Minttu Toropainen

VERKKOON KYTKETTYJEN IOT-LAITTEIDEN TIETO-TURVAONGELMAT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Toropainen, Minttu
Verkkoon kytkettyjen IoT-laitteiden tietoturvaongelmat
Jyväskylä: Jyväskylän yliopisto, 2021, 31 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Kokko, Tuomas

Esineiden internet eli IoT (Internet of Things) on kasvanut viime vuosina yhä laaja-alaisemmin eri aloilla. IoT-laitteita käytetään nykyisin niin terveydenhuollossa kuin älykaupungeissakin. Kuitenkin myös kotioloissa käytettävät IoT-laitteet ovat lisääntyneet merkittävästi. Verkkoihin kytketyt laitteet ovat tuoneet tavallisten käyttäjien ulottuville kehittyneitä, hyödyllisiä ja älykkäitä palveluita. Kuitenkin yksityisyydensuoja ja IoT-laitteiden haavoittuvuudet ovat nousseet pinnalle tehdyissä tutkimuksissa. Tässä tutkielmassa perehdyn tarkemmin tietoturvaongelmiin sekä siihen, kuinka näiltä ongelmilta tulisi suojautua. Tutkimuksen keskeinen osa-alue on tietoturvaongelmat eri ympäristöissä. Tällä tarkoitetaan IoT-laitteiden sovelluskerrosten arkkitehtuuria, teknisiä haasteita sekä muita yleisiä riskejä, joita laitteiden käyttöön liittyy.

Tietoturvaongelmat voivat aiheuttaa vakavia seurauksia käyttäjän yksityisyydensuojan rikkoutumiseen. Tämän vuoksi paneudun tässä tutkielmassa lisäksi siihen, millaisia suojaustapoja voidaan hyödyntää riskien välttämiseksi. Tutkielma on toteutettu kvalitatiivisena kirjallisuuskatsauksena ja sen tärkeimmät tukimuskysymykset ovat: ”*Millaisia tietoturvariskejä IoT-laitteet pitävät sisällään?*” ja ”*Miten näiltä riskeiltä tulisi suojautua?*”. Tutkiessani erilaisia tietoturvariskejä kävi ilmi, että riskit ovat hyvin monitasoisia. Osa riskeistä nivoutui selkeästi käyttäjän huolimattomuuteen tai välinpitämättömyyteen. Huomattava osa tunnistetuista tietoturvariskeistä ja -haavoittuvuuksista liittyi kuitenkin IoT-arkkitehtuurin eri kerroksissa esiintyviin ongelmiin. Näiden tunnistettujen riskien tietoturvahaasteet eivät kuitenkaan olleet ainoa ongelma. Laitteiden turvallisuuden takaamiseksi myös laitevalmistajien aktiivisella toiminnalla on suuri merkitys turvallisuuden parantamiseksi.

Tutkielman toisessa pääteemassa eli suojaamisen parantamisessa nousi esiin laitevalmistajien vastuu myydyistä IoT-laitteista. Tähän ei kuitenkaan yksistään kannata nojautua, vaan myös käyttäjien tavat ja osaaminen huolehtia laitteidensa suojaamisesta ja tietoturvasta on tärkeässä asemassa tietojen väärinkäyttämisen ehkäisyssä. Näiden kahden suojaamistavan yhdistämisellä on parhaat edellytykset laitteiden tietoturvalliseen käyttöön. Tämän tutkimuksen tuloksena on, että nykyisellään olevat IoT-laitteet vaativat parempaa suojaustasoa, vaikka resursseja tälle ei vielä ole. Jatkuvat teknologian muutokset tuovat lisähaasteita niin laitevalmistajille, käyttäjille kuin lainsäädännöllekin.

