Biometristen järjestelmien yksityisyys – haasteet ja mahdollisuudet

Diplomityö
Turun yliopisto
Informaatioteknologian laitos
Ohjelmistotekniikka
2015
Antti Adamsson

Tarkastajat:
Antti Hakkala
Sami Hyrynsalmi

TURUN YLIOPISTO
Informaatioteknologian laitos

ANTTI ADAMSSON: Biometristen järjestelmien yksityisyys – haasteet ja mahdollisuudet

Diplomityö, 92 s., 0 liites.
Ohjelmistotekniikka
Kesäkuu 2015

Biometrinen tunnistaminen tarkoittaa henkilön tunnistamista fysiologisten ja käytökseen perustuvien ominaispiirteiden avulla. Tällä on suuria etuja muihin menetelmiin nähden sekä luotettavuuden että nopeuden suhteen. Biometrisen tunnistamisen kääntöpuolena on myös haasteita yksityisyyden ja tietoturvan osalta.

Tässä opinnäytetyössä esitellään biometristen tunnistusjärjestelmien perusperiaatteet sekä kirjallisuudessa esitettyjä yleisimpiä biometrisia tunnistusmenetelmiä. Opinnäytetyössä tarkastellaan laajasti kirjallisuudessa esitettyjä biometristen järjestelmien heikkouksia, niihin kohdennetuja hyökkäyksiä ja hyökkäyksiltä suojautumisia. Lisäksi käsitellään laajasti yksityisyyttä ja siihen liittyvää lainsäädäntöä.

Työssä tutkitaan, miten biometrinen tunnistus vaikuttaa yksityisyyteen kolmen esimerkkitapauksen havainnollistamana. Lisäksi esitellään erilaisia huolenaiheita ja uhkakuvia, joita on liitetty biometriseen tunnistamiseen. Kirjallisuudesta löydettiin lukuisia perusperiaatteita ja käytänteitä, joita noudattamalla voidaan suunnitella mahdollisimman hyvin yksityisyyttä suojaava biometrinen tunnistusjärjestelmä.

Opinnäytetyön perusteella voidaan havaita, ettei biometrisen tunnistamisen käyttöönotto ole hyödyistään huolimatta ongelmatonta. Yksityisyyden suojaan on kiinnitettävä erityisen paljon huomiota.

Asiasanat: biometrinen tunnistaminen, biometriikat, yksityisyys, tietoturva

UNIVERSITY OF TURKU
Department of Information Technology

ANTTI ADAMSSON: Biometristen järjestelmien yksityisyys – haasteet ja mahdollisuudet

M.Sc. (Tech) thesis, 92 p., 0 app. p.
Software engineering
June 2015

Biometric authentication means the identification of a person based on physiological and behavioral characteristics. This has great advantages over other methods and the reliability and the speed ratio. On the flip side of biometric identification, there are also challenges on privacy and information security.

This thesis presents the biometric systems, the basic principles, as well as the most common biometric identification methods described in the literature. A depth review is presented of the weaknesses of biometric systems presented in the literature, their targeted attacks and attacks' means of defense. In addition the thesis deals extensively with privacy and related legislation.

This master's thesis examines the impact on the privacy of biometric identification illustrated by three case studies. In addition a variety of concerns are presented and threats that are connected with biometric identification. In literature it was discovered a number of basic principles and practices to follow in order to design the best possible biometric identification system for privacy.

On the basis of this thesis can be observed that the introduction of biometric identification is not trouble-free, despite its benefits. Privacy protection requires especially a lot of attention.

Keywords: biometric authentication, biometrics, privacy, information security

Sisältö

Kuvat

Luku 1

Johdanto

Biometrinen tunnistus tarkoittaa henkilön tunnistamista käyttäen hyödyksi ihmisen fysiologisia ja käyttäytymiseen perustuvia ominaispiirteitä.

Biometristen tunnisteiden käytöllä on selkeitä etuja, koska niiden avulla voidaan nopeuttaa tunnistamista ja parantaa sen luotettavuutta. Toisin kuin perinteisessä autentikoinnissa biometrista tunnistetta ei voi kadottaa, kuten avaimia, tai unohtaa, kuten salasanoja, vaan biometrinen tunniste on ominaisuus, joka kulkee aina henkilön mukana.

Alun perin biometrista tunnistamista on hyödynnetty lähinnä rikosten selvittämisessä, jolloin sormenjälkiä tutkittiin hitaasti käsityönä aina 1900-luvun lopulle saakka. Tietokoneiden ja muun tekniikan nopean kehittymisen ansiosta myös muita biometrisia tunnistusmenetelmiä on voitu nykyään automatisoida ja tuoda uusia sovelluksia markkinoille.

Nykyään biometrinen tunnistus on Suomessa laajamittaisessa käytössä käytännössä vain biometrisen passin ominaisuudessa. Siinä perinteisen passin lisäksi varmenteeksi on liitetty passin haltijan kasvokuva sekä sormenjäljet digitaalisessa muodossa etäluettavalle sirulle.

Biometrisessa tunnistamisessa on otettava huomioon lukuisia kysymyksiä, jotka liittyvät yksityisyyteen ja tietoturvallisuuteen. Vaikka biometriset tunnistusjärjestelmät pyritään suojaamaan mahdollisimman hyvin ja tarkasti, löytyy niistä useita potentiaalisia haavoittuvuuksia, joita hyödyntämällä voi ohittaa järjestelmän suojaukset tai päästä käsiksi

järjestelmään tallennetuihin tietoihin.

Biometrisia tunnisteita on mahdollista kerätä henkilöltä tämän huomaamatta ja tiedostamatta. Vääriin käsiin joutuneiden biometristen tunnisteiden avulla on mahdollista esiintyä uskottavasti toisena henkilönä varsinkin tietoverkoissa asioitaessa. Tiettyjen tunnisteiden avulla on myös mahdollista saada tietoa kyseisen henkilön sairauksista ja muista arkaluonteisista ominaisuuksista.

Tässä opinnäytetyössä perehdytään näihin kysymyksiin ja haasteisiin laajamittaisen kirjallisuuskatsauksen menetelmin ja muita lähteitä, muun muassa lainsäädäntöaineistoa hyödyntäen. Edellä mainitun lainsäädännön monimutkaisuuden vuoksi on luonnollista keskittyä tässä työssä Suomen ja soveltuvin osin Euroopan unionin lainsäädäntöön.

Luvussa 2 esitellään aluksi biometristen menetelmien historiaa ja kehitystä lähinnä 1800-luvulta nykypäivään. Seuravaaksi luvussa esitellään yleisimpiä käytössä olevia fysiologisia ja käytökseen perustuvia biometrisia tunnistusmenetelmiä.

Luvussa 3 perehdytään biometrisen tunnistusjärjestelmän yleiseen periaatteeseen. Lisäksi tarkastelleen erilaisten biometristen tunnisteiden ominaisuuksia, jotka vaikuttavat niiden soveltuvuuteen biometrisessa tunnistusjärjestelmässä. Näiden lisäksi tutustutaan biometrisen järjestelmän suorituskykyyn vaikuttaviin tekijöihin, sekä lopuksi kerrotaan, mitä hyötyjä usean biometriikan käytöllä voidaan saavuttaa verrattuna yhden biometriikan käyttöön tunnistusjärjestelmässä.

Luvussa 4 esitellään aluksi periaatetasolla biometrisen järjestelmän mahdollisia haavoittuvuuksia. Tämän jälkeen avataan seikkaperäisesti erilaisia kohteia, uhkavektoreita, jotka ovat kohteita, joita vastaan järjestelmässä voidaan hyökätä. Seuraavaksi kerrotaan myös laajasti puolustusmenetelmistä, joiden avulla on mahdollisuus suojautua uhkavektoreita vastaan.

Luvussa 5 määritellään aluksi yksityisyyden käsitettä yleisellä tasolla. Tämän jälkeen syvennytään lähinnä Suomen ja osittain Euroopan unionin lainsäädännön kohtiin, jotka liittyvät läheisesti yksityisyyteen ja yksityisyyden suojaan. Lisäksi käsitellään identiteetti-

varkauksia.

Luvussa 6 pohditaan tarkemmin, miten erityisesti biometrinen tunnistus vaikuttaa yksityisyyden suojaan ja minkälaisia uhkakuvia biometristen tunnisteiden käyttöön voi liittyä. Aihetta havainnollistetaan kolmen erilaisen esimerkkitapauksen avulla.

Luvussa 7 yritetään löytää ratkaisuja, miten biometriseen tunnistamiseen liittyviä haasteita, kuten yksityisyyden suojaan liittyviä kysymyksiä, voidaan ratkaista.

Luku 8 on yhteenveto tästä opinnäytetyöstä.

Luku 2

Biometriikat

Termi *biometriikka* on johdettu kreikan kielen sanoista *bios* (elämä) ja *metrikos* (mitata). Biometrinen tunnistaminen tarkoittaa henkilön automaattista tunnistamista, joka perustuu ominaisuusvektoreihin (engl. *feature vector*). Ne on johdettu yksilön fysiologisista tai käytökseen perustuvista ominaispiirteistä (engl. *feature*) [7].

Perinteisesti salasanoja ja kulkukortteja on käytetty rajaamaan pääsyä turvallisuusjärjestelmiin, mutta nämä menetelmät ovat sekä helppoja murtaa että epävarmoja. Biometriikkaa ei voi unohtaa, ja sen lainaaminen, varastaminen tai väärentäminen on käytännössä hyvin vaikeaa ellei jopa mahdotonta [7].

Seuraavissa alaluvuissa käsitellään biometristen menetelmien historiaa ja biometrisia menetelmiä yleisellä tasolla. Lisäksi kerrotaan yleisimmistä käytössä olevista menetelmistä jaoteltuina fysiologisiin ja käytökseen perustuviin menetelmiin.

2.1 Biometristen menetelmien historiaa

Automatisoidut biometriset tunnistusjärjestelmät ovat yleistyneet vasta viimeisten vuosikymmenien kuluessa, suurimmalta osin tietokoneiden kehityksen ansiosta. Useimmat automatisoidut järjestelmät kuitenkin pohjautuvat satoja tai jopa tuhansia vuosia vanhoihin ideoihin. Kasvot ovat yksi vanhimmista ja yksinkertaisimmista esimerkeistä sellaisista omi-

naisuuksista, joita ihmiset ovat käyttäneet tunnistamaan toisiansa ihmiskunnan alkuajoista asti. Ihmiset ovat hyödyntäneet myös puhetta ja kävelytyyliä tunnistaessaan toisiaan. Nämä ovat ominaisuuksia, joita ihmiset käyttävät päivittäin jokseenkin tiedostamattaan. [17]

Arviolta 31 000 vuotta vanhasta luolasta on löydetty kalliomaalauksia, joita ympäröi lukuisia kädenjälkiä. Näiden uskotaan olevan tarkoitettu esittämään maalaajan jättämiä ”nimikirjoituksia”. Muinaisessa Babyloniassa 500 vuotta eaa. uskotaan käytetyn sormenjälkiä savitauluissa varmentamaan kaupankäyntimerkintöjä. Myös muinaiset kiinalaiset käyttivät sormenjälkiä suoritettujen maksujen merkiksi. Kiinassa vanhemmat käyttivät sormenjälkiä ja jalanjälkiä myös erottaakseen lapsensa toisistaan. Varhaiset egyptiläiset käyttivät fyysisiä tuntomerkkejä erottaakseen luotettavat ja maineikkaat kauppiaat uusista kauppiaista. [29, 17]

1800-luvun puoliväliin tultaessa kaupunkien nopeasti kasvaessa teollistumisen ansiosta huomattiin tarve tunnistaa ihmisiä virallisesti. Kauppiaat ja viranomaiset eivät voineet enää luottaa pelkästään omiin kokemuksiinsa ja paikallistuntemukseen, kun väestö kasvoi ja muuttui liikkuvammaksi. Esimerkiksi oikeuslaitos halusi kohdella ensikertalaisia rikollisia lievemmin, mutta rikoksenuusijoita ankarammin. Rikoksenuusijoita oli aiemmin merkitty muun muassa polttomerkeillä. Tämän takia tarvittiin virallinen järjestelmä, jolla voitiin luetteloida rikolliset ja varmistaa heidän henkilöllisyytensä. [17, 43]

Ensimmäinen menetelmä oli ranskalaisen Alphonse Bertillonin 1880-luvulla kehittämä niin kutsuttu *Bertillonin järjestelmä* [17], jossa kirjattiin korteille erilaisia vartalon mittasuhteita. Näitä voitiin lajitella esimerkiksi ihmisen pituuden tai käsivarren pituuden mukaan. Lääketiedettä opiskelleena Bertillon keksi mitata ja rekisteröidä yhtätoista eri ihmiskehon mittasuhdetta. Tätä kutsuttiin *antropometriaksi*, joka on johdettu kreikan sanoista *anthropos* (ihminen) ja *metrikos* (mitata). Mittausvirheiden takia antropometria oli kuitenkin epätarkka menetelmä. Lisäksi antropometrian avulla ei voitu havaita rikospaikalle jääneitä jälkiä. Bertillon kehitti myös standardin mukaiset kortistoon liitettävät rikollisten rekisterivalokuvat (engl. epämuodollisesti *mug shot*), joissa toinen kuva on

otettu sivuprofiilista ja toinen suoraan edestäpäin. [43]

Toinen menetelmä oli poliisilaitosten käyttämät viralliset sormenjälkirekisterit. Ensimmäisen merkittävän sormenjälkien luettelointitavan, niin kutsutun *Galton–Henryn järjestelmän*, kehittivät 1800-luvun lopulla englantilaiset Francis Galton ja Edward Henry. Galton oli kiinnostunut antropometriasta ja luokitteli sormenjäljet niiden peruskuvioiden mukaaan. Henry oli puolestaan ammatiltaan poliisi, ja noustuaan Scotland Yardin johtajaksi, hän myötävaikutti uuden järjestelmän laajamittaiseen käyttöönottoon. Galton-Henryn järjestelmän muunnelmia on ollut käytössä yleisesti, kunnes *AFIS-järjestelmät* (engl. Automated Fingerprint Indentification System) syrjäyttivät ne viimeistään 1990-luvulla. [29, 43]

2.2 Biometriset menetelmät

Autentikoinnilla (engl. *authentication*) eli todennuksella tarkoitetaan varmistamista, että sallitulla henkilöllä on sallitut oikeudet sallittuun kohteeseen sallittuna ajankohtana [8]. Yleisesti ottaen voidaan autentikoida kolmella eri tavalla, jotka ovat vähiten turvallisesta ja kätevästä turvallisimpaan ja kätevimpään [7]:

1. Jotain, mitä todennettavalla henkilöllä on, esimerkiksi avain, avainkortti, kulkukortti tai poletti.

2. Jotain, mitä todennettava henkilö tietää, esimerkiksi salasana tai PIN-koodi.

3. Jokin ominaisuus, joka todennettavalla henkilöllä on eli biometriikka.

Biometrista järjestelmää voidaan käyttää sekä henkilöllisyyden *varmentamiseen* (engl. *verification*) että *tunnistamiseen* (engl. *identification*) [7]. Tunnistamisessa verrataan biometrista tunnistetta tietokannassa oleviin kaikkiin tunnisteisiin, kun taas varmistamisen tapauksessa sitä verrataan vain väitetyn henkilön tunnisteeseen. Tämän takia varmentaminen ja tunnistaminen ovat kaksi erikseen käsiteltävää ongelmaa.

Biometriset tunnistusmenetelmät voidaan jakaa fyysisiin (engl. *physical*) ja käytöksellisiin (engl. *behavioral*) ominaispiirteisiin perustuviin menetelmiin [4]. Fyysisiä ominaispiirteitä ovat muun muassa sormenjälki, iiris, kasvot ja kämmenen geometria. Käytöksellisiä ominaispiirteitä ovat puolestaan esimerkiksi nimikirjoitus, näppäinpainallus ja kävelytyyli.

2.3 Fysiologiset tunnistusmenetelmät

Useimmat ihmisen fyysiset ominaisuudet ovat melko pysyviä, mutta ne voivat muokkautua esimerkiksi ikääntymisen myötä. Myös mahdollisen vamman tai sairauden vaikutuksesta jokin ominaisuus voi muuttua. Seuraavassa esitellään yleisimmät käytössä olevat biometriset tunnistusmenetelmät Jain et al. mukaan [4]:

DNA Deoksiribonukleiinihappo (engl. *deoxyribonucleic acid*) eli DNA sisältää solun geneettisen informaation. DNA-tunniste on erittäin tarkka, mutta identtisillä kaksosilla se on kuitenkin täysin samanlainen. DNA:ta voidaan eristää mistä tahansa ihmisen eritteestä tai kudoksesta. DNA-tunnistetta käytetään eniten rikostutkinnassa. Menetelmän haittoja ovat muun muassa mahdollisuus sekoittaa, varastaa ja väärinkäyttää tunnisteita. Lisäksi nykyisellä tekniikalla automaattinen ja reaaliaikainen tunnistus on käytännössä mahdotonta, koska näytteen analysointi vaatii monimutkaisen laitteiston käyttöä ja siihen koulutettua henkilökuntaa. DNA-tunnisteen kerääminen ja tietojen väärinkäytön mahdollisuus koetaan myös yksityisyyttä loukkaaviksi. DNA:n muokkaaminen on käytännössä mahdotonta, joten se on erittäin pysyvä tunniste.

Sormenjälki Sormenjälkiä on käytetty henkilöllisyyden tunnistamiseen ja apuna rikosten selvittämisessä jo pitkään, ja tunnistamistarkkuus on osoittautunut hyvin suureksi. Sormenjälki on sormenpään ihon pienistä kohoumista ja laaksoista muodostuva kuvio. Se muotoutuu jo sikiökaudella, ja sitä pidetään yksilöllisenä ja muuttumattomana. Sormenjälki on jokaisessa sormessa — ja varpaassa — erilainen. Myös identtisillä kaksosilla on yksilölliset sormenjäljet. Nykyään sormenjälkiskannerit

ovat halpoja ja niitä voidaan liittää esimerkiksi kannettaviin tietokoneisiin. Tällöin sormenjäljen lukemisella voidaan korvata perinteinen salasanan syöttämiseen perustuva käyttäjän kirjautuminen tietokoneelle. Sormenjälkitunnistuksen tarkkuus on riittävä henkilöllisyyden varmentamiseen sekä tunnistamiseen pienissä ja keskisuurissa tunnistusjärjestelmissä (muutama sata käyttäjää). Saman henkilön useamman sormenjäljen käyttö lisää tunnistamistarkuutta, ja se riittää suuremmankin joukon tunnistamiseen (miljoonia tunnistettavia). Nykyisissä sormenjälkiin perustuvissa tunnistamisjärjestelmissä on ongelmana sen vaatima suuri laskentateho, varsinkin jos järjestelmää käytetään suuren ihmisjoukon henkillölisyyden tunnistamiseen. Joissain tilanteissa automaattinen sormenjälkitunnistus voi olla mahdotonta. Osalla ihmisistä sormet voivat puuttua kokonaan tai sormenjäljet ovat lukukelvottomat vamman tai sairauden seurauksena. Esimerkiksi käsitöitä tekevien ihmisten sormenpäissä voi olla paljon naarmuja ja viiltoja, jolloin sormenjäljet eivät pysy muuttumattomina.

Iiris Värikalvo eli iiris on silmän etuosassa sijaitseva ympyränmuotoinen, värillinen, pupillia ympyröivä osa, joka säätelee silmään pääsevän valon määrää. Iiriksen hyvin monimutkainen kuvio kehittyy jo sikiökautena, ja se vakiintuu kahden vuoden ikään mennessä. Sormenjäljen tapaan se on yksilöllinen molemmissa silmissä, myös identtisillä kaksosilla. Iiristunnistukseen perustuvien järjestelmien tarkkuus ja nopeus ovat nykyään lupaavia ja suuren mittakaavan järjestelmät toteuttamiskelpoisia. Iiriksen kuviota on erittäin vaikea muokata kirurgisesti, ja keinotekoinen iiris, kuten piilolinssi, on melko helppo havaita. Vaikka aikaisemmat iiristunnistusjärjestelmät vaativat huomattavasti käyttäjän osallistumista ja olivat kalliita, nykyiset järjestelmät ovat sekä käyttäjäystävällisempiä että edullisempia. Silmän iiris voi olla tuhoutunut vamman tai sairauden seurauksena.

Korva Ihmisen korvan muotoa ja rustojen rakennetta pidetään yksilöllisinä. Tämä menetelmä perustuu korvan tiettyjen osien etäisyyksien mittaamiseen. Korvan ominaisuuksia ei pidetä kuitenkaan erityisen selvästi erottuvina. Korvat voivat puuttua

vamman tai sairauden takia.

Kasvot Ihmiset tunnistavat toisensa yleisimmin juuri kasvojen perusteella. Siksi menetelmä on kaikkein intuitiivisin. Kasvontunnistuksessa ei vaadita kontaktia tunnistettavaan henkilöön. Kasvontunnistuksen käyttökohteet vaihtelevat staattisesta, hallituissa olosuhteissa tapahtuvasta varmennuksesta, kuten rikollisten tunnistuskuvat, dynaamiseen, muuttuvissa olosuhteissa tapahtuvaan tunnistukseen, kuten lentokentän valvonta. Kasvontunnistusta varten hyvän kuvan ottaminen on tärkeää. Haasteita aiheuttavat vaihtelevat taustat, eroavaisuudet kuvakulmissa ja valaistuksessa sekä kuvattavan erilaiset ilmeet. Ihmisen kasvot ovat voineet tuhoutua vamman tai sairauden takia.

Kasvojen, käden ja käden verisuonten lämpökuva Ihmiskehon lämpösäteilyn jättämä jälki on yksilöllinen, ja se voidaan kuvata infrapunakameralla samankaltaisesti yhtä huomaamattomasti kuin perinteisellä, näkyvän aallonpituuden kamerallakin otettaessa kuvia. Menetelmää voidaan käyttää huomaamattomaan tunnistamiseen. Lämpökuvaukseen perustuva järjestelmä ei tarvitse kosketusta tunnistettavaan kohteeseen, joten se on hienovarainen menetelmä. Kuvan tallentaminen on kuitenkin haastavaa vakioimattomassa ympäristössä, jossa lämpöä säteileviä pintoja, kuten lämpöpattereita tai ajoneuvojen pakoputkia, on ihmisen lähistöllä. Samankaltaista tekniikkaa, jossa hyödynnetään lähi-infrapuna-alueen kuvantamista (engl. *near-infrared imaging, NIRI*), voidaan käyttää kämmenselän verisuonten rakenteen tutkimiseen. Infrapuna-anturit ovat vielä huomattavan kalliita, mikä estää lämpökuvien laajamittaista käyttöä.

Kämmenen geometria Menetelmässä mitatataan useita ihmisen käden ominaisuuksia, kuten muotoa, kämmenen kokoa sekä sormien pituutta ja leveyttä. Tämä menetelmä on yksinkertainen, helppokäyttöinen ja edullinen. Kuitenkaan käden ominaisuuksia ei pidetä erityisen yksilöllisinä, eikä menetelmä ole kovin tarkka, jos tunnistettavana

on suuri määrä henkilöitä. Kämmen voi puuttua vamman tai sairauden takia.

Kämmenen jälki Ihmisen kämmenessä on erilaisia kuvioita ja kohoumia sormenjälkien tapaan. Sormea paljon suuremman pinta-alansa ansiosta kämmenenjälkeä pidetään jopa erikoislaatuisempana kuin sormenjälkeä. Koska kämmenenjälkiskannerien täytyy kuvata suurempi ala, ne ovat laitteina suurempia ja kalliimpia kuin sormenjälkiskannerit. Kämmenessä on myös useita syviä viivoja ja ryppyjä, joita on mahdollista kuvata matalamman resoluution skannerilla, mikä saattaa olla halvempaa. Kuitenkin käytettäessä suuren resoluution kämmenenjälkiskanneria, voidaan rakentaa erittäin tarkka biometrinen järjestelmä yhdistämällä tiedot käden geometriasta, kuvioista ja kohoumista, viivoista sekä rypyistä. Kämmen voi puuttua tai olla tuhoutunut vamman tai sairauden takia.

Tuoksu Jokainen objekti erittää sen kemialliselle koostumukselle ominaista tuoksua. Tutkittavaa objektia ympäröivää ilmaa johdetaan sensoreille, jotka tunnistavat kemiallisia yhdisteitä. Jokainen ihminen — tai muu eläin — erittää yksilölle ominaista tuoksua, jota voidaan käyttää tunnistamiseen. Menetelmää voivat haitata esimerkiksi hajusteiden käyttö ja ympäristön muut tuoksut.

Verkkokalvo Silmän verkkokalvon verisuonitus muodostaa monimutkaisen kuvion. Se on jokaisen ihmisen molemmissa silmissä yksilöllinen. Verkkokalvotunnistusta pidetään kaikkein turvallisimpana biometriikkana, koska verkkokalvon verisuonitusta on vaikea muuttaa tai jäljentää. Verkkokalvon kuvantaminen vaatii henkilön tarkkaa asettumista okulaarin eteen ja katseen tarkentamista tiettyyn pisteeseen, jotta ennalta määritelty verkkokalvon alue voidaan kuvata. Kuvantaminen vaatii kuvattavan henkilön yhteistyötä ja tietoista osallistumista sekä kontaktia okulaariin. Verkkokalvon verisuonista voidaan todeta myös joitakin sairauksia, kuten verenpainetauti. Nämä seikat saattavat vaikuttaa haitallisesti menetelmän hyväksyttävyyteen. Verkkokalvo voi olla tuhoutunut sairauden tai vamman takia.

