Tuomo Vitikainen

Biometriset tunnistusmenetelmät mobiililaitteissa

Tietotekniikan kandidaatintutkielma

30. huhtikuuta 2020

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Tuomo Vitikainen

Yhteystiedot: tuomo.m.j.vitikainen@student.jyu.fi

Työn nimi: Biometriset tunnistusmenetelmät mobiililaitteissa

Title in English: Biometric identification on mobile devices

Työ: Kandidaatintutkielma

Sivumäärä: 21+0

Tiivistelmä: Biometriset tunnistusmenetelmät ovat mobiililaitteissa yhä yleisempi keino todentaa käyttäjä. Tässä kirjallisuuskatsauksessa tutkitaan, mitä tarkoittaa käyttäjän todentaminen ja biometriset tunnistusmenetelmät. Tutkielmassa tarkastellaan matkapuhelinkäytössä useimmin esiintyviä biometrisia tunnistusmenetelmiä niiden käytettävyyden ja tietoturvan näkökulmasta sekä sitä, millaisia hyötyjä ja haasteita ne tarjoavat. Biometriset tunnistusmenetelmät tekevät käyttäjän todentamisesta nopeaa ja varmaa, mutta niissä on myös omat heikkoutensa.

Avainsanat: Biometrinen tunnistusmenetelmä, mobiililaite, käytettävyys, tietoturva

Abstract: Biometric identification is a common way nowadays to implement user authentication on mobile phones. This study will explain what user authentication and biometrics identification means. The thesis concludes what are the benefits and the questions of biometric identification from a usability and security perspective. Biometric identification methods perform user authentication fast and secure, but it should be noted that they also have their own weaknesses.

Keywords: Biometric identification, mobile device, usability, security

Kuviot

Sisältö

1 Johdanto

Matkapuhelimissa säilytetään yhä enemmän tärkeää henkilökohtaista dataa, jonka ei toivota joutuvan vääriin käsiin (Raja ym. 2014). Biometriset tunnistusmenetelmät puhelimen suojaamiseksi ovat yhä yleisempiä nykypäivän kuluttajalaitteissa, ja niiden avulla pystyy tunnistautumaan ja kirjautumaan esimerkiksi pankkipalveluihin käyttämättä pankkitunnuksia (Tsai, Chen ja Zhuang 2012). Näin ollen tunnistautumismenetelmän käyttäjän tulee olla yhä varmempi siitä, että se on tarpeeksi turvallinen suojatakseen henkilökohtaiset tiedot. On kuitenkin yleistä, että käyttäjillä ei ole tietoa siitä, miten eri biometriset lukitusmenetelmät toimivat ja voiko niihin luottaa. Monelle on myöskin epäselvää se, miten biometrista dataa säilytetään ja mitä riskejä mahdolliseen tietovuotoon voi liittyä.

Tutkielmassa tarkastellaan biometrisia tunnistusmenetelmiä mobiililaitteiden kontekstissa, eli mitä tarkoitetaan biometrisilla tunnisteilla, mitä hyötyjä ja riskejä niihin liittyy ja niiden käytettävyyttä. Termi mobiililaite sisältää perinteisten puhelimien lisäksi myös tabletit eli taulutietokoneet, mutta tutkielmassa keskitytään matkapuhelimiin niihin nojautuvan lähdemateriaalin takia. Kuitenkin käytännössä tabletti on älypuhelin isommassa koossa, joten samat asiat pätevät pitkälti myös niihin. Käyttäjän todentamisen merkitys on tutkielmassa keskeisessä asemassa. Tutkielmassa selvitetään, että millainen on biometristen tunnistusmenetelmien turvallisuus ja tietoturva, sekä mitä asioita käyttäjän tulee ottaa huomioon niihin liittyen. Katsauksessa paneudutaan myös tunnistusmenetelmien käytettävyydeen sekä siihen, mitkä asiat ja olosuhteet saattavat vaikuttaa käyttökokemukseen. Aihe on rajautunut turvallisuuteen ja käytettävyyteen sen takia, että ne ovat merkittävimmät asiat jotka käyttäjän tulee ottaa huomioon tunnistusmenetelmää valittaessa ja käyttäessä. Käsiteltäviksi tunnistusmenetelmiksi ovat valikoituneet matkapuhelimissa yleisimmät biometriset tekniikat, eli sormenjälki- sekä kasvojentunnistus, joiden toteutustapaa ja ominaisuuksia käydään tarkemmin läpi. Tutkielman tyyppi on kirjallisuuskatsaus, ja kirjallisuuden lähteinä ovat toimineet internetin yleisimmät tietokannat, kuten Institute of Electrical and Electronics Engineers (IEEE) Xplore Digital Library.

Seuraavassa luvussa avataan käyttäjän todentamisen tarkoitusta, ja sitä miksi se on tärkeä toimenpide arkielämän lisäksi internetissä liikuttaessa ja älypuhelimia käytettäessä. Luvussa

kolme käydään läpi biometrisen tunnistusmenetelmän määritelmä, menetelmälle vaadittavia ominaisuuksia ja eri tunnistusmenetelmiä. Luvussa kolme myös avataan käytettävyyden käsitettä ja sitä miksi se on tärkeä osa-alue ottaa huomioon, kun suunnitellaan teknologiaa kuluttajakäyttöön. Lisäksi luvussa kolme avataan valittujen biometristen tunnistusmenetelmien käytettävyyden piirteitä ja niihin vaikuttavia tekijöitä. Luvussa neljä keskitytään biometristen tunnistusmenetelmien tietoturvaan ja millaisia ominaispiirteitä ja turvallisuusuhkia niihin liittyy. Luvussa käydään myös läpi biometriaan liittyviä eettisiä kysymyksiä.