Asiasanat: Esineiden Internet, Tietoturvaongelmat, Sovellusarkkitehtuuri, Suojaaminen, Tietoturvatuotteet

ABSTRACT

Toropainen, Minttu
Security problems in network connected IoT devices
Jyväskylä: University of Jyväskylä, 2021, 31 pp.
Information Systems, Bachelor's thesis
Supervisor: Kokko, Tuomas

The Internet of Things (IoT) has grown more widely in various fields in recent years. IoT devices are currently used as in health care and smart cities. However, also IoT devices used at home have seen tremendous growth. Network connected devices have brought advanced, intelligent, and useful services to ordinary users. However, privacy concerns and vulnerabilities in IoT devices have stand out in previous studies. In this research, I will look more closely at security issues, and how to protect against these problems. A key area of this research is security problems in different environments. This covers the architecture of the application layers, technical challenges and other general challenges associated with the use of the IoT devices.

Security issues may cause serious consequences in violation of user privacy. Therefore, in this study I will also look what kind of options can be used to avoid those risks. The research has been implemented as a qualitative literature review and its main research questions are: *"What kind of security risks does IoT involve?"* and *"How to protect against those risks?"*. While I was researching different security risks, it turned out that the risks are a very wide variety. Some of the risks clearly linked to the negligence or indifference of the user. However, a significant part of the identified security risks and -vulnerabilities was related to issues with different layers of architecture. The security challenges identified by these were not the only problem. Also, to ensure the safety of devices, the active involvement of manufacturers is one of the most important things how to improve security.

The second main theme of the research, which is to improve protection, the responsibility for the devices sold by manufacturer stood out. This is not to be trusted alone, but users' habits and skills to protect and secure their own devices plays an important role in preventing the misuse of their data. Combining these two methods is the best way to use IoT devices securely. The result of this research is that current IoT devices require a better standard of security, although there are no resources for this. Ongoing technological changes bring additional challenges for device manufacturers, users, and legislation.

Keywords: Internet of Things, Security problems, Application architecture, Protection, Security products

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Esineiden internet muuttaa tapojamme työskennellä, matkustaa ja elää. IoT-laitteet tallentavat ja analysoivat jatkuvasti uutta tietoa. Toimiakseen hyvin laitteet tarvitsevat pääsyn kaikkeen tiedonsaantiin, mikä koituu yksityisyydensuojan kannalta haasteelliseksi. (Kohli, Cichy & Salge 2021.) Tässä tutkielmassa tulen käsittelemään sitä, mitä edellä mainituille ongelmille voitaisiin tehdä. Sekä yksityisyydensuojan turvaaminen että laitteiden fyysinen rakenne muodostuvat tärkeäksi aspektiksi turvallisemman IoT-tulevaisuuden kannalta. Aiheeni on yhteiskunnallisesti ajankohtainen ja merkittävä nopean IoT:n kasvun vuoksi. IoT-laitteisiin kohdistuvia hyökkäyksiä on tutkittu edelleen liian vähän yksityisyydensuojan näkökulmasta. Laitteet saattavat olla hyvin haavoittuvaisia, eikä kunnolliseen suojaukseen riitä aikaa. Tällä tutkimuksella pyrin selvittämään, millaiseen vaaraan laitteet saattavat käyttäjänsä asettaa.

Yksinkertaistettuna IoT (Internet of Things) eli esineiden internet kattaa kaikki sellaiset laitteet, jotka toimivat verkkoyhteyden avulla. Termiä on kuitenkin yksiselitteisesti vaikea määritellä, sillä se tarkoittaa mitä vain nykyautoista kodin turvajärjestelmiin. Esineiden internet on keskenään toisiinsa liittyvä tietokonejärjestelmä, jolla on kyky yhdistää ja siirtää tietoja verkon välityksellä ilman ihmiskontaktia. (Gilchrist 2017, 5.)

Esineiden internetin uskotaan olevan seuraava sukupolvi nykyiselle internetille. Miljardit laitteet ovat yhteydessä verkkoon, mikä altistaa IoT-laitteet tietoturvaongelmille. Laitteet pystyvät välittämään keskenään tietoa ilman ihmiskontaktia, mutta tietoturvainfrastruktuurin puute on tuonut ongelmia laitteiden nykyisellä käytöllä. (Li, Tryfonas & Li 2016, 337.)

