Tuomas Kontio

Puettavan teknologian tietoturvaongelmat ja käyttäjän yksityisyys

Tietotekniikan kandidaatintutkielma

29. huhtikuuta 2020

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Tuomas Kontio

Yhteystiedot: tuomas.a.kontio@student.jyu.fi

Ohjaaja: Sanna Juutinen

Työn nimi: Puettavan teknologian tietoturvaongelmat ja käyttäjän yksityisyys

Title in English: Security and privacy issues in wearable technology

Työ: Kandidaatintutkielma

Opintosuunta: Kaikki opintosuunnat

Sivumäärä: 28+0

Tiivistelmä: Puettavan teknologian suosio kasvaa jatkuvasti. Erilaiset puettavat laitteet keräävät käyttäjästä suuren määrän arkaluontoista terveyteen liittyvää tietoa, joten sen tietoturvallisesta ja yksityisyyttä kunnioittavasta käsittelystä pitäisi pitää erityistä huolta. Tämän tutkielman tarkoituksena on selvittää mitä tietoturvaan ja käyttäjän yksityisyyteen liittyviä ongelmia puettavaan teknologiaan liittyy ja miten niitä voidaan ehkäistä.

Avainsanat: IoT, puettava teknologia, älykello, aktiivisuusranneke, tietoturva, yksityisyys

Abstract: Popularity of wearable technology is continuously growing. Various wearable devices gather vast amounts of sensitive health related information about the user which is why handling the data in a secure manner that respects the user's privacy requires special attention. Purpose of this thesis is to survey what security and privacy issues are associated with wearable technology and how to prevent them.

Keywords: IoT, wearable technology, smartwatch, wristband, security, privacy

Kuviot

Sisältö

1 Johdanto

Erilaisten itsenäisesti toimivien, ympäristöstään tietoa keräävien ja dataa verkkoon välittävien laitteiden määrä jatkaa kasvamistaan. Älypuhelinmarkkinan saturoiduttua kuluttajalaitteiden valmistajat pyrkivät etsimään uusia laitekategorioita. Yksi tämän hetken suosituista nousevista laitekategorioista on erilaiset puettavat laitteet (*wearables*), kuten älykellot ja aktiivisuusrannekkeet, joiden käyttö alkaa jo arkipäiväistyä. Markkinatutkimuslaitos IDC:n (2019a) mukaan erilaisia puettavia laitteita myydään vuonna 2019 yli 300 miljoonaa kappaletta ja myynnin odotetaan kasvavan yli 20% vuosivauhtia tulevina vuosina.

Puettavien laitteiden toiminnallinen ja rakenteellinen yksinkertaisuus, vähäinen käytössä oleva laskentateho, muisti ja virta, sekä laitteiden edullisuus aiheuttavat haasteita kattavan tietoturvan toteuttamiselle laitteissa. Ympäristö, josta puettavat laitteet keräävät dataa on useimmiten laitteen käyttäjä. Puettavat laitteet muun muassa keräävät sensoreillaan tietoa, joka liittyy suoraan käyttäjän terveyteen ja elintoimintoihin, kuten esimerkiksi käyttäjän sydämen syke, liikunnallinen aktiivisuus ja uni. Lisäksi älykelloihin ja aktiivisuusrannekkeisiin voidaan välittää ilmoituksia käyttäjän puhelimesta ja välitettävät viestit voivat sisältää yksityisenä pidettävää tietoa. Kerätyn tiedon luonne on sellaista, että sen tietoturvallisesta käsittelystä ja käyttäjän yksityisyydestä tulisi pitää erityistä huolta. Yksityisyyden kannalta on olennaista, kenellä on pääsy käyttäjästä kerättyyn tietoon sekä kuinka sitä käsitellään ja säilytetään.

Tutkielman aiheena on puettavien laitteiden tietoturva ja käyttäjän yksityisyys erityisesti erilaisten älykellojen ja aktiivisuusrannekkeiden osalta. Tutkimuksen tarkoituksena on kirjallisuuskartoituksen avulla selvittää minkälaisia tietoturvaan ja käyttäjän yksityisyyteen liittyviä ongelmia puettavaan teknologiaan liittyy ja minkälaisia ratkaisuja on löydetty kyseisten ongelmien korjaamiseksi. Puettavien laitteiden kasvava suosio tekee tutkimusaiheesta ajankohtaisen. Puettavan teknologian ollessa vielä nuorta ja laitteiden kehittyessä nopeasti on tärkeää, että tietoturvaan ja yksityisyyteen liittyviä ongelmia tutkitaan ja tuodaan esiin tässä vaiheessa.

Luvussa 2 esitellään puettavien laitteiden määritelmä, erilaisten laitteiden lajittelua sekä

puettavien laitteiden rakennetta ja yleisimpiä niissä käytettyjä teknologioita. Luvussa 3 käydään läpi, mitä vaatimuksia puettavien laitteiden tietoturvalle ja käyttäjän yksityisyydelle asetetaan ja mitä haasteita näiden toteuttamisessa on. Luvussa 4 käsitellään erilaisia tietoturvauhkia ja löydettyjä hyökkäystapoja puettavia laitteita vastaan. Luvussa 5 käydään läpi, mitä toimenpiteitä voidaan suorittaa, jotta löydetyt tietoturvauhat voidaan ehkäistä.

2 Puettava teknologia – rakenne ja käytetyt teknologiat

Tässä luvussa käydään läpi puettavien laitteiden määritelmä, erilaisten puettavien laitteiden lajittelua ja eri laitekategorioiden kaupallista suosiota. Lisäksi luvussa esitellään puettavien laitteiden rakennetta sekä laitteiden välisessä kommunikaatiossa käytettävää arkkitehtuuria ja siinä yleisimmin käytettyjä teknologioita.

2.1 Määritelmä

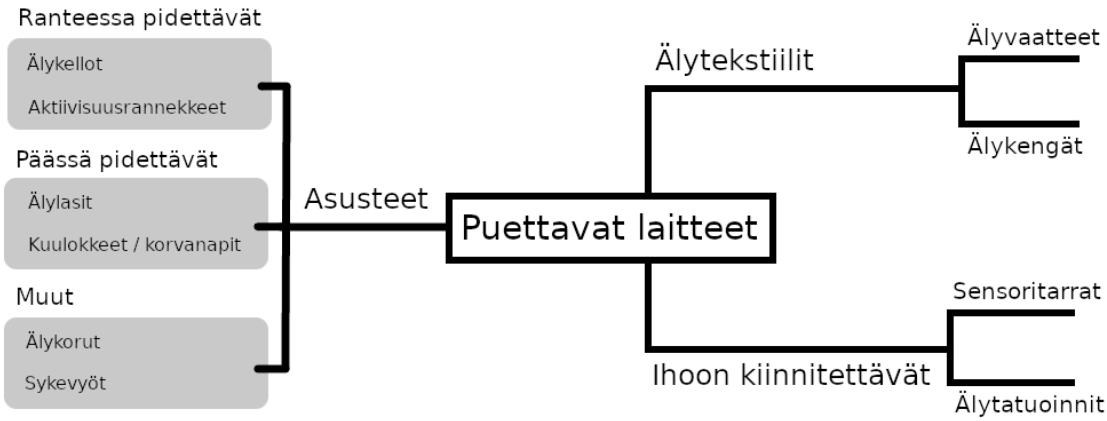
IoT (*Internet of Things* tai suomeksi esineiden Internet) tarkoittaa pieniä, itsenäisesti toimivia, tietoverkkoon kytkettyjä laitteita, jotka esimerkiksi sensoreiden avulla keräävät erilaista tietoa ympäristöstään ja kommunikoivat sen tietoverkon välityksellä toisille laitteille (Alaba ym. 2017). IoT:n erilaiset käyttökohteet ovat laajat, koska nykyään lähes mikä tahansa arkipäiväinen laite voi olla ”esine”, joka välittää keräämäänsä dataa tietoverkkoon. Yksi IoT:n useista kategorioista on puettava teknologia, joka pitää sisällään erilaisia puettavia laitteita.

