Tietoturvan maksimointi biometrisillä järjestelmillä

Oulun yliopisto
Tieto- ja sähkötekniikan tiedekunta
Tietojenkäsittelytieteiden
tutkinto-ohjelma
LuK-tutkielma
Petteri Kärkäs
Joulukuu 2019

Tiivistelmä

Yhteiskunta on vuosi vuodelta enemmän riippuvainen teknologiasta, joka koskee tunnistautumista ja todentamista. Biometriset tunnistusjärjestelmät voisivat luoda lähes erehtymättömän muurin oikeutetun ja oikeuttamattoman käyttäjän välille, joten miksi kaikki tunnistautumisjärjestelmät eivät käytä biometriikkaa? Tutkielman tarkoituksena on saada lukija ymmärtämään biometristen järjestelmien potentiaali ja käytön edellytykset sekä niiden kehityksen tarve.

Avainsanat
Biometrinen järjestelmä, tunnistautuminen, tietoturva

Ohjaaja
Yliopistonlehtori Ari Vesanen

Sisällysluettelo

1. Johdanto

Maailmassa on käytössä enemmän teknologiaa kuin ikinä aikaisemmin, mutta identiteettivarkauksia tapahtuu nykyään enemmän kuin koskaan. Henkilön fyysinen ja virtuaalinen omaisuus, kuten älypuhelimet, pankkitiedot sekä lähes kaikki tunnistautumistiedot, mitkä ovat yhteydessä teknologiaan, ovat helposti kaapattavissa. Jos tunnistautumiseen käytettäisiin uniikkia sormenjälkeä tai silmän verkkokalvoa, väärinkäytön mahdollisuudet hupenisivat huomattavasti, joten miksi näin ei tehdä?

Työssä käsitellään biometristen järjestelmien käyttöä tietoturvan edistäjänä. Tarkoituksena on saada lukija ymmärtämään biometriikan potentiaali tietoturvatekijänä sekä auttaa ymmärtämään biometristen järjestelmien hyödyt ja haitat. Tutkimuksessa tarkastellaan lähemmin sormenjälkitunnistimen toimintaa.

Tekstissä avataan biometristen tunnistusjärjestelmien toimintaa sekä suojausjärjestelmien kehitystä ja käyttöä tietotekniikan alalla. Lukijan tulisi saada myös käsitys tietokantojen evoluutiosta sekä suojausmenetelmistä.

Tutkimusmenetelmänä on käytössä kirjallisuuskatsaus eli dokumenttien kirjon analysointi ja hyödyllisen tiedon kokoaminen loppututkimukseen ymmärrettävästi yhtenäisenä tutkielmana.

Sisällöltään tutkielmani aloittaa katsauksella biometristen tunnistusjärjestelmien historiaan ja niiden kehitysvaiheisiin, joista tärkeimmistä yksityiskohtaisempia kuvauksia. Ymmärrettyään mistä biometrian tarve juontaa juurensa, lukija etenee biometristen turvallisuusjärjestelmien pariin, joista viimeisenä tutkitaan päivittäin käytössä olevien mobiililaitteiden turvallisuutta. Tutkielmani käsittelee myös pintapuolisesti hyökkäystä biometriseen järjestelmään. Viimeisissä kappaleissa esittelen tutkimusmenetelmän lyhyesti sekä omat päätelmäni aiheesta.

2. Historiallinen katsaus biometriaan

Sana biometriikka pohjautuu kreikankielisiin sanoihin “bios” ja “metron” eli suomenkielisiin sanoihin “elämä” ja “mitata” (Anthropometry, n.d.).

Biometriikkaa alettiin käyttää vuosituhansia sitten, kun tunnistautumisen tarve alkoi muodostua (Mayhew, 2012). Ensimmäisen biometrisen tunnistusjärjestelmän käyttöönoton ajankohtaa on hankala määritellä, mutta tiettävästi jo 31000 vuotta vanhoista luolista on löydetty seinämaalauksia ja kädenjälkiä, joiden uskotaan toimineen tekijän ns. allekirjoituksena. Jo muinaisessa Babyloniassa n.500 eKr. liiketoimet hoidettiin savilaattojen avulla, joista kävi ilmi transaktioiden yksityiskohdat sekä osapuolten sormenjäljet (Mayhew, 2012).

1800-luvun puoliväliin mennessä kaupungistumisen seurauksena nähtiin yleisesti suurempi tarve yksilön tunnistautumiselle. Varhaisten oikeusjärjestelmien seurauksena tunnistautumismetodit kehittyivät, jotta rikollisuutta pystyttäisiin seuraamaan. Alettiin harjoittamaan antropometriaa, jota voisi pitää alkeellisena versiona biometrisestä järjestelmästä. Kriminologi Alphonse Bertillonin kehittämässä systeemissä otettiin huomioon useita kehon mittoja mm. hartiaväli, pituus, korvan pituus, arvet ja silmien väri. Vuonna 1903 kuitenkin kävi ilmi identtisten kaksosten tapaus, joka johti Bertillonin systeemin näennäiseen lopulliseen romahtamiseen. Kaksi miestä oli tuomittu vankilaan mutta heitä ei voinut Bertillonin järjestelmällä erottaa toisistaan, koska heidän mittansa olivat tismalleen samat. Bertillonin järjestelmä oli kuitenkin laajalti käytössä lähes 1900-luvulle asti, kunnes lähes erehtymätöntä sormenjälkitunnistusta alettiin käyttää. (Fosdick, 1915, s. 364).