2 Käyttäjän todentaminen

Ihmisen todentaminen on toimenpide, jota kaikki ihmiset tekevät luonnostaan arjessa (Baqeel ja Saeed 2019). Kuitenkin jos henkilö tapaa hänelle ennestään tuntemattoman ihmisen, hän voi selittää kuka on, ja vastapuoli voi vuorostaan päättää uskooko häntä vai eikö (O'Gorman 2003). Formaaleissa tilanteissa yksilö voi myös todistaa henkilöllisyytensä esittämällä henkilökorttinsa tai passinsa. Käyttäjän todentamisen tarkoituksena on, että tietty informaatio tai esimerkiksi pääsy suljetulle alueelle jaetaan vain henkilölle, jolle se kuuluu. (Otti 2016) Digimaailmassa on olemassa sama tunnistamisen tarve, mutta protokolla on erilainen. O'Gorman (2003) toteaa, että emme voi nähdä tai päätellä, onko palveluun kirjautumista yrittävä ystävä vai vihollinen, ja internetissä on esillä erilaisissa palveluissa muun muassa terveys- sekä pankkitietoja, jotka ovat henkilökohtaisia. Internetissä sivustot ja palvelut käyttävät omia todennusmenetelmiään, kuten salasanoja ja biometrisia tietoja, joita käytämme nykyään tottuneesti ollessamme vuorovaikutuksessa tietokoneiden kanssa. (O'Gorman 2003) Tätä kautta on tullut tarpeelliseksi todentaa myös puhelimen käyttäjä sen oikeaksi omistajaksi, sillä laite voi sisältää paljon henkilökohtaista dataa.

Todentamismenetelmät voidaan jakaa Gormanin (2003) mukaan yleisesti kolmeen kategoriaan: Mitä käyttäjä tietää, mitä käyttäjällä on tai mitä käyttäjä itse on. Käyttäjän tietämykseen perustuvalla todentamisella tarkoitetaan sitä, että tunnistamistekijä, kuten salasana, numeroyhdistelmä tai graafinen kuvio, on käyttäjällä muistissa. Toinen todentamistapa on se, että käyttäjällä on jokin ulkoinen fyysinen esine, kuten tavallinen avain tai jokin älylaite, jonka avulla hän pystyy tunnistautumaan. Haittapuolena tässä todentamistavassa on kuitenkin se, että jos käyttäjä hävittää esimerkiksi tavallisen avaimen, sen löytäjällä on avoin pääsy sillä lukittuun kohteeseen. (O'Gorman 2003) Fyysinen esine on mahdollista usein myös kopioida (Otti 2016). O'Gorman (2003) kuvaa, että käyttäjään itseensä perustuva todentamismenetelmä taas perustuu henkilön uniikkeihin ominaisuuksiin. Ominaisuuksia voi olla esimerkiksi sormenjälki, kasvojentunnistus tai ääni. Myös käyttäjän olemusta tai käyttäytymistä voidaan käyttää todentamismenetelmänä, sillä esimerkiksi käsiala, kävelytyyli tai ääni on jokaisella käyttäjällä uniikki. Olemusta ja käyttäytymistä voidaan yrittää jäljitellä, mutta niiden täydellinen kopioiminen on hankalaa. (O'Gorman 2003)