Käden ja sormen geometria Menetelmässä mitataan useita ihmisen käden ominaisuuksia, kuten muotoa, kämmenen kokoa sekä sormien pituutta ja leveyttä. Kaupallisia käden geometriaan perustuvia tunnistusjärjestelmiä on jo käytössä ympäri maailman. Tämä menetelmä on yksinkertainen, melko helppokäyttöinen ja edullinen. Ympäristötekijät, kuten kuiva ilma, tai yksilölliset eroavuudet, esimerkiksi kuiva iho, eivät vaikuta järjestelmän tarkkuuteen huonontavasti. Kuitenkaan käden ominaisuuksia ei pidetä erityisen yksilöllisinä, eikä menetelmä ole kovin tarkka, jos tunnistettavana on suuri määrä henkilöitä. Käden geometriaan liittyvä informaatio ei mahdollisesti säily muuttumattomana esimerkiksi lapsen kasvaessa. Lisäksi tunnistettavan henkilön sormukset tai käden taipuisuus voivat vaikeuttaa käden geometriatiedon tallentamista. Suuremman kokonsa vuoksi käden geometriaa mittaavaa laitetta ei voida liittää esimerkiksi kannettavaan tietokoneeseen, toisin kuin sormenjälkiskanneri voidaan. On olemassa myös järjestelmiä, jotka mittaavat vain muutamaa sormea, yleensä etu- ja keskisormea. Vaikka nämä laitteet ovatkin pienempiä kuin koko kättä mittaavat, ovat ne kuitenkin huomattavasti suurempia kuin esimerkiksi sormenjälkiskannerit. Kädet ja sormet voivat puuttua sairauden tai vamman takia.

Muita fysiologiseen ominaisuuteen perustuvia menetelmiä ovat muun muassa kämmenen ja verisuonten kuvio, kolmiulotteinen kasvontunnistus, rikostekninen hammastunnistus sekä huulten jälki.

2.4 Käyttäytymiseen perustuvat tunnistusmenetelmät

Ihmisen käyttäytymiseen perustuvia ominaisuuksia ei voida pitkällä aikavälillä pitää pysyvinä, ja ne voivat muuttua huomattavastikin ajan kuluessa.

Näppäinpainallus On oletettavaa, että jokainen ihminen kirjoittaa näppäimistöllä omanlaisellaan tyylillä. Tämä käyttäytymiseen perustuva biometriikka ei ole välttämättä

erityisen yksilöllinen, mutta tietyissä sovelluksissa tarpeeksi tarkka henkilöllisyyden varmentamiseksi. Näppäinten painallus voi joillakin ihmisillä vaihdella huomattavan paljon esimerkiksi ympäristön mukaan. Myös näppäimistöllä kirjoittaminen saattaa olla mahdotonta vamman tai sairauden takia. Käyttäjän näppäinpainallukset voidaan rekisteröidä huomiotaherättämättömästi.

Kävelytyyli Henkilölle luenteenomainen kävelytyyli on monimutkainen ihmisen käyttäytymiseen (engl. *behavioral*) perustuva biometriikka, jossa hyödynnetään muuttuvan ajan ja paikan (engl. *spatio-temporal*) informaatiota. Kävelytyyli ei ole erityisen yksilöllinen, mutta tarpeeksi erottuva henkilöllisyyden varmentmiseksi alhaisen turvallisuustason sovelluksissa. Koska kävelytyyli on käyttäytymiseen perustuva biometriikka, se ei ole pysyvä varsinkaan pitkällä aikavälillä. Muutoksia voivat aiheuttaa kehonpainon vaihtelut, vammat, varsinkin nivelissä ja aivoissa, ikääntyminen tai päihtymystila. Lisäksi ihminen voi olla ylipäänsä kykenemätön kävelemään vamman tai sairauden takia. Kävelytyylin kuvaaminen on kohteelleen yhtä vaivatonta kuin kasvojen kuvaaminen ja siksi mahdollisesti helposti hyväksyttävä biometriikka. Kävelytyyli voidaan kuvata videokameralla useiden eri nivelten liikkeiden sarjana. Koska liikkeen kuvaaminen tuottaa paljon dataa, kävelytyyliin perustuva tunnistusjärjestelmä vaatii paljon laskentatehoa.

Ääni Ääni on yhdistelmä fysiologisia ja käyttäytymiseen perustuvia biometriikoita. Yksilölliset äänen ominaispiirteet perustuvat äänentuottamiseen käytettävien elinten, muun muassa äänihuulten, nielun, suu- ja nenäonteloiden sekä huulten kokoon ja muotoon. Äänentuottamiseen osallistuvat yksilölliset fysiologiset ominaisuudet ovat muuttumattomia, mutta puheääni voi muuttua esimerkiksi iän, vilustumisen tai tunnetilojen mukaan. Ääni ei ole erityisen yksilöllinen eikä siten sovelias suuren mittakaavan tunnistusjärjestelmissä. Ääntä muuttavien tekijöiden lisäksi muun muassa taustahälinä vaikeuttaa äänen tunnistamista. Tekstistä riippuvainen puheentunnistus perustuu siihen, että tunnistettava henkilö lausuu ennalta määrättyjä sanoja.

Tekstistä riippumaton järjestelmä tunnistaa puhujan välittämättä siitä, mitä hän puhuu. Jälkimmäinen järjestelmä on paljon vaikeampi toteuttaa, mutta turvallisempi huijausyrityksiä vastaan. Puheentunnistus on tarkoituksenmukaisinta puhelimeen liittyvissä sovelluksissa, kuten ajanvarausjärjestelmissä, mutta usein äänisignaalin laatu heikkenee puhelimen mikrofonin ja viestintäkanavan takia. Ihminen voi olla myös kykenemätön tuottamaan puhetta esimerkiksi vamman tai sairauden takia.

Nimikirjoitus Jokaisella ihmisellä on yksilöllinen tapa kirjoittaa nimensä. Nimikirjoitus on käyttäytymiseen perustuva biometriikka, joka muuttu ajan myötä. Se on altis henkilön fyysisille ja tunnetilojen muutoksille. Nimikirjoitus vaatii käyttäjän puolelta fyysistä kontaktia kirjoitusvälineeseen ja aktiivista osallistumista. Nimikirjoitusta pidetään laajasti hyväksyttynä virallisena tunnisteena, esimerkiksi asiakirjojen allekirjoituksena. Kuitenkin saman henkilön perättäisetkin nimikirjoitukset eroavat huomattavasti toisistaan, ja taitava väärentäjä saattaa onnistua huijaamaan tunnistusjärjestelmää. Ihmisen voi olla myös mahdoton kirjoittaa vamman tai sairauden takia.

Muita jo käytössä olevia tai myöhemmin mahdollisesti hyödynnettäviä biometrisia menetelmiä ovat muun muassa huulten ja kasvojen liikkeen analysointi [9], huulten jälki [9], sydämen toiminnan tarkkailu [31] sekä luuston röntgenkuvaus [32]. Ensiksi mainittua lukuunottamatta näitä menetelmiä voidaan pitää tunnistuksen kohdehenkilön kannalta jokseenkin vaivalloisina ja yhteistyötä vaativina.

Tässä luvussa käsiteltiin biometristen menetelmien historiaa ja biometrisia menetelmiä yleisellä tasolla. Lisäksi kerrottiin yleisimmin käytössä olevista menetelmistä jaoteltuina fysiologisiin ja käytökseen perustuviin menetelmiin.

Luku 3

Biometriset tunnistusmenetelmät

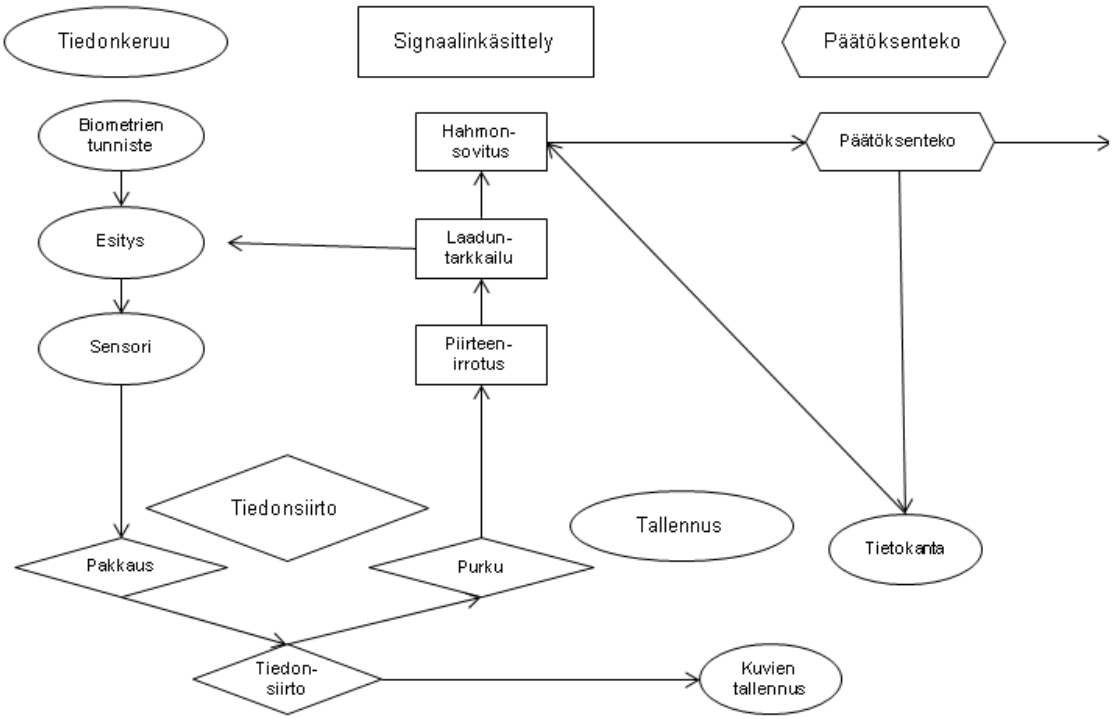
Seuraavissa alaluvuissa esitellään ensin biometrisen tunnistusjärjestelmän perusperiaate, joka on kaikille järjestelmille yhteinen. Tämän jälkeen tutustutaan biometristen tunnisteiden ominaisuuksiin, joilla on vaikutusta niiden soveltuvuuteen käytettäessä tiettyä biometrista sovellusta. Seuraavaksi käsitellään biometrisen järjestelmän suorituskykyyn vaikuttavia tekijöitä. Lopuksi tutustutaan usean biometriikan käyttöön, minkä avulla voidaan parantaa biometrisen järjestelmän suorituskykyä.

3.1 Biometrisen tunnistusjärjestelmän periaate

Vaikka biometriset tunnistusjärjestelmät perustuvat useisiin erilaisiin tekniikoihin, niissä on myös paljon yhtäläisyyksiä. Kuvassa 3.1 on esitetty Waymanin [1] mukaan biometrisen järjestelmän yleinen periaatekaavio. Se koostuu viidestä moduulista, jotka ovat *tiedonkeruu*, *tiedonsiirto*, *signaalinkäsittely*, *päätöksenteko* sekä *tallennus*.

Tiedonkeruuvaiheessa sensorimoduuli (engl. *sensor module*) kerää havaintoja sille esitetystä biometrisesta tunnisteesta. Tarvittaessa tiedonsiirtovaiheessa pakataan kerättyä dataa tiedonsiirron nopeuttamiseksi sekä tallennustilan säästämiseksi. Tämän jälkeen data siirretään käsiteltäväksi sekä tallennetaan tietokantaan myöhempää käyttöä varten. Signaalinkäsittelyvaiheessa piirteenirrotusmoduuli (engl. *feature extraction module*) erottaa

datasta oleellista numeerista tietoa, ominaisuusvektoreita. Lopuksi päätöksentekomoduuli (engl. *decision-making module*) joko tunnistaa henkilöllisyyden tai varmentaa väitetyn henkilöllisyyden, riippuen kyseisen järjestelmän toimintatilasta. [1]



Kuva 3.1: Yleisluonteisen biometrisen järjestelmän periaatekaavio. (Mukaillen [1].)

3.2 Biometristen tunnisteiden ominaisuuksia

Jokaisella eri biometriikalla on etuja ja haittoja, joten tietyn biometrisen piirteen valitseminen tiettyyn sovellukseen riippuu monesta seikasta tunnistamistarkkuuden lisäksi. Jain et al. ovat nimenneet seuraavat seitsemän tekijää [4], jotka määrittävät fysiologisen tai käyttäytymiseen perustuvan piirteen soveltuvuutta käytettäväksi biometrisessa sovelluksessa.

1. **Yleisyys**: Jokaisella sovellusta käyttävällä henkilöllä on oltava tämä piirre.

2. **Ainutlaatuisuus**: Piirteen on oltava riittävän yksilöllinen sovelluksen kohderyhmän henkilöiden välillä.

3. **Pysyvyys**: Piirteen on oltava pitkällä aikavälillä riittävän muuttumaton. Piirre, joka muuttuu huomattavasti ajan kuluessa, ei ole käyttökelpoinen biometriikka.

4. **Mitattavuus**: On oltava mahdollista kerätä ja digitalisoida piirre käyttäen soveltuvia laitteita, jotka eivät aiheuta liiallista vaivaa henkilölle. Lisäksi kerättävä raakadata on oltava mahdollista käsitellä muotoon, josta voidaan erottaa edustava otos ominaispiirteitä.

5. **Suorituskyky**: Tunnistamistarkkuuden ja sen saavuttamiseen vaadittavien resurssien tulee täyttää sovelluksen asettamat rajoitteet.

6. **Hyväksyttävyys**: Sovellusta käyttävän kohderyhmän henkilöiden on oltava halukkaita luovuttamaan biometrinen piirteensä järjestelmän käyttöön.

7. **Kiertäminen**: Yksilöllisen fysiologisen piirteen jäljittelyn helppous esimerkiksi tekosormilla tai käyttäytymiseen perustuvan piirteen matkimisen mahdollisuus.

Yksikään biometriikka ei käytännössä vastaa kaikkiin kaikkien erilaisten sovellusten määrittämiin vaatimuksiin. Yksikään biometriikka ei ole ihanteellinen, mutta monet niistä ovat käyttökelpoisia. Kunkin biometriikan käyttökelpoisuus tietyssä sovelluksessa riippuu kyseisen sovelluksen vaatimuksista ja biometriikan ominaisuuksista.

Seuraavassa taulukossa 3.1 vertaillaan yleisimpien biometriikoiden ominaisuuksia Jain et al. näkemyksen [10] mukaan. Taulukossa ”*suuri*” tarkoittaa piirteen olevan kyseisen ominaisuuden suhteen korkealla tasolla. ”*Keskitaso*” merkitsee verrattain korkeaa tasoa. Vastaavasti ”*matala*” tarkoittaa kyseisen piirteen olevan muihin piirteisiin suhteutettuna selvästi heikompi. Muista sarakkeista poiketen ominaisuuden ”*kiertäminen*” saama arvio ”*matala*” merkitsee, että kyseistä biometrista ominaisuutta on vaikea jäljitellä tai huijata.

Vastaavasti arvio ”*suuri*” tarkoitaa, että kyseinen ominaisuus on muihin ominaisuuksiin suhteutettuna alttiimpi huijausyrityksille.

Taulukko 3.1: Biometriikoiden vertailua ominaisuuksien mukaan. (Mukaillen [10].)

Selite: S = suuri, K = keskitaso, M = matala

Biometriikka	Yleisyys	Ainutlaatuisuus	Pysyvyys	Mitattavuus	Suorituskyky	Hyväksyttävyys	Kiertäminen
DNA	S	S	S	M	S	M	M
Korva	K	K	S	K	K	S	K
Kasvot	S	M	K	S	M	S	S
Kasvojen lämpökuva	S	S	M	S	K	S	M
Sormenjälki	K	S	S	K	S	K	K
Kävelytyyli	K	M	M	S	M	S	K
Käden geometria	K	K	K	S	K	K	K
Käden verisuonet	K	K	K	K	K	K	M
Iiris	S	S	S	K	S	M	M
Näppäinpainallus	M	M	M	K	M	K	K
Tuoksu	S	S	S	M	M	K	M
Kämmenenjälki	K	S	S	K	S	K	K
Verkkokalvo	S	S	K	M	S	M	M
Nimikirjoitus	M	M	M	S	M	S	S
Ääni	K	M	M	K	M	S	S

3.3 Suorituskyky

Tunnistussensorien erilaisesta asemoinnista, epätäydellisistä kuvausolosuhteista, ympäristön häiriötekijöistä, tunnistetattavan henkilön huonosta vuorovaikutuksesta sensorin kanssa sekä kohinan vuoksi on käytännössä mahdotonta, että kaksi *näytettä* (engl. *sample*), jotka on otettu eri näytteenottokerralla, mutta samasta biometrisesta ominaisuudesta, olisivat koskaan täysin yhtenevät. [4]

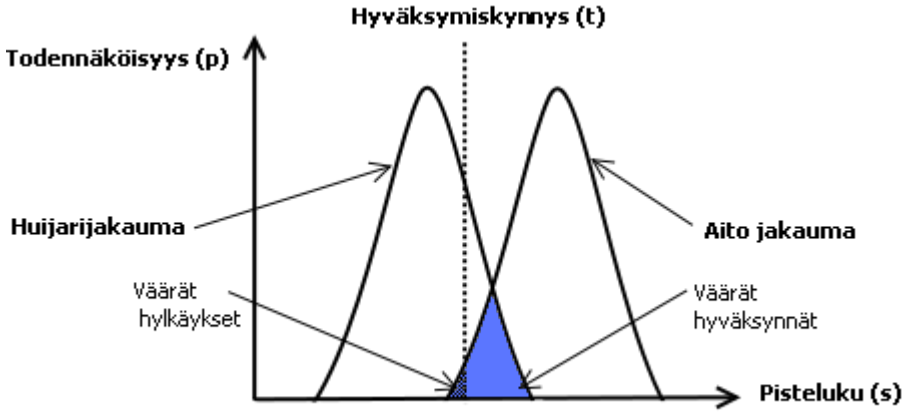
Päinvastoin kuin esimerkiksi salasanoihin perustuvassa autentikoinnissa, jossa vaaditaan täydellistä salasanojen vastaavuutta, jotta henkilön oikeudet voidaan varmentaa, biometrinen tunnistaminen perustuu tilastollisiin menetelmiin. Tästä syystä biometrisen tunnistusjärjestelmän *vastetta* (engl. *response*) mitataan *pisteluvulla* s (engl. *matching score*), joka määrittelee *syötteen* (engl. *input*) ja tietokannassa olevan *mallinteen* (engl. *template*) yhtäläisyyttä. [2] Mitä korkeampi pistemäärä on — tapauskohtaisesti myös päinvastoin — sitä varmemmin kaksi näytettä vastaavat toisiaan.

Pistelukua s verrataan *hyväksymiskynnykseen* t (engl. *decision threshold*), ja jos s on suurempi tai yhtäsuuri kuin t, näytteet ovat peräisin samasta henkilöstä. Vastaavasti, jos s on pienempi kuin t, näytteet ovat peräisin eri henkilöistä. Hyväksymiskynnyksen t sijaintia muuttamalla voidaan vaikuttaa tunnistusjärjestelmän vasteeseen. Kahden eri henkilön näytteistä muodostettua pisteiden jakaumaa kutsutaan *huijarijakaumaksi* (engl. *imposter distribution*). Vastaavasti saman henkilön näytteistä muodostettua pisteiden jakaumaa kutsutaan *aidoksi jakaumaksi* (engl. *genuine distribution*). [2] Kuvassa 3.2 esitetään biometrisen tunnistusjärjestelmän vaste edellä mainittujen todennäköisyysjakaumien suhteen.

Biometrisen tunnistusjärjestelmän virheitä mitataan yleisesti seuraavin käsittein [10]:

FNMR *false nonmatch rate* (suom. *väärien hylkäysten määrä*) Saman henkilön näytteet todetaan virheellisesti eri henkilöiden näytteiksi.

FMR *false match rate* (suom. *väärien hyväksyntien määrä*) Kahden eri henkilön näyt-



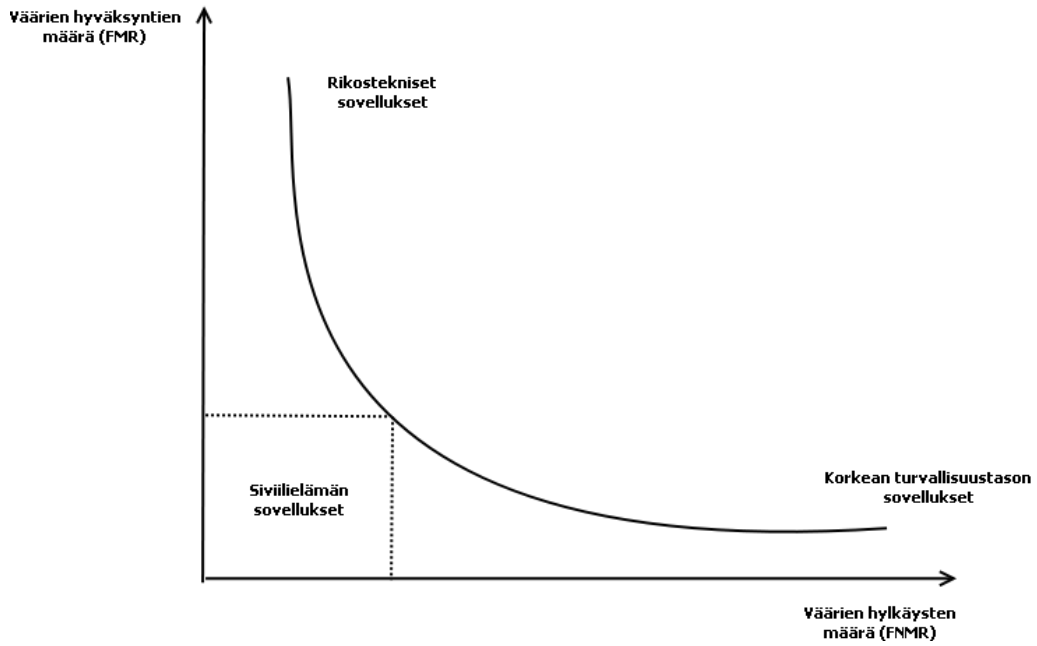
Kuva 3.2: Biometrisen järjestelmän vaste. (Mukaillen [2].)

teet todetaan virheellisesti saman henkilön näytteiksi.

FNMR ja FMR ovat pohjimmiltaan hyväksymiskynnys t:n funktioita. Jos biometrisen tunnistusjärjestelmän suunnittelijat haluavat laskea hyväksymiskynnystä t saadakseen järjestelmästä paremmin syötteiden vaihtelua ja kohinaa sietävän, FMR kasvaa. Vastaavasti kynnystä t voidaan nostaa, jotta järjestelmästä saadaan turvallisempi, jolloin samalla FNMR kasvaa. [2]

Järjestelmän suorituskykyä voidaan mitata kaikkialla sen toiminta-alueella funktiolla ROC (engl. *Receiver Operating Charasteristic*). ROC määritellään FMR:n ja FNMR:n funktiona erilaisilla t:n arvoilla. Kuvasta 3.3 nähdään, että erityyppiset biometriset sovellukset ovat aina kompromisseja FMR:n ja FNMR:n suhteen.

Lisäksi biometrisen tunnistusjärjestelmän tarkkuutta voidaan mitata termeillä FTC (engl. *Failure To Capture*) sekä FTE (engl. *Failure To Enroll*). FTC on käyttökelpoinen vain, jos järjestelmän näytteenotto on automaattinen. Tällöin se kuvaa osuutta tilanteista, jolloin järjestelmä ei onnistu ottamaan näytettä sille esitetystä biometrisesta ominaisuudesta. Näin tapahtuu usein, jos järjestelmä ei pysty havaitsemaan riittävän laadukasta biometrista signaalia, kuten tilanteessa, jossa kohteen kasvot ovat peitetyt. FTE puolestaan kuvaa tilannetta, jossa käyttäjä ei voi rekisteröityä tunnistusjärjestelmään. FTE on kompromissi



Kuva 3.3: Receiver Operating Charasteristic Curve. (Mukaillen [2].)

järjestelmällä saavutetun tarkkuuden suhteen eli FMR:n ja FNMR:n suhteen. Tämä saattaa tapahtua, kun järjestelmä hylkää sille esitetyn huonolaatuisen näytteen. Sen takia halutaan, että järjestelmän tietokantaan tallennetaan vain hyvälaatuisia mallinteita, jotta järjestelmän tarkkuus paranee. [10]

Koska kaikki edellä esitetyt, tarkkuutta ja virheitä kuvaavat termit ovat toisistaan riippuvia, ne muodostavat tärkeät ohjearvot biometriselle järjestelmälle, ja ne pitäisi ilmoittaa järjestelmän suorituskykyä arvioitaessa [2].