Puettavalla laitteella (*wearable*) tarkoitetaan jonkinlaista laitetta, joka on kiinni sen käyttäjässä. Ominaista puettaville laitteille on, että niitä pidetään useimmiten aina päällä ja ne ovat koko ajan mittaamassa, keräämässä ja välittämässä käyttäjää koskevaa tietoa verkkoon (Seneviratne ym. 2017). Arkkitehtuuriltaan puettavat laitteet muistuttavat IoT-laitteita, mutta ne saattavat kerätä jopa enemmän dataa kuin muut IoT-laitteet tyypillisesti (Arias ym. 2015).

2.2 Lajittelu

Erilaisten puettavan teknologian kategoriaan kuuluvien laitteiden määrä on suuri ja laitteet voidaan luokitella eri tavoin käyttötavan tai -tarkoituksen mukaan. Seneviratne ym. (2017) luokittelee puettavat laitteet kolmeen pääkategoriaan – asusteet (*accessories*), älytekstiilit (*E-Textiles*) ja ihoon kiinnitettävät laitteet (*E-Patches*) (Kuvio 1). Asusteet voidaan lisäksi jakaa sen mukaan, missä kohtaa kehoa puettavaa laitetta kannetaan. Ranteessa pidettävät laitteet sisältävät muun muassa älykellot ja aktiivisuusrannekkeet. Päässä pidettäviin laitteisiin kuuluvat älylasit sekä erilaiset älykkäät kuulokkeet ja korvanapit (*hearables*). Lisäksi on

vielä muita asusteita, kuten älysormuksia, älykoruja ja sykevöitä, jotka on luokiteltu erikseen. Älytekstiilit pitävät sisällään erilaiset älykkäät vaatteet ja -kengät. Ihoon kiinnitettäviä laitteita ovat esimerkiksi sensoritarrat ja älytatuoinnit.



Kuvio 1. Puettavien laitteiden lajittelu pohjautuen Seneviratnen ym. (2017) kuvaan.

Sekä markkinatutkimuslaitosten Gartnerin (2018, 2019) että IDC:n (2019a, 2019b) tilastojen mukaan erilaiset asusteet ovat näistä laitekategorioista selkeästi suurin sekä kappalemääräisessä että rahallisesti mitatussa myynnissä. Asusteista erityisesti ranteessa pidettävien laitteiden, kuten älykellojen ja aktiivisuusrannekkeiden, osuus myynnistä on tällä hetkellä noin puolet (Gartner 2018; IDC 2019b). Erilaiset päässä pidettävät laitteet, kuten esimerkiksi langattomat kuulokkeet, kuitenkin nostavat tällä hetkellä eniten suosiotaan (Gartner 2019; IDC 2019a). Ranteessa pidettävien laitteiden suosio ja kuluttajalaitteiden helppo saatavuus ovat tehneet niistä myös soveliaan tutkimuskohteen (Do, Martini ja Choo 2017). Älykelloihin ja aktiivisuusrannekkeisiin liittyvää tutkimusta löytyykin enemmän kuin muihin puettavaan teknologiaan kuuluviin laitetyyppeihin.

2.3 Laitteiden rakenne ja sensorit

Puettavasta laitteesta tyypillisesti löytyy erilaisia sensoreita, jolla mitataan jotain tietoja käyttäjästä tai laitteen muusta ympäristöstä. Yksinkertaisimmillaan aktiivisuusrannekkeessa voi olla vain jokin yksittäinen sensori, kuten kiihtyvyysanturi, jota käytetään askelmäärän mittaamiseen (Rieck 2016). Monissa aktiivisuusrannekkeissa ei ole lainkaan näyttöä toisin kuin älykelloissa, joiden käyttötarkoitus on enemmän suunniteltu korvaamaan myös perinteisiä

rannekelloja (Seneviratne ym. 2017). Tyypillisimmät aktiivisuusrannekkeiden ja älykellojen käyttötarkoitukset ovat käyttäjän fysiologian ja fyysisen aktiivisuuden mittaaminen sekä viestien välitys ja ilmoitukset (Seneviratne ym. 2017). Laitteiden rakenne ja laitteista löytyvät sensorit tukevatkin näitä toimintoja. Teknologian kehittyessä ja laitteiden tarjotessa enemmän ominaisuuksia, myös laitteista löytyvien sensoreiden määrä lisääntyy.

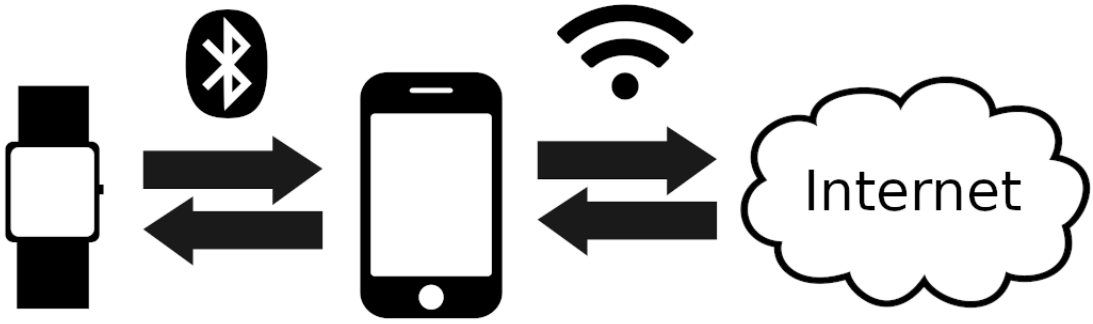
Nykyään laitteista voi löytyä muun muassa optinen sykemittari, joka mittaa käyttäjän fysiologisia ominaisuuksia, kiihtyvyysanturi ja gyroskooppi, joilla mitataan käyttäjän fyysistä aktiivisuutta ja erilaisia ympäristöä havainnoivia sensoreita, joita käytetään esimerkiksi lämpötilan, kosteuden tai ilmanpaineen mittaamiseen (Liew ym. 2015). Lisäksi laitteista voi löytyä paikannuksen avuksi GPS sekä magneettinen kompassisensori (Liew ym. 2015).

Kiihtyvyysanturia (*accelerometer*) käytetään mittaamaan laitteen liikettä kaikissa kolmessa ulottuvuudessa ja sen avulla pystytään määrittämään, onko laite liikkeessä vai paikallaan (Ching ja Singh 2016). Chingin ja Singhin (2016) mukaan yleisin käyttötarkoitus kiihtyvyysanturille on erilaisten liikkeen mallien tunnistaminen, joiden avulla pystytään päättelemään esimerkiksi käveleekö tai juokseeko käyttäjä ja tätä tietoa voidaan edelleen hyödyntää askelten laskemiseen. Gyroskooppi määrittää laitteen asennon maan vetovoimaan perustuen (Ching ja Singh 2016). Vaikka näiden sensoreiden käyttötarkoitus on osin samankaltainen, niitä käytetään puettavissa laitteissa rinnakkain.