Yhdistettyjen IoT-laitteiden määrä on kasvanut räjähdysmäisesti, ja niitä käytetään myös monella eri alalla. Niin kuin kaikissa nykyaikaisissa digitaalisissa järjestelmissä, ohjelmisto laitteiden takana on keskeinen osa arkkitehtuuria (Chi, Liu, Yao, Zhang & Zhu 2019, 205). Ohjelmistojen tekniikalla on tärkeä rooli IoT-järjestelmien kehittämisessä, käyttöönotossa, ylläpidossa ja suunnittelussa (Reggio, Leotta, Cerioli & Alkhabbas 2020, 2). Mikäli ohjelmisto on puutteellinen, voi se pahimmassa tapauksessa johtaa suuriin tietoturvaongelmiin laitetta käyttäessä.

IoT on tällä hetkellä murrosvaiheessa, jossa sen kehitys on hyvin nopeaa. Tulevaisuudessa IoT tulee olemaan täysin yhteiskuntaan integroitunut internet. Tämä tulee muuttamaan ihmisten työskentelyä, ajattelua ja arkipäiväistä elämää. Arkipäiväisessä käytössä olevat esineet tulevat liittymään toisiinsa, jolloin pystymme seuraamaan kaikkea milloin tahansa ja mistä tahansa verkon avulla. (Singh, Tripathi & Jara 2014, 288.) IoT-laitteet ovat kuitenkin teknisesti vielä keskeneräisiä, ja yksi suurimmista ongelmista on niiden tietoturvan puute. Tämä pitää sisällään laitteiden infrastruktuurin, verkon, sovellukset ja yleiset laitteiden tietoturvaongelmat. (Li, Xu, Romdhani 2017, 1–2.)

Jokainen verkkoon kytketty IoT-laite sisältää omat haavoittuvuutensa. Yksilön datan suojaaminen väärinkäytöksiltä on yksi suurista tietoturvaongelmista. Tietosuojariskit kasvavat samaan tahtiin kuin laitteiden monimutkaisuus lisää jo olemassa olevia haavoittuvuuksia. IoT-laitteet sisältävät runsaasti henkilökohtaisia tietoja, kuten syntymäpäiviä, kotiosoitteita ja muuta arkaluontoista informaatiota. Tämän vuoksi laitteiden riskit voivat aiheuttaa jopa identiteettivarkauksia. Laitteiden nykyistä arkkitehtuuria ei ole suunniteltu yhdessä juridisesti luotettavaksi, vaan tämä sisältää ainoastaan teknisen aspektin toiminnallisuudesta. (Li ym. 2016, 340.)

Tämä tutkielma toteutetaan kvalitatiivisen kirjallisuuskatsauksen muodossa. Tärkeimmät tutkimuskysymykseni olivat:

1. Millaisia tietoturvariskejä IoT-laitteet pitävät sisällään?
2. Miten näiltä riskeiltä tulisi suojautua?

Tämän tutkielman pohjana toimivat tieteelliset artikkelit. Suurin osa artikkeleista on kohtalaisen tuore itse aiheen ollessa suhteellisen uusi tutkimusalue. Tutkimuskirjallisuutta hakiessa on yleisimmin käytetty hakusanoja ”IoT”, ”Vulnerabilities on the IoT” ja ”Protection of IoT”. Tärkeimmiksi kirjallisuuden tietokannoiksi valikoitui Scopus, ACM Digital Library sekä IEEE Xplore. Kirjallisuuskatsausta tehtäessä kävi ilmi, että yleistä IoT-haavoittuvuutta ja IoT-arkkitehtuurin rakennetta koskevaa kirjallisuutta löytyi erittäin paljon. Kun taas suojausta koskevaa kirjallisuutta on julkaistu melko vähän. Tämä loi haasteen tutkimuksen tekemiselle suojauksen näkökulmasta. Tutkimukseni erona kuitenkin muihin vastaaviin tutkimuksiin on se, että keskityn myös uudenlaisiin suojausmekanismeihin, kuten tietoturvatuotteisiin.