3.4 Usean biometriikan käyttö

Käytännön sovelluksissa useimmat biometriset tunnistusjärjestelmät ovat *unimodaalisia* (engl. *unimodal*) eli yhden menetelmän järjestelmiä. Tämä tarkoittaa, että ne käyttävät hyväkseen vain yhtä tietolähdettä tunnistusprosessissa, esimerkiksi saman henkilön yhtä sormenjälkeä tai yhtä kasvokuvaa. Yhden menetelmän järjestelmillä on kuitenkin useita erilaisia vajavaisuuksia ja rajoitteita [41]:

Häiriöt eli kohina havainnoissa. Esimerkiksi vilustumisen aiheuttama muutos äänessä tai arpi sormenpäässä aiheuttavat kohinaa havaintoihin. Myös vikaantunut tai huoltamaton sensori, esimerkiksi sormenjälkisensoriin kerääntynyt, lika voi aiheuttaa kohinaa. Samoin epätyydyttävät olosuhteet, kuten huono valaistus kasvokuvaa otettaessa, saattaa aiheuttaa häiriöitä.

Luokkien sisäiset vaihtelut. Aikaisemmin kerätty vertailuaineisto eroaa aina tunnistustilanteessa kerätystä datasta. Henkilö voi olla vuorovaikutuksessa väärällä tavalla sensorin kanssa, esimerkiksi väärässä asennossa kameran suhteen kasvokuvaa otettaessa.

Luokkien väliset samankaltaisuudet. Jokin piirre voi olla liian samankaltainen tietyn ihmisryhmän keskuudessa. Esimerkiksi käden geometrian ja kasvojen tunnistuksessa eniten käytettyjen erottelevien tekijöiden lukumäärä on vain suuruusluokkaa 10^5 ja 10^3 [50].

Harvinaisuus. Biometrinen järjestelmä ei välttämättä kykene saamaan merkitsevää dataa joltakin käyttäjäryhmältä. Esimerkiksi sormenjälkien pienet yksityiskohdat, harjanteet, eivät erotu kaikilla henkilöillä selvästi.

Huijausyritykset. Varsinkin käyttäytymiseen perustuvat tunnistusjärjestelmät ovat alttiita huijausyrityksille, esimerkiksi nimikirjoituksen tai äänen tunnistavat järjestelmät. Kuitenkin myös fysiologisia järjestelmiä on mahdollista huijata.

Joitakin unimodaalisten järjestelmien vajavaisuuksia voidaan parantaa, kun käytetään useampia tietolähteitä tunnistusprosessissa. Tällaisia biometrisia järjestelmiä kutsutaan *multimodaalisiksi* (engl. *multimodal*) järjestelmiksi. Näiden järjestelmien oletetaan olevan myös luotettavampia kuin unimodaaliset järjestelmät. [41] Multimodaaliset järjestelmät esimerkiksi poistavat harvinaisen piirteen ongelman käytettäessä useampaa erilaista piirrettä. Tunnistusjärjestelmää on myös vaikeampi huijata useammalla biometrisella tunnisteella samanaikaisesti. Lisäksi voidaan hyödyntää niin sanottua *haaste / vaste* -menetelmää (engl.

challenge – response), jolloin järjestelmä esimerkiksi pyytää käyttäjää esittämään satunnaisen biometrisen tunnisteen. Tällöin voidaan varmistaa, että käyttäjä on todella elävä ihminen (engl. *liveness detection*).

Multimodaalisen biometrisen järjestelmän käytössä on useita mahdollista skenaarioita riippuen käytettävissä olevista ominaispiirteiden ja sensorien määrästä [51, 41]:

Useita eri sensoreita samalle ominaispiirteelle. Otetaan esimerkiksi sormenjälki samasta sormesta kahdella erilaisella sormenjälkitunnistimella tai sekä kaksi- että kolmiulotteinen kuva kasvoista.

Useita yksiköitä samalle menetelmälle. Otetaan esimerkiksi sormenjälkiä kahdesta tai useammasta sormesta tai esimerkiksi kuva molemmista iiriksistä, mutta samalla sensorilla.

Useita erilaisia biometrisia menetelmiä. Käytetään esimerkiksi sormenjälkeä ja kasvontunnistusta samanaikaisesti.

Useita näytteitä samasta biometriikasta. Otetaan kaksi tai useampi sormenjälki samasta sormesta tai useampia kasvokuvia samasta henkilöstä.

Useita esityksiä ja tunnistusalgoritmeja samasta ominaispiirteestä. Esimerkiksi samasta sormenjälkikuvasta tutkitaan eri yksityiskohtia.

Tässä luvussa esiteltiin ensin biometrisen tunnistusjärjestelmän perusperiaate, joka on kaikille järjestelmille yhteinen. Tämän jälkeen tutustuttiin biometristen tunnisteiden ominaisuuksiin, joilla on vaikutusta niiden soveltuvuuteen käytettäväksi tietyssä biometrisessa sovelluksessa. Seuraavaksi käsiteltiin biometrisen järjestelmän suorituskykyyn vaikuttavia tekijöitä. Lopuksi tutustuttiin usean biometriikan käyttöön, minkä avulla voidaan parantaa biometrisen järjestelmän suorituskykyä.

Luku 4

Tietosuoja ja tietoturva

Biometriset tunnistusjärjestelmät tarjoavat useita etuja verrattuna muihin autentikointijärjestelmiin. Siksi niiden käyttö kasvaa koko ajan, mutta samalla täytyy kiinnittää erityistä huomiota siihen, että järjestelmät sietävät mahdollisesti niihin kohdistuvia hyökkäyksiä.

Seuraavissa alaluvuissa esitellään ensin yleisluonteisen biometrisen järjestelmän mahdollisia hyökkäyskohteita. Tämän jälkeen syvennytään biometrisen järjestelmän hyökkäysvektoreihin, uhkatekijöihin sekä uhkavektoreihin. Lopuksi esitellään mahdollisuuksia edellä mainituilta hyökkäysvektoreilta suojautumiseen.

4.1 Biometrisen järjestelmän haavoittuvuuksia

Yleispätevän biometrisen tunnistusjärjestelmän voidaan nähdä vastaavan hahmontunnistusjärjestelmää. Sen vaiheet on esitetty yksinkertaistettuna kuvassa 4.1.

Ratha et al. mallin [3] mukaisia biometrisen järjestelmän mahdollisia hyökkäyskohteita ovat kuvassa 4.1 esitetyt kahdeksan kohdetta:

1. Väärennetyn biometrisen tunnisteen esittäminen sensorille.

2. Uudelleenesityshyökkäys, jossa aiemmin tallennettu tunniste esitetään järjestelmälle

ohittaen sensori.

3. Piirteenirrotusvaiheen ohitus, jolloin se saadaan tuottamaan hyökkääjän haluamia mallinteita.

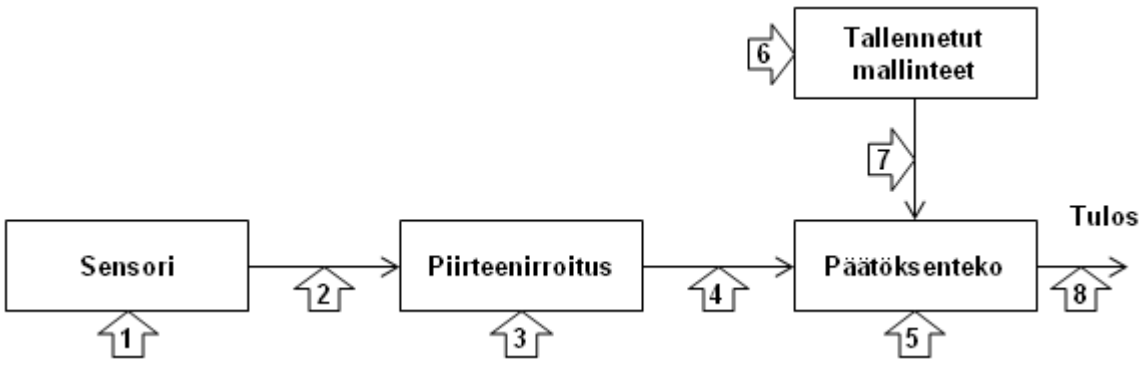
4. Väärennetty mallinne esitetään päätöksentekomoduulille.

5. Päätöksentekovaiheen huijaus, jolloin se saadaan tuottamaan hyökkääjän haluamia vastineita.

6. Tallennettujen mallinteiden muuntelu tai vaihtaminen vääriin.

7. Hyökkäys tallennettujen mallinteiden ja päätöksentekovaiheen väliseen väylään, mallinteiden muuntelu tai vaihtaminen vääriin.

8. Lopullisen tuloksen muuntelu.



Kuva 4.1: Yleisluonteisen biometrisen järjestelmän mahdollisia hyökkäyskohteita. (Mukaillen [3].)

4.2 Hyökkäysvektorit

Hyökkäysvektori (engl. *attack vector*) on kanava, mekanismi tai polku, jota käyttämällä hyökkääjä hyökkää biometrista järjestelmää vastaan tai yrittää kiertää sen suojaukset. *Huijaus* (engl. *spoofing*) tarkoittaa toimintaa, jossa hyökkääjä esittää järjestelmälle artefaktin, väärennettyä dataa tai biometriikkaa, jonka se väittää olevan aitoa yrittäessään kiertää

biometrisen järjestelmän suojaukset. Järjestelmän *haavoittuvuus* (engl. *vulnerability*) on suunnitteluvirhe tai ominaisuus, jonka takia järjestelmän turvallisuus on heikentynyt. Se luo mahdollisuuden hyväksikäyttää tai hyökätä biometrista järjestelmää vastaan. [13]

Biometriikoita käytetään enenevissä määrin turvallisuus- ja autentikointitarkoituksissa, mikä on luonut merkittävästi kiinnostusta aiheeseen informaatioteknologian eri osa-alueilla. Kiinnostus on kasvanut myös tutkimuksessa löytää menetelmiä kiertämään ja vaarantamaan biometrisia järjestelmiä. Kuten kaikkia turvallisuusjärjestelmiä myös biometrisia järjestelmiä on yritetty kiertää yhtä kauan kuin niitä on ollut käytössä. Turvallisuusjärjestelmien suunnittelu voi olla haastavaa. Siksi on tärkeää arvioida järjestelmän suorituskykyä ja turvallisuutta, jotta voidaan tunnistaa ja suojautua uhkia, hyökkäyksiä ja hyödynnettäviä heikkouksia vastaan. Murtautumiset biometrisiin järjestelmiin on yleisimmin saavutettu hyväksikäyttämällä jotakin järjestelmän heikkoutta. Tämä tarkoittaa muun muassa heikkoa fyysistä suojausta, joka on edelleen helposti hyödynnettävä hyökkäysvektori. Usein tällaisia heikkouksia ei ollut edes otettu huomioon tai ne oli arvioitu epätodennäköisiksi järjestelmää suunniteltaessa ja hallinnoitaessa. [13]

Biometrisiin järjestelmiin kohdistuvia hyökkäyksiä on olemassa kolme eri ulottuvuutta, joita jokaista käsitellään seuraavassa erikseen. Näitä ovat *uhkatekijät* (engl. *threat agents*), *uhkavektorit* (engl. *threat vectors*) ja *järjestelmän haavoittuvuudet* (engl. *system vulnerabilities*). [13]

4.2.1 Uhkatekijä

Uhkatekijä on henkilö, joka tarkoituksellisesti tai muuten pyrkii vaarantamaan biometrisen järjestelmän turvallisuuden. Nämä on jaoteltu kolmeen eri luokkaan [13]:

1. *Huijari*: (engl. *impostor*) henkilö, joka tarkoituksellisesti tai muuten käyttäytyy kuten luvallinen käyttäjä. Huijari voi olla luvallinen tai luvaton käyttäjä.

2. *Hyökkääjä*: (engl. *attacker*) henkilö, joka yrittää vaarantaa biometrisen tunnistuslaitteen tai -järjestelmän turvallisuuden. Motiivina voi olla luvaton sisäänpääsy tai

palvelunestohyökkäys.

3. *Luvallinen käyttäjä*: (engl. *authorised user*) henkilö, jolla on lupa käyttää biometrista järjestelmää, mutta joka voi tahattomasti vaarantaa biometrisen tunnistuslaitteen tai -järjestelmän turvallisuuden. Tähän lukeutuvat tahattomat ja inhimilliset virheet, kuten järjestelmän ylläpitäjän virheet järjestelmää konfiguroitaessa.

Uhkatekijöillä on yleensä enemmän tai vähemmän teknistä taitoa, mutta yksityiskohtaisesti järjestelmän tuntevat henkilöt ovat suurempi turvallisuusriski. Uhkatekijöiden tuntemisesta on hyötyä kehitettäessä tehokkaita suojautusmenetelmiä näitä vastaan. Luvalliset käyttäjät ja järjestelmän tuntevat henkilöt ovat jopa suurempi uhka kuin luvattomat käyttäjät. Luvallisia käyttäjiä saatetaan uhkailla ja kiristää tai lupaamalla näille palkkio. Luvaton käyttäjä yrittää saada pääsyn biometriseen järjestelmään. [13]

4.2.2 Uhkavektorit

Uhkavektorit ovat kohteita, joissa biometrista järjestelmää vastaan voidaan hyökätä. Cukic ja Bartlow [14] laajensivat ja lisäsivät Rathan malliin [3] uhkavektoreita. Seuraavassa esitellään nämä uhkavektorit Robertsin [13] mukaan:

1. **Palvelunestohyökkäys** (engl. *Denial of Service, DoS*) Palvelunestohyökkäyksellä pyritään vioittamaan tai lamauttamaan biometrinen tunnistusjärjestelmä niin, ettei se ole käytettävissä. Yksinkertaisimmillaan järjestelmää voidaan vahingoittaa fyysisesti tai aiheuttamalla sähkökatkos. Järjestämällä epäsuotuisat olosuhteet, kuten lämpöä, valoa ja pölyä, voidaan sensorien toimintaa vaikeuttaa ja täten kerättävän datan laatua heikentää. Myös kohdistamalla sensoreihin sähkökenttä tai radioaaltoja voidaan järjestelmän toimintaa häiritä. Esimerkiksi optisia sensoreita voidaan häiritä vilkkuvilla valoilla, sensorien päälle voidaan kaataa nestettä tai aiheuttaa staattisen sähkön purkauksia sensoreihin.

Palvelunestohyökkäykset ovat yleensä sen verran huomiotaherättäviä, että ne havaitaan nopeasti. Toisaalta joissakin tapauksissa onkin tarkoituksena, että hyökkäys huomataan, jolloin aiheutetaan sekaannusta ja järjestelmän on siirryttävä vaihtoehtoiseen tai poikkeustoimintatilaan. Nämä harvoin käytettävät vaihtoehtoiset toimintatilat ovat useimmiten normaalia toimintatilaa haavoittuvampia, ja ne ovat itsessään uhkavektoreita.

2. **Väärennetty ilmoittautuminen** (engl. *False enrollment*) Biometrisen datan tarkkuus perustuu laillisiin ilmoittautumisiin. Jos identiteetti on väärennetty, ilmoittautumiseen käytetty data on oikeanlaista biometrista dataa, mutta identiteetti vastaa väärää henkilöä. Tätä uhkavektoria on käytetty esimerkiksi väärennetyissä passeissa.

3. **Väärenetty fyysinen biometriikka** (engl. *Fake physical biometric*) Ehkä eniten huomiota saanut uhkavektori on väärennetyn fyysisen biometriikan käyttö tarkoituksena huijata biometrista tunnistusjärjestelmää. Tällainen hyökkäys on suhteellisen helppo toteuttaa olemattomalla tai vähäisellä järjestelmän tuntemisella. Väärän biometriikan tekemiseen tarvittavat materiaalit ovat halpoja ja helposti saatavilla. Toisekseen nämä hyökkäykset tehdään järjestelmän fyysisessä rajapinnassa, jolloin järjestelmän digitaalisista suojauksista, kuten tiedon salauksesta tai digitaalisita allekirjoituksista ei ole hyötyä. Näille hyökkäyksille ovat alttiina muun muassa sormenjälkeen, kämmeneen ja iirikseen perustuvat biometriset järjestelmät.

   Alkuperäinen biometrinen tunniste voidaan saada haltuun melko helposti monista lähteistä, joko luvallisesti ja kohdehenkilön avustuksella tai luvattomasti. Ihminen jättää biometrisia jälkiään, kuten sormen- ja kädenjälkiä, esimerkiksi oviin, pöytiin ja moniin muihin esineisiin. Lisäksi tarkkojen kuvien otto ja äänentallennus on yksinkertaista digitaalisten laitteiden avulla.

4. **Väärennetty digitaalinen biometriikka** (engl. *Fake digital biometric*) Näitä on kahta tyyppiä:

(a) *Naamioitu hyökkäys.* Tällöin järjestelmälle esitetään yleisesti saatavilla olevaa biometrista dataa, kuten digitaalisia kasvokuvia tai digitoituja piileviä sormenjälkiä.

(b) *Referenssijoukon uudelleenesitys.* Nämä hyökkäykset kohdistuvat biometrisen tunnistusjärjestelmän sisälle, jolloin digitaalisten suojausten käyttö niitä vastaan on tehokkaampaa. Hyökkääjä tarvitsee enemmän tietoa järjestelmästä ja yleensä pääsyn sen sisälle.

5. **Piilevän jäljen uudelleenaktivointi** (engl. *Latent print reactivation*) Tämä uhkavektori on ominainen sormenjälki- ja kämmenenjälkiskannereille. Biometriseen sensoriin jää jälkiä ihon erittämästä hiestä ja rasvasta. Nämä piilevät jäljet voidaan kopioida tai uudelleenaktivoida lukukelposiksi jäljiksi käyttäen apuna esimerkiksi puutereita tai höyryjä tai asettamalla lämmintä vettä sisältävä muovipussi jäljen päälle.

6. **Jälkien uudelleenkäyttö** (engl. *Reuse of residuals*) Joidenkin biometristen laitteiden ja järjestelmien paikalliseen muistiin jää tiedot muutamasta edellisestä sen irrottamasta biometrisesta piirteestä ja käytetystä mallinteesta. Jos hyökkääjä pääsee käsiksi tähän dataan, sitä voi olla mahdollista uudelleenkäyttää ja muodostaa laillinen biometrinen tunniste. Tätä uhkaa vastaan voidaan puolustautua tyhjentämällä järjestelmän muisti ja estämällä sitä käyttämästä monta kertaa peräkkäin identtisiä näytteitä.

7. **Uudelleenesityshyökkäys / väärän datan ujutus** (engl. *Replay attack / false data injection*) Nämä ovat luonteeltaan *epärehellisen välittäjän* eli *mies välissä* -hyökkäyksiä (engl. *man-in-the-middle attack*). Järjestelmälle esitetty biometrinen data kaapataan ja esitetään uudelleen. Vaihtoehtoisesti väärennetty biometrinen data ujutetaan sensorin ja datan prosessointijärjestelmän väliin. Useimmiten hyökkääjän täytyy päästä fyysisesti käsiksi järjestelmään. Jos mallinteet on tallennettu esimerkik-

si etäluettaville korteille, data on monissa tapauksissa salaamattomassa muodossa, jolloin datan kaappaaminen on helppoa myöhempää käyttöä varten.

Uudelleenesityshyökkäys on kaksi- tai kolmivaiheinen: ensiksi sensorin lähettämä signaali kaapataan tai kopioidaan, seuraavaksi dataa mahdollisesti muunnetaan ja lopuksi signaali esitetään uudelleen. Lähetyksen salaaminen lisää turvallisuutta, koska kaapattu signaali täytyy ensin purkaa, sitten muunnella ja vielä salata uudelleen. Salatun datan purkaminen ja uudelleensalaaminen voi olla hyökkääjälle haastavaa ja vaatia erikoistuneita työkaluja ja teknistä osaamista.

8. **Synteettinen ominaisvektori** (engl. *Synthesised feature vector*) Väärennettyä biometriikkaa esittävä datavirta ujutetaan järjestelmään. Yksi keino luoda hyväksyttävää dataa on Jain et al. mukaan [15] niin sanottu *hill climbing* -hyökkäys. Tämän hyökkäyksen tapauksessa toistuvasti muunnetaan väärennettyä dataa säilyttäen vain ne muutokset, jotka parantavat pistelukua, kunnes riittävä pisteluku on saavutettu ja biometrinen tunnistusjärjestelmä hyväksyy sille esitetyn väärennetyn datan. Tämä tekniikka edellyttää, että hyökkääjällä on pääsy järjestelmän pistelukuihin ja tietoliikenteeseen.

9. **Piirteenirrotuksen ohittaminen** (engl. *Override feature extraction*) Tämä hyökkäys kohdistuu piirteenirrotusrutiineihin yrittämällä manipuloida tai tarjoamalla väärennettyä dataa jatkokäsittelyä varten. Hyökkäystä voidaan käyttää myös vaurioittamaan järjestelmää ja aiheuttamaan palvelunestohyökkäyksen. Tämä toteutetaan usein hyökkäämällä biometrisen järjestelmän ohjelmistoa tai *laiteohjelmistoa* (engl. *firmware*) vastaan.

10. **Järjestelmän parametrien ohitus / muutos** (engl. *System parameter override / modification*) Tällä hyökkäysvektorilla muutetaan väärien hyväksyntien määrää (engl. *false acceptance rate, FAR*), väärien hylkäysten määrää (engl. *false rejection rate, FRR*) tai muita biometrisen järjestelmän olennaisia parametreja. Jos hyökkääjä

pääsee manipuloimaan FAR:a, järjestelmä voidaan saada hyväksymään heikkolaatuista tai väärennettyä dataa. Esimerkiksi Yhdysvaltain puolustusministeriö (engl. *United States Department of Defense, DoD*) suosittaa ohjeissaan [16], että FAR olisi pienempi kuin 1:100 000 ja FRR olisi pienempi kuin 5:100 liittovaltion biometrisissa järjestelmissä.

11. **Vertailun ohitus / väärennetty vertailu** (engl. *Match override / false match*) Tällä uhkavektorilla voidaan hyökätä ohjelmistoa, laiteohjelmistoa tai järjestelmän asetuksia ja parametreja vastaan. Piirteiden vertailuvaiheessa mallinteet ovat yleensä salaamattomia, mikä altistaa ne helpommin manipuloinnille. Vertailun tulos voidaan ohittaa tai jättää huomioimatta ja korvata väärennetelyllä osumalla. Järjestelmän luvalliset käyttäjät eivät todennäköisesti huomaa poikkeavaa toimintaa, jos järjestelmä hyväksyy edelleen heidän kirjautumisensa järjestelmään.

12. **Tallennuskanavan salakuuntelu ja datan ujutus** (engl. *Storage channel intercept and data inject*) Tällä hyökkäyksellä voi olla merkittävimmät seuraukset, koska sillä voidaan hyökätä prosessointijärjestelmää ja kaikkea tallennettua dataa vastaan. Jos hyökkääjällä on pääsy järjestelmään, muisti on helppo kohde, koska säilytettävät mallinteet ovat kooltaan pienempiä ja tiedostot ovat yksinkertaisempia kuin käsittelemätön biometrinen data. Hyökkääjä voi esimerkiksi kaapata laillisia mallinteita myöhempää käyttöä varten ja ujuttaa järjestelmään väärennettyjä mallinteita. Tällainen on ihanteellinen tapa suorittaa aiemmin mainittu hill climbing -hyökkäys. Onnistunut hyökkäys vaatii yleensä tarkkaa järjestelmän ja mallinteiden tuntemusta.

13. **Mallinteiden luvaton muuntelu** (engl. *Unauthorised template modification*) Mallinteita voidaan tallentaa biometriseen lukijaan, sensoriin, kulkukortille tai itse järjestelmään. Tässä hyökkäysvektorissa luvattomat muutokset tehdään siinä vaiheessa, kun järjestelmä on modifioimassa, vaihtamassa tai lisäämässä mallintei-

ta järjestelmään. Lisäämällä luvattomia mallinteita järjestelmään voidaan ohittaa virallinen mallinteen rekisteröinti. Oikeat mutta luvattomat biometriikat voidaan esittää järjestelmälle, ja järjestelmä käsittelee ne luvallisten mallinteiden mukana. Palvelunestohyökkäys voidaan tehdä vioittamalla mallinteiden dataa tai assosioimalla käyttäjät muunneltuihin mallinteisiin. Palvelunestohyökkäyksen aiheuttama järjestelmän vioittuminen, järjestelmän toimintahäiriö tai ylläpidon virhe voivat myös vioittaa mallinteita. Mallinteiden vioittuminen voi heikentää järjestelmän identifiointi- tai autentikointikykyä.

14. **Mallinteiden jälleenrakennus** (engl. *Template reconstruction*) Vastaavasti kuten ominaisvektoreiden syntetisoinnissa myös tässä hyökkäyksessä käytetään hill climbing -tekniikkaa hyväksyttävän datan luomiseen. Mallinteiden jälleenrakennuksessa voidaan hyödyntää tiedostojärjestelmästä etsittäviä tiedostojen palasia, joiden avulla luodaan väärennettyjä mallinteita. Myös tämä hyökkäys vaatii pääsyn järjestelmän muistiin.