2.4 Tiedonvälityksen arkkitehtuuri ja siinä käytetyt teknologiat

Puettaville laitteille on tyypillistä, että verkkoon välitettävä tieto kulkee jonkin yhdyskäytävänä (*gateway*) toimivan laitteen välityksellä, mikä on useimmiten käyttäjän matkapuhelin (Kuvio 2) (Ching ja Singh 2016). Tätä tarkoitusta varten käyttäjän älypuhelimeen asennetaan jokin erityinen sovellus, joka välittää kerätyn tiedon verkkopalvelimelle, jossa tietoa analysoidaan ja se lähetetään takaisin sovellukseen esitettäväksi käyttäjälle (Lee ym. 2016). Älykellot ja aktiivisuusrannekkeet tarjoavat myös toisen suunnan kommunikaatiolle välittämällä ilmoituksia käyttäjän puhelimeensa saaduista puheluista, tekstiviesteistä ja sähköposteista. (Seneviratne ym. 2017).

Laitteiden väliseen kommunikointiin käytetään erilaisia lyhyen kantaman radioteknologioi-



Kuvio 2. Puettavien laitteiden tiedonvälityksen arkkitehtuuri pohjautuen Chingin ja Singhin (2016) kuvaan.

ta, kuten Bluetooth, BLE, ANT/ANT+, ZigBee ja NFC, mutta nykyään useimmiten Bluetooth-protokollaa sen eri muodoissa. Jotkin ensimmäisistä kuluttajalaitteista, kuten Fitbit, käyttävät ANT-protokollaa tiedon siirtoon rannekkeen ja erityisen telakan välillä (Rahman, Carbunar ja Banik 2013). ZigBee-protokolla on käytössä erityisesti lääketieteelliseen tarkoitukseen suunniteltujen puettavien laitteiden yhteydessä ja WBAN (*Wireless Body Area Network*) -verkon muodostamisessa (Baker, Xiang ja Atkinson 2017). Vähäisen virrankulutuksen vuoksi BLE (*Bluetooth Low Energy*) on nykyään muodostunut standardiksi, jota useimmiten käytetään puettavien laitteiden ja älypuhelimen välisessä tietojen vaihdossa (Das ym. 2016). Myös suurin osa Seneviratne ym. (2017) luokittelemista älykelloista ja aktiivisuusrannekkeista hyödyntää BLE-protokollaa. BLE tarjoaa riittävän toimintaetäisyyden, tiedonsiirtonopeuden, vähäisen virrankulutuksen ja se on käytössä myös yhdyskäytävänä toimivissa älypuhelimissa, joten se sopii hyvin käytettäväksi myös tässä tarkoituksessa (Baker, Xiang ja Atkinson 2017; Yaqoob, Abbas ja Atiquzzaman 2019). Laitteiden maksuominaisuuksien lisääntyessä, myös NFC-teknologia on yleisemmin käytössä nykyisissä älykelloissa ja aktiivisuusrannekkeissa tai sitä voidaan myös käyttää avustamaan laitteiden pariutumista (Seneviratne ym. 2017). Laitteiden keräämän tiedon välittämisessä verkossa sijaitsevalle palvelimelle käytetään älypuhelimen käyttämää WLAN- tai mobiilidatayhteyttä (Lee ym. 2016). Monet IoT-teknologiassa käytettyyn tiedonvälitykseen liittyvät tietoturvaongelmat koskevat siten myös puettavia laitteita.

3 Vaatimukset tietoturvalle ja käyttäjän yksityisyydelle sekä haasteet niiden toteuttamisessa

Tässä luvussa käsitellään, miksi puettavien laitteiden tietoturvaan ja käyttäjän yksityisyyteen pitäisi kiinnittää erityistä huomiota ja miksi niiden toteuttaminen on haasteellista tässä laitekategoriassa.

3.1 Vaatimuksia

Koska puettavat laitteet keräävät arkaluontoista käyttäjän terveyteen liittyvää tietoa, sen tietoturvallisesta ja yksityisyyttä kunnioittavasta käsittelystä tulee keskeinen järjestelmävaatimus (Fafoutis ym. 2017). Kerätty tieto on käyttäjän elintoimintoihin ja terveyteen liittyvää, kuten esimerkiksi käyttäjän sydämen syke, kulutetut kalorit ja uni, joten se on luonteeltaan arkaluontoista ja yksityistä. Käyttäjän yksityisyyden kannalta on olennaista, kenellä on pääsy käyttäjästä kerättyyn tietoon sekä kuinka tietoa käsitellään ja tallennetaan. Lisäksi laitevalmistajalla on tapana yhdistää aktiivisuusdataa muuhun yksilöivään käyttäjätietoon, kuten esimerkiksi nimi, sähköpostiosoite, puhelinnumero ja sijainti (Ching ja Singh 2016). Koska tieto on luonteeltaan arkaluontoista ja yksityistä on tärkeää, että sitä ei voida muuttaa tiedonsiirron aikana ja että vain asiaankuuluvilla osapuolilla on pääsy tietoon (Seneviratne ym. 2017). Laitteiden käyttäjät asettavat vaatimuksia laitteiden pienelle koolle ja kannettavuudelle, jotka osaltaan rajoittavat laitteiden akkukestoa ja laskentehoa (Liew ym. 2015).

3.2 Haasteita

Samoin kuin IoT-laitteet yleensä, puettavat laitteet ovat usein varustettu laskentateholtaan pienitehoisella prosessorilla, jonka takia monimutkaisten turvallisuusmekanismien ja salausalgoritmien toteuttaminen laitteessa on vaikeata (Ching ja Singh 2016). IoT-laitteissa on käytettävissä vähän virtaa, vähän muistia ja vähän laskentatehoa, joten myös tietoturvan toteuttamiseen on löydettävä kevyempiä ratkaisuja (Alaba ym. 2017). Vaikka laitteiden valmistajat ovat tietoisia tietoturvaan ja käyttäjän yksityisyyteen liittyvistä haasteista, kiire laitteiden

tuomisessa markkinoille ja halu säästää kustannuksissa laitteiden kehittämisprossissa vaikuttavat niiden toteuttamiseen (Arias ym. 2015). Laitteissa ei yksikertaisesta rakenteesta johtuen ole näppäimistä, tai monesti edes kosketusnäyttöä, jotta laitteisiin voidaan toteuttaa kunnollinen laitteen lukitseminen tai käyttäjän autentikointimenetelmä (Ching ja Singh 2016). Laitteisiin ei usein voi syöttää käyttäjän tunnistamista varten PIN-koodia ja laitteet säilyttävät tiedot salamattomana (Ching ja Singh 2016). Tämä voi vaarantaa käyttäjän yksityisen tiedon esimerkiksi laitteen varastamisen tai katoamisen yhteydessä.

Hilts, Parsons ja Knockel (2016) toteavat raportissaan, että puettavien laitteiden käyttäjät ovat usein huolissaan valtavasta datan määrästä, jota puettavien laitteiden valmistajat keräävät. Käyttäjille on usein epäselvää, kuinka päästä käsiksi kaikkeen heistä kerättyyn tietoon, kuinka tietoa käsitellään ja tallennetaan sekä kuinka sitä jaetaan ulkopuolisille tahoille. Myös kolmannet osapuolet ovat enenevissä määrin kiinnostuneita siitä, miten käyttäjien aktiivisuusdataa voitaisiin hyödyntää muissa käyttötarkoituksissa (Hilts, Parsons ja Knockel 2016). Laitevalmistajien intresseissä usein onkin kerätä mahdollisiman paljon käyttäjädataa, josta voi myös aiheutua haasteita käyttäjän yksityisyydelle.