Tutkielmassani heijastuu tietoturvaongelmien moninaisuus käyttäjän arkipäivän elämään. Huolenaiheeksi nousi, mitä kaikkea nykyiset IoT-laitteet keräävät yksityishenkilöistä ja mihin tätä tietoa käytetään. Tietoturvaongelmat ovat osa nykyaikaista elämäämme, eikä niiltä voi kokonaan välttyä. On kuitenkin tärkeä selvittää, kuinka suurilta osin näiltä ongelmilta pystytään suojautumaan jatkossa. IoT-laitteiden puutteellinen suojaus on haitaksi niin yksilölle kuin yhteiskunnallekin. Käytämme nykyisellään IoT-laitteita kotiympäristöstä työympäristöön, joten suojauksen on oltava riittävällä tasolla.

Tutkielma jakautuu neljään päälukuun, joista ensimmäisessä luvussa kerron yleisesti IoT-laitteista sekä niiden historiasta, jotta ymmärretään, millainen

merkitys IoT:llä on nykyisellään koko yhteiskunnalle. IoT:n nopea kasvu on tuonut meille monia erilaisia tapoja hyödyntää nykyteknologiaa yhä tehokkaammin. Tässä luvussa kerron lisäksi, mitä IoT-laite pitää rakenteellisesti sisällään. Tämä auttaa ymmärtämään myöhemmässä vaiheessa arkkitehtuurin haavoittuvuutta.

Toisessa luvussa vastaan ensimmäiseen tutkimuskysymykseen eri näkökulmien avulla. Tässä luvussa selviää arkkitehtuurin rakenteen erilaisten riskien laatu. Riskejä muodostuu myös käyttäjän itsensä aiheuttamana laitetta käytettäessä. Tutkimustuloksissa kerron miten fyysiset riskit vaikuttavat laitteen rakenteellisiin suojaustekijöihin. Paneudun myös siihen, kuinka käyttäjän tietoiset riskit sekä inhimilliset erheet vaikuttavat mahdollisiin tietoturvaongelmiin.

Kolmannessa luvussa paneudun toiseen tutkimuskysymykseen, eli miten tietoturvaongelmilta tulisi suojautua. Tässä luvussa kerron suojautumistapoja kolmesta eri näkökulmasta: käyttäjät, laitevalmistajat ja tietoturvatuotteita myyvät yritykset. Suurin vastuu on laitevalmistajalla, mutta käyttäjällä on myös monia keinoja tukea omaa yksityisyydensuojaansa. Tutkimuksessani käy ilmi, että olisi erittäin suotavaa, jos käyttäjä suojaisi omaa laitettaan asiaan kuuluvalla tavalla esimerkiksi, kaksivaiheisen todennuksen sekä vahvojen salasanojen turvin. Tämä ei kuitenkaan yksistään riitä, jos laitevalmistaja on jättänyt suuria tietoturva-aukkoja huomiotta. Kerron myös tietoturvayritysten myymistä tietoturvatuotteista apuna IoT-laitteiden yksityisyydensuojan ongelmiin. Nämä tuotteet ovat yleistyneet vasta viime vuosina, joten tutkimustietoa tästä aiheesta on hyvin vähän.

Viimeinen luku kokoaa tutkielman aiemmissa luvuissa löydetyt havainnot. Yhteenvedon tarkoitus on antaa lyhyt kuvaus siitä, mitä muissa pääluvuissa on käsitelty ja mitkä olivat keskeisimmät ongelmat, jotka nousivat esille. Kerron tärkeimmät keräämäni tulokset ja sen, millaisia johtopäätöksiä näistä voidaan tehdä. Lisäksi tässä luvussa kertaan tutkimuskysymykset ja niihin tutkimuksen pohjalta saadut vastaukset. Kerron myös siitä, millaisia tutkimusaiheita olisi vielä hyvä tutkia jatkossa ja mihin seikkoihin näissä voisi kiinnittää huomiota. Pohdin myös sitä, millaiset IoT:n tutkimusalan näkymät tulevaisuudessa saattaisivat olla.