15. **Päätöksen ohittaminen / väärä hyväksyminen** (engl. *Decision override / false accept*) Tässä hyökkäyksessä ohitetaan kaikki datan prosessointivaiheet ja päätöksentekovaihe tai ujutetaan väärennetty hyväksyminen järjestelmän ja sen ohjaaman laitteen, esimerkiksi oven tai pankkiautomaatin väliin. Tarkoituksena on saada järjestelmä hyväksymään käyttäjä kaikissa tilanteissa. Tämän hyökkäyksen aikaansaaminen voi vaatia järjestelmän fyysistä käsittelemistä.

16. **Kulkulupien muuntelu** (engl. *Modify access rights*) Kulkulupien luvaton muuntelu voi aiheuttaa palvelunestohyökkäyksen, kun laillisia kulkuoikeuksia rajoitetaan. Vaihtoehtoisesti se murtaa turvallisuuden, kun kulkuoikeuksia lisätään. Tällainen hyökkäys toteutetaan yleensä hankkimalla järjestelmän ylläpitäjän oikeudet ja muuttamalla käyttäjien oikeuksia tai muita järjestelmän parametrejä.

17. **Järjestelmien yhteydet** (engl. *System interconnections*) Järjestelmien väliset yhtey-

det aiheuttavat lisäksi vielä ainakin kaksi uhkavektoria: luvattoman ulkopuolisen pääsyn järjestelmään sekä järjestelmän vaarantumisen. Jos toisiinsa kytkettyjen järjestelmien turvallisuus on vaarantunut, siitä muodostuu uhkavektori biometriselle järjestelmälle. Myös järjestelmien välinen kommunikointikanava on altis uhille. Usein biometrisen järjestelmän operaattorilla on vähän vaikutusmahdollisuuksia ulkoisten järjestelmien toimintaan.

4.2.3 Järjestelmän haavoittuvuudet

Biometrisen järjestelmän suunnittelussa, arkkitehtuurissa, tuotannossa tai käyttöönotossa tapahtuvat virheet voivat aiheuttaa järjestelmään haavoittuvuuksia. Joissakin tapauksissa biometriseen järjestelmään liitetyt toissijaiset järjestelmät voivat olla alttiita hyökkäyksille ja samalla vaarantaa itse biometrisen järjestelmän turvallisuuden. Seuraavat kohteet ovat erityisen alttiita haavoittuvuuksille [13]: käyttöjärjestelmät, tallennusjärjestelmät, biometriset sovellukset, sensorien ohjelmistot sekä laitteistot ja laiteohjelmistot.

Muita haavoittuvia kohteita ovat järjestelmän toiminnanhallinta, etähallinta ja järjestelmän konfigurointi. Luetellut haavoittuvuudet ovat verrattavissa myös muiden teknisten järjestelmien haavoittuvuuksiin. Järjestelmän haavoittuvuudet voivat mahdollistaa järjestelmän vaarantumisen ja vaikutukset voivat olla samanlaisia kuin uhkavektoreissakin.

4.3 Hyökkäysvektoreilta suojautuminen

On olemassa lukuisia menetelmiä minimoimaan riskejä, joita uhkatekijät, uhkavektorit ja haavoittuvuudet aiheuttavat. Puolustusmenetelmät ovat toisiaan täydentäviä, eikä turvallisuuden pitäisi perustua vain yhteen menetelmään. Menetelmät voidaan jakaa kuuteen eri luokkaan [18, 16], joissa kussakin on on useita käyttökelpoisia menetelmiä. Seuraavassa esitellään näitä puolustusmenetelmiä Robertsin [13] mukaan.

1. **Haaste / vaste** (engl. *Challenge / Response*) Haaste / vaste tarkoittaa tekniikkaa,

jossa toinen osapuoli asettaa kysymyksen eli ”haasteen” ja toisen osapuolen täytyy antaa hyväksytty vastaus eli ”vaste”, jotta autentikointi voidaan suorittaa. Yksinkertaisin esimerkki tästä on salasana-autentikointi, jossa haaste on kysyttävä salasana ja hyväksyttävä vastaus on oikea salasana. Haaste / vaste -autentikointia käytetään nykyään hyvin laajasti erilaisissa verkkopalveluissa, kuten internetpankeissa.

Biometrisiin järjestelmiin sovellettuna haaste voidaan liittää johonkin muuhun suojuautumismenetelmään, kuten elävyyden tunnistukseen. Tällöin käyttäjä voidaan haastaa esimerkiksi toistamaan jokin lause, nyökkäämään päätään, räpyttämään silmiään tai asettamaan tietty sormi sensorille. Haaste / vaste -tekniikkaa voidaan käyttää myös järjestelmän muiden komponenttien välillä. Tämä tekniikka voi olla tehokas datan uudelleenesitys- ja väärän datan ujutushyökkäyksiä vastaan, varsinkin jos hyökkäyksen kohteena ovat etäällä olevat sensorit, muisti tai muut järjestelmän fyysisesti erillään olevat komponentit.

2. **Syötetyn biometrisen datan satunnaistaminen** (engl. *Randomising input biometric data*) Edellä esitetyn haaste / vaste -tekniikan muunnos, jossa käyttäjältä vaaditaan ilmoittautuessa useamman biometrisen näytteen antamista, kuten useita sormenjälkiä. Tunnistusvaiheessa järjestelmä satunnaistaa pyydettävän näytteen, jolloin kiertämisyritykset vaikeutuvat. Tällaisessa järjestelmässä saatetaan vaatia myös useaa eri biometrista tunnistetta, jolloin järjestelmän huijaaminen vaikeutuu entisestään. Tällä menetelmällä voidaan suojautua myös esimerkiksi piilevien sormenjälkien uudelleenesitystä vastaan.

3. **Datan säilyttäminen** (engl. *Retention of data*) Biometrisen järjestelmän sensorit ovat yleensä helpommin fyysisesti saavutettavissa kuin muut järjestelmän komponentit, joten ne ovat siksi hyökkäyksille alttiimpia. Jotkin sensorit säilyttävät paikallisesti mallinteiden kopioita, jolloin ne ovat hyökkääjiä kiinnostavia kohteita. Useimmissa järjestelmissä varsinainen tunnistedata hylätään mallinteen luonnin jälkeen. Kuiten-

kin tunnistedatan säilyttäminen voi auttaa huijausyritysten selvittämisessä, vaikkakin se lisää järjestelmän monimutkaisuutta muistin suojaamisen osalta. Tyhjentämällä data ja puskurimuistit voidaan suojautua mies välissä -hyökkäyksiä vastaan, jolloin huijarin täytyy luoda dataa, joka vaikuttaa biometriseltä datalta sekä ihmisen että järjestelmän mielestä.

4. **Elävyyden tunnistus** (engl. *Liveness detection*) Huijausten havaitsemisessa elävyyden tunnistamisella on tärkeä merkitys varmistaa, että sensorille esitetty biometrinen tunniste on elävältä henkilöltä, eikä se ole keinotekoinen tai peräisin ruumiilta. Jotkin menetelmät hyödyntävät haaste / vaste -tekniikkaa, ja toiset menetelmät toimivat itsenäisesti. Elävyyden tunnistus voidaan liittää sensoriin tai toteuttaa erillisellä laitteella. Näitä menetelmiä ovat seuraavat:

   (a) Sormen hikijälkien mittaus.

   (b) Happisaturaation mittaus sormesta valon avulla.

   (c) Ihon spektroskopia, jossa mitataan valon absorptiota.

   (d) Iiriksen photoninen ja spektrografinen mittaus.

   (e) Lämmön mittaus.

   (f) Pään, kasvojen, silmän ja pupillin liikkeen mittaus.

   (g) Huulten liikkeen ja äänen synkronismin mittaus.

   (h) Kolmiulotteinen piirteiden mittaus.

   (i) Tulosteen ja painomusteen tunnistus.

   Kolmiulotteisen piirteiden mittauksen on katsottu parantavan järjestelmän suorituskykyä esimerkiksi kasvojen asennon ja ilmeiden muuttuessa sekä ympäristöolosuhteiden, kuten valaistuksen ja lämpötilan vaihdellessa. [19] Kolmiulotteisuus lisää kerättävän datan määrää, ja varsinkin kasvontunnistuksessa se vaikeuttaa huijaamista merkittävästi.

5. **Useampi biometriikka** (engl. *Multiple biometrics*) Useamman biometriikan käyttö lisää käsittelyaikaa ja monimutkaisuutta, jos samalla kertaa vaaditaan esimerkiksi sormenjäljen ja iiriksen tunnistusta. Useampaa ja erilaista biometriikkaa on selvästi vaikeampi huijata. Kuitenkin myös järjestelmä monimutkaistuu esimerkiksi useamman sensorin käytön takia.

6. **Multimodaalinen biometriikka** (engl. *Multi-modal biometrics*) Multimodaalisessa tunnistamisessa samasta piirteestä otetaan useampi näyte tai useampi piirre yhdistetään uuteen mallinteeseen. Sama sensori voi ottaa useamman näytteen, tai voidaan käyttää useita sensoreita. Pisteluku voidaan laskea yksinkertaisesti keskiarvona tai painotettuna keskiarvona. Pisteluvut voidaan laskea myös erikseen ja käyttää äänestystekniikkaa ratkaisemaan pisteluku. Multimodaalinen tunnistaminen voi lisätä datan laatua, tarkuutta ja oikeellisuutta ja siten auttaa torjumaan huijaamisessa. Samalla kuitenkin laskentatehon tarve kasvaa ja järjestelmä monimutkaistuu.

7. **Useampitekijäinen autentikointi** (engl. *Multi-factor authentication*) Biometrisen tunnisteen lisäksi voidaan käyttää samanaikaisesti esimerkiksi kulkukorttia, polettia, PIN-koodia tai salasanaa. Tämä voi kuitenkin lisätä järjestelmän vaatimaa käsittelyaikaa ja vähentää järjestelmän käytettävyyttä. Tällaisen tunnistusjärjestelmän kiertäminen vaatii siis molempien tunnistustekijöiden ohittamista. Järjestelmään voidaan yhdistää myös haaste / vaste -tekniikka, mikä vaikeuttaa entisestään hyökkäysyrityksiä.

8. **Pehmeät biometriikat** (engl. *Soft biometrics*) Niin kutsutut pehmeät biometriikat ovat ominaisuuksia, jotka eivät yksinään ole tarpeeksi erikoislaatuisia erottaakseen henkilöt toisistaan, mutta yhdessä varsinaisten biometriikoiden kanssa ne riittävät tarkkaan tunnistukseen. Tällaisia piirteitä, joita myös ihmiset käyttävät luonnostaan toistensa tunnistamiseen, ovat esimerkiksi ikä, sukupuoli, pituus, paino, silmien väri, etnisyys sekä huomattavat arvet ja tatuoinnit. Nämä ominaisuudet voivat auttaa

huijausyritysten estämisessä. Samalla järjestelmän suorituskyky voi parantua, jos tietokannan haut voidaan kohdistaa pienempään joukkoon [20].

9. **Signaalin ja datan eheys ja identiteetti** (engl. *Signal and data integrity and indentity*) Luotettava data on oleellinen osa järjestelmän eheyttä. Sensorilla luotavan datan on oltava oikeellista ja säilyttävä eheänä useiden prosessointivaiheiden läpi. Tämä on tärkeä puolustuskeino uudelleenesitys- ja mies välissä -hyökkäyksiä vastaan. Puolustustekniikoita ovat muun muassa seuraavat:

   (a) Lisätään aikaleima sensorilta saatuun dataan. Aikaleima voi paljastaa vanhan tai uudelleenesitetyn datan käytön.

   (b) Digitaalisen allekirjoituksen käyttö.

   (c) Steganografian eli datan piilotuksen käyttö. Tärkeä data piilotetaan toisen datan sekaan, esimerkiksi sormenjäljen mallinne kasvokuvaan [15].

   (d) Vesileimojen käyttö esimerkiksi sormenjälkitunnistuksessa, jolloin tärkeä data piilotetaan vesileimoihin [21].

   (e) Asetetaan rajoituksia, montako tunnistautumissyritystä tai hylättyä tunnistusta sallitaan tietyssä ajassa.

10. **Salaus ja digitaalinen allekirjoitus** (engl. *Cryptography and digital signatures*) Datan salaus voi olla tehokas puolustuskeino datan sieppaus- ja ujutusyrityksiä vastaan. Digitaalisella allekirjoituksella voidaan suojata sekä prosessoitavaa että tallennettua dataa muutoksilta. Tällöin myös salausavainten suojaamiseen on kiinnitettävä huomiota.

11. **Mallinteen oikeellisuus** (engl. *Template integrity*) Koska biometrinen tunniste on mahdollista luoda mallinteesta hill climb -hyökkäystä käyttäen [15, 22], mallinteen oikeellisuus on tärkeää myös yksityisyydensuojan kannalta. Hill climb -hyökkäyksiltä voidaan suojautua kvantisoimalla osumatarkkuuden pistelukua. Tällöin

hyökkääjän on vaikeampi saada tietoa, kuinka paljon syötetyn kuvan osumatarkkuus on parantunut pienten muutosten jälkeen [23].

12. **Peruutettavat biometriikat** (engl. *Cancellable biometrics*) Biometrisille tunnisteille ominaista on niiden korvaamattomuus, ja jos ne on kerran saatu kaapattua, niitä ei voida enää käyttää. Kuitenkin alkuperäistä tunnistetta voidaan käyttää uudelleen menetelmällä, jota kutsutaan peruutettavaksi biometriikaksi [3]. Tässä menetelmässä esitettävää biometrista tunnistetta tarkoituksellisesti vääristetään joka kerta samalla tavalla. Muunnoksen on oltava sellainen, ettei sitä voida käänteistää. Vain muunnettu data tallennetaan, ja jos data on joutunut vääriin käsiin, voidaan tehdä uusi muunnos ja korvata alkuperäinen mallinne.

13. **Laitteiston eheys** (engl. *Hardware integrity*) Vahvistetaan, että data on peräisin sensorilta. Luodaan yksilöllinen tunniste laitteiston eri osille. Tyhjennetään sensorin paikallinen muisti sensorin keräämästä datasta ja luoduista mallinteista. Voidaan myös luoda autentikointi sensorin ja muun laitteiston välille ennen näiden välistä tiedonsiirtoa.

14. **Tietoverkon puhtaus** (engl. *Network hygiene*) Hyvin järjestetyt tietoverkon yhteyskäytännöt ovat tärkeä osa koko biometrisen järjestelmän turvallisuutta. Monet olemassa olevat teknologiset viitekehykset ja käytännöt ovat sovellettavissa myös biometrisiin järjestelmiin.

15. **Fyysinen turvallisuus** (engl. *Physical security*) Monet hyökkäysvektorit on helpompi toteuttaa, jos hyökkääjä pääsee fyysisesti käsiksi biometrisen järjestelmän johonkin osaan. Fyysisen turvallisuuden parantaminen on usein halvin ja tehokkain keino estää biometrisen järjestelmän huijausyritykset. Hyviä keinoja ovat sensoreille pääsyn rajoittaminen, tekninen valvonta ja vartijoiden käyttö. Kulunvalvonnan tarkkailu ja jo vartijoiden pelkkä läsnäolo voivat estää järjestelmään kohdistuvia hyökkäysyrityksiä. Järjestelmän säännöllinen toiminnan tarkastus ja laitteiden puh-

distaminen ovat myös tärkeitä. Sensorien puhdistamisella voidaan estää piilevien jälkien hyväksikäyttöä ja myös parantaa sensorien tarkkuutta.

Sensorien, käyttöpaneelien ja kaapeloinnin fyysinen suojaaminen lukitsemalla ja niihin kajoamisen havaitsevilla hälyttimillä on tärkeä osa turvallisuutta, samoin sensorien valvonta valvontakameroilla. Jos biometrista järjestelmää käytetään kulunvalvontaan, on tärkeää myös estää, ettei laillisesti kulkevan henkilön perässä pääse kukaan livahtamaan mukana, esimerkiksi asentamalla kääntöportit.

16. **Aktiivisuuden tallentaminen** (engl. *Activity logging*) Määrätietoinen hyökkääjä saattaa tiedustella tai yrittää hyökkäystä useiden päivien, jopa kuukausien ajan kerätäkseen tarpeeksi tietoa tehokasta hyökkäystä varten. Aktiivisuuden seurannalla ja käyttäytymisen tarkkailulla voidaan yrittää paljastaa tällainen tiedustelu tai hyökkäys. Myös tiedonsiirrossa tapahtuvia virheitä, sensorien lukuvirheitä ja toistuvia epäonnistuneita autentikointiyrityksiä on syytä tarkkailla.

17. **Menettelytavat** (engl. *Policy*) Turvallisuusjärjestelmien tärkeä viitekehitys on menettelytavat. Ilman selkeästi määriteltyjä menettelytapoja organisaation suuntaviivat voivat olla hukassa, turvallisuustoimenpiteet tehottomia ja ne toimivat odotettua huonommin. Toisaalta hyvät menettelytavat lisäävät turvallisuutta ja toimivat pelotteena epätoivottua, epäasiallista ja vahingollista toimintaa vastaan. On olemassa useita yleisesti hyväksyttyjä standardeja ja viitekehyksiä, jotka on luotu tietoturvan hallintaa varten.

18. **Sääntöjen noudattaminen** (engl. *Compliance checking*) Turvallisuuden arviointi ja sääntöjen noudattaminen ovat tärkeitä turvallisuuden ylläpitämisessä, tunnistettassa uhat ja mukauduttaessa jatkuvasti muuttuviin tekniikoihin sekä osoitettaessa lainsäädännön ja säännösten noudattamista.

Tässä luvussa esiteltiin ensin yleisluonteisen biometrisen järjestelmän mahdollisia hyökkäyskohteita. Tämän jälkeen syvennyttiin biometrisen järjestelmän hyökkäysvek-

toreihin, uhkatekijöihin sekä uhkavektoreihin. Lopuksi esiteltiin mahdollisuuksia edellä mainituilta hyökkäysvektoreilta suojautumiseen.

Luku 5

Yksityisyys

Tässä luvussa ja koko opinnäytetyössä tarkastellaan yksityisyyttä ja siihen liittyviä käsitteitä pääasiassa Suomen lainsäädännön näkökulmasta. Yksityiselämän suoja juontuu perustavanlaatuisesti Yhdistyneiden kansakuntien ihmisoikeuksien yleismaailmalliseen julistukseen.

Yksityisyys on yläkäsite, joka sisältää useita hyvin erilaisia tutkimusalueita ja käytännön tilanteita. Yleisesti ottaen yksityisyyden sanotaan olevan henkilökohtainen etu. Usein se ilmenee siten, että ihminen suojelee itseään, etteivät muut henkilöt tai organisaatiot puutu hänen vapauteensa. [25] Yksityisyys tarkoittaa myös muitakin kuin henkilökohtaisesti salassa pidettäviä asioita. Useat käsitykset salassapidosta väittävät, että kun salaisuus on kerran paljastunut, se on vapaasti julkisessa käytössä. Toisin sanoen, yksittäinen salaisuuden omistaja menettää kaikki vaateensa tiedon hallinasta. Toisaalta yksityisyyden vaatimukseen voi sisältyä myös muihin liittyvää tietoa tai toimintaa, esimerkiksi pankin hallinoimat pankkitilit tai lääkärin potilaalle määräämä lääkitys [25].

Yksityisyys on noussut yhä näkyvämmäksi puheenaiheeksi tietotekniikan kehittyessä. Julkiset tietoverkot, mobiililaitteet sekä video-, RFID- ja biometriset valvontajärjestelmät ovat saaneet ihmiset tiedostamaan enemmän yksityisyyden merkitystä ja toisaalta tuntemaan epävarmuutta. Näistä seuraavassa muutama esimerkki Nissenbaumin mukaan [57]:

Monet julkiset kuntien ja valtion viranomaisten laatimat asiakirjat ovat ennenkin olleet

julkisuuslain perusteella vapaasti nähtävillä. Kuitenkin näiden asiakirjojen siirtäminen tietoverkkoihin, jolloin ne ovat vieläkin helpommin saatavilla, on aiheuttanut epäluuloisuutta ja tyytymättömyyttä myös viranomaisten keskuudessa.

Useimmat ihmiset ovat tietoisia, että heidän asioidessaan kaupoissa siitä jää jälkiä. Asiakkaiden profilointi ja tiedon louhinta ovat suurta liiketoimintaa. Tietoja käytetään hyväksi muun muassa kehitettäessä mainontaa ja tuotevalikoimia. Usein ihmiset huolestuvat näiden tietojen keruusta, kun medioissa uutisoidaan asiasta. Kuitenkaan kerättävät tiedot eivät ole salaisia tai arkaluonteisia.

RFID- eli radiotaajuutta käyttäviä etätunnistustarroja käytetään muun muassa tuotteiden varastoinnin ja logistiikan seuraamisen, mutta myös varkauksien ja muun hävikin estämiseen. Jotkin ihmiset ovat näistä huolissaan, koska RFID-seurantaa voitaisiin käyttää heiltä lupaa kysymättä tai heidän tiedostamattaan, mutta yleensä näitä käytetään muutenkin kaikille julkisilla ja avoimilla alueilla.

Seuraavissa alaluvuissa määritellään aluksi termi yksityisyys ja siihen läheisesti liittyvät käsitteet. Lisäksi havainnollistetaan, miten nämä termit liittyvät biometriseen tunnistamiseen. Seuraavaksi perehdytään Suomen lainsäädännön lukuisiin eri kohtiin, joissa viitataan yksityisyyteen tai sivutaan sitä. Tämän jälkeen tutustutaan muutamiin yhdysvaltalaisiin havaintoihin sikäläisen yksityisyydensuojan ja lainsäädännön suhteesta toisiinsa. Lopuksi käsitellään vielä lyhyesti identiteettivarkauksia sekä muita käytössä olevia sähköisiä tunnistusmenetelmiä.

5.1 Mitä on yksityisyys

Käsite *yksityisyys* tarkoittaa luonnollisen henkilön oikeutta tai käytännön mahdollisuutta suojautua ulkopuoliselta puuttumiselta. Lisäksi se voi tarkoittaa oikeutta tai käytännön mahdollisuutta määrätä itseään koskevien henkilötietojen käytöstä. [44]

Yksityisyyden suoja tarkoittaa periaatetta, jonka mukaan luonnollista henkilöä tulee

suojata puuttumiselta hänen yksityiselämäänsä ja sitä koskeviin tietoihin. [44] Lisäksi sillä voidaan viitata mainitun periaatteen toteuttamiseen tähtääviin säädöksiin ja muihin järjestelyihin. [44]

Yleisessä mielessä yksityisyyden eri käsitteet sisältävät yhteisen lähtökohdan: *yksilön*. Yksityisyyden voidaan ajatella kattavan neljä laajempaa käsitettä [25]:

1. Päätöksentekoon liittyvää: Yksilöllä on valta tehdä omaan elämäänsä ja kehoonsa liittyviä päätöksiä. Näillä päätöksillä voi olla vaikutusta myös yksilön omaisiin tämän kuoltua.

2. Tilaan liittyvää: Yksilöllä on valta päättää, kuka saa osallistua yksilön toimintaan kuuluviin asioihin, esimerkiksi kotirauhan piirissä, tai tarkkailla niitä.

3. Tarkoituksellisuuteen liittyvää: Yksilöllä on valta päättää julkisesti havaittavissa olevan toiminnan tai ominaisuuden välittämisestä edelleen. Esimerkiksi hänellä on valta päättää, saako julkisella paikalla käydyn keskustelun saattaa myös muiden kuin asianosaisten tietoon tai saako esimerkiksi ihmisestä julkaista valokuvan, jossa tämä esiintyy tahattomasti alasti.

4. Tietoon liittyvää: Yksilöllä on valta päättää, missä laajuudessa häneen liittyvää tietoa käytetään, ketkä käyttävät ja mihin tarkoitukseen. Vastaavasti yksilön tietoja käyttävillä muilla henkilöillä tai organisaatioilla on vastuu noudattaa yksilön päätöksiä.

Tarkasteltaessa käytännössä olemassa olevaa biometrista tunnistusjärjestelmää pitäisi ensiksi määritellä, mitkä edellä mainitut käsitteet soveltuvat siihen. Jokainen näistä käsitteistä liittyy eri tavalla yhteiskuntaan, lainsäädäntöön, teoriaan ja käytäntöön. Havaittavissa oleva biometrinen tunnistetieto voidaan kerätä viranomaisen toimesta, esimerkiksi biometrista passia varten (päätöksentekoon liityvä). Tunniste saatetaan kerätä myös henkilön huomaamatta kotirauhan piirissä, esimerkiksi salakatselemalla tai -kuuntelemalla (tilaan liittyvä) tai vastaavasti julkisella paikalla (tarkoituksellisuuteen liittyvä). Biometrinen

tunniste on voitu alun perin kerätä toiseen tarkoitukseen, mutta sitä käytetäänkin muussa yhteydessä (tietoon liittyvä). Myös kaikkien edellä mainittujen tapausten yhdistelmä saattaa olla mahdollinen [25].