4 Tietoturvauhat

Tässä luvussa käydään läpi tieturvan yleinen määritelmä sekä käsitellään erilaisia lähdekirjallisuudesta löytyneitä hyökkäystapoja, joille puettava teknologia on haavoittuvaa.

4.1 Määritelmä

Tietoturvalla tarkoitetaan, että pidetään huolta tiedon luottamuksellisuudesta (*confidentiality*), eheydestä (*integrity*) ja saatavuudesta (*availability*). Seneviratnen ym. (2017) mukaan sama yleinen tietoturvan lajittelu kolmeen kategoriaan pätee myös puettavien laitteiden osalta. Uhat tiedon luottamuksellisuuteen liittyvät tilanteisiin, jossa hyökkääjä saa luvattoman pääsyn tietoon esimerkiksi salakuuntelemalla langatonta viestintää. Uhat tiedon eheyteen koskevat tilanteita, joissa hyökkääjä pääsee muuttamaan esimerkiksi laitteen ohjelmistoa tai resursseja luvattomasti. Uhat tiedon saatavuuteen liittyvät tilanteisiin, joissa hyökkääjä esimerkiksi pyrkii estämään palvelujen käyttämisen (Seneviratne ym. 2017).

4.2 Hyökkäystapoja

Puettavien laitteiden tiedonvälityksen arkkitehtuurista (Kuvio 2) johtuen, puettavien laitteiden hyökkäyspinta-ala on laaja (Ching ja Singh 2016). Mahdollisia hyökkäyskohtia ovat itse puettava laite, yhdyskäytävänä toimiva älypuhelin, pilvipalvelu sekä eri kommunikaatiokanavat näiden välillä.

Tässä alaluvussa käydään läpi joitain kirjallisuudesta löytyneitä tyypillisiä puettavaa teknologiaa koskevia hyökkäystapoja. Eri hyökkäystavoista käytetään pääasiassa niiden englanninkielisiä nimityksiä, mutta myös vakiintunut suomenkielinen termi ilmaistaan, jos sellainen on olemassa.

4.2.1 Eavesdropping/sniffing/MITM attack

Erilaiset puettavaan teknologiaan liittyvät hyökkäystavat, jotka pohjautuvat salakuunteluun (*eavesdropping*), nuuskimiseen (*sniffing*) tai mies välissä hyökkäykseen (*man-in-the-middle*)

perustuvat laitteiden välisen BLE liikenteen kaappaamiseen, analysoimiseen tai uudelleenohjaamiseen. Laitteiden välisen BLE-liikenteen kaappaamiseen on saatavilla useita erilaisia työkaluja, kuten *Ubertooth One*, *Adafruit sniffer* ja *HCI snoop log* (Yaqoob, Abbas ja Atiquzzaman 2019).

BLE-protokolla tarjoaa mahdollisuuksia käyttää eritasoisia tietoturvaominaisuuksia. Laitteiden pariutumiseen on käytettävissä kolme eri menetelmää – *just works*, *numeric comparison* ja *passkey entry* (Lotfy ja Hale 2016). Näistä ensimmäinen, *just works*, nimensä mukaisesti vain toimii ja laitteiden pariutumiseen ei tarvita käyttäjän syötettä, joten sitä tyypillisesti käytetäänkin laitteissa, joissa ei ole näyttöä tai näkyvää käyttöliittymää. Toinen, *numeric comparison*, tarvitsee laitteeseen käyttöliittymän, jossa käyttäjälle esitetään jokin tunnusluku, jota verrataan pariutuvien laitteiden välillä. Kolmas menetelmä, *passkey entry*, tarjoaa näistä vahvimman tunnistautumisen, mutta se vaatii laitteelta myös käyttöliittymän, jossa käyttäjä voi itse syöttää jonkin tunnusluvun (Lotfy ja Hale 2016). Laitteiden MAC-osoitteiden määrittämiseen on myös käytössä kolme eri tapaa – staattinen osoite, ei selvitettävä yksityinen osoite ja selvitettävä yksityinen osoite (Das ym. 2016). Staattinen osoite on pysyvä ja se ei muutu pariutumiskertojen välillä, joten se tarjoaa näistä heikoimman yksityisyyden. Ei selvitettävä yksityinen osoite luo laitteelle täysin satunnaisen uuden MAC-osoitteen aika ajoin. Selvitettävä yksityinen osoite taas hyödyntää MAC-osoitteiden luomisessa erityistä avainta identiteetin selvittämiseen (*identity resolving key*), mikä on jo aikaisemmin pariutuneiden laitteiden tiedossa ja minkä avulla ne voivat tunnistaa laitteen vaihtuvasta ja näennäisesti satunnaisesta MAC-osoitteesta huolimatta (Das ym. 2016).

Lotfy ja Hale (2016) tutkivat kolmea markkinoilta löytyvää aktiivisuusrannekkeita, jotka kukin käyttävät eri menetelmiä laitteiden pariutumisessa. BLE-liikenteen paketteja kaapattiin *Ubertooth One* -laitteistolla laitteiden pariutumisen aikana. Laitteiden pariutumisessa tapahtuva kättely saatiin kaapattua kaikissa kolmessa tapauksessa (Lotfy ja Hale 2016). Laitteiden pariutumisen aikana muun muassa vaihdetaan avaimet, joita käytetään jatkossa liikenteen salaamiseen. Tämän osalta vahvemman tunnistautumistavan käyttäminen laitteiden pariutumisessa ei tuo lisää turvallisuutta, sillä liikenne on kaapattavissa kaikkia kolmea menetelmää käytettäessä. Ryan (2013) on tutkinut BLE-protokollan tarjoaman salauksen kiertämistä. Kättelyssä vaihdettavan tilapäisen avaimen arvaaminen väsytyshyökkäyksellä (*brute-force*)

onnistuu nykyisillä tietokoneille alle sekunnissa, jos käytössä on *just works* tai numeerinen tunnusluku (Ryan 2013). Tilapäistä avainta käytetään muodostamaan lyhytaikainen avain, jota edelleen käytetään luomaan pitkäaikainen avain, jolla lopulta salataan laitteiden välinen liikenne. Myös näiden avaimien muodostaminen onnistuu, ja laitteiden välinen tietoliikenteen salaus saadaan purettua, jos kättelyn aikana vaihdettu tilapäinen avain saadaan murrettua (Ryan 2013). Bluetooth-standardin mukaiset laitteiden pariutumismenetelmät eivät täten pysty täysin estämään liikenteen seuraamiseen perustuvia hyökkäyksiä (Lotfy ja Hale 2016). Salauksen osalta numeerisen tunnusluvun käyttäminen on kuitenkin turvallisempi kuin *just works* -menetelmä, koska niiden käyttämä tilapäinen avain on vaikeammin murrettavissa (Ryan 2013). Liikenteen salauksen purkaminen on kuitenkin erittäin vaikeata, jos paketteja ei ole kaapattu laitteiden pariutumisen aikana, jolloin salauksessa käytetyt avaimet vaihdetaan (Das ym. 2016).