2 ESINEIDEN INTERNET NYKYMUODOSSAAN

Tässä luvussa tarkastellaan IoT-laitteiden historiaa, arkkitehtuuria sekä laitteiden tuottamaa arvoa yhteiskunnalle. On tärkeää ymmärtää, millainen arkkitehtuurin rakenne on, jotta pystytään myöhemmässä tutkielman vaiheessa ymmärtämään tietoturvaongelmien fyysisten ulottuvuuksien näkökulmat. Jotta ymmärretään IoT-laitteiden kokonaiskuva, on myös tärkeä hahmottaa sen historiaa ja sitä, millaisia hyötyjä laitteista on tähän mennessä saatu. Näin pystytään punnitsemaan sitä, ovatko hyödyt yhtä painoarvoisia kuin tietoturvapuutosten aiheuttamat ongelmat.

2.1 IoT-laitteiden historia

IoT-laitteiden historia ulottuu 1980-luvulle asti, jolloin ARPANET kehittyi pakettikytkentäisestä verkosta internetiksi. Vuoteen 1985 mennessä internetistä kehittyi vakiintunut teknologia. (Leiner, Cerf, Clark, Kahn, Kleinrock 2009, 23–28.) Varhaisimpia IoT-laitteiden keksintöjä voidaan sanoa olevan vuonna 1982 ARPANET-verkkoon yhdistetty juoma-automaatti. Ensimmäinen oikea IoT-laite kehitettiin kuitenkin vasta vuonna 1990. Tämä oli australialaismiehen keksimä verkkoon yhdistetty leivänpaahdin, jonka asetuksia pystyi säätämään tietokoneen avulla. Tämän jälkeen termi ”Internet of Things” vakiintui 1999 Kevin Ashtonin toimesta. (Irmak & Bozdal 2018, 22.)

Vuonna 1999 keksittiin myös ensimmäinen maailmanlaajuinen RFID- järjestelmä eli radiotaajuinen etätunnistusmenetelmä ja jo vuonna 2003 tämä otettiin käyttöön amerikkalaisissa vähittäiskaupoissa (Suresh, Daniel, Parthasarathy & Aswathy 2014, 2). Järjestelmän keksiminen oli suuri hyppy tulevaisuuteen 2000-luvun alussa.

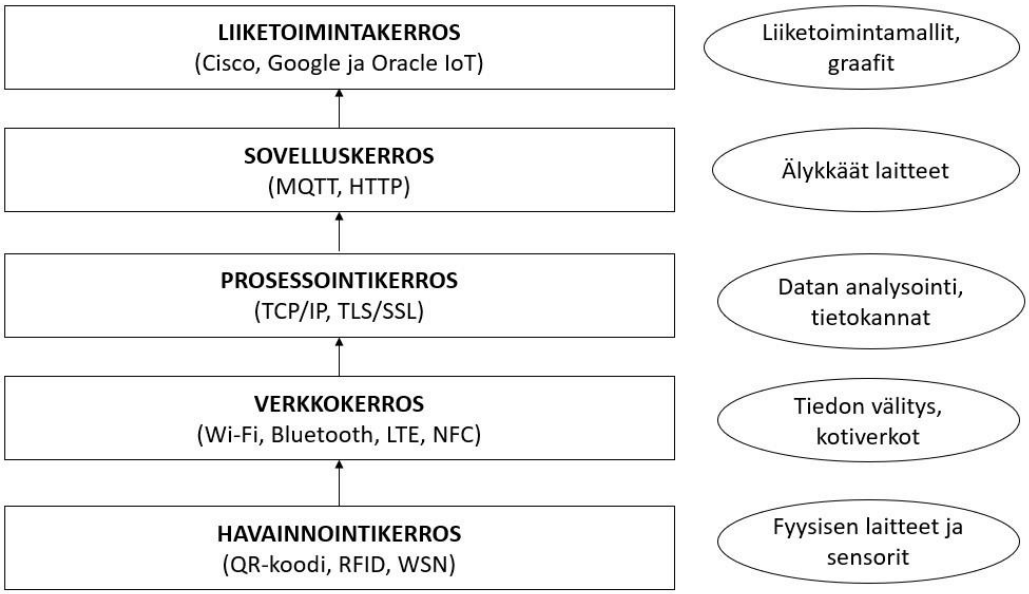
Ensimmäiset myytävät markkinoille saadut IoT-laitteet olivat LG-merkin älyjääkaapit vuonna 2000. Lopulta vuonna 2011 internet protokolla IPv6 lanseerattiin, mikä mahdollisti IoT:n räjähdysmäisen kasvun. Suuret IT-yritykset kuten Cisco, Ericson ja IBM käyttivät IoT:tä hyödyksi kaupallisella puolella sekä