Yksityisyys on kykyä viettää häiriötöntä elämää, mahdollisuutta pysyä itsenäisenä ja valvoa, kuka pääsee käsiksi yksityisiin tietoihisi [2]. Perinteisesti ihmiset ovat pitäneet toistensa tunnistamista kahden ihmisen vastavuoroisena ja molemminpuolisena toimintana. Automaattinen biometrinen tunnistaminen saatetaan mieltää arvoa alentavaksi toiminnaksi. Varsinkin rikosten selvittämisessä useimmiten käytetyt sormenjälki- ja DNA-tunnistukset voivat saada ihmisissä aikaan negatiivisia mielikuvia.

5.2 Lainsäädännöstä

Suomalaisessa lainsäädännössä ei ole varsinaisesti määritelty yksityisyyden käsitettä, mutta luonnollisen henkilön yksityisyyttä ja yksityisyydensuojaa käsitellään useiden erilaisten lainkohtien ja asetusten yhteydessä.

Esimerkiksi *Rikoslaissa* [33] määritellään teonkuvaukset sekä säädetään rangaistuksista, jotka seuraavat muun muassa salakatselusta, salakuuntelusta, yksityiselämää loukkaavan tiedon levittämisestä, salassapitorikoksesta ja viestintäsalaisuuden rikkomisesta.

Henkilötietolain [35] tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.

Vastaavasti *Laki yksityisyyden suojasta työelämässä* [34] säätää työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta.

Sähköisen viestinnän tietosuojalain [52] tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen vies-

tinnän tietoturvaa.

Laki viranomaisen toiminnan julkisuudesta [53] selvittää muun muassa, mitkä viranomaisten asiakirjat ovat julkisia ja mitkä salassa pidettäviä, esimerkiksi yksityisyyden suojan takia.

Seuraavissa alaluvuissa käsitellään yllä mainittuja lainkohtia tarkemmin.

5.2.1 Yksityiselämän suoja

Yksityiselämän suoja [42] on yksi *Suomen perustuslakiin* kirjatuista perusoikeuksista:

> Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla.
>
> Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.
>
> Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana. [42]

Tämän Suomen valtion perustuslaillisen suojan voidaan nähdä perustuvan Yhdistyneiden kansakuntien *Ihmisoikeuksien yleismaailmalliseen julistukseen* (*engl. Universal Declaration of Human Rights*) [45], jonka myös Suomi on ratifioinut. Se ei sinänsä ole laillisesti sitova, vaan enemmän ohjeen luonteinen. Se on kuitenkin tullut allekirjoittajavaltioissa yleisesti osaksi lainsäädäntöä ja saanut kansainvälisen hyväksynnän, joten julistus on näitä valtioita velvoittava. Julistuksen 12. artiklassa todetaan:

> Älköön mielivaltaisesti puututtako kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon älköönkä loukattako kenenkään kunniaa ja

> mainetta. Jokaisella on oikeus lain suojaan sellaista puuttumista tai loukkausta vastaan. [45]

Edellistä julistusta velvoittavampi on Suomen allekirjoittama *Euroopan ihmisoikeussopimus*, virallisesti *Yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi* [46]. Mikäli yksilö kokee oikeuksiaan loukatun, voi hän valittaa loukkauksesta Euroopan neuvoston alaiseen Euroopan ihmisoikeustuomioistuimeen. Tämän sopimuksen 8. artiklassa todetaan:

> Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. [46]

5.2.2 Yksityisyyden suoja työelämässä

Laki yksityisyyden suojasta työelämässä [34] vastaa yksityiselämän suojaa koskeviin kysymyksiin työelämän eri osa-alueilla. Laki koskee vain työntekijän ja työnantajan välistä suhdetta ja on pidettävä työntekijöiden nähtävänä työpaikoilla.

Työelämään liittyvät yksityisyyden suojan kysymykset saattavat olla nykypäivänä laajempia ja monimutkaisempia sekä koskettavat useampia osa-alueita kuin muilla elämän alueilla. Yksityisyyden suojaan työelämässä liittyvät esimerkiksi kulunvalvonta ja videovalvonta työpaikalla, työntekijän sähköpostien lukeminen, soveltuvuustestien tekeminen, huumausainetestestit sekä terveystietojen käsittely.

Työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työtehtävien erityisluonteesta.

Laissa säädetään työnantajalle velvollisuus käydä yhteistoiminta- tai kuulemismenettelyssä läpi työntekijöiden teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestäminen, määritellä valvonnan käyttötarkoituks ja tiedottaa henkilöstöä valvonnasta sekä sähköpostin ja tietoverkon käyttämisestä.

Laissa säädetään henkilötietojen tarpeellisuusvaatimuksesta, työntekijän ja työnhakijan henkilötietojen keräämisen yleisistä edellytyksistä sekä työnantajan tiedonantovelvollisuudesta ja terveydentilaa koskevien henkilötietojen käsittelyperusteista ja menettelytavoista.

Työelämän tietosuojalakia valvovat työsuojeluviranomaiset ja tietosuojavaltuutetun toimisto. [55]

5.2.3 Henkilötietolaki

Henkilötietolaki [35] on säädetty toteuttamaan yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistämään hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.

Suomen henkilötietolaki puolestaan perustuu Euroopan unionin direktiiviin [63], joka luo pohjan yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta Euroopan unionissa.

Lakia sovelletaan henkilötietojen automaattiseen käsittelyyn. Myös muuhun henkilötietojen käsittelyyn sovelletaan tätä lakia silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa.

Henkilötietolaissa säännellään henkilötietojen käsittelyn yleisistä edellytyksistä, niistä velvoitteista, joita kaikessa henkilötietojen käsittelyssä tulee aina noudattaa, rekisteröityjen henkilötietojen käsittelyyn liittyvistä oikeuksista, lain soveltamisen valvontajärjestelmästä sekä sanktioista, jotka voivat seurata henkilötietolain vastaisista käsittelyistä. Laki osoittaa muun muassa, missä tapauksissa henkilötietojen käsittely on mahdollista ilman rekisteröidyn suostumusta.

Henkilötietojen käsittelyn yleisten edellytysten lisäksi yleisvelvoitteiden noudattamisen merkitys on keskeinen hyvän tietojenkäsittelytavan saavuttamiseksi. Laissa säädetään vaatimuksesta määritellä aina henkilötietojen käsittelyn tarkoitus sekä suunnitella henkilötietojen käsittely etukäteen. Lain muita yleisvelvoitteita ovat tarpeellisuus- ja virheettömyysvaatimukset sekä huolellisuus- ja suojaamisvelvoitteet, jotka niin ikään tulee

ottaa huomioon kaikessa henkilötietojen käsittelyssä.

Rekisterinpidon avoimuuden periaatetta edustaa rekisteriselosteen laatimis- ja saatavillapitovelvoite. Rekisterinpitäjälle on säädetty velvoite informoida rekisteröityjä henkilötietoja kerättäessä. Rekisteröidyillä on oikeus saada tarkastaa itseään koskevat tiedot ja myös oikeus vaatia virheellisen tiedon korjaamista.

Henkilötietolailla on pyritty löytämään ratkaisumalli yksityisyyden suojan ja muiden henkilötietojen käsittelyyn liittyvien intressien välillä. Muun muassa laissa säädetty henkilötietojen kaikkiin käsittelyvaiheisiin ulottuva tarpeellisuus- ja virheettömyysvaatimus toteuttavat osaltaan myös toiminnallisia ja hyvän tiedonhallinnan tavoitteita. Rekisteröityjen yksityisyyden ja heidän etujensa ja oikeuksiensa suojaaminen ei ole erillinen velvoite, vaan se liittyy olennaisena osana toiminnallisiin tavoitteisiin.

Henkilötietolaissa on säädetty myös henkilötietojen lainvastaisesta käsittelystä seuraavasta vahingonkorvausvelvollisuudesta. Henkilötietolaissa ja rikoslaissa on sanktiot henkilötietolain vastaisesta menettelystä.

Henkilötietolainsäädännön täytäntöönpanoa ohjaa ja valvoo tietosuojavaltuutettu. Tietosuojavaltuutetun on edistettävä hyvää tietojenkäsittelytapaa sekä ohjein ja neuvoin pyrittävä siihen, että lainvastaista menettelyä ei tapahdu. [54]

5.2.4 Sähköisen viestinnän tietosuojalaki

Sähköisen viestinnän tietosuojalain [52] tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä. Lain tavoitteena on myös selkeyttää tietoturvan toteuttamismahdollisuuksia ja antaa pelisäännöt evästeiden käytölle sekä paikkatietojen käsittelylle.

Lakia sovelletaan yleisissä viestintäverkoissa tarjottaviin verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin, kuten paikkatietoihin perustuviin palveluihin, sekä palveluihin, joissa käsitellään palvelun käyttöä kuvaavia tietoja. Lakia sovelletaan myös

suoramarkkinointiin viestintäverkoissa sekä tilaajaluettelopalveluihin ja numerotiedotuspalveluihin.

Teleyritys saa käsitellä paikkatietoja, jollei tilaaja, käytännössä yksityishenkilö, ole sitä kieltänyt. Paikkatiedot ovat matkapuhelimen maantieteellisen sijainnin ilmaisevia tietoja, joita käytetään muuhun kuin viestin välittämiseen. Ennen kuin luovuttaa paikkatietoja lisäarvopalvelun tarjoajalle, teleyrityksen on varmistuttava, ettei tilaaja ole kieltänyt niiden käsittelyä ja että luovutuksensaaja on saanut paikannettavalta palvelukohtaisen suostumuksen.

Paikannuspalvelut ovat niin sanottuja lisäarvopalveluja. Ketään ei saa paikantaa ilman suostumusta eli paikannuspalvelun tarjoajan on saatava paikannettavalta käyttäjältä suostumus ennen paikannuksen aloittamista. Paikannuspalvelut perustuvat teleyritykseltä saatuihin paikkatietoihin, jotka ovat matkaviestinnän välityksessä valttämättömiä. Laki sallii teleyrityksille paikkatietojen käsittelyn myös lisäarvopalvelujen tuottamiseksi, mutta näiltä osin käyttäjällä on oikeus kieltää tällainen viestinnän välitykseen kuulumaton paikkatietojen käsittely.

Sähköisen viestinnän tietosuojalain ja sen nojalla annettujen määräysten noudattamista valvoo pääasiassa Viestintävirasto. Paikkatietojen käsittelyä, automatisoitujen järjestelmien avulla tapahtuvaa suoramarkkinointia koskevien säännösten noudattamista ja puhelinluetteloita, numerotiedotuspalveluita sekä käyttäjän erityistä tiedonsaantioikeutta koskevien säännösten noudattamista valvoo tietosuojavaltuutettu. [56]

5.2.5 Yksityisyyden, rauhan ja kunnian loukkaamisesta

Rikoslain [33] 24. luvussa säädetään *yksityisyyden, rauhan ja kunnian loukkaamisesta*. Näihin sisältyvät pykälät kotirauhan, viestintärauhan, salakatselun, salakuuntelun ja yksityiselämää loukkaavan tiedon levittämisestä.

Kotirauhan ja viestintärauhan rikkominen on sanktioitu sakolla tai enintään kuudella kuukaudella vankeutta. Lainkohtia salakatselusta ja salakuuntelusta voitaneen soveltaa

myös biometrisiin järjestelmiin.

Salakuuntelu [33] määritellään seuraavasti:

> Joka oikeudettomasti teknisellä laitteella kuuntelee tai tallentaa
>
> 1) keskustelua, puhetta tai yksityiselämästä aiheutuvaa muuta ääntä, jota ei ole tarkoitettu hänen tietoonsa ja joka tapahtuu tai syntyy kotirauhan suojaamassa paikassa, taikka
>
> 2) muualla kuin kotirauhan suojaamassa paikassa salaa puhetta, jota ei ole tarkoitettu hänen eikä muunkaan ulkopuolisen tietoon, sellaisissa olosuhteissa, joissa puhujalla ei ole syytä olettaa ulkopuolisen kuulevan hänen puhettaan, on tuomittava salakuuntelusta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Vastaavasti *salakatselu* [33] on määritelty seuraavasti:

> Joka oikeudettomasti teknisellä laitteella katselee tai kuvaa
>
> 1) kotirauhan suojaamassa paikassa taikka käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa oleskelevaa henkilöä taikka
>
> 2) yleisöltä suljetussa 3 §:ssä tarkoitetussa rakennuksessa, huoneistossa tai aidatulla piha-alueella oleskelevaa henkilöä tämän yksityisyyttä loukaten, on tuomittava salakatselusta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

5.3 Huomioita yksityisyydestä

Yhdysvaltalainen oikeustieteen professori Daniel J. Solove on erikoistunut tietosuojalainsäädäntöön ja siihen, miten yksityisyydensuoja suhteutuu informaatiotekniikkaan. Kuten edellisissä kappaleissa todettiin, yksityisyydensuoja on kansainvälisestikin laajasti tunnustettu perusoikeus, joten tässä kohdassa on perusteltua tarkastella eräitä kohtia hänen artikkelistaan *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy* [26]. Lisäksi on perusteltua tutustua kyseisen artikkelin yhdysvaltalaisiin näkökulmiin, koska Suomessa ei ole aiheesta juurikaan käyty vastaavaa argumentointia.

Vuoden 2001 syyskuun 11. päivän terrori-iskujen jälkeen paljastui vähitellen tietoja, joiden mukaan Yhdysvaltain hallitus harjoitti laajamittaista valvontaa ja tiedonlouhintaa. Kansallisella turvallisuusvirastolla (engl. *National Security Agency, NSA*) on ollut lupa kuunnella yhdysvaltalaisten puheluita ilman nimenomaista oikeuden määräystä. Samoin Yhdysvaltain puolustusministeriö (engl. *Department of Defense, DoD*) on harjoittanut tiedonlouhintaa analysoidakseen ihmisten henkilökohtaisia tietoja ja löytääkseen epäilyttävää käytöstä. Lisäksi paljastui, että myös kansainvälisiä tilisiirtoja oli valvottu perusteellisesti. Näitä valvontaohjelmia on perusteltu sillä, että voidaan estää ennalta mahdollisia uusia terrori-iskuja.

Muutama vuosi myöhemmin näiden valvontaohjelmien tultua julkisuuteen monet ihmiset raivostuivat, toisaalta taas monet eivät nähneet valvonnassa mitään ongelmaa. Yleinen argumentti oli: ”Minulla ei ole mitään salattavaa.” Monet ihmiset ajattelevat, ettei siinä ole mitään yksityisyyttä loukkaavaa ongelmaa, kun viranomaiset keräävät ja analysoivat henkilökohtaisia tietoja, jos kyseinen ihminen ei ole tehnyt mitään laitonta. Kyseessä voidaan ajatella olevan kompromissi turvallisuuden ja yksityisyyden suhteen: ”Jos ei ole mitään salattavaa, miksi pitäisi pelätäkään mitään?”

Monia vasta-argumenttejakin voidaan esittää. Esimerkkejä: ”Minulla ei ole mitään salattavaa, mutta ne ovat yksityisasioita.” ”Jos sinulla ei ole mitään salattavaa, sinulla ei ole myöskään elämää.” ”Miksi asunnossasi on verhot?” ”Saanko nähdä luottokorttilaskusi?” ”Näytä ensin omat salaisuutesi, sitten näytän omani.” Nämä voidaan ehkä tiivistää parhaiten argumenttiin: ”Miksi minun pitäisi puolustella kantaani, että haluan pitää salaisuuteni. Päinvastoin sinun pitää perustella oma kantasi.”

Solove mainitsee artikkelissaan [26] myös muutamia yksityisyydensuojan rikkomiseen liittyviä yhdysvaltalaisia oikeustapauksia, joissa kantajina ovat olleet yksityishenkilöt ja vastaajina yritykset. Nämä esimerkit antavat ymmärtää, että sikäläiset tapaukset voivat kaatua kantajien vahingoksi usein vain muotoseikkojen vuoksi.

Koska Suomessa henkilötietolaki [35] ei vastaa riittävän hyvin nykytilannetta biomet-

riseen tunnistukseen soveltuvaksi, Suomi et al. ovat artikkelissaan [62] esittäneet siihen muutoksia ja täydennyksiä. Tärkeimpinä kohtina mainitaan, että kaupallisessa käytössä sen käyttöä koskevia henkilöitä tulee aina tiedottaa biometrisesta tunnistuksesta. Lisäksi biometrisen tunnistetiedon käytön tulee olla sallitua vain siinä laajuudessaan, kuin se on tarpeellista alkuperäisessä tunnistustarkoituksessaan. Tämän lisäksi tunnistetieto pitää myös säilyttää tavalla, jossa sitä ei voi suoranaisesti yhdistää tiettyihin henkilöihin. Erityisen tärkeänä tulee pitää tietoturvaa riippuen siitä, missä laajuudessa tunnistusjärjestelmä on liittyneenä sisäisiin tai ulkoisiin tietoverkkoihin.

5.4 Identiteettivarkaudet

Identiteettivarkaus eli toisen ihmisen henkilöllisyydellä esiintyminen ei ole rikos, ellei sitä hyväksikäyttäen syyllistytä esimerkiksi petokseen tai kunnianloukkaukseen. Väärien henkilötietojen esittäminen viranomaiselle on rikos [33], mutta ei yksityiselle toimijalle kuten yritykselle tai yksityishenkilölle. Tämän opinnäytetyön osana käsitellään identiteettivarkauksia, koska identiteettivarkauksia olisi mahdollista estää ja niiltä suojautua biometristen tunnisteiden laajemalla käytöllä.

Väärillä henkilötiedoilla esiintymistä on pohdittu Sisäasiainministeriössä, mutta sitä ei ole vielä kriminalisoitu [38]. Suomen rikoslain mukaan identiteettiä ei voi varastaa, koska tällöin varkaus ei kohdistu irtaimeen omaisuuteen. [33] Näin ollen esimerkiksi teleoperaattorille voi rekisteröityä asiakkaaksi väärillä henkilötiedoilla ja käyttää näin saatua varmennetta tunnistautumiseen. Samoin yksityishenkilöiden välisessä kaupankäynnissä internetissä, esimerkkeinä kotimainen *Huuto.net* ja kansainvälinen *Ebay.com*, on mahdollista esiintyä toisen tai kuvitteellisen henkilön nimissä. Identiteettivarkaudet ovat yleistyneet ja helpottuneet sähköisen kaupankäynnin ja muun asioinnin laajentuessa tietoverkkoihin.

5.5 Muut sähköiset tunnistusmenetelmät

Tällä hetkellä Suomessa biometrinen tunnistautuminen ei ole julkisessa käytössä muualla kuin matkustusasiakirjana käytettävässä biometrisessa passissa. Sen sijaan sähköisessä asioinnissa on laajasti käytössä pankkien yhteinen tunnistuspalvelu *TUPAS*. [39] Se on Finassialan Keskusliiton määrittelemä tapa tunnistaa verkkoasiakkaat pankkitunnusten avulla. Tässä kohdassa TUPAS-palvelua on perusteltua käsitellä siksi, että se on Suomessa vakiinnuttanut asemansa yleisimpänä tunnistautumisvälineenä ja keinona suojata yksityisyyttä tietoverkoissa.

Käytännössä pankkitunnuksilla tunnistautuminen verkossa tapahtuu syöttämällä verkkopalveluun käyttäjän muuttumaton, noin kahdeksan numeron mittainen käyttäjätunnus ja käyttäjän hallussa olevasta avainlukulistasta noin neljän numeron mittainen avainluku. Pankkipalveluissa tämän lisäksi vaaditaan yleensä vielä toinen verkkopankin satunnaisesti kysymä neljän numeron mittainen avainluku, jotta esimerkiksi uusi maksusuoritus voidaan hyväksyä. Tätä voidaan kutsua useamman avainluvun haaste / vaste -menetelmäksi.

TUPAS-palvelua käytetään alkuperäisen tarkoituksensa, verkkopankkien, lisäksi tunnistautumiseen erilaisiin viranomaisten, kuten Kansaneläkelaitoksen ja verohallinnon verkkopalveluihin. Näiden lisäksi myös monet yksityiset yritykset, kuten vakuutusyhtiöt, käyttävät TUPAS-tunnistamista sähköisessä asioinnissa. Tämän ongelmana voidaan nähdä, että tunnukset myöntää ja niitä hallinoi yksityinen yritys eikä viranomainen. Ongelmallisena voidaan myös pitää, kuinka luotettavasti asiakassuhdetta luotaessa tunnuksia hakeva henkilö voidaan alunperin tunnistaa tunnuksia myöntävässä yrityksessä, käytännössä pankissa. Tästä tunnistusvälineen hakijan ensitunnistamisen kriteereistä on säädetty tarkoin omassa laissaan. [61] Tämän lain mukaan, jos yritys ei voi luotettavasti todentaa tunnusten hakijan henkilöllisyyttä, poliisin tulee suorittaa ensitunnistaminen.

Toisaalta ongelmallisena voidaan pitää myös sitä, että TUPAS-tunnuksia, käytännössä verkkopankkitunnuksia, ei välttämättä myönnettä, jos hakijalla on maksuhäiriömerkintä [60]. Pankkiasioinnin ohella yhä suuremmissa määrin myös muut palvelut ovat siirtyneet

sähköisiksi verkkkoon, jolloin ilman verkkopankkitunnuksia erilaisten palveluiden käyttö voi olla huomattavan hankalaa tai yleensä verkkoasiointia kalliimpaa. Lisäksi TUPAS-tunnuksia on suhteellisen helppo käyttää oikeudettomasti sähköisessä asioinnissa, kunhan ulkopuolinen henkilö saa tunnukset ja salasanalistan käyttöönsä.

Viranomaisasiointiin on kehitetty myös sähköinen henkilökortti eli HST-kortti ja tähän liitetty kansalaisvarmenne [40]. HST-korttiin liitetylle sirulle on tallennettu käyttäjän julkinen ja salainen avain, jolloin korttia voidaan käyttää myös digitaaliseen allekirjoitukseen. HST-kortin myöntää poliisi, ja Väestörekisterikeskus luo kansalaiselle vastaavan sähköisen henkilöllisyyden kuin henkilötunnuksenkin. Sähköisen henkilöllisyyden tunnuksena toimii sähköinen asiointitunnus eli *SATU*-tunnus.

Sähköinen asiointi kansalaisvarmenteella tapahtuu kahdella eri tunnusluvulla. Verkkopalveluihin kirjautumisessa käytetään tunnistautumiseen tarkoitettua tunnuslukua (PIN1). Sähköinen allekirjoitus tehdään allekirjoitustunnusluvulla (PIN2). Se on juridisesti yhtä sitova ja kiistämätön kuin perinteinen allekirjoitus. [40] HST-kortti kelpaa tavallisen henkilökortin tavoin ja passin asemesta matkustusasiakirjana EU-maissa. Kortille voidaan liittää myös KELA-kortin sisältämät sairausvakuutustiedot. HST-kortin ongelmina voidaan pitää, ettei se ole edelleenkään suhteellisen laajassa käytössä, korttejahan on myönnetty vain noin $450\ 000$ kappaletta. Lisäksi HST-kortti vaatii tietokoneeseen liitettävän lukulaitteen.

Tässä luvussa määriteltiin aluksi termi yksityisyys ja siihen läheisesti liittyvät käsitteet. Lisäksi havainnollistettiin, miten nämä termit liittyvät biometriseen tunnistamiseen. Seuraavaksi perehdyttiin Suomen lainsäädännön lukuisiin eri kohtiin, joissa viitataan tai sivutaan yksityisyyttä. Tämän jälkeen tutustuttiin muutamiin yhdysvaltalaisiin havaintoihin sikäläisestä yksityisyydensuojan ja lainsäädännön suhteesta toisiinsa. Lopuksi käsiteltiin lyhyesti identiteettivarkauksia sekä muita käytössä olevia sähköisiä tunnistusmenetelmiä.

Luku 6

Biometrinen tunnistus ja yksityisyys

Kaikki biometrisesti tallennettu data on henkilökohtaista ja yksilöllistä. Se on johdettu yksilön fysiologisista tai käytökseen perustuvista ominaispiirteistä, ja sitä käytetään tapauksesta riippuen henkilöllisyyden varmistamiseen tai tunnistamiseen. Vaikka biometrinen data voidaan nähdä arkaluonteisena ja kyseisestä henkilöstä muitakin tietoja paljastavana asiana, sen keräämiselle, tallentamiselle ja käytölle on perusteltuja tilanteita. Kun biometriikoita käytetään tarkoituksenmukaisesti, niiden avulla on mahdollista suojata vieläkin arkaluonteisempia, kuten terveyteen tai omaisuuteen liittyviä tietoja.

Jokaisella biometrisella teknologialla on toisistaan eroava vaikutus yksityisyyteen. Joillakin niistä ei ole juuri lainkaan vaikutusta yksityisyyteen, eli ne voidaan nähdä yksityisyyden suhteen neutraaleina. Toisilla teknologioilla on taas suuri vaikutus yksityisyyden suojaan negatiivisesti joko niiden sisäisen toiminnan tai ulkoisten tekijöiden takia. Joitakin teknologioita voidaan käyttää yksityisyyden suojan parantamiseen. [69]

Seuraavissa alaluvuissa käsitellään ensin erilaisten biometristen teknologioiden riskejä yksityisyyden suojan näkökulmasta. Tämän jälkeen käytetään esimerkkeinä kolmea erilaista tapausta, miten biometriikat voivat vaikuttaa yksityisyyteen. Lopuksi tarkastellaan biometriseen tunnistamiseen liittyviä huolenaiheita ja uhkakuvia.