Dasin ym. (2016) tutkimuksessa kaapattiin kuuden kaupallisesti suositun aktiivisuusrannekkeen BLE-liikennettä kontrolloidussa ympäristössä sekä kontrolloimatonta BLE-liikennettä aidossa kuntosaliympäristössä. Kuntosalilla kaapatusta liikenteestä pystyttiin erottamaan, että havaituista laitteista suurin osa (89%) ei käyttänyt satunnaistettua MAC-osoitetta (Das ym. 2016). Myös yksikään tutkituista kuudesta laitteesta ei satunnaistanut MAC-osoitettaan. Lisäksi laitteet tyypillisesti lähettävät jonkin selkokielisen laitetyyppiin yhdistettävän nimen, jota käytetään esimerkiksi laitteiden pariutumisen yhteydessä. Näiden tietojen perusteella yksittäinen laitteen käyttäjä pystytään yksilöimään ja tunnistamaan melko helposti, jos on myös nähtävillä kuka kantaa mitäkin laitetta (Das ym. 2016). Laitteen muuttumattoman MAC-osoitteen yhdistäminen tiettyyn henkilöön mahdollistaa laitteen käyttäjän seurannan. Das ym. (2016) tutkivat myös tarkemmin yksittäisen Fitbit-aktiivisuusrannekkeen lähettämää BLE-liikennettä. Vaikka BLE-pakettien sisältö olisikin salattua, niin pakettien koosta ja määrästä pystytään tekemään päätelmiä käyttäjän fyysisestä aktiivisuudesta (Das ym. 2016; Fafoutis ym. 2017). BLE-pakettien koko ja määrä korreloivat laitteen liikesensoreilta mitatun aktiivisuusdatan kanssa niin hyvin, että jopa yksittäisen käyttäjän tunnistaminen yksilöllisen kävelytyylin perusteella on mahdollista (Das ym. 2016).

4.2.2 Firmware modification attack

Firmware modification attack tarkoittaa hyökkäystä, jossa hyökkääjä pääsee tekemään muutoksia laitteen varusohjelmistoon (*firmware*) tai käyttöjärjestelmään. Tämä käytännössä mahdollistaa hyökkääjälle laitteen täydellisen haltuun ottamisen ja minkä tahansa ohjelmakoodin suorittamisen laitteessa (Shim ym. 2017). Mahdollisuus päivittää laitteen ohjelmisto on kuitenkin erittäin tärkeä ominaisuus nykyisissä laitteissa, jotta laitteen käyttäjäkokemusta voidaan parantaa myös myöhemmin (Yaqoob, Abbas ja Atiquzzaman 2019). Aktiivisuusrannekkeiden ohjelmisto päivitetään usein langattomasti yhdyskäytävänä toimivan älypuhelimen välityksellä (Shim ym. 2017). Rieck (2016), Arias ym. (2015) ja Shim ym. (2017) ovat tutkimuksissaan huomanneet, että aktiivisuusrannekkeiden varusohjelmiston korvaaminen hyökkääjän muokkaamalla versiolla onnistuu kuitenkin helposti, koska laitteet eivät tarkasta ohjelmistopaketin allekirjoitusta tai siihen käytetyt menetelmät ovat helposti kierrettävissä.

4.2.3 Side channel attack/mole attack

Side channel attack eli sivukanavahyökkäys on hyökkäystapa, jossa hyödynnetään jotain heikkoutta tietojärjestelmän toteutuksessa. Esimerkiksi älykellojen osalta mikä tahansa laitteeseen asennettu sovellus voi saada pääsyn laitteen kiihtyvyysanturin ja gyroskoopin mittaamaan dataan (Maiti ym. 2015). Älykellojen liikesensorien hyödyntämistä erilaiseen näppäinten painallusten ja kirjoituksen tunnistamiseen on tutkittu eri tavoin. Sekä Wang, Lai ja Roy Choudhury (2015) että Liu ym. (2015) ovat tutkineet älykellojen sensoreiden hyödyntämistä näppäimistöllä kirjoitettujen sanojen tunnistamiseen. Menetelmät perustuvat sensoridatan keräämiseen, mallintamiseen ja sanojen vertailuun (*word matching*) tietyn ennalta kootun opetusdatan pohjalta (Liu ym. 2015). Menetelmän tehokkuutta rajoittaa, että puettava laite on käytössä vain yhdessä kädessä, jonka seurauksena tiettyjen, enimmäkseen toisella kädellä näppäiltyjen, sanojen tunnistaminen vaikeutuu (Wang, Lai ja Roy Choudhury 2015). Mitä pidempi sana, sen suurempi todennäköisyys oikean sanan tunnistamiseen kuitenkin on (Wang, Lai ja Roy Choudhury 2015). Sekä Maiti ym. (2015) että Liu ym. (2015) käsittelivät tutkimuksissaan älykellojen liikesensoreiden käyttöä PIN-koodien kaappaamiseen numeronäppäimistöiltä, kuten matkapuhelimen lukitusnäytöltä tai maksupäätteeltä. Molemmat tutkimukset totesivat menetelmän tehokkaaksi ja todennäköisyys oikean PIN-koodi sel-

vittämiseen on hyvä (Maiti ym. 2015; Liu ym. 2015). Jiang (2019) tutki älykellon liikesensoreiden käyttöä käsinkirjoitetun tekstin tunnistamiseen ja myös tässä tutkimuksessa todettiin liikesensoreiden datan olevan riittävän tarkkaa sanojen tunnistamiseen. Hyökkäystapojen toimivuutta vähentää se, että ranteessa pidettävää puettavaa laitetta yleensä kannetaan ei-dominoivassa kädessä ja kirjoittaminen tapahtuu kuitenkin dominoivalla kädellä (Liu ym. 2015; Jiang 2019).

4.2.4 User account injection attack

User account injection attackilla tarkoitetaan hyökkäystapaa, jossa pyritään syöttämään väärennettyä dataa käyttäjätilille. Fereidooni ym. (2017) tutkivat 17:ää markkinoilla olevaa aktiivisuusranneketta, jotka välittävät käyttäjän aktiivisuusdataa laitteen valmistajan pilvipalveluun tai tallentavat tiedot paikallisesti käyttäjän matkapuhelimeen. Tutkimuksessa suoritettiin mies välissä hyökkäys matkapuhelimeen asennettavan kumppanisovelluksen ja valmistajan pilvipalvelun välillä. Kaikki tutkitut aktiivisuusrannekkeet, jotka välittävät tietoja valmistajan palvelimelle, olivat haavoittuvia tämän kaltaiselle hyökkäykselle ja väärennettyjen aktiivisuustietojen syöttäminen valmistajan palvelimelle oli mahdollista (Fereidooni ym. 2017). Aktiivisuusrannekkeet, jotka tallensivat tiedot paikallisesti, eivät käyttäneet salausta, joten myös tämän tiedon turvallisuus on mahdollisesti vaarantunut (Fereidooni ym. 2017).

Laitevalmistajan pilvipalvelu voi olla haavoittuva myös muunlaisille hyökkäystavoille. Lee ym. (2016) huomasivat tutkimuksessaan, että valmistajan pilvipalvelusta löytyi haavoittuvuuksia, joita vastaan voisi hyökätä käyttämällä SQL-injektiota ja tämän seurauksena saada verkkopalvelu vuotamaan tietoja tietokannan rakenteesta tai jopa muiden käyttäjien terveystiedoista.

4.2.5 Mule attack

Mule attackilla tarkoitetaan hyökkäystä, jossa pyritään väärentämään laitteen mittaamaa dataa asettamalla laite jonkin ”muulin” kyytiin. Tämä voi tapahtua esimerkiksi kiinnittämällä laite auton tai polkupyörän renkaaseen tai kiinnittämällä laite naruun, jonka päässä sitä pyö-

ritetään (Rahman, Carbunar ja Banik 2013). Tällä tavoin laite saadaan huijattua tulkitsemaan sensoreiden havaitsema liike esimerkiksi askeleiksi tai muuksi fyysiseksi aktiivisuudeksi.