koulutuksessa. (Suresh ym. 2014, 2.) Tästä lähti käyntiin nykyisellään käytössä oleva esineiden internetin aikakausi.

2.2 Arkkitehtuurin rakenne

IoT-arkkitehtuurille ei ole toistaiseksi määriteltyä standardia. Aiemmin arkkitehtuuria pidettiin perusmallin mukaan kolmikerroksisena, johon kuuluu havainto-, verkko- ja sovelluskerros. Tämän jälkeen tutkijat ovat ehdottaneet myös neljän ja viiden kerroksen arkkitehtuuria. Kuitenkin piirteiden lisääminen, kuten koneoppiminen ja algoritmit vaativat, että IoT:n arkkitehtuuri pitää sisällään havainnointi-, verkko-, prosessointi-, sovellus- sekä liiketoimintakerroksen (Kuvio 1). Jokaisella näistä viidestä kerroksesta on omat haavoittuvuutensa ja riskinsä. (Mrabet, Belguith, Alhomoud & Jemai 2020, 2–5.)

Kuviota tarkasteltaessa on hyvä ottaa huomioon, että tutkijat ovat ehdottaneet muutamia eri vaihtoehtoja parhaan arkkitehtuurin saavuttamiseksi. Sovellusarkkitehtuurin kerrosten määrästä tutkijat ovat olleet eri mieltä. Tutkijat ovatkin ehdottaneet esimerkiksi kolmikerroksisista arkkitehtuuria, johon kuuluvat havainnointi- verkko- ja sovelluskerrokset (Ammar, Russello & Crispo 2018, 9). Kolmikerroksisen arkkitehtuurin lisäksi on ehdotettu nelikerroksista arkkitehtuuria, joka sisältää kolmikerroksisen rakenteen lisäksi palvelukerroksen (Li ym. 2016, 340.) Kuitenkin viisikerroksinen arkkitehtuuri on näistä nykyään yleisin, joten tässä tutkimuksessa tarkastellaan viisikerroksisen mallin mukaista rakennetta. Viisikerroksinen arkkitehtuuri on turvallinen mutta ei yhtä skaalautuva. (Mrabet ym. 2020, 12.)



KUVIO 1 IoT-arkkitehtuurin kerrokset. Muokattu mukaelma (Mrabet, Belguith, Alhomoud & Jemai 2020, s.3) kuviosta.

Ensimmäisellä kerroksella sijaitsee havainnointikerros, johon kuuluvat kaikki fyysisesti tunnistettavat laitteet. Tämä kerros on ikään kuin laitteiden perusrunko. Sensoreiden tehtävänä on tuoda informaatiota sähköiseen muotoon tavallisesti sähköttömistä asioista, kuten lämpötilasta tai ilmankosteudesta. Sensorit keräävät tietoa laitteista, joihin se on asennettu. Sensorilaitteet ovat pieniä laitteita, jotka voivat tallentaa keräämäänsä informaatiota. Sensoreiden tietoja yhdistelemällä saadaan kerättyä hyvinkin laajamittaista informaatiota. (Collin & Saarelainen 2016, 154–156.)

Erityisesti radiotaajuustunnistuksella eli RFID:llä on suuri rooli havainnointikerroksella. Tämä on kustannustehokas ratkaisu yleiseen tietojenkäsittelyyn. RFID on yksilöllinen ja yksityiskohtainen tunnistusmenetelmä. Tämän lisäksi langaton anturiverkko eli WSN koostuu älykkäistä antureista, jotka pystyvät keräämään, prosessoimaan ja analysoimaan merkittävää dataa ympäristöstä. (Giri, Dutta, Neogy, Dahal & Pervez 2017, 1–2.) Sekä RFID, että WSN toimivat kummatkin havainnointikerroksella ja ovat vain yksi esimerkki tämän kerroksen toiminnasta.