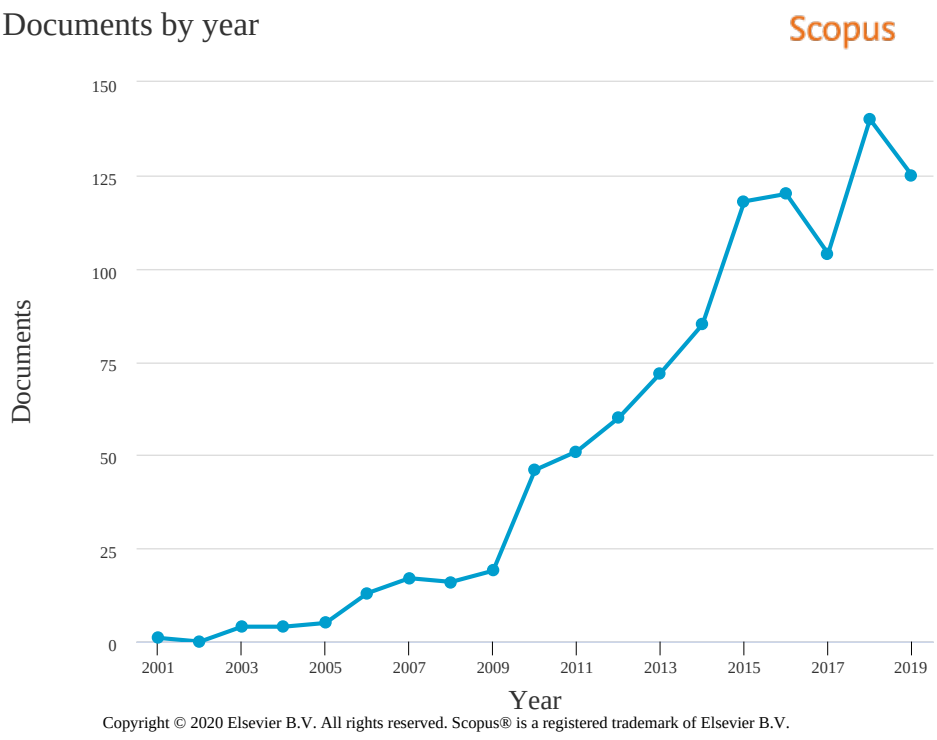
2.1 Todentaminen matkapuhelimissa

Älypuhelimet ovat nykypäivänä entistä monipuolisempia, ja niillä voidaan tehdä paljon samoja asioita kuin mitä tietokoneellakin. Tämän vuoksi on myös tärkeää, että puhelin sisältää jonkunlaisen lukituksen. Lisäksi puhelin on usein käyttäjän mukana kodin ulkopuolella liikuttaessa, joten riski puhelimen kadottamiselle on tietokoneen kadottamista suurempi. Verman, Sawhneyn ja Chalian (2017) mukaan yleisin tapa todentaa käyttäjän henkilöllisyys on matkapuhelimissa pitkään ollut salasana. Salasana terminä käsittää sanat ja kirjain- tai numeroyhdistelmät. Niissä ongelmana kuitenkin on, että salasana on tallessa vain käyttäjän mielessä, ja monimutkaiset ja siten turvalliset salasanat voivat olla vaikeita muistaa. (Verma, Sawhney ja Chalia 2017) Voidaan myös olettaa, että vanhemmilla ihmisillä saattaa olla enemmän ongelmia salasanojen kanssa, sillä muistamisen lisäksi kirjoittaminen voi olla hankalampaa. Myös O'Gorman (2003) on havainnut samat ongelmat salasanan käytössä omassa tutkimuksessaan. Myös salasanan kirjoittaminen väärin on yleistä, ja käyttäjä voi turhautuneena poistaa lukitusjärjestelmän, jolloin puhelin on kokonaan vailla suojausta. Salasana on myös mahdollista arvata tai murtaa hyökkääjän toimesta. (Verma, Sawhney ja Chalia 2017) Käyttäjän todentaminen on siis monelle ihmiselle toimenpide joka tehdään useita kertoja päivässä, joten on syytä panostaa sen turvallisuuteen ja käytettävyyteen.

2.2 Biometriset tunnistusmenetelmät

Biometrisella tunnistautumisella tarkoitetaan kehonpiirteistä mitattavia tietoja, joiden avulla pystytään yksilöimään eliö, joka on useimmiten ihminen. Sana biometria (engl. *biometrics*) tulee kreikan kielen sanoista *bios* joka tarkoittaa elämää ja *metrikos* joka tarkoittaa mittaa (Faundez-Zanuy 2006). Biometrisessa tunnistautumisessa käytettäviä piirteitä ovat esimerkiksi sormenjälki, kasvot, käsiala, ääni ja silmät (Bhatia 2013). Näistä tekniikoista matkapuhelimissa tunnetuimpia eniten käytetyimpiä ovat sormenjälki- ja kasvojentunnistus, joista kasvojentunnistus on uudempi tulokas (Baqeel ja Saeed 2019; Das ym. 2018). Biometrinen menetelmä mobiililaitteessa käsittää lukijan tai sensorin jolla mitata biometristä dataa, sekä sovelluksen jonka avulla prosessoitua dataa pystyy hyödyntämään. Tyypillisesti biometrisiä tunnistusmenetelmiä hyödyntävä mobiililaite on älypuhelin tai tablettitietokone. (Das ym. 2018) Kasvojentunnistuksen toivat ensimmäisenä puhelimiinsa Apple sekä Sam-

sung, mutta nykyään se on yhä useamman valmistajan malleissa (Baqeel ja Saeed 2019). Kuviossa 1 on havaittavissa, kuinka myös aiheeseen liittyvien tutkimusjulkaisujen määrä on selkeästi noussut, ja kaikista vuosista vuonna 2018 onkin julkaistu eniten tieteellisiä julkaisuja Scopus-tietokannassa.



Kuvio 1. Graafi tieteellisten julkaisujen määrästä väliltä 2001-2019 jotka sisältävät hakusanat *biometrics* ja *mobile devices* (www.scopus.com)

Bhatia (2013) toteaa, että biometrisella piirteellä täytyy olla tiettyjä ominaisuuksia, jotta se on soveltuva ihmisen tunnistamiseen. Näitä ominaisuuksia ovat muun muassa universaalisuus, joka tarkoittaa sitä, että jokaisella ihmisellä on oltava kyseinen ominaisuus. Toinen vaatimus on piirteen poikkeamattomuus, eli piirteiden tulisi olla vakioita pitkälläkin ajanjaksolla. Kolmas piirteeltä vaadittava ominaisuus on mitattavuus, eli piirre tulisi olla mitattavissa helposti ja ilman odotusaikaa. (Bhatia 2013) Varsinkin mobiilikäytössä piirteen nopea mitattavuus on tärkeää. Näin ollen vaikka esimerkiksi DNA-testi on yksi tarkimmista menetelmistä, se ei sovellu automatisoituun tunnistamiseen sen viiveen takia (Otti 2016). Seuraavana vaadittavana asiana Bhatia (2013) kuvaa sitä, että piirteen tulee olla tarpeeksi yksilöivä, jotta sillä voidaan todentaa ihminen. Esimerkiksi pituus, paino ja silmien väri ovat yksilölli-

siä, mutta liian vähän yksilöiviä biometrista tunnistautumista varten, joten niiden perusteella voidaan enemminkin luokitella kuin yksilöidä ihmisiä. Viidentenä on luotettavuus ja väärentämisen vaikeus, jolla tarkoitetaan että piirteen tulisi olla vaikea väärentää ja sen mittausten tulosten tulisi olla luotettavia. Viimeinen ominaisuus on vertailukelpoisuus, jolla tarkoitetään että piirteen tulisi olla muunnettavissa kompaktiin digitaaliseen muotoon siten, että sitä on helppo vertailla ja säilyttää. (Bhatia 2013) Myös Faundez-Zanuy (2006) määrittelee tärkeät ominaisuudet samalla tavalla omassa tutkimuksessaan. (Faundez-Zanuy 2006)

