljet tai iiriskuva ovat heidän ”privaattia” aluettaan.
Mobiilitunnistus on ollut mediassa paljon esillä viime aikoina; minkälaisia tulevaisuuden näkymiä mobiilitunnistamisella on?	Mobiilitunnistautumista voitaisiin alkaa käyttämään laajasti autentikoinneissa, esimerkiksi pieniä ostoksia tehtäessä. Hyvänä puolena on, että ihmisillä on jo matkapuhelin, minkä takia heille ei tarvitsisi toimittaa enää erillisiä salasanalistoja tai laitteita.
Mitä ongelmia mobiilitunnistamiseen liittyy?	Yhtenäisten toimintamallien puuttuminen. Jokainen palveluntarjoaja soveltaa vähän eri tavalla. Mobiilitunnistautumisia ei myöskään ole verifioitu, kuten esimerkiksi Visa-maksaminen.
Onko mobiilitunnistuksessa mahdollista väärentää mobiilivarmennetta?	Mielestäni se ei käytännössä ole mahdollista, mutta teoriassa kyllä. Tämä tietysti riippuu siitä, mihin mobiilivarmenne perustuu. Jos sertifikaatti on sim-kortilla, niin väärentäminen ei ole mahdollista. Mutta jos tunnistautuminen perustuu johonkin puhelimen tietoon, joka on muutettavissa/huijattavissa, niin silloin väärentäminen on mahdollista.
Minkälaiset palvelut soveltuvat salasanatunnistautumiselle ja minkälaiset ehdottomasti eivät?	Kun samaan asiaan tarvittaisiin paikanpäällä asioidessa henkilöllisyystodistuksen näyttämistä, niin silloin ei pitäisi mielestäni riittää pelkkä salasana. Eikä myöskään silloin, jos ollaan tekemisissä pankkitilien tai rahan kanssa.
Onko salasanan käyttö turvallista, jos tietokoneessa ei ole haittaohjelmia?	Tämä riippuu siitä, onko yhteys palveluntarjoajaan salattu ja onko palveluntarjoajalla asianmukaiset salasanamenettelyt.

Ovatko pankkitunnukset idioottivarma tunnistusmenetelmä, jos tunnukset ovat fyysisesti turvassa?	Käytännössä kyllä. Todellisuudessa salasanat kiertävät noin parin miljoonan salasanan ”kehää” jolloinka seuraavat luvut saattavat teoriassa olla laskettavissa, jos päästään käsiksi tarpeeksi moneen edelliseen salasanaan. Myös edellisen kysymyksen vastaus pätee tässäkin kohtaa. Kasvava riski ovat myös huijaussivustot, jotka esittävät olevansa joitain muita sivustoja, mitä todellisuudessa ovat.
Minkälaisia ongelmia tunnistuspalveluihin liittyy?	Varastot, joissa salasanoja pidetään, ovat riskialttiita. Myös koneilla olevat haittaohjelmat aiheuttavat ongelmia tunnistuspalveluille.
Mistä palvelun loppukäyttäjä voi tietää, voiko tunnistuspalveluun luottaa?	Perusperiaate on tarkistaa verkkosivun sertifikaatin tulevan luotettavalta sivulta, eikä luottaa sellaisiin palveluihin, joista ei tiedä mitään.
Onko tunnistuspalvelun käyttäjällä mitään lain takaamaa suojaa esimerkiksi siinä tapauksessa, että palvelun tarjoaja vuotaa käyttäjän tietoja?	Ei oikeastaan muuta kuin mitä henkilörekisterilaissa sanotaan.
Onko turvallisuusmielessä merkitystä sillä, onko palvelu Suomessa tai ulkomailla, ja onko sitä edes mahdollista saada selville?	Riippuu tiedoista, mitä palvelulle syötetään. On tietoja mitä ei saa suomen ulkopuolelle siirtää. Näissä tapauksissa maalla on merkitystä. Käyttäjän on lähes mahdotonta saada selville, missä hänen tietonsa ”makaa”, eli missä on fyysisesti se kovalevy, johon hänen tietonsa on kirjoitettu. Pilvipalvelut hankaloittava entisestään asiaa, koska tieto voi siirtyä paikasta toiseen useaan otteeseen.