6.1 Teknologioiden riskit yksityisyyden suojan kannalta

Biometriset järjestelmät voidaan jakaa neljään eri luokkaan sen perusteella, minkälainen vaikutus yksityisyyteen niillä nähdään olevan. Nämä luokat ovat seuraavat [69]:

1. **Yksityisyyteen kajoava:** Järjestelmä kerää biometrista tietoa ilman käyttäjän suostumusta, tietoja käytetään salaiseen tarkoitukseen tai muuhun kuin alkuperäiseen tarkoitukseen. Tästä ovat esimerkkeinä erilaiset valvontajärjestelmät ja mahdollisesti biometrinen passi.

2. **Yksityisyyden kannalta neutraali:** Biometrisen tiedon käytöllä ei ole suurta vaikutusta yksityisyyteen. Esimerkkeinä voivat olla henkilökohtaiset mobiililaitteet ja tietokoneet sekä kotien kulunvalvontajärjestelmät.

3. **Yksityisyyttä ylläpitävät:** Huolellisella järjestelmän suunnittelulla voidaan varmistaa, että biometrinen tieto on suojattu luvattomalta pääsyltä ja käytöltä. Useimpiin järjestelmiin voidaan sisällyttää yksityisyyttä ylläpitäviä elementtejä.

4. **Yksityisyyttä suojaavat:** Järjestelmässä käytetään biometrista tunnistusta suojaamaan muuta henkilökohtaista tietoa, joka voisi olla muuten alttiina luvattomalle käytölle. Tästä ovat esimerkkeinä erilaiset yritystason turvallisuusjärjestelmät sekä internetpankkien käyttäjien tunnistaminen.

International Biometric Group (IBG) on arvioinut erilaisten biometristen teknologioiden riskejä yksityisyyden suojan kannalta seuraavasti [28]:

Verifiointi / identifiointi: Verifiointiin liittyy pienempi riski yksityisyyden suojan kannalta, koska verifioinnissa verrataan vain yhteen mallinteeseen $1:1$. Identifiointiin liittyy suurempi riski yksityisyyden suojan kannalta, koska identifioinnissa vertailu tehdään suureen joukkoon (kaikkiin) mallinteita $1:N$.

Julkinen / salainen: Teknologiaan, joka vaatii käyttäjän osallistumista, eli se on julkinen, liittyy yksityisyyden suojan kannalta pienempi riski. Teknologiaan, joka ei vaadi käyttäjän osallistumista, eli se on salainen, liittyy yksityisyyden kannalta suurempi riski.

Fysiologinen / käyttäytyminen: Fysiologiaan perustuva piirre on pysyvä, joten siihen liittyy yksityisyyden kannalta suurempi riski. Käyttäytymiseen perustuva piirre on muuttuva, joten siihen liittyy yksityisyyden suojan kannalta pienempi riski.

Tietokannat: Teknologiaan, jossa ei käytetä suuria tietokantoja, liittyy yksityisyyden suojan kannalta vähemmän riskitekijöitä. Vastaavasti teknologiaan, jossa käytetään suuria tietokantoja, liittyy yksityisyyden kannalta suurempia riskejä.

Biometriset tekniikat voidaan jakaa edelleen matalan, keskisuuren tai korkean riskin luokkiin seuraavasti:

Matala: Tekniikan perustoiminta takaa, että sillä on vain vähäinen vaikutus yksityisyyteen.

Keskisuuri: Tekniikkaa voidaan käyttää yksityisyyttä häiritsevästi, mutta väärinkäytön mahdollisuus on rajoittunutta.

Korkea: Tietyissä käyttötarkoituksissa pitää huolehtia kunnollisista suojaustoimenpiteistä, ettei tekniikkaa käytetä väärin.

On huomioitava, ettei tarkasti mitattavia arvoja tietyn tekniikan vaikutuksesta yksityisyyden suojan kannalta ole tehty. Näiden luokkien tarkoituksena on antaa yleiskäsitys mahdollisista riskeistä.

Seuraavassa taulukossa 6.1 on jaoteltu neljän tärkeimmän [9] biometrisen tekniikan riskit edellä mainittujen luokkien mukaisesti. Taulukon arviot ovat vain yleisellä tasolla, ja

taulukossa ”yleinen riski” tarkoittaa kyseisen tekniikan arvioitua kokonaisriskiä yksityisyyden suojan kannalta. Jotkin arviot voivat muuttua tulevaisuudessa esimerkiksi teknologisen kehityksen myötä.

Taulukko 6.1: Neljän tärkeimmän biometrisen teknologian riskit yksityisyyden suojan kannalta. (Mukaillen [9].) Selite: S = suuri, K = keskitaso, M = matala

PIIRRE / TEKNIIKKA	Sormenjälki	Kasvot	Iiris	Ääni
Verifiointi / Identifiointi	S	S	S	M
Julkinen / Salainen	K	S	M	S
Käyttäytymiseen / fysiologiaan	S	K	S	M
Tietokannat	S	S	M	M
Yleinen riski	S	S	K	K

Seuraavissa alaluvuissa käsitellään tarkemmin edellä mainittuja neljää yleistä biometrista tunnistetta: sormenjälkeä, kasvoja, iiristä ja ääntä yksityisyydensuojan kannalta.

6.1.1 Sormenjälki

Sormenjälkeen perustuva automaattinen biometrinen tunnistus on yksi yleisimmistä käytössä olevista tekniikoista. Viranomaiskäytössä esimerkiksi biometrinen passi, johon on tallennettu passinhaltijan sormenjälki sekä henkilökohtaisessa käytössä esimerkiksi tietokoneen tai oven sormenjälkilukija, ovat yleisesti käytettyjä sovelluksia kulunvalvonnassa ja henkilöllisyyden verifioinnissa. Rikostutkinnassa sormenjälkitunnistuksessa on käytössä erilaisia *AFIS*-järjestelmiä (engl. *Automated Fingerprint Indentification System*) [43], esimerkiksi Yhdysvaltain keskurikospoliisin (Federal Bureau of Investigation, FBI) käyttämä *IAFIS* (engl. *Integrated Automated Fingerprint Identification System*) [29].

Sormenjälkitunnistuksen hyvänä puolena yksityisyydensuojan kannalta voidaan pitää

sitä, että henkilö voi käyttää eri järjestelmissä tunnistautuessaan eri sormia. Koska ihmisen jokaisen sormen sormenjälki on erilainen, esimerkiksi tietokantojen yhdistäminen on hankalaa. Eri valmistajien sormenjälkijärjestelmät sekä niiden käyttämät algoritmit ovat erilaisia, jolloin myös järjestelmien luomat mallinteet ovat erilaisia. Täten eri laitevalmistajien sormenjälkitunnistusjärjestelmien tietokannat eroavat toisistaan huomattavasti. [9] Kuitenkin viranomaisjärjestelmissä, esimerkiksi biometrisen passin tapauksessa, sormenjäljet on annettava pääsääntöisesti molemmista etusormista [58].

Viranomaisilla on käytössään tietokantoja, joissa säilytetään sormenjäljen mallinteen sijasta varsinaista kuvaa sormenjäljestä. Kaikilta Yhdysvaltoihin matkustavilta kerätään sormenjäljet maahan saavuttaessa. Suomessa biometrista passia varten sormenjäljet kerätään hallinnollisessa menettelyssä poliisin tietokantaan, vaikkei Euroopan Unionin asetus [30] tätä edellytäkään. Eräissä EU:n jäsenvaltioissa, kuten Saksassa, sormenjäljen mallinne tallennetaan ainoastaan paikallisesti passin sirulle [36]. Euroopan unionin jäsenvaltiot saavat itse päättää mahdollisesta sormenjälkien tallettamisesta ja rekisterin perustamisesta ja myös passin sormenjälkitietojen käyttämisestä muuhun kuin niiden tallettamistarkoitukseen. Suomessa on päädytty ratkaisuun, jossa sormenjälkitiedot talletetaan kansalliseen rekisteriin, mutta niiden käyttö muuhun kuin tallettamistarkoitukseensa sallitaan poikkeuksellisesti vain, kun on kysymys tuntemattomien vainajien tunnistamisesta esimerkiksi luonnonkatastrofien ja suuronnettomuuksien yhteydessä.

Nykyisen passilain mukaan sormenjäljet tallennetaan passin tekniseen osaan sirulle sekä passirekisteriin, ja passirekisteriin tallennetut sormenjäljet on pidettävä erillään rikoksesta epäiltyjen henkilötuntomerkeistä. Passin sormenjälkitietoja on oikeus käyttää vain henkilöllisyyden varmentamiseksi ja asiakirjan valmistamiseksi [59].

Suomessa on kuitenkin viime vuosina muun muassa poliisin taholta esitetty, että passia varten tallennetuja sormenjälkiä voitaisiin käyttää myös rikostutkinnassa [47]. Kuitenkin sormenjälkitiedot on kerätty vain passin myöntämiseen liittyviin tarkoituksiin eli passin haltijan luotettavaan tunnistamiseen ja asiakirjan aitouden varmistamiseen. Käyttötarkoi-

tussidonnaisuus on erittäin tärkeä periaate, jolloin tietoja saa käyttää vain siihen tarkoitukseen, joihin niitä on alunperin kerätty. Euroopan ihmisoikeustuomioistuimen (EIT) päätöksen [48] jälkeen Suomessa on jälleen kiinnitetty huomiota kyseiseen sormenjälkien käyttötarkoitussidonnaisuuteen. Viimeisimpien tietojen mukaan perustuslakivaliokunnan kannanotot estävät säätämästä lakia, joka sallisi passia varten kerättyjen sormenjälkien käytön myös rikostutkinnassa [49]. Nykyisen lain mukaan passirekisterin sormenjälkiä saa käyttää vain suuronnettomuuksien tai rikoksen uhrien tunnistamisessa.

6.1.2 Kasvontunnistus

Kasvontunnistus on käytännöllisesti katsoen ainoa menetelmä, jolla henkilö voidaan tunnistaa tämän tietämättä, huomaamatta ja myötävaikuttamatta tapahtumaan. Tällaista tekniikkaa saattaa olla käytössä julkisilla paikoilla, esimerkiksi lentokentillä, joissa liikkuu suuria ihmismääriä. Yksityisyydensuojan kannalta tämä on ongelmallista. Toisaalta dynaamisessa kasvontunnistuksessa, jolloin kuvattava kohde ei ole aktiivisesti myötävaikuttamassa tapahtumaan, voi järjestelmän tunnistustarkkuus olla huono. Esimerkiksi valaistusolosuhteet, henkilön asento kameraan nähden, mahdollisesti henkilön muuttuva ulkonäkö, kuten aurinkolaisit, päähineet, hiukset ja parta voivat vaikeuttaa tunnistamista. Tämä voidaan nähdä yksityisyydensuojan kannalta hyvänä, koska henkilöstä ei saada tämän tietämättä tai hyväksymättä välttämättä vertailukelpoista kasvokuvaa. [9]

6.1.3 Iiristunnistus

Iiristunnistusta pidetään teknisessä mielessä tarkimpana biometrisenä tunnistusmenetelmänä. Kuitenkin esimerkiksi sormenjälkitunnistukseen verrattuna tunnistamisen kohteelta vaadittava suuri myötävaikutus, järjestelmien kalleus ja käyttäjien epäluuloisuus menetelmää kohtaan hidastavat iiristunnistuksen yleistymistä. Juuri tunnistettavalta vaadittava myötävaikutus eli asettautuminen kuvattavaksi tarkasti kameran eteen, voidaan nähdä yksityisyydensuojan kannalta hyvänä seikkana. Tiettävästi iiristunnistus ei ole käytössä

rikostutkinnassa, ja siten viranomaisilla ei ole laajoja rekistereitä iirismallinteista, mutta tulevaisuudessa asia saattaa muuttua. Iiristunnistuksen kehittyessä tulevaisuudessa voi olla mahdollista, että henkilön iiris voidaan kuvata tämän huomaamatta. [9]

6.1.4 Ääni

Kaupallisissa sovelluksissa on jo jossain määrin käytössä puhujantunnistus esimerkiksi puhelimella käytettävissä palveluissa. Soittaja tunnistetaan ensin tämän puheäänen perusteella, minkä jälkeen palvelun käyttö myös jatkuu puhekomennoilla. Puheääni ei ole erityisen tarkka henkilön identifioinnissa, koska ääni saattaa muuttua suhteellisen nopeastikin esimerkiksi puhujan tunnetilan, sairauden tai taustamelun takia. Tämä voidaan nähdä yksityisyydensuojan kannalta hyvänä. Toisaalta puhetta on hyvin helppo tallentaa henkilön huomaamatta. [9] Tällä hetkellä kuitenkin yleisempiä ovat palvelut, joissa käytetään vain puheentunnistusta palvelun ohjaamiseen ja itse käyttäjä tunnistetaan jollakin muulla tavoin, esimerkiksi näppäilemällä salasana.

6.2 Biometrinen tunnistus eri näkökulmista

Voidaan ajatella, että biometriikoihin liittyy kolme erilaista toimijaa: *yhteiskunta*, *yhteisö* ja *yksilö*. Yhteiskunnan voidaan ymmärtää tarkoittavan käytännössä valtiota. Se määrittelee alaa koskevaa lainsäädäntöä, luo toimintaympäristön, asettaa vaatimuksia ja luo mahdollisuuksia toimia näiden sääntöjen puitteissa. Yhteisö voi tarkoittaa esimerkiksi yritystä tai muuta työpaikkaa, yhdistystä tai muuta valtiota pienempää yksikköä. Se saattaa määritellä oman toimintaympäristönsä yhteiskunnan määrittelemien sääntöjen rajoissa. Yksilö on käytännössä luonnollinen henkilö, joka toimii yhteiskunnan ja / tai yhteisön sääntöjen mukaan.

Kaikki mainitut kolme eri toimijaa voivat vuorovaikuttaa keskenään joko suoraan tai toistensa kautta. Näillä toimijoilla voi olla myös erilaiset intressit toistensa suhteen,

ja ne ovat erilaisessa asemassa lainsäädännössä. Seuraavien esimerkkitapausten avulla selvennetään eri toimijoiden suhdetta toisiinsa erilaisissa biometriikoiden käyttötapauksissa. Esimerkkitapaukset on valittu muun muassa sillä perusteella, että niissä on edustettuina kolme edellä mainittua toimijaa eri suhteissa toisiinsa. Lisäksi esimerkkitapauksissa on edustettuina kolmen erilaisen biometrisen tunnisteen kolme erilaista käyttökohdetta.

6.2.1 Tapaus: Biometrinen passi

Edellä mainitut kolme eri toimijaa voivat olla vuorovaikutuksessa keskenään vertaistensa kanssa. Esimerkiksi yhteiskunnat eli valtiot ovat sopineet keskenään hyväksyvänsä yhtenäisen eurooppalaisen matkustusasiakirjan, biometrisen passin, ja sopineet siinä käytettävistä standardeista.

Biometrisen passin tapauksessa myös yksilöt ja yhteiskunnat ovat selvästi vuorovaikutuksessa toistensa kanssa. Yksilöiden eli kansalaisten voidaan nähdä olevan enemmän alisteisessa asemassa yhteiskuntiin eli valtioihin nähden, koska kansalaisten osaksi jää lähinnä hyväksyä passin käyttäminen tai olla ottamatta lainkaan käyttöön biometrista passia.

Kolmas toimija, yhteisöt, ovat yrityksiä, jotka käytännössä toteuttavat biometriset tunnistusjärjestelmät ja valmistavat passit. Suomalaiset biometriset passit valmistaa ulkomaalaisomisteinen Gemalto Oy [66], joka jatkaa entisen Suomen Pankin setelipainon ja sittemmin valtion omistaman Setec Oy:n toimintaa.

Biometrisen passin tapauksessa voidaan nähdä yksityisyyden suojan kannalta ongelmallisena suomalainen toteutus, jossa biometriset tunnisteet tallennetaan keskitettyyn kansalliseen tietokantaan passin paikallisen RFID- (engl. *Radio Frequency IDentification*) eli radiotaajuudella toimivan sirun lisäksi [36]. Verrattuna esimerkiksi saksalaiseen toteutukseen, jossa biometriset tunnisteet tallennetaan ainoastaan paikallisesti passin sirulle, suomalaisessa toteutuksessa on mahdollista, että biometriset tunnistetiedot voivat joutua helpommin väärinkäytöksen uhriksi, tai niitä voidaan käyttää ennalta määrittelemättömään

tarkoitukseen, kuten rikosten selvittämiseen [36]. Kansainvälisen siviili-ilmailujärjestön (International Civil Aviation Organization, ICAO) määritelmissä biometrisen passin tunnistetiedoilta ei vaadita muuta kuin paikallista tallentamista passin RFID-sirulle [37].

Vahvuudet: Biometrisen passin käytön hyvinä puolina voidaan nähdä, että se on laajasti käytössä oleva, turvallinen ja vahva tunnistamisväline matkustusasiakirjana. Sen avulla rajavalvontaa voidaan nopeuttaa ja sujuvoittaa, kun käytetään automaattisia passinlukulaitteita. Biometrisen passin väärentäminen ja kopioiminen on huomattavasti vaikeampaa kuin perinteisten passien.

Biometrinen passi täytyy uusia suhteellisen usein eli viiden vuoden välein. Tällöin passiin saadaan myös aina tuoreempi valokuva passin haltijasta, koska passiin kelpaa hakemisen hetekellä korkeintaan kuusi kuukautta vanha valokuva. Passin kuvan uusimista puoltaa se, että vaikka kasvot ovatkin fysiologinen biometrinen tunniste, ne voivat muuttua ajan mittaan melko paljon.

Heikkoudet: Tällä hetkellä saman standardin mukainen biometrinen passi on käytössä vain Euroopan unionin alueella. Muissakin maissa on laajalti käytössä biometrisia passeja, mutta niiden tekniikat saattavat hieman poiketa toisistaan. Maailmassa on kuitenkin lukuisia maita, joissa ei ole käytössä biometrista passia. Tästä syystä, ja muutenkin erilaisten teknisten häiriötilanteiden varalta, tarvitaan edelleen miehitettyjä rajavalvontapisteitä.

Mahdollisuudet: Voidaan esittää kysymys, voiko biometrinen passi korvata tulevaisuudessa nykyisen henkilökortin niin, että siihen sisällytetään lisäksi esimerkiksi nykyisen ajokortin ja kelakortin tiedot. Tällöin kuitenkin nykyinen passi olisi mielekästä muuttaa käytännön syistä nykyisen henkilökortin kokoiseksi ja malliseksi. Tämä taas ei liene kovinkaan todennäköistä, koska nykyinen passin ulkomuoto on kansainvälisesti sovittu standardi. Nykyinen henkilökortti tosin sisältää jo automaattisesti kelakortin tiedot, mutta ajokortin tiedot halutaan säilyttää erillisessä rekisterissä.

Toisena kysymyksenä voidaan esittää, olisiko mahdollista käyttää biometrista passia myös muussa viranomaisasioinnissa biometrisesti kuin vain matkustusasiakirjana. Tällä hetkellä varsinkin ajokorttia ja kuvallista henkilökorttia käytetään, ja ne ovat myös laajasti hyväksyttyjä *de facto* henkilöllisyystodistuksena asioinnissa eri viranomaisten kanssa, mutta niissä ei ole vahvaa biometrista tunnistetta. Biometrisen passin käyttäminen vaatisi taas vielä tällä hetkellä kalliiden ja harvinaisten lukulaitteiden käyttöönottoa.

Uhat: Biometrisessa passissa on edelleen teknisiä puutteita, ja sitä on mahdollista kopioida tai väärentää. Lisäksi biometrinen passi ei ole alkuunkaan turvallinen ja vahva tunnistusväline, jos sitä alunperin hakenutta henkilöä ei voida tunnistaa varmasti. Tämä kohta tosin pätee kaikkiin henkilöllisyystodistuksiin, ja ongelma korostuu varsinkin, kun henkilö on hakemassa ensimmäistä passiaan tai henkilökorttiaan.

6.2.2 Tapaus: Sormenjälkitunnistus verkkokaupassa

Uusimmissa älypuhelimissa on integroituna sormenjälkiskanneri, jonka pääasiallinen käyttötarkoitus on toimia vaihtoehtona puhelimen suojakoodille näytön lukituksen avaamiseen. Uudempana käyttösovelluksena tätä sormenjälkiskanneria voidaan käyttää myös verkkokaupassa maksujen hyväksymiseen perinteisten salasanojen sijaan [67].

Tässä esimerkkitapauksessa selvinä toimijoina on useita yrityksiä, jotka ovat vuorovaikutuksessa keskenään. Yksi toimija on puhelinvalmistaja tai sen alihankkija, joka toteuttaa itse sormenjälkiskannerin. Seuraava toimija on *FIDO Alliance* [68], joka on useiden eri yritysten yhteenliittymä ja jonka tarkoituksena on edistää verkossa tapahtuvaa turvallista autentikointia. Yksi toimija on maksutapahtuman välityspalvelu *PayPal*, joka lopulta välittää maksutapahtuman tiedot maksun saavalle yritykselle.

Palvelua käyttävän yksityishenkilön roolina tässä tapauksessa on lähinnä valita se, haluaako hän käyttää kyseistä palvelua.

Vahvuudet: Puhelimen käyttäjän kannalta maksutapahtuma on nopeampi ja myös turvallisempi, koska käyttäjän ei tarvitse syöttää salasanaa maksun varmistamiseksi. Tällöin salasanaa ei voi unohtaa, eikä toisaalta tarvitse huolehtia, ettei kukaan voi nähdä, kun salasanaa syötetään. PayPalin etuna yleisesti maksunvälittäjänä on myös se, ettei maksunsaaja saa tietoonsa maksajan kaikkia luottokortin tietoja, vaan Paypal ainoastaan välittää maksun perille.

Heikkoudet: Tällä hetkellä sormenjälkitunnistus on käytössä vasta PayPal-maksunvälitysjärjestelmässä, ja se on yhteensopiva vain tiettyjen Samsungin puhelinmallien kanssa. Lisäksi PayPal-maksunvälitysjärjestelmä ei ole erityisen laajalti käytössä varsinkaan suomalaisissa verkkokaupoissa.

Mahdollisuudet: Mikäli sormenjälkiskannerilla varustetut älypuhelimet yleistyvät ja ne todetaan tarpeeksi turvallisiksi, voidaan sormenjälkitunnistusta hyödyntäviä palveluita lisätä. Esimerkiksi nykyään suomalaisissa verkkopankeissa käytetään muuttumattoman käyttäjätunnuksen ja vaihtuvan tunnuslukulistan yhdistelmää tunnistautumiseen. Tämä olisi mahdollista korvata esimerkiksi älypuhelimen sormenjälkitunnistuksella. Tätä maksutapaa voisi käyttää tulevaisuudessa myös perinteisessä kaupankäynnissä korttimaksamisen sijaan turvallisempana vaihtoehtona.

Uhat: Älypuhelinten sormenjälkiskannerit ovat suhteellisen epäluotettavia, ja niitä voidaan huijata melko yksinkertaisin menetelmin. Lisäksi tarvitaan vaihtoehtoinen salasanavarmistus, jos esimerkiksi älypuhelimen sormenjälkiskanneri menee epäkuntoon. On mahdollista, että maksunvälityssovelluksen kautta käyttäjän sormenjälkitiedot vuotavat ulkopuolisten saataville.

6.2.3 Tapaus: DNA-tunnistus rikostutkinnassa

Teknisessä rikostutkinnassa pyritään etsimään rikospaikalta etenkin sormenjälki- ja DNA-näytteitä. Nykyään käytetään yhä enemmän DNA-näytteitä niiden suuremman tarkkuuden

takia.

Rikostutkinnassa selvä toimija on yhteiskunta, jonka voidaan nähdä harjoittavan niin sanottua vallan kolmijako-oppia. Biometriikoiden hyödyntämiseen rikostutkinnassa tarvitaan tämän mahdollistavaa lainsäädäntöä, tuomioistuinta, joka tekee mahdolliset päätökset, ja toimeenpanovaltaa, joka tekee tutkimukset. Käytännössä nämä eivät erotu selkeästi toisistaan ja voivat olla päällekkäisiä.

Yksittäinen kansalainen on taas alisteisessa asemassa yhteiskuntaan verrattuna, mutta lainsäädännöllä täytyy varmistaa heidän oikeusturvansa.

Vahvuudet: Varsinkin DNA-tunnisteen avulla voidaan hyvin suurella todennäköisyydellä tunnistaa henkilöllisyys, jos on käytettävissä vertailunäyte. DNA-tunnistusta voidaan käyttää rikostutkinnassa sekä todisteena että poissulkemaan epäiltyjä.

Heikkoudet: Tarvitaan vertailunäyte, johon voidaan verrata tutkittavaa näytettä. Rikospaikalta löytynyt DNA-näyte ei itsessään kerro muuta kuin sen, että kyseisen henkilön DNA:ta on jollakin tavalla kulkeutunut jossakin vaiheessa näytteen löytöpaikalle. Jos vertailunäytettä ei ole saatavilla, rikospaikalta taltiotu DNA-näyte saattaa kuitenkin paljastaa sukupuolen. Lisäksi DNA-tunnisteiden analysointi vaatii edelleen paljon resursseja: tarvitaan erityisesti koulutettua henkilöstöä ja kalliita laboratoriolaitteistoja. Lisäksi se on hidasta.