Biometrisen menetelmän käyttötarkoitus voidaan jakaa kahteen eri osa-alueeseen, joko tunnistamiseen *(1:n)* tai varmentamiseen *(1:1)* (Bhatia 2013). Tunnistamisessa on tarkoituksena määrittää käyttäjän henkilöllisyys, ilman että sitä kysytään käyttäjältä (Faundez-Zanuy 2006). Tällainen tilanne voi olla esimerkiksi silloin, kun poliisi etsii tiettyjä kasvoja datasta, mikä on tallennettu väkijoukosta. Varmentaminen taas tarkoittaa henkilöllisyyden todentamista, kuten matkapuhelinten lukitusmenetelmien tapauksessa tai silloin kun tarvitaan pääsylupa rajatulle fyysiselle alueelle. (Bhatia 2013)

2.2.1 Sormenjälki

Sormenjälki on sormen ihon kohoumista muodostunut kuvio. Sormenjälkiä käytettiin tunnistamiseen Kiinassa jo 1400-luvulla. Sittemmin biometriaa on tutkittu ja kehitetty eri tutkijoiden toimesta, ja muun muassa matemaatikko Karl Pearson teki tärkeitä löytöjä biometrian alalla 1900-luvun alkupuolella. (Bhattacharyya ym. 2009) On arvioitu, että todennäköisyys sille että kahdella henkilöllä on sama sormenjälki on yksi miljardista (Faundez-Zanuy 2006). On siis erittäin epätodennäköistä, että joku toinen kuin puhelimen omistaja saisi avattua puhelimen omalla sormenjäljellään.

Perinteinen keino saada sormenjälki talteen paperille on ollut käyttää mustetta, mutta nykypäivänä ovat yleistyneet erilaiset sormenjälkiskannerit. Bhattacharyyan ym. (2009) mukaan skannereita on pääasiassa kahdenlaisia: optisia- ja ultraääniskannereita. Optinen sormenjälkitunnistin on vanhin ja yleisin skannerityyppi. Yksinkertaistettuna se valaisee lasipinnalle asetetun sormen, ja tunnistin kerää siitä heijastuneen valon. Harvinaisempi ja uudempi keino sormenjäljen tallentamiseen on ultraääni. Ultraäänisensoreissa käytetään ultraäänipulsseja,

jotka skannaavat sormen. Mobiilikäytössä skannereiden haasteena on niiden koko, sillä niitä ei pysty tekemään kovin pieniksi, koska valonheijastuspinnan on oltava riittävän iso saadakseen sormenjäljestä kuvan. (Bhattacharyya ym. 2009) Erillään näytöstä oleva skanneri ei myöskään edistä näytön pinta-alan tehokasta käyttöä. Siksi nykyisin skannereita on alettu yhdistämään näyttöön, ja näin käyttäjä pystyy myös käyttämään laitetta nopeammin vain koskettamalla näyttöä erillisen sormenjälkiskannerin sijasta (Yena Yoo ym. 2014).

2.2.2 Kasvojentunnistus

Kasvojentunnistus toimintona on ollut olemassa ihmiskunnan alusta lähtien. Olemme oppineet tunnistamaan kasvoja ja niiden perusteella pystymme luokittelemaan ihmiset tutuiksi tai muukalaisiksi. Teknologian puolesta biometrinen kasvojentunnistus on tullut mahdolliseksi vasta viime vuosikymmeninä, sillä vaikka kasvojentunnistus on ihmisille luonnollinen visualisointitehtävä, on se tietokoneelle haastavaa. (Otti 2016; Baqeel ja Saeed 2019). Kasvojentunnistuksessa henkilö tunnistetaan kuvasta tai videolähteestä mobiililaitteen sovelluksen avulla. Menetelmässä analysoidaan kasvojen piirteitä, kuten ääriviivoja sekä poskipäitä ja suun, nenän ja silmien sijaintia kasvoissa. Muutokset hiustyylissä eivät juurikaan vaikuta menetelmän käyttöön, sillä analysoitava alue on hiusrajan alapuolella. (Bhattacharyya ym. 2009; Baqeel ja Saeed 2019)

Bhatian (2013) mukaan kasvojentunnistusprosessi sisältää viisi eri vaihetta. Ensimmäisenä tarvitaan dataa jota analysoida. Sen jälkeen sovellus paikantaa datasta kasvot, josta mitataan edellä mainittujen osien etäisyyksiä ja näin kasvoista voidaan luoda malli sovellukseen. Sitten sovellus vertaa luotua kasvomallia jo tietokannassa olevaan kasvomalliin. Viimeisenä sovellus päättää, ovatko kasvot samat ja hyväksytäänkö käyttäjän pääsy mobiililaitteeseen. (Bhatia 2013) Tunnistautuminen voi myös epäonnistua, vaikka kasvot olisivatkin samat. Siihen voi vaikuttaa esimerkiksi huono valaistus tai pään vääränlainen asento suhteessa kameraan. (Baqeel ja Saeed 2019; Bhatia 2013)