2.1 Biometrinen tunnistautuminen

Tunnistautuminen tarkoittaa prosessia, jolla varmistetaan asian, tai henkilön olevan oikeaksi väitetty (Authentication n.d.). Tunnistautuminen voi tapahtua tietämällä, kuten salasanan kautta tai esineellä, kuten avainkortilla. Kolmas tapa tunnistautua on ominaisuus, kuten sormenjälki tai verkkokalvo. Biometrisellä tunnistautumisella varmistetaan, anatomisen yksilöllisyyden kautta, henkilön olevan väitetty henkilö. Uniikit ominaisuudet ihmisessä estävät väärinkäytön sekä identiteettivarkauden biometrisen tunnistautumisen kautta (Biometria, n.d.).

2.2 Biometristen järjestelmien kehityksen alku

Mayhew on tarkastellut biometristen järjestelmien kehitystä eri vuosina. Tämän kappaleen aikajanan lähteenä on käytetty Mayhew:n (2012) artikkelia biometrian historiasta. Bertillonin järjestelmästä kertova kappale on kuitenkin Raymond B. Fosdickin kirjasta, joka käsittelee tarkemmin kyseistä harppausta biometrisessä tunnistautumisessa. Historiassa on käytetty monia biometriaa hyödyntäviä järjestelmiä, joskin ne ovat olleet ennen

1800-lukua erittäin alkeellisella tasolla. Merkittävän järjestelmällisenä tapana voisi kuitenkin pitää kiinalaisten kauppiaiden 1400-luvulla käyttämää biometrista systeemiä, jossa vanhemmat erottelivat lapsensa ottamalla musteutetulle paperille lasten käden ja jalanjäljet. Kyseinen tapa on vielä tänäkin päivänä käytössä.

1823 Tsekkiläinen luonnontieteilijä julkaisi työn, jossa käsiteltiin käsien ja jalkojen piirteitä. Työ oli ensimmäinen, joka sisälsi kategorisointia sormenjälkien uurteista.

1858 Sir William James Herschel, Brittiläinen konstaapeli, joka toimi Intiassa, oli ensimmäinen eurooppalainen, joka käytti sormenjälkitunnistusta. Hän uskoi sormenjälkien olevan uniikkeja, joten hän käytti niitä paperien allekirjoittamiseen.

1870 Alphonse Bertillon kehitti rikollisten tunnistamiseen tarkoitetun systeemin, joka pohjautui antropologiaan. Järjestelmässä käytettiin myös sormenjälkeä, joka ei ironisesti kylläkään Bertillonin itsensä mielestä ollut tärkeä. Nykypäivänä sormenjälkitunnistus on yleisin biometrinen tunnistautumistapa.

1880 Henry Fauld ja Sir Francis Galton kehittivät sormenjälkien luokitussysteemin. Fauld oli ensimmäinen eurooppalainen, joka ajoi päättäväisesti sormenjälkitunnistusta rikollisten tunnistamiseen. 12 vuotta myöhemmin Galton julkaisi kirjan ”Finger Prints”, jossa kuvaillaan kolmea pääuurretyyppiä: engl. loops, whorls, arches.

1900-luvulla biometriasta tuli käytetympää sekä tunnetumpaa. Bertillonin järjestelmän käyttö lopetettiin sekä USA:ssa puolustusvoimat ja useat osavaltiot ottivat käyttöönsä sormenjälkitunnistuksen (Fosdick, 1915, s. 364).

1960-luvulla kehitettiin automatisoitu sormenjälkitunnistusjärjestelmä. Tähän aikaan alettiin myös pohtia kasvojentunnistuksen mahdollisuuksia. Woodrow Bledshoeta voidaan pitää kasvojentunnistuksen pioneerina, sillä hänen mielestään silmien, nenän, suun ja korvien sijainti oli tärkeää henkilöä kuvattaessa.

1969 FBI (Federal Bureau of Investigation) ponnisteli saadakseen automaattisen sormenjälkitunnistusjärjestelmän ottamalla yhteyttä USA:n teknologian instituuttiin, tuloksetta.

1974 ensimmäinen kädenjäljen kartoitusjärjestelmä tuli julki, jonka jälkeen pian Standfordin instituutti alkoi työskennellä allekirjoituksentunnistamisen parissa.

1980 Goldstein, Harmon ja Lesk kehittivät idean kasvojentunnistuksesta. Tunnistuksessa käytettiin 21 tarkasti määriteltyä tekijää. Samaan aikaan sana ”biometria” alettiin käyttää kuvaamaan automatisoituja tapoja henkilön tunnistamiseksi.

1980-1990 Biometriaa alettiin testaamaan USA:ssa useissa laitoksissa sekä verkkokalvonkuvausjärjestelmä otettiin käyttöön USA:n puolustusvoimissa. 1986 ensimmäinen biometrinen yhdistys perustettiin, nimellä International Biometric Association.

1990-luvulla verkkokalvontunnistukseen käytettävä teknologia valmistettiin Cambridgen yliopistossa sekä perustettiin Britannian biometrinen yhdistys. Myös pakolaistoiminnassa alettiin käyttää sormenjälkitunnistusta.

2002 aloitettiin biometristen järjestelmien toimivuuden standardisointi.

3. Biometrinen turvallisuusteknologia

Biometrisia järjestelmiä käytetään useissa laitoksissa ja yrityksissä turvallisuuden ja luvattoman kulun valvonnan edistämiseksi. Seuraavissa kappaleissa on avattu biometrian avainkäsitteitä ja toimivuutta sekä yleisimpiä sovelluskohteita.