Liite 2: Yhteenveto Petri Heinälän haastattelusta 20.12.2010

Kumpi on yleensä tärkeämmässä roolissa tunnistautumisen luotettavuuden kannalta, käyttäjä vai menetelmä?	Luotettavuuden kannalta tärkeintä ovat tunnistusmenetelmän ympärillä olevat prosessit, käytännöt ja politiikat.
Mistä elementeistä tunnistusmenetelmän luotettavuus koostuu?	Edellisessä kysymyksessä mainituista: prosesseista, käytännöistä ja politiikoista. Käyttäjän näkökulmasta luotettavuuteen vaikuttavat myös esimerkiksi menetelmän imago ja näkyvyys. Tuttuun menetelmään luotetaan.
Mitä vahvuuksia biometrisillä tunnistusmenetelmillä on muihin tunnistusmenetelmiin nähden?	Biometriikka oikeasti kertoo kuka sinä olet, kun taas muut menetelmät perustuvat siihen, mitä omistat tai tiedät. Sitä, mitä olet, et pysty lainaamaan kenellekään. Verisuonikarttaa on mahdoton kopioida, ja koska se ei ole "pintainformaatiota", eli se perustuu kehon sisäiseen tietoon, sitä ei tule jätetyksi mihinkään.
Mitä ongelmia biometrisiin tunnistusmenetelmiin liittyy?	Puhetta voidaan nauhoittaa. Kasvoja kuvataan. Sormenjälkiä jätetään kaikkialle. Kun biometrisen tiedon saa kerran kopioitua, on se hyödytön.
Mitä tulevaisuuden näkymiä biometrisillä tunnistusmenetelmillä on?	Verisuoniteknologia tulee laajenemaan ja eri biometrisistä tunnistusmenetelmistä tullaan näkemään yhdistelmiä.
Mobiilitunnistus on ollut mediassa paljon esillä viime aikoina; minkälaisia tulevaisuuden näkymiä mobiilitunnistamisella on?	Operaattoreiden mobiilivarmenne on ollut esillä viimeaikoina, koska ne ovat julkaisseet mobiilivarmennepalvelunsa. Mobiilitunnistaminen ei ole kuitenkaan rajattu vain operaattoreiden tarjoamaan tapaan, vaan sitä voidaan käyttää erilaisissa tilanteissa eri variaatioina. Tulevaisuuden näkyvistä olen pessimistinen, sillä mobiilitunnistusta on pyritty edistämään jo noin 15 vuotta. Markkinoinnilla on tietysti suuri osuus asiaan.
Mitä ongelmia mobiilitunnistamiseen liittyy?	Tekstiviestiin perustuvassa menetelmässä ei esimerkiksi ole viestin perillemenon kuittausta, jolloinka esimerkiksi virhetilanteiden käsittely on hankalaa. Mobiilivarmenne on sidottu operaattorin simkorttiin, joten operaattoria vaihtaessa on myös hankittava uusi varmenne.
Onko mobiilitunnistuksessa mahdollista väärentää mobiilivarmennetta?	Mobiilivarmenne on sim-kortilla ja sen väärentäminen on hankalaa. Palvelun tarjoaja, eli simkortin hallinoijat pystyvät väärentämään mobiilivarmenteen.
Minkälaiset palvelut soveltuvat salasanatunnistautumiselle ja minkälaiset ehdottomasti eivät?	Sellaset missä ei käsitellä henkilö/terveystietoja tai muita arkaluontoisia asioita. Sosiaaliseen mediaan salasana sopii. Jos käyttäjillä on syytä pelätä identiteettivarkauksia