3 Käytettävyys

Biometrisissa tunnistusmenetelmissä käytettävyyden muutos on keskeisessä roolissa verrattaessa perinteisiin menetelmiin. Vuonna 2017 toteutetun tutkimuksen mukaan 60 prosenttia mobiililaitteiden käyttäjistä kertoi avaavansa laitteen yli 15 kertaa päivässä (Verma, Sawhney ja Chalia 2017). Tällöin voidaan todeta, että käytettävyys on suuressa osassa lukitusmenetelmää, sillä vuorovaikutusta käyttäjän ja laitteen välillä on paljon. Käytettävyys (engl. *usability*) voidaan määritellä kansainvälisen standardisoimisjärjestö International Organization for Stantardization (ISO) vuonna 1998 julkaistun ISO 9241-11 stantardin mukaan: tuloksellisuus, tehokkuus ja tyytyväisyys (Bevan, Carter ja Harker 2015). Julkaisussa myös korostetaan, että käytettävyys on enemmänkin vuorovaikutusta kuin tuotteen ominaisuus, eikä siten käytettävyyttä voi mitata ilman käyttäjää. (Bevan, Carter ja Harker 2015) Teknologian helppokäyttöisyydellä on suuri merkitys siihen, miten käyttäjät hyväksyvät uuden teknologian, ja tätä varten on kehitelty erilaisia teknologian hyväksymismalleja, joista paljon käytetty on vuonna 1989 kehitetty TAM-malli. Malli yksinkertaistettuna kertoo, että aikomukseen käyttää teknologista innovaatiota vaikuttaa käyttäjän omat odotukset liittyen helppokäyttöisyyteen ja hyödyllisyyteen. (Baqeel ja Saeed 2019) Käytettävyydellä on merkittävä vaikutus kuluttajatyytyväisyyteen ja siihen, kuinka ihmiset omaksuvat itselleen uuden teknologian.

3.1 Sormenjäljen käytettävyys

Sormenjälkitunnistin on yleisin biometrinen tunnistusmenetelmä mobiililaitteissa (Das ym. 2018). Bhatian (2013) mukaan sen etuna on helppokäyttöisyys, tarkkuus ja kustannustehokkuus sekä mobiili että tietokonekäytössä. Eduksi on luettavissa myös biometriselle mallille vaadittava pienehkö tallennustila. Sormenjälkitunnistuksen yhteydessä ongelmia saattaa aiheuttaa liian kuiva, kostea tai likainen iho, jolloin saatavan mallin laatu heikkenee, kuten kuviosta 2 pystyy näkemään. (Bhatia 2013) On huomioitava, että vanhuksilla tai käsiä kuluttavan työn tekijöillä ei välttämättä ole sormenjälkiä tai niistä saatava jälki on liian epätarkka tunnistautumistarkoitukseen (Faundez-Zanuy 2006).

Sormenjälkitunnistinta käytettäessä tulee olla tarkkana siinä, että sormi asetetaan oikein lu-

kijaan, sillä on havaittu, että väärin tai huonosti lukijaan asetettu sormenjälki on yleinen syy epäonnistuneeseen tunnistustapahtumaan. (Patrick 2004). Sormenjälkitunnistinta ei luonnollisesti pysty käyttämään käsineet kädessä.

Kuvio 2. Vasemmalla kuiva, keskellä kostea ja oikealla hyvälaatuinen sormenjälki (Bartunek 2004)

3.2 Kasvojentunnistuksen käytettävyys

Kasvojentunnistus pyrkii tekemään todennusprosessista entistä nopeampaa ja helpompaa. Bhatian (2013) mukaan kasvojentunnistuksen etuna on lukitusjärjestelmän passiivisuus, sillä käyttäjän ei tarvitse tehdä muuta kuin suunnata katseensa puhelinta kohti. Passiivisten lukitusmenetelmien kanssa on kuitenkin hyvä luoda vuorovaikutusta käyttäjän kanssa esimerkiksi ilmoitusten avulla niin, että käyttäjälle ilmoitetaan onnistuneesta todentamistapahtumasta. Käyttäjät tuntevat näin olonsa turvallisemmaksi, varsinkin jos kyse on pankki- tai maksuasioista. (Bhatia 2013)

Vuonna 2019 tehdyn tutkimuksen mukaan kasvojentunnistuksen omaavista käyttäjistä 48 prosenttia käyttää menetelmää puhelimen lukituksen avaamiseen, mutta vain 28 prosenttia sovellusten ostoon. Tämä tarkoittaa sitä, että vaikka käyttäjät voivat käyttää menetelmää puhelimen avaamiseen, he eivät välttämättä luota siihen niin paljoa, että tekisivät sen

avulla maksutransaktioita vaativia sovelluslatauksia. (Baqeel ja Saeed 2019) Kuitenkin tutkimukseen osallistuneista suurin osa oli tyytyväisiä kasvojentunnistuksen käytettävyyteen ja uskoivat sen olevan turvallinen menetelmä, joten he aikoivat käyttää menetelmää jatkossakin (Baqeel ja Saeed 2019).