3.1 Tunnistautumisen ja todentamisen erot

Todentaminen ja tunnistaminen ovat biometrian kannalta keskeisiä, samankaltaisia käsitteitä, jotka voivat helposti mennä sekaisin; joskus on vaikea ymmärtää niiden eroa ja tarkoitusta. Käsitteet toimivat myös läheisesti verifikaation ja valtuuttamisen kanssa. (Authentication, n.d.)

Biometrinen tunnistautuminen on automaattista elävän yksilön tunnistamista sen fysiologisiin ominaisuuksiin ja käyttäytymiseen perustuen. Biometristä tunnistetta ei voi vaihtaa, kuten salasanaa. Koodi tai salasana voi olla hukassa ja se voidaan korvata, toisin kuin biometrinen ominaisuus. (Biometria, n.d.)

Todentaminen tarkoittaa henkilön identiteetin varmistamista. Esimerkki todentamisesta käytännössä: Nainen tulee luoksesi ja kertoo olevansa Maija. Otat Maijasta kuvan ja laitat sen järjestelmään. Järjestelmä löytää Maijan tiedot ja yhdistää ne Maijan kuviin. Mikäli positiivinen tulos löytyy, osoittautuu nainen todellakin Maijaksi. Mikäli tulos on negatiivinen, nainen ei todennäköisesti ole Maija. Tunnistautuminen ja verifikaatio ovat käytännössä sama asia. Tunnistautumisen tarkoitus on vahvistaa henkilön todella olevan se, joka hän väittää olevansa.

Valtuuttamisella voidaan määritellä, onko henkilöllä valtuudet päästä tiettyyn sisältöön käsiksi. Valtuuttamisesta yksinkertainen esimerkki on elokuvissa käyminen: Ostat lipun, jotta pääset sisälle saliin tiettyyn näytökseen. Salin ovella tarkastaja päästää sisään henkilöt, joiden lipun lukulaite hyväksyy. Valtuuttamisessa ei ole kyse tunnistautumisesta, tai verifikaatiosta, joskin ne voivat toimia yhdessä.

Suuren yrityksen tietokonejärjestelmä voi toimia samalla tavalla: Päästäksesi sisään tutkimusalueelle, sinun tulee katsoa ovitunnistimeen määrätyltä lähietäisyydeltä, jotta tunnistin voi suorittaa iirisskannauksen. Tunnistin vertaa iiristä kaikkiin tietokannassa oleviin tuloksiin, jos positiivinen tulos löytyy, ovi aukeaa; jos ei, laukeaa esimerkiksi hiljainen hälytys tunkeilijasta. Kun silmää kuvataan, alkaa verifikaatioprosessi. Valtuutus tapahtuu tai jää tapahtumatta, kun tunnistin antaa positiivisen tai negatiivisen vastauksen. (Laux, 2007, s. 7–15.)

3.2 Biometrian toiminnallisuus

Biometriikan toimivuuden kannalta herää varmasti kysymyksiä siitä, mitä ominaisuuksia voidaan mitata biometrian avulla. Vastaus on: lähes kaikkia. Artikkelin Jain, Bolle, Ruud

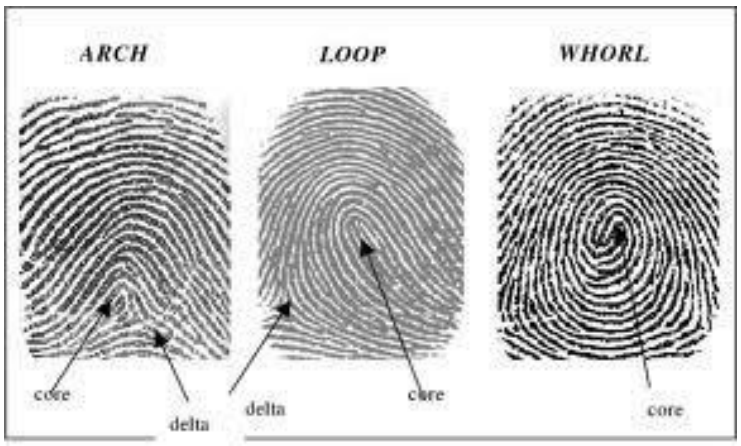
& Pankanti (2006) mukaan ominaisuuden tulee täyttää kaikki alla luetellut vaatimukset,jotta sitä voidaan mitata biometrian avulla.

1) Universaali: Ominaisuus pitää löytyä kaikilta ihmisiltä.
2) Ainutlaatuinen: Ominaisuuden pitää erottaa ihmiset toisistaan. Kaikki ominaisuudet eivät ole biometrian avulla mitattavia.
3) Muuttumattomuus: Mitattavan piirteen ei tule muuttua ajan myötä. Täten esimerkiksi pituutta ei voida käyttää biometrisena mitattavana.
4) Mitattavuus: Ominaisuuden pitää olla mitattavissa hyödyllisesti ja tehokkaasti ajan ja hinnan kannalta; mittauksen ei tule olla pitkäkestoinen prosessi, joka vaatii tarkoitukseensa nähden kallista laitteistoa tai työaikaa.
5) Suoritettavuus: Ominaisuuden pitää olla mitattavissa riittävän tarkasti, mittaukseen vaadittavalla laitteistolla, mittausympäristössä.
6) Hyväksyttävyys: Kuinka pitkälle ihmiset ovat valmiita menemään mittauksen suorittamiseksi.
7) Kierrettävyys: Kuinka helposti tunnistautumista voi tahallisesti huijata. Tämä vaatimus on erittäin tärkeä informaation kasvaneen arvon myötä. (Jain, et al. 2006, s. 1–15.)