Väärennetyn käyttäjädatan syöttämisen motiivina *user account injection* -hyökkäyksen tai *mule attackin* keinoin voi olla esimerkiksi taloudellinen hyöty lahjakorttien ja rahapalkintojen muodossa, joita jotkin palvelut antavat aktiivisille käyttäjille tai kun jokin aktiivisuustavoite on saavutettu (Rahman, Carbunar ja Banik 2013). Aktiivisuusrannekkeiden mittaamaa dataa on käytetty Yhdysvalloissa rikostutkinnan apuna ja jotkin vakuutusyhtiöt tarjoavat alennuksia fyysisesti aktiivisille ja terveellisiä elintapoja noudattaville asiakkailleen, jotka suostuvat jakamaan aktiivisuusdatansa vakuutusyhtiön kanssa (Fereidooni ym. 2017). Myös nämä voivat toimia mahdollisena motiivina syöttää virheellistä aktiivisuusdataa palveluihin.

5 Tietoturvauhkien ehkäisy

Tässä luvussa käsitellään mitä toimenpiteitä laitteiden valmistajien ja käyttäjien pitäisi tehdä, jotta edellisessä luvussa esitetyt tietoturvauhat ja hyökkäystavat voidaan estää. Lisäksi tarkastellaan mitä rajoituksia lainsäädäntö ja tietosuoja-asetukset asettavat tiedon käsittelylle, jotta käyttäjän yksityisen tiedon vaarantuminen voidaan ehkäistä.

5.1 Laitevalmistaja

Tyypillisesti kommunikaation turvallisuuteen liittyvät ongelmat johtuvat protokollien puutteellisesta käyttöönotosta, kuten esimerkiksi BLE-protokollan tarjoamaa MAC-osoitteen satunnaistamista ei ole otettu käyttöön, salauksen puuttumisesta ja puutteellisesta käyttäjän autentikoinnista (Seneviratne, 2017). Nämä ongelmat myös osittain linkittyvät yhteen, sillä puutteellisista käyttäjän autentikointimenetelmistä johtuen ei myöskään voida ottaa käyttöön BLE-protokollan turvallisempia laitteiden pariutumismenetelmiä, jotka vaativat PIN-koodin esittämisen tai syöttämisen laitteessa.

BLE-protokollaan liittyviä haavoittuvuuksia vastaan suojautuminen on haastavaa, koska liikenne on kaapattavissa avoimilla radiotaajuuksilla, mikä mahdollistaa muun muassa liikenteen salakuunteluun ja nuuskimiseen pohjautuvat hyökkäykset. Laitteissa tulisi kuitenkin ottaa käyttöön BLE-protokollan tarjoamat vahvemmat tietoturvaominaisuudet, kuten tunnuslukuun pohjautuva laitteiden pariutuminen ja satunnaistettu laitteen MAC-osoite. Yaqoob, Abbas ja Atiquzzaman (2019) suosittelee *passkey entry* menetelmän käyttämistä laitteiden pariutumisessa, koska se on turvallisempi kuin kaksi muuta menetelmää. Laitteen valmistajan on myös mahdollista toteuttaa BLE-standardista poikkeava tapa liikenteen salauksessa käytettävien avaimien vaihtamiseen (Lotfy ja Hale 2016). Liikenteen salauksessa käytettävien avaimien vaihtaminen myös muutoin kuin ilmateitse (*out-of-band*), esimerkiksi käyttämällä jotain langallista menetelmää laitteen käyttöönoton tai latauksen yhteydessä, voisi olla mahdollista (Seneviratne ym. 2017). Käyttäjän seuraamisen estämiseksi laitteissa tulisi käyttää satunnaisia MAC-osoitteita (Das ym. 2016).

Firmware modification attackin estämiseksi on olennaista, että laite tarkastaa päivitettävän

ohjelmiston aitouden (Rieck 2016; Shim ym. 2017). Pelkkä päivityksen eheyden varmistaminen esimerkiksi tarkastussumman avulla ei riitä, koska hyökkääjä voi muuttaa myös tarkastussumman alkuperäisen ohjelmiston muokkaamisen jälkeen (Rieck 2016). Ohjelmiston allekirjoittaminen voitaisiin toteuttaa esimerkiksi käyttämällä julkisen avaimen epäsymmetristä kryptografiaa, mutta puettavien laitteiden rajallinen käytettävissä oleva laskentateho ja virta rajoittavat tämän toteuttamista (Rieck 2016). Sekä Arias ym. (2015) että Do, Martini ja Choo (2017) ehdottavat myös virheen etsintään (*debugging*) käytettyjen fyysisten porttien poistamista tuotantolaitteista, koska niiden välityksellä voidaan saada hyödyllistä tietoa laitteen ohjelmiston toiminnasta, mikä edelleen auttaa hyökkääjää muokatun ohjelmistoversion toteuttamisessa.

Side channel attackin estämiseksi Liu ym. (2015) ehdottavat, että laitteisiin pitäisi toteuttaa erillinen turvallisen toiminnan tila, jossa käyttäjälle annetaan mahdollisuus tilapäisesti kytkeä pois päältä kaikki laitteen sensorit.

User account injection attackin estämiseksi välitettävä tieto pitäisi olla suojattua, kun sitä siirretään. Tämän osalta Fereidoonin ym. (2017) mukaan puettavien laitteiden turvallisuuden vahvuutta lisääviä tekijöitä ovat muun muassa päästä päähän salauksen (*end-to-end encryption*) käyttäminen, paikallisten tietokantojen salaaminen, siirrettävän tiedon suojaaminen käyttämällä salattua HTTPS-protokollaa, tiedon koodaaminen omien sovelluskohtaisten (*proprietary*) menetelmien avulla sekä tiedon eheyden tarkastaminen. Lee ym. (2016) ehdottaa, että laitteisiin asennettavien kumppanisovellusten rakennetta pitäisi tarkoituksenmukaisesti piilottaa (*obfuscation*), jotta niiden toiminnan takaisinmallintaminen (*reverse engineering*) olisi mahdollisimman hankalaa. Tutkimalla kumppanisovelluksen toimintaa, hyökkääjä voi selvittää mitä tietoja sovellus lähettää, missä muodossa ja mihin osoitteeseen, ja näin saada myös selville tietoja valmistajan pilvipalvelimen toiminnasta.

Mule attackia vastaan Liu ja Sun (2016) ehdottavat, että valmistajien tulisi toteuttaa laitteisiin parempia liikkeen malleja tunnistavia algoritmeja, joiden avulla epäilyttävä data voidaan suodattaa.

5.2 Käyttäjä

Kuluttajalaitevalmistaja HP (2015) esittää älykellojen turvallisuutta koskevassa raportissaan erinäisiä toimia laitteiden käyttäjille. Olisi suositeltavaa kytkeä kaikki laitteen tarjoamat turvallisuusominaisuudet päälle, kuten salasana, lukitusnäyttö, kaksivaiheinen tunnistautuminen ja laitteen tietojen salaus. Laitteiden toimintoja, jotka avaavat pääsyn esimerkiksi käyttäjän taloon tai autoon tai mahdollistavat maksujen suorittamisen, ei tulisi käyttää jos ne eivät tarjoa mahdollisuutta käyttää vahvaa käyttäjän tunnistautumista. Laitteiden käyttäjän tulisi myös evätä tuntemattomien laitteiden Bluetooth-pariutumispyynnöt (HP 2015). Yksinkertaisimmat aktiivisuusrannekkeet eivät kuitenkaan tarjoa käyttäjälle mitään mahdollisuuksia kytkeä päälle edistyneempiä tietoturvaominaisuuksia.