Mahdollisuudet: DNA-näytteiden avulla hankittujen uusien todisteiden avulla on myös vapautettu useita aiemmin rikoksista syyllisiksi tuomittuja henkilöitä.

Uhat: Esimerkiksi rikoksesta epäiltyjen oikeusturvan kannalta mahdollista syyllisyyttä ei pitäisi koskaan ratkaista pelkästään DNA-näytteiden perusteella. DNA-näytettä pitäisi käyttää ainoastaan rikostutkinnassa lisänäytöksi ja tukemaan muuta rikostutkintaa. Lisäksi voidaan esittää kysymys, kuinka laajasti ja minkätyyppisten rikosten selvittämisessä on mielekästä käyttää apuna DNA-tutkintaa. Tästä on esimerkkinä vuonna 2014 Tampereella tapahtuneen henkirikoksen tutkinta, jossa poliisi

on kerännyt suurelta joukolta lähialueen miespuolisten henkilöiden DNA-näytteitä poissulkeakseen epäiltyjä [64].

6.3 Biometrisen tunnistamisen huolenaiheita

Biometrista tunnistetietoa kerättäessä on mahdollista saada selville samalla muutakin henkilökohtaista, muun muassa terveydentilaan liittyvää tietoa. Useimmat muut tunnistusmenetelmät kuin kasvontunnistus, sormenjälkitunnistus, puhujantunnistus ja käsialatunnistus voidaan samalla kokea tunkeileviksi.

Esimerkiksi silmän iiriksen eli värikalvon, samoin kuin silmän verkkokalvon kuvaaminen voivat paljastaa tunnistettavasta henkilöstä useita erilaisia sairauksia. Lisäksi esimerkiksi käden verisuonien tunnistuksessa voidaan saada tietoa sydän- ja verisuonitaudeista. Näiden pitäisi olla kuitenkin merkityksettömiä, mikäli kuitenkin itse tunnistuksen kannalta saadaan taltioitua edustava kuva henkilöstä.

Esimerkiksi tietyllä tavalla epämuodostuneet sormet voidaan yhdistää tiettyyn perinnöliseen vaivaan [2]. Geenitekniikan kehittyessä on pelkona, että biometrisista tunnisteista voidaan päätellä yhä enemmän ihmisen terveyteen liittyvää tietoa. Tämä voi johtaa esimerkiksi riskialttiiksi luokiteltavien ihmisten järjestelmälliseen syrjintään vakuutusyhtiöissä [2].

Toisaalta käyttäytymiseen perustuvia tunnistusmenetelmiä ei yleensä pidetä yhtä tunkeilevina kuin fysiologisia menetelmiä, mutta esimerkiksi kävelytyyliin, puhujantunnistukseen ja käsialantunnistukseen perustuvissa menetelmissä voi olla mahdollista saada tietoa esimerkiksi tunnistettavan neurologisista sairauksista.

Yllä mainitut tunnistettavan henkilön terveydentilaan liittyvät mahdolliset sivulöydökset eivät ole ongelmana, jos näitä tietoja ei etsitä eikä talleneta biometrisessa tunnistusjärjestelmässä. Mahdollisuutena kuitenkin on, että esimerkiksi vakuutusyhtiö saisi tiedon piilevistäkin sairauksista ja käyttäisi näitä tietoja perusteena tehdessään päätöksiä

esimerkiksi sairaus- ja tapaturmavakuutuksista.

6.3.1 Yleisiä harhakäsityksiä, jotka liitetään biometrisen tunnistamisen käyttöön

Seuraavassa on esitetty muutamia kirjallisuudesta [25] poimittuja biometriseen tunnistamiseen yleisesti liitettyjä harhakäsityksiä, jotka saattavat aiheuttaa biometristen järjestelmien käyttäjissä epäluottamusta niiden turvallisuutta ja yksityisyyden suojaa kohtaan.

Monet henkilöt saattavat kokea, että biometriset tunnistusjärjestelmät keräävät liikaa henkilökohtaista tietoa. Tällöin järjestelmän käyttäjä voi tuntea luovuttavansa liikaa tietoa saamatta siitä tarpeeksi hyötyä. Tämän vuoksi kerättävällä tiedolla ja sen käyttökohteella pitää olla selvä yhteys toisiinsa, ja tämä pitää tuoda esille riittävän selkeästi järjestelmän käyttäjille.

Biometrisia tunnisteita saatetaan kerätä ja jakaa ilman lupaa tai riittävää selitystä. Voidaan esittää kysymys, onko käyttäjän hallitavissa, mihin ja miten henkilökohtaista tietoa käytetään. Myös tällöin käyttäjälle pitää selventää, missä rajoissa tiettyä biometrista tunnistetta käyteään ja miten käyttäjä voi kontrolloida antamansa tiedon muuta käyttöä.

Biometrisillä järjestelmillä on mahdollista valvoa ja tunnistaa henkilöitä julkisilla paikoilla esimerkiksi kasvontunnistuksen avulla sekä liittää tunnistukseen paikka- ja aikatietoja. Tässäkin tapauksessa käyttäjälle pitää selventää jo ennen tietojen keräämistä, missä rajoissa tiettyä biometrista tunnistetta käyteään ja mihin tarkoitukseen.

Biometriikat paljastavat henkilön terveydentilaa koskevia asioita. Biometrista dataa on mahdollista käyttää alkuperäisen käyttötarkoituksen lisäksi myöhemmin myös muun muassa terveystietojen selvittämiseen ilman henkilön lupaa. Biometrisen tunnisteen käytölle on asetettava tarkat rajat, ja niitä on valvottava.

Biometriikka on mahdollista varastaa ja käyttää uudelleen. Jos biometrinen tunniste onnistutaan varastamaan tai kopioimaan, sitä ei voida käyttää enää alkuperäisen käyttäjän tunnistamiseen. Näitä uhkakuvia vastaan voidaan puolustautua kappaleessa 4.3 esitetyin

toimenpitein.

Eräs väärinkäsitys on, että biometrinen tunnistusjärjestelmä voisi vahingoittaa käyttäjäänsä, kuten esimerkiksi iiristunnituksessa käytettäisiin laseria, mutta todellisuudessa käytetään kameraa. Käyttäjille on selvitettävä tarkasti, miten todellisuudessa biometrinen tunnistusjärjestelmä toimii vahingoittamatta käyttäjäänsä.

6.3.2 Biometriaan liitetyt uhkakuvat

Seuraavassa on esitelty joitakin biometriikoiden käytölle ja käyttöönotolle liittyviä mahdollisia uhkakuvia Ailisto et al. mukaan [9].

Yksi jo todellinen uhkakuva on, että biometrista dataa saatetaan käyttää muuhun tarkoitukseen kuin alunperin on suunniteltu ja luvattu käyttää. Esimerkiksi Suomessa poliisi on halunnut avata passien sormenjälkirekisterin myös rikostutkinnan käyttöön [47]. Tällaisessa tapauksessa on vakavan pohdinnan paikka, onko käyttötarkoitussidonnaisuus vahvempi periaate kuin mahdollisten rikosten selvittäminen.

Mahdollinen tulevaisuuden kehityskulku voi olla joidenkin henkilöiden syrjäytyminen tietoyhteiskunnasta. Tällöin henkilö, joka jostakin syystä ei voi, osaa tai halua käyttää biometrista järjestelmää, voi jäädä paitsi varsinkin sellaisista palveluista tai eduista ja alennuksista, joissa vaadittaisiin biometrisen tunnistamisen käyttöä. Tämä kehityskulku on havaittavissa jo muutenkin monien viranomaispalveluiden keskittyessä yhä enemmän verkossa tapahtuvaksi. Yksinomaan biometrisen tunnistamisen käytölle pitäisi olla vaihtoehtoinen tunnistusmenetelmä ainakin viranomaisasioinnissa.

Viranomainen, yritys, yrityksen työntekijä tai yksityinen henkilö saattavat luottaa liikaa järjestelmän toimivuuteen ja varmuuteen. On pidettävä mielessä, että mikään tekninen järjestelmä ei voi olla täysin luotettava ja toimintavarma. Sama pätee yhtä lailla biometriseen tunnistamiseen. Biometristen järjestelmien tapauksessa on myös punnittava tasapainoa väärien hylkäysten ja väärien hyväksyntien välillä.

Biometrinen tieto saattaa vuotaa järjestelmän ulkopuolelle, ja sitä saatetaan myydä

edelleen. Luvattoman ja rikollisen käytön lainsäädännölinen sanktioiminen ei pelkästään riitä, vaan järjestelmä on rakennettava alunperinkin tarpeeksi luotettavaksi. Jos rikollisilla on houkutus saada haltuunsa muiden ihmisten biometrista tai muuta henkilökohtaista tietoa, näin todennäköisesti tapahtuu teon laittomuudesta huolimatta.

Edelliseen liittyen identiteettivarkauksien ja -huijausten mahdollisuus pitäisi vähentyä, kun siirrytään käyttämään yhä enemmän biometrista tunnistamista. Toisaalta kun verkkoasioiminen yleistyy, on yksinkertaisempaa esiintyä muuna henkilönä kuin on todellisuudessa tai syrjäyttää toisen henkilön identiteetti. Tällöin korostuu biometrisen järjestelmän kaikkien osien turvallisuudesta huolehtiminen.

On mahdollista, että biometrista tunnistusta ryhdytään käyttämään sellaisissa kohteissa ja käyttötarkoituksissa, joissa se ei ole tarkoituksenmukaista tai perusteltua. Tällöin ihmiset voivat rekisteröityä biometrisiin järjestelmiin liian kevyin perustein. Saattaa olla, että esimerkiksi kaupat ja muut yritykset ryhtyvät tarjoamaan alennuksia ja muita etuja vain biometrista tunnistusta vastaan. Tällöin jokaisen kuluttajan on harkittava, ovatko tarjotut edut tunnistautumisen arvoisia.

6.4 Pohdintaa

Biometristen tunnisteiden käyttökohteet saattavat lisääntyä tulevaisuudessa suuresti yleisen tekniikan kehittymisen ja halpenemisen trendin sekä uusien kaupallisten sovellusten ideoinnin myötä. Yksityisyyden suojan kannalta eräs olennainen kysymys onkin, onko mielekästä ylipäätään soveltaa biometrista tunnistamista muualla yhteiskunnassa kuin viranomaistoiminnassa, esimerkiksi matkustusasiakirjoissa sekä rikosteknisessä tunnistamisessa. Viranomaisyhteyksissä käytetyt biometriikat eivät todennäköisesti tule aiheuttamaan suuria riskejä yksityisyyden suojan kannalta, kunhan huolehditaan riittävästä tietosuojasta sekä pitäydytään alkuperäisessä käyttötarkoituksessa.

Biometristen tunnisteiden laajeneva käyttö itsessään saattaa olla ongelmallista. Jos

kaupallisia sovelluksia ryhdytään käyttämään yhä useammin ja arkipäiväisemmin, ihmiset eivät välttämättä tiedosta oikeuksiaan eikä tieto- ja yksityisyydensuojan periaatteita. Mitä useammassa biometrisessä järjestelmässä henkilö on rekisteröityneenä, sitä hankalampaa voi olla kontrolloida itseään koskevien tietojen käsittelyä ja mahdollista poistumista järjestelmästä. Samalla kasvaa todennäköisyys, että näistä jonkin järjestelmän tiedot joutuvat vääriin käsiin.

Eräs perustavanlaatuinen kysymys on, miten alun perin voidaan tunnistaa oikea henkilöllisyys, kun henkilö on rekisteröitymässä biometriseen järjestelmään, esimerkiksi hakemassa biometrista passia. Tämä niin sanottu ensitunnistamisen ongelma on ollut olemassa jo ennen biometriikoiden aikakautta. Mikäli esimerkiksi passia hakevalla henkilöllä ei ole jo voimassa olevaa passia tai henkilökorttia, poliisin ohjeiden [65] mukaan hakijan henkilöllisyys pyritään selvittämään muiden asiakirjojen, rekistereiden ja haastattelun avulla. Selvästikin vain viranomaisella on riittävät valtuudet ja valmiudet suorittaa ensitunnistus riittävän huolellisesti biometriseen järjestelmään rekisteröidyttäessä. Myös vahvan biometrisen tunnisteen kaupallisen palveluntarjoajan, esimerkiksi pankin, on kyettävä tunnistamaan henkilöllisyys jo lain mukaan [61]. Muussa tapauksessa poliisin on suoritettava ensitunnistus edellä mainituin keinoin.

Edellä mainittuja tapauksia suurempi ensitunnistamisen haaste voikin olla muut kaupalliset biometriset järjestelmät. Jos esimerkiksi yritys haluaisi ryhtyä käyttämään biometrista tunnistusta työntekijöidensä kulunvalvontaan tai vastaavasti kuntosali asiakkaidensa kulunvalvontaan, näillä tahoilla ei ole käytettävissä biometrisen passin lukulaitetta eikä todennäköisesti yhtä kokenutta ja koulutettua henkilökuntaa tunnistamaan henkilöä muusta henkilöllisyystodistuksesta. Toisaalta voidaan ajatella, että näissä tapauksissa yrityksen työntekijöiden ja vastaavasti asiakkaiden ensitunnistaminen matkustusasiakirjan vaatimalla tarkkuudella ei ole edes välttämätöntä. Lisäksi vain paikallisesti käytettävissä järjestelmissä, kuten henkilökohtaisessa käytössä olevan tietokoneen tai älypuhelimen sormenjälkilukijaan rekisteröitymisessä ei ole nähtävissä ensitunnistamisen ongelmaa, koska

näissä tapauksissa käyttäjän sormenjäljen on tarkoitus vain korvata muutoin käytettävä salasana.

Biometriset tunnistusjärjestelmät voivat olla houkuttelevia kohteita rikollisille, joiden tavoitteena on varastaa tunnistetietoja. Toistaiseksi biometristen tunnisteiden käytöllä voidaan katsoa olevan vielä suhteellisen pieni riski yksityisyyden suojan kannalta. Biometristen tunnistetietojen todennäköisyys joutua vääriin käsiin on vielä pieni, koska biometrisen tunnistuksen käyttö on rajallista muualla kuin viranomaisyhteyksissä. Kuitenkin toteutuessaan identiteettivarkaudesta koituvat seuraukset ovat todellisia, jos käytetään peruuttamattomia biometrisia tunnisteita. Identiteettivarkaudesta voi seurata taloudellisten menetysten ohella vahinkoa myös henkilön maineelle ja kunnialle, mitä voi olla hyvin hankala kompensoida.

Tässä luvussa käsiteltiin ensin erilaisten biometristen teknologioiden riskejä yksityisyyden suojan näkökulmasta. Tämän jälkeen käytettiin esimerkkeinä kolmea erilaista tapausta, miten biometriikat voivat vaikuttaa yksityisyyteen. Lopuksi tarkasteltiin biometriseen tunnistamiseen liittyviä huolenaiheita ja uhkakuvia.

Luku 7

Ratkaisut

Tässä luvussa esitellään suuri joukko eri lähteissä yleisesti hyväksyttyjä menettelytapoja, joilla voidaan parantaa biometristen tunnistusjärjestelmien turvallisuutta.

7.1 Yleisiä periaatteita

Koska biometrinen data on yksityisyyden suojan näkökulmasta tarkasteltuna sekä haasteellisempaa että arkaluontoisempaa kuin muut henkilötiedot, on sen turvaamiseen kiinnitettävä erityistä huomiota. Tällöin voidan varmistaa yksityisyyden suojan säilyminen ja luoda luottamusta biometrisia tunnistusjärjestelmiä käyttävien ihmisten keskuudessa. Harkittaessa biometrisen tunnistusjärjestelmän käyttöönottoa, olisi Ailisto et al. [9] mukaan kiinnitettävä huomiota ainakin seuraviin perusasioihin:

1. Tunnistusjärjestelmää, joka perustuu ainoastaan biometriikkaan, on suositettavaa käyttää vain sellaisissa sovelluksissa, joihin liittyy käyttäjän ja palveluntarjoajan kannalta vähäinen taloudellinen tai muunlainen arvo.

2. Edellistä suuremman taloudellisen tai muun arvon sovelluksissa on suositettavaa käyttää ratkaisua, jossa on yhdistettynä biometriikkan sekä samanaikaisesti esimerkiksi älykortin tai salasanan käyttö.

3. Biometrinen tieto on suositettavaa säilyttää hajautetusti järjestelmän käyttäjän hallitsemalla välineellä, kuten älykortilla, verrattuna paikallisiin ja keskitettyihin tietokantoihin. Tällöin voidaan pienentää väärinkäytösten riskiä ja minimoida järjestelmään murtautumisen haittavaikutuksia.

4. Järjestelmään tallennettava biometrinen data on salattava mahdollisimman varhaisessa vaiheessa, ja siihen pääsy on tehtävä hankalaksi.

5. Biometriset ja muut henkilötiedot on tallennettava toisistaan erilleen, ja mikäli mahdollista, myös fyysisesti erilleen toisistaan. Tällöin voidaan toteuttaa myös anonyymejä biometrisia tunnistusjärjestelmiä.

6. Biometrinen tieto tulisi tallentaa mahdollisuuksien mukaan käyttäjän hallussa olevalle tallennusvälineelle, kuten älykortille. Ellei se ole mahdollista, tiedot on tallennettava vain tiettyyn, suojattuun paikkaan.

7. Biometrisen datan vuotaminen järjestelmän ulkopuolelle kaikissa tiedonsiirron vaiheissa on pyrittävä estämään huolellisella järjestelmän suunnittelulla ja käytön sekä ylläpidon ohjeistuksella.

7.2 Parhaat käytänteet yksityisyyden suojaamiseksi

Seuraavassa esitellään International Biometric Groupin (IBG) ehdottamat [27] *parhaat käytänteet* (engl. *best practices*) eli menettelytavat, joilla voidaan parantaa biometristen järjestelmien yksityisyyden suojaa niiden käyttöönotossa. Parhaat käytänteet voidaan nähdä suosituksina, joiden avulla voidaan rakentaa kappaleessa 6.1 esitettyjä yksityisyyttä ylläpitäviä ja yksityisyyttä suojaavia biometrisia järjestelmiä. Ei voida kuitenkaan olettaa, että biometrinen järjestelmä voitaisiin käytännössä toteuttaa noudattamaan kaikkia esitettyjä parhaita käytänteitä. Siksi kyseisiä suosituksia voidaan käyttää tietynlaisena

tarkistuslistana, kun halutaan rakentaa mahdollisimman hyvä järjestelmä yksityisyyden suojan kannalta.

Käytänteet on jaettu neljään ryhmään: Laajuus ja mahdollisuudet, Datan suojaaminen, Henkilökohtaisen datan hallinta sekä Tiedonanto, auditointi, vastuullisuus ja valvonta.

Laajuus ja mahdollisuudet

Käyttöalueen rajaus. Biometrista järjestelmää ei pitäisi laajentaa toimimaan alun perin suunniteltua käyttötarkoitusta suuremmassa mittakaavassa. Käyttötarkoituksen laajentamisesta tai supistamisesta pitäisi ilmoittaa julkisesti riippumattoman tarkastajan valvomana. Tällöin järjestelmään rekisteröityneillä käyttäjillä pitäisi olla halutessaan mahdollisuus jättäytyä pois.

Yleisen ja yksilöllisen tunnisteen luominen. Biometrista tietoa ei pitäisi käyttää yleisen ja yksilöllisen tunnisteen (engl. *Universally Unique Identifier, UUID*) toteuttamiseen. Yleisen ja yksilöllisen tunnisteen käytössä on väärinkäytöksen vaara, jos sen avulla kerätään ja yhdistetään eri tietokantoja.

Biometrisen tiedon rajoitettu tallennus. Biometrista tietoa tulisi tallentaa vain tiettyä tarkoitusta varten eikä tietoa pitäisi säilyttää kauemmin kuin sille on tarvetta. Biometrinen tieto tulisi poistaa tai hävittää, jos järjestelmän käyttö lopetetaan tai tietty käyttäjä lopettaa järjestelmän käytön. Tämä koskee myös esimerkiksi mallinteita, jotka on luotu verifiointivaiheessa.

Järjestelmän mahdollisuuksien arviointi. Järjestelmän yksityisyyden suojalle aiheuttamia riskejä analysoitaessa pitäisi tutkia myös, mitä mahdollisia muita riskejä järjestelmän käytöllä on sen alkuperäisen käyttötarkoituksen lisäksi. Biometrisia järjestelmiä suunnitellaan harvoin yksityisyyttä loukkaaviksi, mutta esimerkiksi verifiointiin tarkoitettua järjestelmää voi olla myös mahdollista käyttää identifiointiin.

Epäoleellisen tiedon kerääminen tai tallennus. Muun kuin biometrisen tiedon kerääminen pitäisi rajoittaa niin vähiin kuin tarpeellista identifioinnin tai verifioinnin suorittamiseksi. Useissa järjestelmissä henkilökohtainen data on jo tallennettu biometrisesta datasta erilleen, joten sitä ei tarvitse kerätä uudestaan.

Alkuperäisen biometrisen datan tallennus. Alkuperäistä biometrista tietoa ei pitäisi tallentaa tunnistettavassa muodossa. Esimerkiksi alkuperäinen kasvokuva tai sormenjälkikuva tulisi tallentaa ainoastaan mallinteen luomisen ajaksi. Sen jälkeen alkuperäinen data olisi tuhottava.

Datan suojaaminen

Biometrisen datan suojaaminen. Biometrinen data pitää suojata järjestelmän kaikissa vaiheissa, kuten rekisteröitymisessä, mallinteen luomisessa, tallennuksessa, tiedonsiirrossa ja tunnistuksessa. Suojaamisessa voi tulla kyseeseen tiedon salaus, yksityiset tietoverkot, fyysisesti turvalliset tilat, tietohallinto sekä tiedon eristäminen.

Tunnistamisen jälkeisen datan suojaaminen. Biometrisen tunnistamisen päätöksentekoa koskeva data pitäisi suojata. Vaikka tämä data ei välttämättä sisällä biometrista tietoa, sen sieppaus saattaa mahdollistaa pääsyn muuhun henkilökohtaiseen dataan. Tämä suojaus on erityisen tärkeä lähtökohtaisesti epäluotettavissa ympäristöissä, kuten internetissä.

Rajoitettu järjestelmään pääsy. Biometrisen järjestelmän hallinta ja ylläpito pitäisi olla rajoitettu vain tietyille henkilöille ja määrätyissä tilanteissa. Erityisen arkaluonteista dataa käsiteltäessä saatetaan vaatia useamman ylläpitäjän hyväksyntä. Esimerkiksi biometrista dataa sisältäviin tietokantoihin pitää olla vahva hallinta ja valvonta.

Biometrisen datan eristäminen. Biometrinen data pitäisi säilyttää erillään muusta henkilökohtiasesta tiedosta, kuten nimestä, osoitteesta tai potilastiedoista. Tilanteesta riippuen tiedot voivat olla loogisesti tai fyysisesti erillisissä tietokannoissa.

Järjestelmän lopettaminen. Biometrisen järjestelmän toiminnan päättyessä olisi oltava valmiina menetelmät, joilla tiedot voidaan tuhota luotettavasti. Tätä voisi valvoa riippumaton auditointiryhmä.

Henkilökohtaisen datan hallinta

Mahdollisuus perua rekisteröityminen. Järjestelmän käyttäjällä pitäisi olla oikeus hallita hänen oman biometrisen datansa käyttöä. Pyydettäessä tulisi olla mahdollisuus tuhota häntä koskeva biometrinen data. Viranomaiskäytössä tämä ei välttämättä ole mahdollista ilman, että järjestelmä muuttuu toimimattomaksi.

Mahdollisuus korjata omia tietoja. Biometrisen järjestelmän käyttäjällä pitäisi olla mahdollisuus korjata, päivittää ja tarkistaa hänestä tallennetut biometriset tiedot. Jo lähtökohtaisesti tilanne, jossa ei ole mahdollisuutta tarkistaa itseään koskevia henkilötietoja, on ristiriidassa yksityisyyden suojan perusperiaatteiden kanssa.

Nimetön rekisteröityminen. Sovelluksesta riippuen käyttäjillä tulisi olla mahdollisuus rekisteröityä järjestelmään anonyymisti. Jos sovellus ei vaadi tarkkoja henkilötietoja, niitä ei pitäisi tarvita antaa järjestelmälle. Esimerkiksi tietoverkoissa tietyissä tapauksissa, joissa voidaan muutenkin käyttää keksittyjä nimimerkkejä, biometrisen järjestelmän ei tarvitse tallentaa henkilön aitoa identiteettiä.

Tiedonanto, auditointi, vastuullisuus ja valvonta

Kolmannen osapuolen vastuullisuus, auditointi ja valvonta. Varsinkin julkisen sektorin ja suuren mittakaavan biometristen järjestelmien tulisi olla riippumattoman tahon valvottavissa ja tarkistettavissa.

Auditoinnin julkisuus. Riippumattoman auditoinnin tuottama data pitäisi olla kaikille vapaasti saatavilla. Riippumattomien osapuolten tulee seurata ja tarkastaa biometrisia järjestelmiä, jotka voivat vaarantaa yksityisyyttä. Näin saatua dataa voidaan

käyttää herättämään julkista keskustelua biometristen järjestelmien vaikutuksesta yksityisyyteen.