Chun ja Rajendran (2009) tutkivat George Washingtonin yliopisto-opiskelijoiden mielipidettä biometrian hyödyllisyydestä. Kyselyn mukaan 77% vastanneista piti biometriaa hyödyllisenä työkaluna identiteetin tunnistamiselle. 16% oli sitä mieltä, että vain osa biometrian tuomista hyödyistä olivat sen arvoisia. Vain 7% oli biometriaa vastaan. Suosituin tunnistautumistapa oli sormenjälkitunnistus. Chun ja Rajendran (2009) tutkimuksen mukaan ihmiset arvostavat biometrisissä järjestelmissä eniten turvallisuuden tunnon kasvua sekä tunnistautumisen tarkkuutta. Miinuksena oli ylitse muiden yksityisyyden hupeneminen sekä järjestelmien korkeaksi koettu hinta.

3.3 Sormenjälkitunnistimen toiminnallisuus

Sormenjälkitunnistin on yleisin käytössä oleva biometrinen tunnistautumistapa (InAuth, 2017). Nykypäivänä suurtenkin tietomurtojen ollessa arkipäivää, sormenjälkitunnistin turvaa satojen miljoonien ihmisten puhelimien, tietokoneiden sekä turvajärjestelmien väärinkäytön vaatimalla uniikin tunnisteen käyttäjältä.



Kuva 1. Esimerkki sormenjäljen skannattavista piirteistä (Prateek, J. 2017.)

Sormenjälkitunnistin skannaa sormenpään yksityiskohtaisesti ja tallentaa sen laitteen tietokantaan, jonka jälkeen uniikit mitatut arvot muuttuvat tunnistekoodiksi laitteen sisällä (Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. 2009, s. 57-61). Kun sormenjälkiä on tallennettu, muodostuu niistä tietokanta, joihin käyttäjän sormenjälkeä verrataan, kun hän tunnistautuu laitteeseen.

Sormenjäljestä mitataan laitteen algoritmin kompleksisuudesta riippuen yleisimmin viivojen jakautumiskohdat, jotka ovat tietyssä etäisyydessä sormen keskipisteestä (core, kuva 1) sekä tietyssä etäisyydessä toisistaan. Algoritmi piirtää viivoja yksityiskohtien väliin ja niiden etäisyydet muunnetaan uniikeiksi koodeiksi, joten kun käyttäjä asettaa sormensa laitteen tunnistimeen, verrataan kyseistä koodia tietokannan koodeihin; mikäli sama koodi, tai riittävästi samankaltainen koodi löytyy tietokannasta, pääsee käyttäjä sisään. (Maltoni, et al. 2009, s. 57-61).

3.4 CERN- järjestelmät

Conseil Europeen pour la Recherce Nucleaire, lyhyemmin CERN on hiukkasfysiikan tutkimuskeskus, joka sijaitsee lähellä Geneven kaupunkia Ranskan ja Sveitsin rajalla.

CERN:issä otettiin käyttöön 55 iiristunnistinta vuonna 2008. Tunnistimet takaavat vain valtuutetun pääsyn LHC:n (hiukkaskiihdyttimen) maanalaisiin tiloihin. Laitoksen turvallisuuspäällikön mukaan iiristunnistimet ovat tärkein osa CERN:in tunnistautumisprosessia: ”Noin 10,000 tieteilijää, teknikkoa tai vierailijaa on rekisteröity järjestelmään sekä noin 3000 henkilöä kulkee laitoksen tiloissa tyypillisesti päivittäin”. Turvallisuuspäällikön mukaan korkea-arvoinen työ sekä työntekijät vaativat erittäin tiukkaa turvallisuuspolitiikkaa ja tähän ovat tuoneet merkittävän hyötynsä iiristunnistimet, jotka toimivat asianmukaisesti jopa sadan metrin syvyydessä maan alla. Turvatoimet on säädetty estämään ylimääräisten henkilöiden pääsy sisään tarkasti vartioituihin tiloihin. Työntekijät astuvat sisään pieneen ilmalukolliseen tilaan, jossa infrapunatunnistimet ja painoa tunnistavat lattialaatat varmistavat vain yhden henkilön läsnäolon. Tilassa iiristunnistin prosessoi kuvaamansa iiriksen ja päättää valtuuden myöntämisen vain sekunnissa, jolloin ilmalukon toinen ovi hyväksyttäessä avautuu vartioidulle alueelle. Työntekijät ovat valtuutettuja kulkemaan vain niillä alueilla, joita työ vaatii. Iiristunnistimet tukevat järjestelmää, johon

jää kulkua valvova jälki, josta laitoksen ylläpitäjät voivat seurata kaikkien työntekijöiden kulkua. (CERN, n.d.).

Iiristunnistimien kehittäjäyhtiön varapresidentin Mohammed Muradin sanoin: ”Iris ID-teknologia luo standardin identiteetin vahvistamiselle, pääsyn hallitsemiselle, ajan ja kulun seurannalle.” Iris ID:n tulevista projekteista yksi on pankkiautomaattien käyttäjien tunnistusmetodi, jota kehitetään yhteistyössä Etelä-Korean Woori- pankin kanssa. (Mayhew, 2012)

3.5 Mobiililaitteet

Mobiililaitteiden yleisin biometrinen tunnistusjärjestelmä on sormenjälkitunnistin. Tunnistin on kehittynein ja vanhin biometrisen tunnistusjärjestelmän muoto, joka on hyväksi havaittu ja nykypäivänä lähes jokaisessa uudessa älypuhelimessa. Järjestelmä perustuu sormen kuvioihin, joita avattiin kappaleessa 3.3.