Toisella kerroksella sijaitsee verkkokerros, joka yhdistää havainnointikerroksen laitteet verkkoon. Kerrosta kutsutaan myös kuljetuskerrokseksi, sillä sen päätehtävänä on ensimmäiseltä kerrokselta saadun datan vieminen eteenpäin. Tyypillisiä verkkokerroksen esimerkkejä ovat langaton lähiverkko WLAN eli Wi-Fi ja langaton tiedonsiirto kuten Bluetooth Low Energy (Giri ym., 2). Wi-Fi:n etuna on sen nopeus, kantaman vahvuus ja mahdollisuus suureen samaan verkkoon liitettävien laitteiden määrään. Kun taas Bluetooth-teknologian vahvuuksia on edullisuus ja sen sulauttaminen uusiin järjestelmiin. Bluetooth-teknologian

heikkous on kuitenkin lyhyt kantama sekä sensoreilta saadun tiedon keskittämisperusteinen verkkomalli. (Collin ym. 2016, 171–173.)

Seuraava kerros viisikerroksisessa arkkitehtuurissa on prosessointikerros. Tämä on vastuussa IoT-prosesseista, jotka ovat verkkokerroksella suunniteltuja. Prosessointikerros vastaanottaa erilaisista lähteistä tulevan tiedon ja analysoi, säilyttää sekä prosessoi tämän, jotta tietojen hyödyntäminen seuraavalla kerroksella olisi helpompaa. IoT-tietoisia prosessimalleja hyödynnetään erilaisissa suoritusympäristöissä. IoT-palvelun vaatimukset täytyy määritellä, ennen kuin sopivaa IoT-prosessimallia voidaan hyödyntää oikein. (Bassi, Bauer, Fiedler, Kramp, Kranenburg, Lange & Meissner 2013, 168–169.) Prosessointikerros hyödyntää monia teknologioita, kuten tietokantoja ja pilvipalveluita. Tällä kerroksella sijaitsee esimerkiksi pakettipohjaista tietoliikennettä hyödyntävä TCP/IP-protokolla. (Bassi ym., 2013, 169.)

Prosessoinnin jälkeen neljännellä kerroksella oleva sovelluskerros on vastuussa sovelluskohtaisten palveluiden toteuttamisesta käyttäjälle. Sovelluskerros pitää sisällään uudenlaiset sovellukset, joissa esineiden internet on käytössä (Sethi & Sarangi 2017, 2). Tällä tarkoitetaan älykkäitä ympäristöjä, kuten liikennettä, rakennusalaa, kaupunkeja, vähittäiskauppoja, tehtaita ja terveydenhuoltoa. Sovelluskerroksen tehtävänä on jäsennellä saatu tieto sellaiseen muotoon, että sovellusten tuottaminen käyttäjille on konkreettista ja harkittua (Patel & Patel 2016, 6125). Tämän jälkeen viimeinen arkkitehtuurimallin taso eli liiketoimintakerros pitää huolta siitä, että muilla kerroksilla jäsennellyt palvelut saadaan markkinoille. Tämä pitää sisällään koko IT-liiketoiminnan, kuten sovellukset, liiketoiminnan tuotot ja käyttäjien yksityisyyssuojan. Liiketoimintakerroksen esimerkkeinä ovat isot liiketoimijat kuten Google, Oracle ja Cisco (Sethi ym. 2017, 2–3.) Jokaisen kerroksen on toimittava linjassa ja harkitusti toisten kerroksien kanssa, jotta IoT:n arkkitehtuuri säilyy mahdollisimman eheänä koko prosessin läpi.