Side channel attackin ehkäisemiseksi käyttäjän kannattaa pitää älykelloja ja aktiivisuusrannekkeita ei-dominoivassa kädessä, koska se vaikeuttaa kirjoitetun tekstin ja syötettyjen PIN-koodien tunnistamista laitteen sensoreilla havaitseman liikkeen perusteella (Liu ym. 2015; Jiang 2019). Joissain tapauksissa myös laitteen käyttäjä voi olla hyökkääjä, kuten esimerkki *mule attackin* käytöstä aktiivisuusdatan väärentämisessä osoittaa.

5.3 Sääntely

Paikallinen lainsäädäntö ja tietosuoja-asetukset voivat määritellä, miten laitteiden valmistajien tulee tallentaa ja käsitellä käyttäjää koskevaa tietoa. Maailmanlaajuisesti sääntelyyn liittyy paljon epävarmuutta, mutta Yhdysvalloista ja Euroopan unionissa on aktiivisesti pyritty parantamaan terveystietojen tallentamiseen liittyvää lainsäädäntöä (Steinhubl, Muse ja Topol 2015). Yhdysvalloissa HIPAA (*Health Insurance Portability and Accountability Act*) tarjoaa suojan yksityisyydelle määrittelemällä, kuinka terveystietoihin liittyvää tietoa tulisi käsitellä ja tallentaa. Tämä lainsäädäntö ei kuitenkaan kata kuluttajakäytössä olevien älykellojen ja aktiivisuusrannekkeiden keräämää dataa, koska tietoja keräävä taho ei ole terveydenhoitoalan toimija (Paul ja Irvine 2014). Euroopan unionissa EDPS (*European Data Protection Supervisor*) taas on ottanut kannan, että yksilön terveyttä ja hyvinvointia mittaava data on yksityistä ja sitä käsittelevien yritysten on kiinnitettävä erityistä huomiota tiedon tietoturvalliseen käsittelyyn (Hilts, Parsons ja Knockel 2016). Lisäksi EU:ssa 2018 käyttöönotettu

yleinen tietosuoja-asetus GDPR (*General Data Protection Regulation*) määrittää, että EU-kansalaisten henkilökohtainen data tulee säilyttää EU:n alueella ja se antaa kuluttajalle mahdollisuuden tarkastaa itsestään kerätyt tiedot sekä saada tiedon siitä kuinka niitä on kerätty, käsitelty ja luovutettu muille osapuolille.

Laitteen käyttöönoton yhteydessä hyväksyttävät käyttöehdot kuitenkin osaltaan määrittävät, miten laitteen valmistalla on mahdollisuuksia hyödyntää kerättyä tietoa ja jakaa sitä kolmansille osapuolille. Paulin ja Irvinen (2014) tutkimista käyttöehdoista on löytynyt kohtia, joissa muun muassa sallitaan laitevalmistajan käyttää ja kaupallisesti hyödyntää kaikkea tekstiä, kuvia ja muuta dataa – mukaan lukien käyttäjän aktiivisuusdatan, jota palveluun lähetetään. Yhdysvalloissa FTC (*Federal Trade Commission*) testasi 12 terveys- ja hyvinvointisovellusta ja ne jakoivat tietoja käyttäjästä 76:lle kolmannen osapuolen yritykselle (Steinhubl, Muse ja Topol 2015).

6 Yhteenveto

Puettavat IoT-laitteet ovat usein pienikokoisia, vähävirtaisia, pienitehoisia, vähämuistisia, toiminnoiltaan yksinkertaisia sekä edullisia, mikä aiheuttaa haasteita tietoturvan toteuttamiselle laitteissa. Lisäksi niiden tietoturvaan ei kiinnitetä samalla tavalla huomiota, kuin muuhun tietotekniikkaan. Puettavien laitteiden kategoria on vielä varsin uusi ja laitteet kasvattavat edelleen suosiotaan, joten laitevalmistajat kiirehtivät uusia tuotteita markkinoille. IoT-laitteita yleisesti koskevat haasteet tietoturvallisessa tiedonvälityksessä verkkoon koskevat myös puettavia laitteita. Lisäksi kerätyn tiedon luonne on sellaista, että se aiheuttaa haasteita käyttäjän yksityisyydelle.

Puettaviin laitteisiin kohdistuvia erilaisia hyökkäystapoja löytyy lähdekirjallisuudesta runsain määrin. Hyökkäystavat ovat kuitenkin tyypillisesti varsin teoreettisia, teknisiä ja vaativat hyökkääjältä paljon tietoa yksittäisen laitemallin toiminnasta. Yhdessä laitteessa toimiva hyökkäystapa ei välttämättä toimikaan samalla tavalla seuraavassa laitteessa, mikä tekee näistä hyökkäystavoista vähemmän yleisesti hyödynnettäviä.

Laitteiden tietynlaisesta yksinkertaisesta luonteesta johtuen tarjotut ratkaisut löydettyihin tietoturvaongelmiin ovat sellaisia, että niiden toteuttaminen jää suurimmaksi osaksi laitevalmistajien vastuulle. Käyttäjällä ei ole tällä hetkellä juurikaan mahdollisuutta itse vaikuttaa puettavan teknologian tietoturvaan. Käyttäjän ainoaksi vaihtoehdoiksi voikin jäädä olla käyttämättä joitain laitteen toiminnallisuuksia, kuten sykemittausta, paikannusta tai ilmoituksia viesteistä, jos laitteen tietoturva ja tiedon yksityisyyttä kunnioittava käsittely näiltä osin huolettaa.

Nykyisissä tutkimuksissa löydetyt tietoturvaongelmat tulevat kuitenkin todennäköisesti korjaantumaan teknologian kehittyessä ja seuraavien laitesukupolvien tullessa markkinoille. Laitteiden kasvava laskentateho mahdollistaa tehokkaampien salausalgoritmien käyttämisen laitteissa. Myös laitteiden rakenne kehittyy tukemaan lisääntyviä ominaisuuksia. Esimerkiksi suurempikokoisten kosketusnäyttöjen yleistyminen laitteissa mahdollistaa parempia menetelmiä käyttäjän autentikointiin. Puettavien laitteiden kasvava suosio tekee tutkimusaiheesta joka tapauksessa mielenkiintoisen ja ajankohtaisen. Mahdollisena jatkotutkimuskohteena

voisi esimerkiksi olla, ovatko tässä tutkimuksessa löydetyt hyökkäystavat edelleen hyödynnettävissä uusimmissa, tällä hetkellä markkinoilla olevissa, älykelloissa ja aktiivisuusrannekkeissa tai löytyykö niistä uusia haavoittuvuuksia.

Lähteet

Alaba, Fadele Ayotunde, Mazliza Othman, Ibrahim Abaker Targio Hashem ja Faiz Alotaibi. 2017. “Internet of Things security: A survey”. *Journal of Network and Computer Applications* 88:10–28. ISSN: 1084-8045. doi:10.1016/j.jnca.2017.04.002.

Arias, O., J. Wurm, K. Hoang ja Y. Jin. 2015. “Privacy and Security in Internet of Things and Wearable Devices”. *IEEE Transactions on Multi-Scale Computing Systems* 1, numero 2 (huhtikuu): 99–109. ISSN: 2372-207X. doi:10.1109/TMSCS.2015.2498605.

Baker, S. B., W. Xiang ja I. Atkinson. 2017. “Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities”. *IEEE Access* 5:26521–26544. ISSN: 2169-3536. doi:10.1109/ACCESS.2017.2775180.

Ching, Ke Wan, ja Manmeet Mahinderjit Singh. 2016. “Wearable technology devices security and privacy vulnerability analysis”. *International Journal of Network Security & Its Applications* 8 (3): 19–30.