Kasvojentunnistus, kuten uusimmassa Applen älypuhelimessa iPhone X:ssä, toimii sormenjälkitunnistimen tavoin. Kasvojentunnistus voidaan perustaa infrapunatunnistuksen varaan, jolloin algoritmit mittaavat kasvojen osien välisiä etäisyyksiä ja syvyyksiä.

Äänentunnistus on myös erittäin yleinen laitevalmistajan apuohjelma (kuten Applen Siri.), jolla voidaan ohjata puhelinta äänen avulla. Äänentunnistus kalibroidaan sanomalla esimerkkilauseita, joita ohjelma analysoi ja muodostaa äänelle käyttöluvan puhelimeen. Äänentunnistusteknologian kaavaillaan olevan seuraava suuri ns. helpotus teknologian käytölle. Äänentunnistus lienee haavoittuvaisempi kuin sormenjälki tai kasvojentunnistus, sillä toisin kuin sormenjälkeä tai kasvoja, voidaan sitä huijata helposti nauhoitteella. Äänentunnistus on myös merkittävä hyöty autoilevalle ihmiselle, mikäli sen kehityksen edetessä, sillä voisi vastata puheluihin ja myös kirjoittaa tekstiviestejä; mahdollisuudet ovat käytännössä rajattomat.

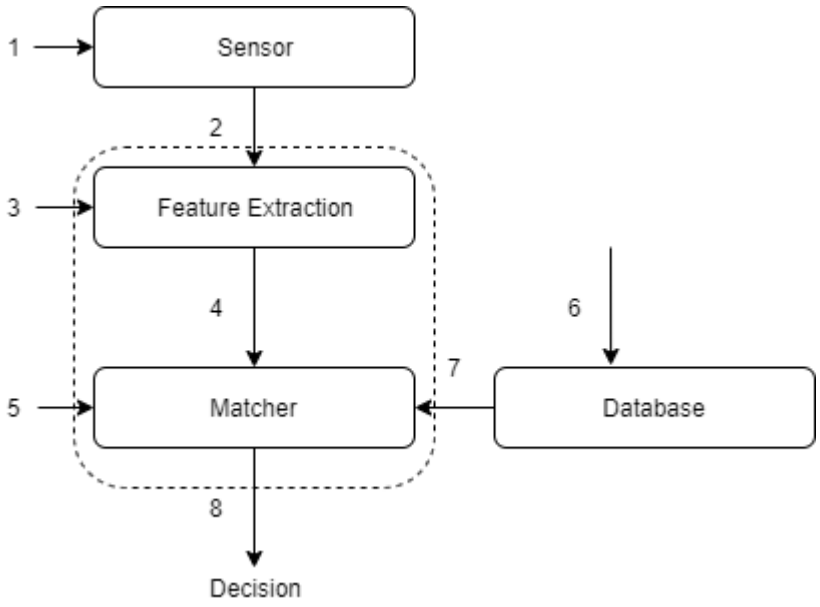
Mobiililaitteet kehittyvät huimaa vauhtia ominaisuuksiensa ansiosta. Kun niin paljon tehoa mahtuu kädessä pidettävään laitteeseen, kehitysmahdollisuudet ovat valtavat. Mobiililaitteiden käytön kasvuun liittyy myös ongelmia, kuten alati kasvavat tietoturvariskit (Trader, 2017). Ihmisillä on mobiililaitteessaan lähes aina riittävä määrä tietoa myös identiteettivarkauteen, mikä lisää tietynlaista kaoottisuutta nyky-yhteiskuntaan. Monissa älypuhelimissa on silti vieläkin käytössä vain halpa ja jokseenkin tehoton ratkaisu käyttää pelkkää salasanaa tai pin-koodia puhelimen lukitsemiseen. Biometrisen järjestelmän käyttöönoton pakottaminen olisi helppo askel nykysukupolvelle, todennäköisesti myös vanhemmalle, mikäli siitä tehtäisiin standardi. Käyttöjärjestelmät muuttuvat koko ajan, joten miksi pientä hyödyllistä ominaisuutta ei voisi pitää itsestäänselvyytenä, kuten nelinumeroista SIM-koodia. Puhelimeen luvaton pääsy estyisi käytännössä kokonaan. Mikäli sormenjälkitunnistimesta tai vastaavasta saataisiin niin luotettava, että se voisi olla ainoa tunnistautumisen keino, parantaisi tämä yksityishenkilöiden tietoturvaa huomattavasti.

Mobiililaitteille soveltuva hybriditunnistautuminen, joka yhdistäisi kahta biometristä tunnistautumistapaa, olisi jo lähes vedenpitävä keino pitää kaikki tunkeutujat poissa myös

puhelimen hukkuessa tai tullessa varastetuksi (Clarke, Furnell & Reynolds, P. 2002, s. 63–64).

4. Hyökkäys biometriseen järjestelmään

Biometriset järjestelmät ovat yleisesti ottaen turvallisempia kuin perinteiset turvallisuusmenetelmät, jotka perustuvat ”tokeneihin” tai salasanoihin. Biometriaa vastaan voidaan silti hyökätä useilla tavoilla; tässä kappaleessa käsitellään yleisimmän tunnistusjärjestelmän eli sormenjälkitunnistimen heikkoja kohtia ja järjestelmää sekä sitä vastaan hyökkäystä.