Järjestelmän tarkoituksen julkisuus. Biometrisen järjestelmän käyttötarkoituksen pitäisi olla kaikille julkista tietoa. Esimerkiksi jos järjestelmän käyttötarkoitukseksi on ilmoitettu verifiointi, sitä ei pitäisi käyttää identifiointiin. Jos järjestelmän käyttötarkoitus ei ole täysin julkinen, sen vaikutuksia yksityisyyteen voi olla vaikea arvioida perusteellisesti.

Rekisteröitymisen julkisuus. Käyttäjälle on selvästi ilmoitettava, kun hän on rekisteröitymässä biometriseen järjestelmään, näin myös silloin, kun mallinteita ei tallenneta pysyvästi. Esimerkiksi ajokortin valokuvaa voidaan käyttää kasvontunnistusjärjestelmässä tai puhelun tallennetta puheentunnistusjärjestelmässä käyttäjän tietämättä.

Tunnistamisen julkisuus. Käyttäjälle on selvästi ilmoitettava, kun hän siirtyy paikkaan tai alueelle, jossa käytetään biometrista tunnistamista ilman käyttäjän nimenomaista suostumusta.

Biometrisen tiedon käytön julkisuus. Biometrista tietoa käyttävien tahojen on selvästi kerrottava käyttäjille, mihin tarkoitukseen tietoa käytetään. Tietoa pitäisi käyttää vain siihen tarkoitukseen, mihin se alunperin kerättiin. Jos tiedon käyttöä laajennetaan, siihen on saatava järjestelmän käyttäjien suostumus, eikä kieltäytymisestä pidä seurata sanktioita.

Rekiströitymisen pakollisuuden tai vapaaehtoisuuden julkisuus. Käyttäjälle on selvästi ilmoitettava, onko biometriseen järjestelmään rekisteröityminen pakollista, esimerkiksi biometrisen passin tapauksessa, vai vapaaehtoista. Jos rekisteröityminen on vapaaehtoista, pitäisi vaihtoehtoinen rekisteröityminen olla valmiiksi olemassa.

Järjestelmän operaattorien ja valvojien julkisuus. Biometrisesta järjestelmästä vastuulliset henkilöt pitäisi olla selkeästi tiedossa, samoin se, kenelle voi esittää kysymyksiä

tai vaatimuksia ja kenelle voi valittaa järjestelmän ongelmista.

Rekisteröitymisen, verifioinnin ja identifioinnin julkisuus. Biometrisen järjestelmän käyttäjille pitäisi tiedottaa, miten järjestelmä toimii sen kaikissa eri vaiheissa.

Biometrisen datan ja järjestelmän turvaamisen julkisuus. Biometrisen järjestelmän käyttäjien pitäisi olla tietoisia siitä, miten järjestelmän sisältämä data turvataan kaikissa eri vaiheissa. Tähän sisältyy muun muassa tietojen salaaminen, eristettyjen tietoverkkojen käyttö ja biometrisen tiedon eristäminen muista henkilötiedoista.

Varajärjestelmän julkisuus. Tarvittaessa biometrisen järjestelmän varajärjestelmän tulisi olla niiden henkilöiden käytettävissä, jotka eivät halua tai voi rekisteröityä biometriseen järjestelmään, eikä varajärjestelmän käyttö pitäisi olla rangaistavaa tai syrjivää.

Yhteenvetona biometristen järjestelmien suunnittellussa voidaan yleisinä periaatteina mainita myös seuraavia seikkoja:

1. Yksityisyyden suojan kunnioittaminen pitää olla aina etusijalla.

2. Suhteellisuusperiaatteen eli saavutettavien etujen ja mahdollisten haittojen suhteen pitää olla hyväksyttävä. Esimerkiksi, miten tunnistamisen turvallisuus ja tehokkuus suhtautuvat tietoturvaan ja yksityisyydensuojan säilyttämiseen. Tärkeä arviointioperuste on suhteellisuusperiaate, kun ollaan valitsemassa tunnistusmenetelmää biometrisen tai jonkin muun perinteisen menetelmän välillä.

3. Käyttäjän lupa ja tiedonanto. Biometrisen järjestelmän käyttäjältä tulee saada suostumus järjestelmän käyttöön, ja se pitää voida myös perua. Käyttäjän pitää ymmärtää biometrisen järjestelmän käyttötarkoitus, biometristen tietojen säilytyspaikka ja se, kenellä tai keillä on oikeus käyttää sitä.

4. Henkilötietolain noudattaminen. Biometrisista tiedoista syntyvää rekisteriä tulee käyttää vain rekisterissä ilmoitettuun tarkoitukseen, eri rekisterien tietojen yhdistäminen pitää estää luvatta sekä rekisteröidyllä henkilöllä tulee olla laillinen mahdollisuus tarkistaa ja oikaista häntä koskevat väärät tiedot.

5. Biometrisia menetelmiä, jotka ovat yksityisyydensuojan kannalta ongelmallisia, tulee — mikäli mahdollista — välttää käyttämästä. Esimerkiksi DNA-tunniste on tällainen, koska siitä on mahdollista saada tietoa perinnöllisistä sairauksista.

6. Biometrisen tiedon suojaaminen tulee suunnitella huolellisesti.

Tässä luvussa esiteltiin suuri joukko eri lähteistä koottuja ja yleisesti hyväksyttyjä menettelytapoja, joilla voidaan parantaa biometristen tunnistusjärjestelmien turvallisuutta ja yksityisyyden suojaa.

Luku 8

Yhteenveto

Tässä opinnäytetyössä on tarkasteltu lukuisia biometristen järjestelmien yksityisyyden suojaan liittyviä kysymyksiä. Kirjallisuuskatsauksessa löydettiin suuri joukko kohteita, joita vastaan biometrisissä järjestelmissä voidaan hyökätä ja täten vaarantaa koko järjestelmän turvallisuus ja käyttäjien yksityisyyden suoja. Lisäksi löydettiin biometrisen tunnistamisen uhkakuvia ja huolenaiheita. Biometrisen tunnistamisen etuja ja haittoja pohdittiin useasta eri näkökulmasta. Ratkaisuksi yksityisyyden suojan turvaamiseksi kirjallisuudesta löydettiin suositusmalleja.

Biometristen tunnistusmenetelmien historiaa tarkasteltiin aluksi lyhyesti. Seuraavaksi käsiteltiin yleisimpiä käytössä olevia fysiologisia ja käytökseen perustuvia biometrisia tunnistusmenetelmiä. Tämän jälkeen perehdyttiin aluksi biometrisen tunnistusjärjestelmän yleiseen periaatteeseen. Lisäksi tarkasteltiin erilaisten biometristen tunnisteiden ominaisuuksia, jotka vaikuttavat niiden soveltuvuuteen biometrisessa tunnistusjärjestelmässä. Näiden lisäksi tutustuttiin biometrisen järjestelmän suorituskykyyn vaikuttaviin tekijöihin sekä kerrottiin, mitä hyötyjä usean biometriikan käytöllä voidaan saavuttaa verrattuna yhden biometriikan käyttöön tunnistusjärjestelmässä.

Opinäytetyössä esiteltiin ensin luvussa 4 periaatetasolla biometrisen järjestelmän mahdollisia haavoittuvuuksia. Tämän jälkeen avattiin seikkaperäisesti erilaisia kohteia, uhkavektoreita, joita vastaan järjestelmässä voidaan hyökätä. Seuraavaksi kerrottiin myös

laajasti puolustusmenetelmistä, joiden avulla voidaan suojautua uhkavektoreita vastaan. Tarkastelussa havaittiin, että sekä mahdollisia uhkavektoreita että puolustuskeinoja on suuri määrä.

Luvussa 5 määriteltiin aluksi yksityisyyden käsitettä yleisellä tasolla. Tämän jälkeen syvennyttiin lähinnä Suomen ja osittain Euroopan unionin lainsäädännön kohtiin, jotka liittyvät läheisesti yksityisyyteen ja yksityisyyden suojaan. Havaittiin, että Suomen lainsäädäntö ei yksiselitteisesti määrittele käsitettä yksityisyys, vaan siitä löytyy mainintoja monen eri lakikokonaisuuden alta. Lisäksi käsiteltiin identiteettivarkauksia.

Opinnäytetyön luvussa 6 pohdittiin tarkemmin, miten erityisesti biometrinen tunnistus vaikuttaa yksityisyyden suojaan ja minkälaisia uhkakuvia biometristen tunnisteiden käyttöön voi liittyä. Biometrisen tunnistuksen vaikutusta yksityisyyteen havainnollistettiin kolmen esimerkkitapauksen avulla. Niistä löydettiin kolme selkeää toimijaa: yhteiskunta, yhteisö ja yksilö.

Luvussa 7 koottiin ratkaisuja, miten biometriseen tunnistamiseen liittyviä haasteita, kuten yksityisyyden suojaa koskevia kysymyksiä, voidaan ratkaista. Havaittiin, että on muutamia yleisiä periaatteita, joita noudattamalla voidaan tarkistaa biometrista järjestelmää suunniteltaessa yksityisyyden suojaan liittyvät tärkeimmät perusasiat. Lisäksi löydettiin kattavampi lista asioita, jotka ottamalla huomioon voidaan rakentaa yksityisyyttä suojaava biometrinen järjestelmä.

Opinnäytetyössä käytettiin lähdemateriaalina runsaasti vertaisarvioituja tieteellisiä julkaisuja ja alan muuta kirjallisuutta, joiden näkökulma on aihepiirin luonteesta johtuen painottunut Yhdysvaltojen suuntaan. Tämä on luonnollista, koska biometristen järjestelmien tutkimus ja kehitys on vahvinta juuri Yhdysvalloissa. Opinnäytteessä haluttiin tuoda esille myös aihepiirin suomalaista näkökulmaa, mutta alan vertaisarvioitujen julkaisujen määrä havaittiin vähäiseksi. Kotimaisten lähteiden vähäisyydestä johtuen jouduin käyttämään opinnäytetyössäni runsaasti itse suomentamaani terminologiaa. Edellä mainituista syistä lähdemateriaalina käytettiin myös kotimaisessa lehdistössä viime aikoina

esiintyneitä alaan liittyviä artikkeleita. Lisäksi lähdemateriaalina oli lukuisia viitteitä Suomen lainsäädännöstä.

Koska useimmat Suomessa käytössä olevat biometriset järjestelmät liittyvät viranomaistoimintaan, tämän opinnäytetyön puitteissa ei ollut mahdollista toteuttaa aihepiiriin liittyvää empiiristä tutkimusta. Kuitenkin opinnäytetyössä haluttiin toteuttaa nimenomaisesti tieteidenvälistä lähestymistapaa. Lisäksi biometrisen tunnistuksen yhteiskunnallisia vaikutuksia ja mahdollisia tulevia käyttökohteita olisi voinut arvioida laajemminkin. Yleisen tekniikan kehittymisen trendin jatkuessa samanlaisena on todennäköistä, että tulevaisuudessa biometrinen tunnistus tulee lisääntymään elämän eri osa-alueilla jatkuvasti. Toivottavasti silloin myös yksityisyyden suojaan kiinnitetään huomiota yhä enemmän.

Lähdeluettelo

[1] J. L. Wayman. Fundamentals Of Biometric Authentication Technologies. *International Journal of Image and Graphics*, 1(1):93–113, Tammikuu 2001.

[2] Salil Prabhakar, Sharath Pankanti ja Anil K. Jain. Biometric Recognition: Security and Privacy Concerns. *IEEE Security and Privacy*, 1(2):33–42, 2003. ISSN 1540-7993.

[3] N. K. Ratha, J. H. Connell ja R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.*, 40(3):614–634, maaliskuu 2001. ISSN 0018-8670. URL `http://dx.doi.org/10.1147/sj.403.0614`.

[4] Anil K. Jain, Patrick Flynn ja Arun A. Ross. *Handbook of Biometrics*. Springer-Verlag New York, Inc., 2007.

[5] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc., 2008.

[6] John R. Vacca. *Biometric Technologies and Verification Systems*. Butterworth-Heinemann, 2007.

[7] K. Delac ja M. Grgic. A survey of biometric recognition methods. Teoksessa *Proceedings of 46th International Symposium Electronics in Marine Elmar 2004*, ss. 184 – 193. Kesäkuu 2004. ISSN 1334-2630.

[8] John D. Woodward Jr., Christopher Horn, Julius Gatune et al. Biometrics: A Look at Facial Recognition. *RAND*, 2003. URL http://www.rand.org/.

[9] Heikki Ailisto, Pasi Ahonen ja Mikko Lindholm. *Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja*. Edita Publishing, 2005. URL http://www.lvm.fi/fileserver/80_2005.pdf.

[10] Anil K. Jain, Arun Ross ja Salil Prabhakar. An introduction to biometric recognition. *IEEE Transaction on Circuits and Systems for Video Technology*, 14:4–20, 2004.

[11] Anil K. Jain, Arun Ross ja Sharath Pankanti. Biometrics: A tool for information security. *IEEE transactions on information forensics and security*, 1:125–143, 2006.

[12] Ville Eloranta. *Silmät auki! Tietoyhteiskunnan uhat ja mahdollisuudet*. Edita Prima, 2008. URL http://web.eduskunta.fi/dman/Document.phx?documentId=xe11608093708578\&cmd=download.

[13] Chris Roberts. Biometric attack vectors and defences. *Computers & Security*, 26(1):14–25, 2007.

[14] Bojan Cukic ja Nick Bartlow. Biometric System Threats and Countermeasures: A Risk Based Approach. *Biometric Consortium Conference*, 2005. http://www.biometrics.org/bc2005/Presentations/Conference/2\%20Tuesday\%20September\%2020/Tue_Ballroom\%20B/Cukic_Threats\%20and\%20countermeasures.pdf
Viitattu 16.3.2012.

[15] Anil K. Jain, Arun Ross ja Umut Uludag. Biometric template security: Challenges and solutions. Teoksessa *In Proceedings of European Signal Processing Conference (EUSIPCO*. 2005.

[16] Defense Information Systems Agency for the US Department of Defense. Biometric Security Checklist for the Access Control STIG, Version 2, Release 1.1,

2007. http://iase.disa.mil/stigs/downloads/doc/biometric_security_checklist_v2r1-1_20071017.doc
Viitattu 22.3.2012.

[17] National Science Technology Council: Subcommittee on Biometrics. Biometrics History, 2006. http://www.biometrics.gov/documents/biohistory.pdf
Viitattu 23.3.2012.

[18] Biometrics information resource. Liveness Detection in Biometric Systems. http://www.biometricsinfo.org/whitepaper1.htm
Viitattu 30.3.2012.

[19] Girija Chetty ja Michael Wagner. Audio-Video Biometric System with Liveness Checks, 2005. URL http://pixel.otago.ac.nz/ipapers/24.pdf.

[20] Anil K. Jain, Sarat C. Dass ja Karthik Nandakumar. Soft Biometric Traits for Personal Recognition Systems. Teoksessa *ICBA*, ss. 731–738. 2004.

[21] Minerva M. Yeung ja Sharath Pankanti. Verification watermarks on fingerprint recognition and retrieval. *J. Electronic Imaging*, ss. 468–476, 2000.

[22] Manfred Bromba. On the reconstruction of biometric raw data from template data, 2006. http://www.bromba.com/knowhow/temppriv.htm
Viitattu 12.4.2012.

[23] Colin Soutar. Biometric System Security. *SECURE - The Silicon Trust Report*, 5, 2002. http://silicontrust.files.wordpress.com/2010/05/secure5.pdf
Viitattu 12.4.2012.

[24] Ruud Bolle ja Sharath Pankanti. *Biometrics, Personal Identification in Networked Society*. Kluwer Academic Publishers, Norwell, MA, USA, 1998. ISBN 0792383451.

[25] National Science Technology Council: Subcommittee on Biometrics. Privacy & Biometrics: Building a Conceptual Foundation, 2006. www.biometrics.gov/docs/privacy.pdf
Viitattu 4.5.2012.

[26] Daniel J. Solove. "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review*, 44(May):745–772, 2007. URL http://ssrn.com/paper=998565.

[27] International Biometric Group (IBG). Best Practices for Privacy-Sympathetic Biometric Deployment. http://bioprivacy.org/best_practices_main.htm
Viitattu 18.5.2012.

[28] International Biometric Group (IBG). BioPrivacy Technology Risk Ratings. http://bioprivacy.org/technology_assessment_main.htm
Viitattu 8.6.2012.

[29] Scientific Working Group on Friction Ridge Analysis, Study and Technology et al. *The Fingerprint Sourcebook*. National Institute of Justice, 2011. https://www.ncjrs.gov/pdffiles1/nij/225320.pdf
Viitattu 26.10.2012.

[30] Euroopan Unionin Neuvosto. NEUVOSTON ASETUS (EY) N:o 2252/2004, 2004. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:FI:PDF
Viitattu 26.10.2012.

[31] John M. Irvine, Steven A. Israel, W. Todd Scruggs et al. eigenPulse: Robust human identification from cardiovascular function. *Pattern Recogn.*, 41(11):3427–3435,

marraskuu 2008. ISSN 0031-3203. URL http://dx.doi.org/10.1016/j.patcog.2008.04.015.

[32] Lior Shamir, Shari Ling, Salim Rahimi et al. Biometric identification using knee X-rays. *Int. J. Biometrics*, 1(3):365–370, maaliskuu 2009. ISSN 1755-8301. URL http://dx.doi.org/10.1504/IJBM.2009.024279.

[33] Valtioneuvosto. Rikoslaki 19.12.1889/39. http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001
Viitattu 18.1.2013.

[34] Valtioneuvosto. Laki yksityisyyden suojasta työelämässä 13.8.2004/759. http://www.finlex.fi/fi/laki/ajantasa/2004/20040759
Viitattu 18.1.2013.

[35] Valtioneuvosto. Henkilötietolaki 22.4.1999/523. http://www.finlex.fi/fi/laki/ajantasa/1999/19990523
Viitattu 18.1.2013.

[36] Olli I. Heimo, Antti Hakkala ja Kai K. Kimppa. How to Abuse Biometric Recognition Systems. *Journal of Information, Communication & Ethics in Society*, 10(2):68–81, 2012.

[37] ICAO. Machine Readable Travel Documents. http://www2.icao.int/en/MRTD/Downloads/Doc%209303/Doc%209303%20English/Doc%209303%20Part%201%20Vol%201.pdf
Viitattu 28.3.2013.

[38] MTV3. Identiteettivarkaus ei ole Suomessa vieläkään aina rikos. http://www.mtv3.fi/uutiset/rikos.shtml/identiteettivarkaus-ei-ole-suomessa-vielakaan-aina-rikos/2012/12/1670947
Viitattu 20.9.2013.

[39] Finanssialan Keskusliitto. Pankkien Tupas–tunnistuspalvelun tunnistusperiaatteet. https://www.fkl.fi/teemasivut/sahkoinen_asiointi/Dokumentit/Tupas_tunnistusperiaatteet_v20c_FI.pdf
Viitattu 11.11.2014.

[40] Väestörekisterikeskus. Kansalaisvarmenne. http://fineid.fi/default.aspx?docid=4044&site=9&id=292
Viitattu 4.10.2013.

[41] Arun Ross ja Anil K. Jain. Multimodal Biometrics: An Overview. Teoksessa *12th European Signal Processing Conference (EUSIPCO)*, ss. 1221–1224. 2004.

[42] Valtioneuvosto. Suomen perustuslaki 11.6.1999/731. http://www.finlex.fi/fi/laki/ajantasa/1999/19990731
Viitattu 21.9.2014.

[43] Kimmo Himber. *Tekninen rikostutkinta: Johdatus forensiseen tieteeseen*. Poliisiammattikorkeakoulu, 2002. ISBN 951-815-039-7.

[44] MOT Tietotekniikan liiton ATK-sanakirja. http://mot.kielikone.fi
Viitattu 22.9.2014.

[45] Yhdistyneet kansakunnat. Ihmisoikeuksien yleismaailmallinen julistus. http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/fin.pdf
Viitattu 22.9.2014.

[46] Euroopan neuvosto. Euroopan ihmisoikeussopimus. http://www.finlex.fi/fi/sopimukset/sopsteksti/1999/19990063
Viitattu 22.9.2014.

[47] YLE. Poliisi haluaa suomalaisten sormenjäljet rikostutkintaansa. http://yle.fi/uutiset/poliisi_haluaa_suomalaisten_

sormenjaljet_rikostutkintaansa/5607626
Viitattu 22.9.2014.

[48] Helsingin Sanomat. Ihmisoikeustuomioistuimelta tiukka kanta sormenjälkien rekisteröintiin. http://www.hs.fi/kotimaa/a1367460286158
Viitattu 22.9.2014.

[49] Helsingin Sanomat. Passien sormenjälkirekisteriä ei avata rikostutkinnalle. http://www.hs.fi/kotimaa/a1402623591660
Viitattu 22.9.2014.

[50] Matteo Golfarelli, Dario Maio ja Davide Maltoni. On the Error-Reject Trade-Off in Biometric Verification Systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(7):786–796, 1997. ISSN 0162-8828.

[51] Arun Ross ja Anil Jain. Information fusion in biometrics. *Pattern Recognition Letters*, 24:2115–2125, 2003.

[52] Valtioneuvosto. Sähköisen viestinnän tietosuojalaki 16.6.2004/516. http://www.finlex.fi/fi/laki/ajantasa/2004/20040516
Viitattu 16.10.2014.

[53] Valtioneuvosto. Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621. http://www.finlex.fi/fi/laki/ajantasa/1999/19990621
Viitattu 16.10.2014.

[54] Tietosuojavaltuutetun toimisto. Henkilötietolaki. http://www.tietosuoja.fi/fi/index/lait/Henkilotietolaki.html
Viitattu 27.10.2014.

[55] Tietosuojavaltuutetun toimisto. Työelämän tietosuojalaki. http://www.tietosuoja.fi/fi/index/lait/tyoelamantietosuojalaki.

html

Viitattu 28.10.2014.

[56] Tietosuojavaltuutetun toimisto. Sähköisen viestinnän tietosuojalaki. http://www.tietosuoja.fi/fi/index/lait/sahkoisenviestinnantietosuojalaki.html

Viitattu 28.10.2014.

[57] Helen Nissenbaum. Privacy as Contextual Integrity. *Washington Law Review*, 79(1), 2004.

[58] Poliisi. Sormenjälkien ottaminen. https://www.poliisi.fi/poliisi/home.nsf/0/68AF3EED579E87B7C22577D7003D0AD8?opendocument

Viitattu 25.11.2014.

[59] Valtioneuvosto. Passilaki 21.7.2006/671. http://www.finlex.fi/fi/laki/ajantasa/2006/20060671

Viitattu 25.11.2014.

[60] Kilpailu ja kuluttajavirasto. Peruspankkipalvelut puutteellisia ilman verkkopankkitunnuksia. http://www2.kuluttajavirasto.fi/fi-FI/arkisto2010/verkkolehti-7-2010/peruspankkipalvelut-puutteellisia-ilman-verkkopankkitunnuksia-2

Viitattu 20.1.2015.

[61] Valtioneuvosto. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617. https://www.finlex.fi/fi/laki/ajantasa/2009/20090617

Viitattu 20.1.2015.

[62] Reima Suomi, Tuomas Aho, Tom Björkroth et al. *Biometrical Identification as a Challenge for Legislation: The Finnish Case*, ss. 233–245. IRM Press, 2008.

[63] Euroopan parlamentti. Euroopan parlamentin ja neuvoston direktiivi 95/46/EY. http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:31995L0046
Viitattu 17.2.2015.

[64] Yle uutiset. Tesoman surman tutkinnassa poikkeukselliset menetelmät käyttöön – poliisi ottaa DNA-näytteet suurelta miesjoukolta. http://yle.fi/uutiset/tesoman_surman_tutkinnassa_poikkeukselliset_menetelmat_kayttoon__poliisi_ottaa_dna-naytteet_suurelta_miesjoukolta/7779185
Viitattu 18.5.2015.

[65] Poliisi. Ohje hakemukseen tunnistamisesta tunnistamisasiakirjaa varten. https://www.poliisi.fi/luvat/ohje_hakemukseen_tunnistamisesta_tunnistamisasiakirjaa_varten
Viitattu 25.5.2015.

[66] Gemalto Oy. http://www.gemalto.fi/
Viitattu 31.5.2015.

[67] The FIDO Alliance Announces First FIDO Authentication Deployment - PayPal and Samsung Enable Consumer Payments with Fingerprint Authentication on New Samsung Galaxy S5. https://fidoalliance.org/the-fido-alliance-announces-first-fido-authentication-deployment---paypal-and-samsung-enable-consumer-payments-with-fingerprint-authentication-on-new-samsung-galaxy-s5/
Viitattu 31.5.2015.

[68] FIDO Alliance. https://fidoalliance.org/
Viitattu 31.5.2015.

[69] Michael Thieme. Identifying and Reducing Privacy Risks in Biometric Systems. 13th Annual Conference on Computers, Freedom & Privacy, 2003. http://bioprivacy.org/CFP_2003.pdf
Viitattu 31.5.2015.