	esimerkiksi sosiaalisessa mediassa, pitäisi mielestäni olla tarjolla myös vaihtoehto salasanatunnistautumiselle. On tietysti käyttäjästä kiinni, mitä vaatii palvelulta.
Onko salasanan käyttö turvallista, jos tietokoneessa ei ole haittaohjelmia?	Salasanan heikkous perustuu myös salasanapolitiikkaan. Politiikan kautta tulevat myös käytännöt, esimerkiksi miten helposti salasanan pystyy resetoimaan. Asiaton henkilö voisi esimerkiksi soittaa helppariin käyttäjän nimellä ja pyytää resetoimaan salasanan. Salasanoja voidaan murtaa myös bruteforcella, eli kokeilemalla kaikkia mahdollisia salasanoja jonkin ohjelman avulla.
Ovatko pankkitunnukset idioottivarma tunnistusmenetelmä, jos tunnukset ovat fyysisesti turvassa?	Kertakäyttösalasanat perustuvat tunnistusmenetelmänä siihen lappuun, missä salasanat ovat. Lapun voi kopioida tai se voidaan lainata. Kertakäyttösalasanoja voidaan selvittää myös esimerkiksi kalasteluyrityksillä. Käyttäjä voidaan ohjata valesivustolle huomaamattaan, jolloinka saadaan seuraava numero kertakäyttösalasanalistalta.
Millaisessa asioinnissa/palveluissa tarvitaan vahvaa tunnistusta?	Aina kun on rahasta tai henkilötiedoista kyse sekä aina viranomaisasioissa.
Minkälaisia ongelmia tunnistuspalveluihin liittyy?	Yleisesti ongelmana on se, että on paljon asioita, joita on otettava huomioon. Menetelmät saattavat teknisesti toimia, mutta menetelmän ympärillä olevilla asioilla (esimerkiksi rekisteröityminen tai salasanan uusiminen) saadaan palvelu pilattua. Heikko lenkki löytyy aina jostain.
Mistä palvelun loppukäyttäjä voi tietää, voiko tunnistuspalveluun luottaa?	Aina ei voi saada selville, voiko palveluun luottaa. Paljolti perustuu imagoon ja palvelun antamaan mielikuvaan. Nykyään on olemassa laki vahvasta tunnistamisesta. Viestintävirastosta voi käydä tarkistamassa, onko palveluntarjoaja vahvojen tunnistuspalveluiden tarjoajien listalla. Tavalliset loppukäyttäjät eivät yleensä tarkasta luotettavuutta mistään, vaan heille luotettavuus perustuu ”musta tuntuu”-mielikuvaan.
Miten tunnistuspalvelun luotettavutta tutkitaan?	Palvelun luotettavuus perustuu yleensä menetelmän vahvuuteen, mutta palvelun kokonaisuutta ei niinkään mietitä tai kyseenalaisteta. Valtio on esimerkiksi asettanut tietyt vaatimukset tietyille palveluille, joita sitten auditoidaan niiden mukaan.
Onko tunnistuspalvelun käyttäjällä mitään lain takaamaa suojaa esimerkiksi siinä tapauksessa, että palvelun tarjoaja vuotaa käyttäjän tietoja?	Henkilötietolaki ja tietosuojalaki ottavat kantaa asiaan. Luottokorttiyhtiöt esimerkiksi vaativat tiettyjen vaatimusten täyttämistä maksukorttiyri-

	tyksiltä ja palveluntarjoajilta. Esimerkiksi jos palveluntarjoaja kadottaa korttinumeroita, joutuu hän maksamaan luottokorttiyhtiölle korvauksia. Käyttäjä hyväksyy käyttöehdot rekisteröityessään palveluun, eikä käyttöehdoissa yleensä luvata mitään erityisiä korvauksia siltä varalta, että jotain katoaa.
Onko turvallisuusmielessä merkitystä sillä, onko palvelu Suomessa tai ulkomailla, ja onko sitä edes mahdollista saada selville?	Kaikista palveluista ei ole mahdollista saada maata selville. Periaatteessa asialla ei ole väliä, kunhan palveluun liittyvät prosessit on hoidettu asianmukaisesti. Lain puitteissa on vaikea lähteä hakemaan oikeuksiaan esimerkiksi Etelä-Afrikassa sijaitsevalta palveluntarjoajalta.