Kuva 2. Sormenjälkitunnistimessa voi olla kahdeksan tai jopa useampi väylä sisään tunkeilijalle (Uludag & Jain. 2004, 2.).

Tyypin 1. hyökkäys keskittyy esittämään tunnistimen sensorille oikean sormenjäljen käyttäen vääriä keinoja esimerkiksi kuvaa sormenjäljestä. Toinen hyökkäystapa käyttää aiemmin annettua sormenjälkeä, jonka sensori mieltää reaaliajassa esitetyksi. Kolmas hyökkäys antaa sensorin tulkkaajalle hyökkääjän luomaa tietoa, jolloin ”matcher” eli komponentti, joka vertaa sormenjälkeä tietokannassa oleviin hyväksyttäviin sormenjälkiin, päästää hyökkääjän läpi. Neljännessä hyökkäyksessä tulkilta lähtevä viesti korvataan hyökkääjän antamalla viestillä, jossa on sopivat arvot jälleen läpipääsemiseen. Matcherille voidaan antaa hyökkääjän omia arvoja sormenjälkeä vastaamiseksi, jolloin päästään sensorin läpi. (Uludag & Jain, 2004, s. 1–4, 11).

Tietokantaan voidaan hyökätä kahdella tapaa (Kuva 2. kohdat 6, 7), jolloin tallennetut sormenjäljet, joita vastaan annettuja jälkiä verrataan, pyyhitään kokonaan tai asetetaan vastaamaan esimerkiksi hyökkääjän sormenjälkeä. Viimeinen hyökkäys kohdistuu viestiin, joka lähtee matcheriltä komponenttiin, joka avaa laitteen; hyökkääjä voi manipuloida viestin olevan aina tosi, jolloin laite avataan. Yleisin tapa hyökätä on pitkälti samankaltainen kuin salasanan murtaminen: Kokeillaan kaikkia mahdollisia yhdistelmiä sormenjälkitunnistimeen, kunnes sormenpään urista mitattavat parametrit vastaavat jotain tallennetuista sormenjäljistä riittävän korkealla prosenttiluvulla.

On sanomattakin selvää, että tunkeilijalla täytyy olla suuri tietämys älylaitteiden toiminnasta sekä biometrisen järjestelmän toiminnasta päästäkseen sisään laitteeseen. Hyökkäyksiä vastaan pystytään kuitenkin suojautumaan yhä enemmän, kun teknologia edistyy ja järjestelmät yleistyvät. Yleisin tapa suojata laitteet on asettaa tietty raja yrityskerroille, jolloin esimerkiksi sormenjäljen voi asettaa puhelimeen viisi kertaa väärin tietyn ajan kuluessa. Aidon käyttäjän sormenjälkeä on hyvin vaikea saada monta kertaa peräkkäin väärin. Mikäli hakkeri varastaisi puhelimesi, jonka tunnistautumisraja olisi vaikkapa viisi kertaa (väärin) päivässä tai puhelin lukittautuu, menisi hakkerilla vain tuhanteen yrityskertaan jo 200 päivää (Uludag & Jain, 2004, s. 1–4, 11).

4.1 Biometrisen järjestelmän kehitys & ylläpito

Biometriset järjestelmät ovat hyväksi ja turvalliseksi koettu vaihtoehto tavanomaisille salasanoille. Järjestelmiä kehitetään jatkuvasti ja niihin investoidaan, mutta silti moni ihminen on käyttänyt vain sormenjälkitunnistinta, miksi?

Biometristen järjestelmien globaali kasvu johtaa myös uhkien muodostumiseen nopeasti; lisäksi järjestelmien kehityskulut ovat vielä massiivisia, puhumattakaan itse laitteista. Globaalisti nopeimmin kasvanut sensori kuluttajalaitteissa on sormenjälkitunnistin, joka on myös verrattaen edullisin biometrinen järjestelmä. Kun harkitaan yrityksen tietoturvaa ja mahdollisuuksia tunnistautumisen saralla, on useita tekijöitä, mitkä pitää ottaa huomioon. Biometristen järjestelmien levinneisyys lienee vielä pieni osakseen sen takia, että ne maksavat yksinkertaisesti liian paljon hyötyynsä nähden. Tietomurto biometriseen järjestelmään olisi katastrofaalinen, mikäli hyökkääjä saisi haltuunsa tietokannan työntekijöiden biometrisistä ominaisuuksista.

Biometrics Type	Accuracy	Cost	Size of Template	Long Term Stability	Security Level
Facial Recognition	Low	High	Large	Low	Low
Iris Scan	High	High	Small	Medium	Medium
Fingerprint Recognition	Medium	Low	Small	Low	Low
Finger Vein	High	Medium	Medium	High	High
Voice Recognition	Low	Medium	Small	Low	Low
Retina Scan	High	High	Medium	High	High

Kuva 3. Vertaillaan järjestelmien tyyppiä ja hinta/laatusuhdetta (Thakkar, n.d.)

Biometrisen järjestelmän hinta on sidonnainen tarkkuuteen sekä järjestelmässä käytettävään teknologiaan, joskin täydellistä tarkkuutta ei nykyjärjestelmillä voida vielä saavuttaa (Pankanti, Bolle & Jain, A. 2000, s. 1–3). Sensoreiden kysynnän ja tarjonnan kasvu

kuitenkin johtaa massatuotantoon ja sen kautta varmasti myös innovaatioihin, jotka voivat tuoda uudenlaisia biometrisiä järjestelmiä saataville, sillä nykypäivänä prosessointiteho laitteissa on erittäin laadukasta hintaansa nähden.