Kasvojentunnistusta vaikeuttavana tekijänä on yleisesti pidetty huonoa valaistusta, sillä heikossa valaistuksessa kasvot on vaikeampi kuvata (Bhatia 2013). Nykyisin kuitenkin esimerkiksi Applen käyttämä FaceID teknologia sisältää infrapunavalon, joten se ei tarvitse ollenkaan luonnonvaloa toimiakseen (Dempsey 2018). Vuonna 2019 tehdyssä tutkimuksessa kävi myös ilmi, etteivät vastaajat olleet varmoja, ovatko ongelmat valaistuksessa olleet syynä lukitusmenetelmää käytettäessä ilmaantuneisiin ongelmiin, sillä esimerkiksi myös pään asento suhteessa puhelimen sensoreihin vaikuttaa tunnistautumiseen (Baqeel ja Saeed 2019). Jos kasvojentunnistusta ei jostain syystä pysty käyttämään, on puhelimissa varamenetelmä lukituksen avaamiseksi. Jos kasvojen tunnistaminen epäonnistuu, puhelin tarjoaa vaihtoehtoisesti tavallista lukituskoodia. (Baqeel ja Saeed 2019)

4 Tunnisteiden tietoturva

Turvallisuusuhalla tarkoitetaan tilannetta, jossa tunnistusta pystytään huijaamaan ja täten toteuttamaan identeettivarkaus tai pääsemään käsiksi henkilökohtaiseen dataan (Manabe ym. 2009). Tällaiset ovat epätoivottuja tilanteita, ja kuluttajille on tärkeää, että lukitusmenetelmöt ovat turvallisia ja tarkkoja. Biometrinen tunnistautuminen asettaa siis uusia haasteita liittyen tietosuojaan, ja niiden ollessa uudehkoa teknologiaa kuluttajalaitteissa kuluttajien ymmärrys niistä ei välttämättä ole parhaalla tasolla. Patrickin (2004) mukaan yleistä on myös käyttäjien vähäinen ymmärrys biometrisista malleista ylipäätään. Käyttäjät eivät välttämättä ymmärrä ja järjestelmät eivät kerro, miten mallit luodaan, säilytetään ja suojataan. On myös huomioitava että biometrinen ominaisuus ei ole kuitenkaan salaisuus, ja esimerkiksi kasvot ovat kaikkien nähtävillä, mutta sitä vastaava malli on kuitenkin syytä pitää salassa. (Patrick 2004)

Jos biometrisia tietoja kaapataan tai varastetaan hyökkääjän toimesta, niitä voidaan kopioida tai käyttää vääriin tarkoituksiin (Campisi 2013). Biometrisista tiedoista on myös mahdollisuus löytää merkityksellistä tietoa henkilön terveydestä tai ominaisuuksista. Useat niistä näkyvät ulospäin eivätkä sinänsä riko yksityisyyttä, mutta tutkimuksissa on havaittu että esimerkiksi sormenjäljistä voidaan havaita onko henkilöllä kromosomaalinen häiriö. (Faundez-Zanuy 2005) Biometriaa hyödyntävä teknologia voi siis rikkoa tai suojata yksityisyyttä riippuen siitä, kumpaan käyttötarkoitukseen sitä käytetään. Faundez-Zanuyn (2005) mukaan maalaisjärjen käyttö riittää välttämään suurelta osin turvallisuusuhkia, ja biometriasta saatavat hyödyt ovat suuremmat kuin mahdolliset haitat.

Biometriset ominaisuudet ovat muuttumattomia, joka luo oman haasteensa. Kun esimerkiksi salasanan pystyy vaihtamaan ja tätä kautta luomaan turvallisuutta, biometrinen piirre pysyy aina samana. Teoh ym. (2006) tutkimuksessa ongelman ratkaisemiseksi on kehitetty biometrinen formulaatio, joka on peruutettavissa. Menetelmässä yhdistetään käyttäjäkohtainen tokenisoitu satunnaisluku ja biometrinen ominaisuus, josta syntyy sarja binäärikoodia. Tällainen biometrinen malli on peruutettavissa vaihtamalla siihen käytettyä tokenia. (Teoh ja Ngo 2006) Biometrisissa lukitusmenetelmissä etuna verrattuna perinteisiin keinoihin on se, että ne ovat kaikilla käyttäjillä yhtä turvallisia - perinteisen salasanan turvallisuus riippuu

siitä, miten monimutkaisen salasanan käyttäjä valitsee (Faundez-Zanuy 2006).

Biometristen tunnisteiden yleistyminen herättää kysymyksiä myös liittyen eettisyyteen. Altermanin (2003) mukaan pakollinen biometrinen kuvantaminen esimerkiksi ajo- tai luottokortin hankkimisessa rikkoo yksityisyyttä, eikä se ole verrattavissa valokuvaan, ja yksityisten biometristen tietojen käyttäminen pitäisi olla sallittua vain rikostapauksissa. Tästä johtuen sormenjälkien otto saatetaan yhdistää rikollisuuteen (Faundez-Zanuy 2006). Altermanin (2003) mukaan pitäisi estää myös kaikenlainen biometristen tietojen myyminen ja vaihto. Voidaan myös miettiä, onko kuluttajilla tieto siitä mitä hänen biometrisilla tiedoillansa saatetaan tehdä tai millä tavalla niitä säilytetään, kun hän ottaa lukitusmenetelmän käyttöön matkapuhelimessaan. Matkapuhelimissa biometriset tiedot tallennetaan yleisesti vain salattuna lokaalisti laitteen muistiin (Das ym. 2018). Tällöin biometristen tietojen säilytys on myös omistajan vastuulla, siihen verrattuna kuin että tietoja säilytettäisiin palvelimella. Turvallisuutta voisi parantaa esimerkiksi ottamalla käyttöön edellä mainitun peruutettavan biometrisen mallin, jolloin mitään alkuperäistä tietoa ei voisi joutua tietomurron yhteydessä vääriin käsiin.