Das, Aveek K., Parth H. Pathak, Chen-Nee Chuah ja Prasant Mohapatra. 2016. “Uncovering Privacy Leakage in BLE Network Traffic of Wearable Fitness Trackers”. Teoksessa *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications,* 99–104. HotMobile ’16. St. Augustine, Florida, USA: Association for Computing Machinery. ISBN: 9781450341455. doi:10.1145/2873587.2873594.

Do, Quang, Ben Martini ja Kim-Kwang Raymond Choo. 2017. “Is the data on your wearable device secure? An Android Wear smartwatch case study”. *Software: Practice and Experience* 47 (3): 391–403. doi:10.1002/spe.2414.

Fafoutis, X., L. Marchegiani, G. Z. Papadopoulos, R. Piechocki, T. Tryfonas ja G. Oikonomou. 2017. “Privacy Leakage of Physical Activity Levels in Wireless Embedded Wearable Systems”. *IEEE Signal Processing Letters* 24, numero 2 (helmikuu): 136–140. ISSN: 1558-2361. doi:10.1109/LSP.2016.2642300.

Fereidooni, H., T. Frassetto, M. Miettinen, A. Sadeghi ja M. Conti. 2017. “Fitness Trackers: Fit for Health but Unfit for Security and Privacy”. Teoksessa *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE),* 19–24. Heinäkuu. doi:10.1109/CHASE.2017.54.

Gartner. 2018. “Gartner Says Worldwide Wearable Device Sales to Grow 26 Percent in 2019”. Viitattu 4. maaliskuuta 2020. https://www.gartner.com/en/newsroom/press-releases/2018-11-29-gartner-says-worldwide-wearable-device-sales-to-grow-.

———. 2019. “Gartner Says Global End-User Spending on Wearable Devices to Total $52 Billion in 2020”. Viitattu 4. maaliskuuta 2020. https://www.gartner.com/en/newsroom/press-releases/2019-10-30-gartner-says-global-end-user-spending-on-wearable-dev.

Hilts, Andrew, Christopher Parsons ja Jeffrey Knockel. 2016. “Every step you fake: A comparative analysis of fitness tracker privacy and security”. *Open Effect Report* 76 (24): 31–33. https://openeffect.ca/reports/Every_Step_You_Fake.pdf.

HP. 2015. *Internet of things security study: Smartwatches.* https://www.ftc.gov/system/files/documents/public_comments/2015/10/00050-98093.pdf.

IDC. 2019a. “Worldwide Wearables Market to Top 300 Million Units in 2019 and Nearly 500 Million Units in 2023, Says IDC”. Viitattu 8. maaliskuuta 2020. https://www.idc.com/getdoc.jsp?containerId=prUS45737919.

———. 2019b. “Worldwide Wearables Shipments Surge 94.6% in 3Q 2019 Led by Expanding Hearables Market, Says IDC”. Viitattu 8. maaliskuuta 2020. https://www.idc.com/getdoc.jsp?containerId=prUS45712619.

Jiang, Hao. 2019. “Motion Eavesdropper: Smartwatch-Based Handwriting Recognition Using Deep Learning”. Teoksessa *2019 International Conference on Multimodal Interaction,* 145–153. ICMI ’19. Suzhou, China: Association for Computing Machinery. ISBN: 9781450368605. doi:10.1145/3340555.3353740.

Lee, M., K. Lee, J. Shim, S. Cho ja J. Choi. 2016. “Security threat on wearable services: Empirical study using a commercial smartband”. Teoksessa *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia),* 1–5. Lokakuu. doi:10.1109/ICCE-Asia.2016.7804766.

Liew, Chee Sun, Teh Ying Wah, Junaid Shuja, Babak Daghighi ym. 2015. “Mining personal data using smartphones and wearable devices: A survey”. *Sensors* 15 (2): 4430–4469. doi:10.3390/s150204430.

Liu, J., ja W. Sun. 2016. “Smart Attacks against Intelligent Wearables in People-Centric Internet of Things”. *IEEE Communications Magazine* 54, numero 12 (joulukuu): 44–49. ISSN: 1558-1896. doi:10.1109/MCOM.2016.1600553CM.

Liu, Xiangyu, Zhe Zhou, Wenrui Diao, Zhou Li ja Kehuan Zhang. 2015. “When Good Becomes Evil: Keystroke Inference with Smartwatch”. Teoksessa *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security,* 1273–1285. CCS ’15. Denver, Colorado, USA: Association for Computing Machinery. ISBN: 9781450338325. doi:10.1145/2810103.2813668.

Lotfy, K., ja M. L. Hale. 2016. “Assessing Pairing and Data Exchange Mechanism Security in the Wearable Internet of Things”. Teoksessa *2016 IEEE International Conference on Mobile Services (MS),* 25–32. Kesäkuu. doi:10.1109/MobServ.2016.15.

Maiti, Anindya, Murtuza Jadliwala, Jibo He ja Igor Bilogrevic. 2015. “(Smart)Watch Your Taps: Side-Channel Keystroke Inference Attacks Using Smartwatches”. Teoksessa *Proceedings of the 2015 ACM International Symposium on Wearable Computers,* 27–30. ISWC ’15. Osaka, Japan: Association for Computing Machinery. ISBN: 9781450335782. doi:10.1145/2802083.2808397.

Paul, Greig, ja James Irvine. 2014. “Privacy Implications of Wearable Health Devices”. Teoksessa *Proceedings of the 7th International Conference on Security of Information and Networks,* 117–121. SIN ’14. Glasgow, Scotland, UK: Association for Computing Machinery. ISBN: 9781450330336. doi:10.1145/2659651.2659683.

Rahman, Mahmudur, Bogdan Carbunar ja Madhusudan Banik. 2013. “Fit and vulnerable: Attacks and defenses for a health monitoring device”. arXiv: 1304.5672.

Rieck, Jakob. 2016. “Attacks on fitness trackers revisited: A case-study of unfit firmware security”. arXiv: 1604.03313.

Ryan, Mike. 2013. “Bluetooth: With low energy comes low security”. Teoksessa *7th {USENIX} Workshop on Offensive Technologies*. https://www.usenix.org/conference/woot13/workshop-program/presentation/ryan.

Seneviratne, S., Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna, M. Hassan ja A. Seneviratne. 2017. “A Survey of Wearable Devices and Challenges”. *IEEE Communications Surveys Tutorials* 19 (4): 2573–2620. ISSN: 2373-745X. doi:10.1109/COMST.2017.2731979.

Shim, Jaewoo, KH Lim JM Jung, SJ Cho, MK Park ja SC Han. 2017. “A case study on vulnerability analysis and firmware modification attack for a wearable fitness tracker”. *IT Converg. Pract.* 5 (4): 25–33.

Steinhubl, Steven R., Evan D. Muse ja Eric J. Topol. 2015. “The emerging field of mobile health”. *Science Translational Medicine* 7 (283): 283rv3–283rv3. ISSN: 1946-6234. doi:10.1126/scitranslmed.aaa3487.

Wang, He, Ted Tsung-Te Lai ja Romit Roy Choudhury. 2015. “MoLe: Motion Leaks through Smartwatch Sensors”. Teoksessa *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking,* 155–166. MobiCom ’15. Paris, France: Association for Computing Machinery. ISBN: 9781450336192. doi:10.1145/2789168.2790121.

Yaqoob, T., H. Abbas ja M. Atiquzzaman. 2019. “Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review”. *IEEE Communications Surveys Tutorials* 21 (4): 3723–3768. ISSN: 2373-745X. doi:10.1109/COMST.2019.2914094.