5. Tutkimusmenetelmä

Käytetty tutkimusmenetelmä on kirjallisuuskatsaus biometriasta ja sitä sivuavista aiheista useiden tieteenalan ja teknologian julkaisuiden kautta. Lähteiden avulla olen tutkinut biometrian kehitystä hyötyjä ja tarpeellisuutta; pyrkimyksenä on luoda kuva biometrian tarpeellisuudesta, jonka mittarina toimii käyttöympäristö ja työn laatu. Biometrian historia liittyy läheisesti aiheeseen, koska biometrisen tunnistautumisen tarve ajoi järjestelmät alkuunsa. Google Scholar on merkittävin lähde kirjallisuuden ja aiemman aiheesta tehdyn tutkimuksen kannalta, joskin käsitteitä on selitetty Wikipedian avulla. Muita tutkimuksessani käyttämiä tietokantoja ovat Scopus sekä Oula-Finna -palvelun kautta selaamani IEEE-julkaisujen tietokanta. Kriteerinä oli valita suuresta joukosta lähteitä uusimmat ja luotettavimmat julkaisut. Lähteiden nuori-ikäisyys on merkittävä tekijä lähteen olennaisuudelle, sillä biometrian alalla tieto voi vanheta nopeasti. Lähteet vaihtelevat lehtijulkaisun, sähköisen kirjan ja satunnaisen, mutta luotettavan nettisivun välillä. Erikseen mainittakoon hyödyllisenä lähteenä Alexandra Babichin tekemä kandidaatintutkielma: Biometric Authentication. Types of biometric identifiers, josta löytyy paljon hyvin jäsenneltyä tietoa biometrian toiminnasta (Babich, 2012).

Google Scholar tietokannasta hakutuloksia oli erittäin vaikea seuloa, sillä aiheesta oli niin paljon tietoa: ”Biometric*” AND ”Security” AND ”technology” haun tuloksista olen käyttänyt ensimmäisen sivun artikkeleita, joista helposti erotti hyödyllistä tietoa käsittelevät aiheet. Rajasin hakutuloksia erityisesti mainittujen hakusanojen yhdistelmiin sopivaksi sekä katselmoin lukuisia töitä ennen kuin perehdyin valitsemiini artikkeleihin. Pidin kriteerinä hyvälle lähteelle siihen osuvaa viittauksien määrää sekä sitä, kuinka koin sen osuvan tutkimukseni aihealueeseen; minulle tärkeää oli biometristen järjestelmien yleiskuvaus ja käyttöympäristö, ilman syvempää tutkimusta tai selitystä teknisestä toiminnallisuudesta.

Muita hakusanoja:

Biometric* AND Histor*

Biometric* AND Evolution

Biometric* Recognition

Laadullisia tutkimusmenetelmiä, kuten haastatteluja on mahdollista suorittaa tutkimukseni jatkoksi, mikä varmasti lisäisi tietoarvoa aiheeseen. Mikäli haastatteluja voisi suorittaa suurten yritysten tietoturvavastaaville tai turvallisuusjohdolle, tulisi varmasti esiin mielenkiintoisia näkökulmia biometrisiin turvallisuusjärjestelmiin sekä niiden tarpeeseen. Vertailua voisi suorittaa yritysten välillä, jotka ovat muuten samankaltaisia, mutta eroavat turvatoimissaan (biometrinen järjestelmä vs. ei-biometrinen järjestelmä). Järjestelmien budjettia olisi mielenkiintoista vertailla. Voisi olettaa, että tavanomainen avainkorttijärjestelmä olisi varmasti promillen luokkaa iiristunnistus-järjestelmän budjetista.

6. Löydökset: Tietoturvan maksimointi biometrisilla järjestelmillä

Tutkimuksen puitteissa tehdyn analyysin perusteella biometriset järjestelmät lisäävät ihmisten turvallisuudentunnetta henkilökohtaisten älylaitteiden käytössä sekä parantavat turvallisuutta, sillä biometriaa yhdistettynä järkevään valvontaan on erittäin vaikea väärinkäyttää tai huijata (Chu & Rajendran, 2009). CERN:in systeemiä ei tiedettävästi ole ikinä päästy väärinkäyttämään sisältä käsin.

6.1 Biometrisen järjestelmän tarve

Biometria luo lähes absoluuttisesti oikein toimivan järjestelmän mahdollisuuden ihmisten tunnistamiselle ja laitteiden käytön vahvistamiselle, joten miksi sitä ei käytettäisi? Biometriset järjestelmät ovat kalliita kehittää (ainakin vielä), joten pienen yrityksen ei luonnollisesti kannata panostaa sellaiseen, ellei käsiteltävien tietojen tai tavaroiden laatu vaadi erittäin tarkkaa turvallisuuspolitiikkaa. Sama pätee valtioiden ja kansainvälisiin laitoksiin. Mobiililaitteissa biometria toimii ja kehitykselle ei näy loppua, joten olisi tärkeää saada tutkijat ja ammattilaiset keskittymään biometristen järjestelmien kehittämisen pariin ja jakaa tietoa aiheesta enemmän nuorille.

Biometrinen järjestelmä voi toimia käytännössä minkä tahansa käyttäjätilin suojaamiseksi niin mobiililaitteella kuin muullakin teknisellä työkalulla, jossa on jokin tunnistin.