4.1 Biometristen lukitusmenetelmien murtaminen

Vaikka biometrisia piirteitä on vaikea jäljitellä, on lukitusmenetelmien huijaaminen silti mahdollista. Vuonna 2016 Michiganin yliopistossa tehdyssä tutkimuksessa onnistuttiin huijaamaan kahden eri puhelimen sormenjäljenlukijaa. Väärennetty sormenjälki luotiin tulostamalla sormenjälki läpinäkyvälle erikoispaperille, jolloin sormenjäljestä saadaan 2D-malli. Rajoituksena on, että tulostettava kuva sormenjäljestä täytyy olla tarkkuudeltaan vähintään 300 pikseliä per tuuma. Tutkimuksessa testatut ja hakkeroidut puhelimet olivat malliltaan Samsung Galaxy S6 sekä Huawei Honor 7. Tutkimuksessa kuitenkin huomautettiin, että valmistajat kehittävät koko ajan turvallisempia lukituskeinoja eikä tutkimuksessa käytetty keino välttämättä toimi enää uudemmissa puhelinmalleissa. (Cao ja Jain 2016)

Myös kasvojentunnistuksen huijaamiseksi on kehitetty vastaavanlaisia menetelmiä. Hyökkäyksiä, joissa pyritään jäljittelemään kasvoja, on Sunin ym. (2020) mukaan kolmenlaisia: kuva kasvoista, video kasvoista tai kolmiulotteinen silikonista valmistettu maski. Varsinkin

3D-maskit ovat uudehko haaste, sillä 3D-tulostaminen on viime vuosina merkittävästi kehittynyt ja halventunut, mikä ajaa tunnistusmenetelmien kehittäjät suunnittelemaan tekniikoita, joilla maski voidaan erottaa oikeista kasvoista. (Sun ym. 2020) 3D-tulostimien hinnat ovat niiden halventumisesta huolimatta useita tuhansia euroja, joten yleisiä ne eivät tavallisten kuluttajien keskuudessa ole. Voidaankin pitää epätodennäköisenä, että tavallinen kuluttaja voisi joutua tällaisen hyökkäyksen kohteeksi.

Biometristen lukitusmenetelmien helppokäyttöisyys sisältää myös tietoturvauhan, sillä on olemassa riski, että lukitusmenetelmän voi avata nukkuvan tai tiedottoman ihmisen avulla, mikä taas ei ole mahdollista salasanalukitusta käytettäessä. Kuitenkin esimerkiksi Apple on kehittänyt FaceID teknologiaansa ratkaisuksi menetelmän, jossa käyttäjän on suunnattava katse puhelinta kohti ja käyttäjän silmät ovat oltava auki lukituksen avaamiseksi, jolloin voidaan varmistaa käyttäjän hyväksyntä (Rui ja Yan 2019). Sormenjälkitunnistusta käytettäessä on luonnollisesti vaikeampaa varmistaa, että käyttäjä on tietoisesti avaamassa lukitusta.

5 Yhteenveto

On ennustettu, että yli 80 prosentissa älypuhelimista olisi vuonna 2023 jonkunlainen biometrinen tunnistautumismenetelmä (Das ym. 2018). Älypuhelimien käyttö on nykypäivänä kasvanut huimasti, ja ne sisältävät useasti paljon henkilökohtaista salassapidettävää dataa ja siitä johtuen helppokäyttöiselle ja turvalliselle lukitusmenetelmälle on tarvetta. Biometristen menetelmien selkeäksi eduksi nousi teknologian helppokäyttöisyys kuluttajalle - käyttäjän ei tarvitse enää muistaa monimutkaisia ja pitkiä salasanoja tai syöttää numerosarjoja joka kerta avatessaan puhelimen lukituksen. Suorittimien suorituskyvyn lisääntyessä myös tunnistautumisprosessi tapahtuu nopeasti vailla viivettä. Biometrisia lukitusmenetelmiä käytettäessä lukituksen avaava piirre on aina mukana, mutta piirteiden valikoima rajoittuu muutamaan siltä vaadittavien ominaisuuksien takia.

Tutkimusten perusteella biometrisia lukitusmenetelmiä voidaan pitää turvallisina, mutta niihin ei kuitenkaan tule luottaa liikaa. Hieman vanhemmat menetelmät ovat suhteellisen helposti murrettavissa, mutta uudet ja kehittyneemmät menetelmät vaativat taitavan murtautujan. Vaikka silikonisten sormi- tai kasvojäljitelmien valmistaminen on nykypäivänä entistä helpompaa ja halvempaa, tarvitaan myös puhelimen lisäksi käyttäjän piirre mitä jäljitellä. Helppoa puhelimeen murtautuminen ei siis ole, ja tavallisella käyttäjällä ei siis juuri ole syytä huoleen. Myös kun ollaan tekemisissä henkilökohtaisten tietojen kanssa, tärkeää on niiden säilytys. Matkapuhelimissa biometriset piirteet säilytetään matkapuhelimen muistissa eikä esimerkiksi pilvipalvelussa, joten piirteitä ei tarvitse siirtää verkon kautta missä data on helpoiten varastettavissa. Käyttäjän kannattaa kuitenkin selvittää, onko taho jolle biometrisia tietoja annetaan luotettava, käytetäänkö niitä vain ennalta sovittuun tarkoitukseen ja että säilyykö omistajalla kaikki oikeudet niihin.

Biometriset tunnistusmenelmät ovat yhä luotettavampia ja nopeampia kuluttajalaitteissa. Sekä sormenjälki- että kasvojentunnistus ovat tehokkaita menetelmiä todentaa käyttäjä, mutta niissä molemmissa on omat ominaispiirteensä ja heikkoutensa. Biometrisen tunnistusmenetelmän toteustapa vaikuttaa paljon turvallisuuteen, ja jos menetelmä on toteutettu huolella, se on turvallinen ja helppokäyttöinen vaihtoehto mobiililaitteen lukitusmenetelmäksi.

Lähteet

Baqeel, H., ja S. Saeed. 2019. “Face detection authentication on Smartphones: End Users Usability Assessment Experiences”. Teoksessa *2019 International Conference on Computer and Information Sciences (ICCIS),* 1–6. Huhtikuu. doi:10.1109/ICCISci.2019.8716452.

Bartunek, Josef Ström. 2004. “Minutiae Extraction from Fingerprint with Neural Network and Minutiae based Fingerprint Verification”.

Bevan, Nigel, James Carter ja Susan Harker. 2015. “ISO 9241-11 Revised: What Have We Learnt About Usability Since 1998?” Teoksessa *HCI.*

Bhatia, Renu. 2013. “Biometrics and Face Recognition Techniques”. *International Journal of Advanced Research in Computer Science and Software Engineering* 3 (5).

Bhattacharyya, Debnath, Rahul Ranjan, Farkhod Alisherov, Minkyu Choi ym. 2009. “Biometric authentication: A review”. *International Journal of u-and e-Service, Science and Technology* 2 (3): 13–28.

Campisi, Patrizio. 2013. *Security and privacy in biometrics.* Nide 24. Springer.

Cao, Kai, ja Anil K Jain. 2016. “Hacking mobile phones using 2D printed fingerprints”.

Das, A., C. Galdi, H. Han, R. Ramachandra, J. Dugelay ja A. Dantcheva. 2018. “Recent Advances in Biometric Technology for Mobile Devices”. Teoksessa *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS),* 1–11.

Dempsey, P. 2018. “The teardown - Apple iPhone X [Reviews Consumer Technology]”. *Engineering Technology* 13, numero 1 (helmikuu): 80–81. ISSN: 1750-9637. doi:10.1049/et.2018.0126.

Faundez-Zanuy, Marcos. 2005. “Privacy issues on biometric systems”. *Aerospace and Electronic Systems Magazine, IEEE* 20 (maaliskuu): 13–15. doi:10.1109/MAES.2005.1397143.

Faundez-Zanuy, Marcos. 2006. “Biometric security technology”. *Aerospace and Electronic Systems Magazine, IEEE* 21 (heinäkuu): 15–26. doi:10.1109/MAES.2006.1662038.

Manabe, H., Y. Yamakawa, T. Sasamoto ja R. Sasaki. 2009. “Security Evaluation of Biometrics Authentications for Cellular Phones”. Teoksessa *2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing,* 34–39. Syyskuu. doi:10.1109/IIH-MSP.2009.51.

O’Gorman, L. 2003. “Comparing passwords, tokens, and biometrics for user authentication”. *Proceedings of the IEEE* 91, numero 12 (joulukuu): 2021–2040. ISSN: 1558-2256. doi:10.1109/JPROC.2003.819611.

Otti, C. 2016. “Comparison of biometric identification methods”. Teoksessa *2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI),* 339–344. Toukokuu. doi:10.1109/SACI.2016.7507397.

Patrick, Andrew. 2004. “Usability and Acceptability of Biometric Security Systems”, 3110:105. Helmikuu. doi:10.1007/978-3-540-27809-2_11.

Raja, K. B., R. Raghavendra, M. Stokkenes ja C. Busch. 2014. “Smartphone authentication system using periocular biometrics”. Teoksessa *2014 International Conference of the Biometrics Special Interest Group (BIOSIG),* 1–8. Syyskuu.

Rui, Z., ja Z. Yan. 2019. “A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification”. *IEEE Access* 7:5994–6009.

Sun, Pengcheng, Dan Zeng, Xiaoyan Li, Lin Yang, Liyuan Li, Zhouxia Chen ja Fansheng Chen. 2020. “A 3D Mask Presentation Attack Detection Method Based on Polarization Medium Wave Infrared Imaging”. *Symmetry* 12 (maaliskuu): 376. doi:10.3390/sym12030376.

Teoh, A. B., ja D. C. Ngo. 2006. “Biophasor: Token Supplemented Cancellable Biometrics”. Teoksessa *2006 9th International Conference on Control, Automation, Robotics and Vision,* 1–5. Joulukuu. doi:10.1109/ICARCV.2006.345404.

Tsai, C., C. Chen ja D. Zhuang. 2012. “Secure OTP and Biometric Verification Scheme for Mobile Banking”. Teoksessa *2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing,* 138–141. Kesäkuu. doi:10.1109/MUSIC.2012.31.

Verma, M., R. Sawhney ja R. Chalia. 2017. “Biometric Based User Authentication in Smart Phones”. Teoksessa *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS),* 183–188. Joulukuu. doi:10.1109/ICNGCIS.2017.38.

Yena Yoo, Kyungmin Na, Heedon Jang ja F. Bien. 2014. “Low capacitance sensing circuit for fingerprint sensor integrated into display screen based on charging and extracting process”. Teoksessa *2014 International SoC Design Conference (ISOCC),* 100–101. Marraskuu. doi:10.1109/ISOCC.2014.7087550.