6.2 Päätelmät ja pohdintaa

Tutkimuksen tavoitteena oli tehdä katsaus biometrisiin järjestelmiin sekä niiden kehityksen kautta auttaa ymmärtämään järjestelmien potentiaalia 2020-luvulla. Tutkimusmenetelmäksi on kuitenkin rajattu vain kirjallisuuskatsaus ja lähdeaineistoa on satojatuhansia artikkeleita ja lukemattomia nettisivuja, suurimmaksi osaksi samankaltaisilla avainsanoilla. Tutkimuksessa käsitellään myös biometrisen järjestelmän tarvetta, josta olisi erittäin mielenkiintoista ja uskoakseni myös hyödyllistä jatkaa tutkimusta.

Tutkimusta tehdessäni huomasin yllätyksekseni, kuinka paljon biometriset järjestelmät ovat yleistyneet arkipäiväiseen käyttöön muuallekin, kuin älypuhelimiin. Tutkielmani löydökset ovat lähinnä pääteltävissä ja osaan voi löytyä useampi näkökulma. Tutkimuksessa ei ole käytetty tilastoja vertailemaan biometrian hyötyjä ja haittoja, yhtä mielipidekyselyä lukuun ottamatta. Kysely kuvaa myös näkökulmanvaraista asiaa, joten en usko, että biometrisen järjestelmän tarvetta voi suoraan mitatakaan. On kuitenkin pääteltävissä, että biometrinen järjestelmä lisää ihmisen kokeman turvallisuudentunnetta enemmän kuin tavallinen salasanapohjainen järjestelmä.

Jatkotutkimusta voisi tehdä haastattelemalla tietoturvayrityksiä ja vertailemalla yritysten turvallisuusjärjestelmiä sekä haastattelemalla mobiililaitteiden käyttäjiä siitä, lisääkö biometrinen järjestelmä vain turvallisuudentunnetta, vai myös oikeasti turvallisuutta. Haastattelujen tulisi olla laajoja, sillä vertailun kohteeksi tulisi löytää käyttäjiä, jotka omistavat mobiililaitteen ilman biometrista tunnistinta. Analyysi kohdistuisi varastettujen laitteiden väärinkäyttöön. Mikäli pystyttäisiin haastattelemaan hakkeria tai valkolakkia, voitaisiin myös kokeilla, kuinka paljon vaikeampaa on murtaa biometrinen tunnistusjärjestelmä kuin pelkkä avainkoodi.

Lähteet

Anthropometry. (n.d.) In Wikipedia. Viitattu 19.12.2017. https://en.wikipedia.org/wiki/Anthropometry

Authentication. (n.d.) In Wikipedia. Viitattu 11.12.2019. https://en.wikipedia.org/wiki/Authentication

Babich, A. (2012). Biometric Authentication. Types of biometric identifiers. Haaga-Helia University of Applied Sciences.

Biometria. (n.d.). In Wikipedia. Viitattu 28.11.2019. http://fi.wikipedia.org/wiki/Biometria

CERN. (n.d.) In Wikipedia. Viitattu 29.11.2017. https://fi.wikipedia.org/wiki/CERN

Chu, V., & Rajendran, G. (2009). Use of biometrics. TechCast Article Series, 5.

Clarke, N., Furnell, S. & Reynolds, P. 2002. Biometric Authentication for Mobile Devices. ResearchGate. Viitattu 27.11.2019. https://www.researchgate.net/profile/Nathan_Clarke/publication/253717880_Biometric_Authentication_for_Mobile_Devices/links/5416c40b0cf2788c4b35e550/Biometric-Authentication-for-Mobile-Devices.pdf

Fosdick, R. B. (1915). Passing of the Bertillon System of Identification. J. Am. Inst. Crim. L. & Criminology, 6, 363-369.

History of Biometrics. (n.d.). In Wikipedia. Viitattu 28.11.2019. https://en.wikipedia.org/wiki/Biometrics#History_of_Biometrics

InAuth. (9.1.2017). Fingerprints: The Most Popular Biometric [blogikirjoitus]. Haettu osoitteesta. https://www.inauth.com/blog/fingerprints-popular-biometric/

Jain, A. K., Bolle, Ruud M. & Pankanti, S. (2006). Biometrics: Personal Identification in Networked Society. Springer.

Laux, D. D. (2007). A study of biometric authentication adoption in the credit union industry. Iowa State University Digital Repository.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition. Springer Science & Business Media.

Mayhew, S. (2012). History of Biometrics. Biometric update. Viitattu 02.12.2019. https://www.biometricupdate.com/201802/history-of-biometrics-2

Pankanti, S., Bolle, R. M., & Jain, A. (2000). Biometrics: The future of identification [guest eeditors' introduction]. Computer, 33(2), 46-49.

Prateek, J. (2012). Fingerprint Recognition. Viitattu 11.12.2019. https://prateekvjoshi.com/2012/07/22/fingerprint-recognition/

Thakkar, D. (n.d.). Increasing Importance of Biometric Security, Challenges and Opportunities. Bayometric. https://www.bayometric.com/increasing-importance-of-biometric-security/

Trader, J. 2017. 5 Ways biometric technology is used in everyday life. M2sys.com. Viitattu 29.11.2019. http://www.m2sys.com/blog/guest-blog-posts/5-ways-biometric-technology-is-used-in-everyday-life/

Uludag, U., & Jain, A. K. (2004, June). Attacks on biometric systems: a case study in fingerprints. In Security, Steganography, and Watermarking of Multimedia Contents VI (Vol. 5306, pp. 622-633). International Society for Optics and Photonics.