2.3 Hyödyt nykyteknologiassa

Fyysisten objektien liityttyä verkkoon on arkipäivän elämästä tullut helpompaa. Tutkijat odottavatkin IoT-laitteiden määrän kasvavan 27 miljardiin vuoteen 2025 mennessä (IOT Analytics 2021). IoT:n hyödyt nähdään hyvin moninaisina. Laitteita pystytään hyödyntämään muun muassa kuluttajaelektroniikassa, terveydenhuollossa, älyliikenteessä ja energia- ja tehdastyössä (Matthews, 2014). Esimerkiksi puhelin, älykellot tai muut päälle puettavat älyvaatteet pystyvät seuraamaan käyttäjän askelia, aktiivisuutta, sydämensykettä ja poltettuja kaloreita. Lisäksi älypuhelimella pystyy säätämään ja ohjaamaan kotona olevaa termostaattia kovemmalle tai vastaavasti pienemmälle. (Geng 2017, 6.)

IoT-laitteet nähdään tiedon talteenoton automatisoijana, jolloin manuaalinen tietojen talteenotto on jäänyt vähälle. Nykyaikaiset IoT-järjestelmät ovat kokonaan automatisoituja ja sisältävät yhä enemmän älykkäitä piirteitä. Ne

pystyvät esimerkiksi skannaamaan varastoon tulevat tavarat ja tallentamaan kerätyt tiedot reaaliajassa tietojärjestelmän tietokantaan. (Boos, Guenter, Grote & Kinder 2013, 455.) Ennen automatisointia vastaavanlainen prosessi vaati toimenpiteen manuaalista suorittamista.

Automatisoinnin lisäksi IoT-sovellukset mahdollistavat tehokkaan tiedonkeruun. Liikenteessä älykkäät liikennejärjestelmät pystyvät tiedottamaan reaaliajassa kansalaisille sen hetkisen liikennetilanteen, esimerkiksi mahdolliset liikenneruuhkat ja -onnettomuudet (Rathore, Ahmad, Paul & Thikshaja 2016, 135). IoT-laitteiden tiedonkeruun ja datan tallentamisen ansiosta pystytään ennakoimaan liikennevirtoja ja liikenteen eri tapahtumia. Älykkäät liikennejärjestelmät pyrkivät lisäämään kansalaisten viihtyvyyttä ja edistämään talouden kasvua. (Rathore ym. 2016, 136.)

Koko yhteiskuntaa hyödyttävien älykkäiden järjestelmien lisäksi IoT:n hyötyjä on myös joidenkin alojen kustannusten aleneminen. IoT mahdollistaa esimerkiksi työvoimakustannusten alentumisen antamalla kansalaisille enemmän valtaa tehdä päätöksiä (Brous, Janssen & Herder 2020, 3–4). Esimerkkinä päätöksenteon lisääntymisestä ovat nykyaikaiset itsepalvelukassat, jotka ovat lähes arkipäivää tämän päivän supermarketeissa. IoT-järjestelmien avulla ostoksista ja ostokäyttäytymisestä analysoidut tiedot pystytään tallentamaan tietokantaan. Näin ollen systemaattisella data-analyysilla ja tiedolla johtamisella voidaan esimerkiksi parantaa supermarkettien valikoimaa ja asiakastyytyväisyyttä. (Brous ym., 2020, 3–4.) Älykkäiden järjestelmien ansiosta suuret kauppaketjut pystyvät helpommin tarkastelemaan sitä, millaisia tarpeita kuluttajilla on ja kuinka nopeasti nämä tarpeet muuttuvat.

IoT on muuttanut rakenteita myös palvelualalla. IoT-avusteiset ja mobiilipohjaiset sähköiset terveydenhoitopalvelut ovat muuttaneet perinteisiä tapoja toimia terveydenhuoltoalalla. Sähköisen terveydenhuollon tavoitteena on tarjota parempaa terveydenhuoltoa huolimatta siitä, että potilaan ja lääkärin fyysinen sijainti ei ole aina samassa paikassa. (Adewale 2004, 222.) IoT:n luomat mahdollisuudet tarjoavat jatkuvasti sensoreiden luoman informaation pohjalta uusia ratkaisuja. Valtavasta määrästä tietoja saadaan informaatiota siitä, miten sähköistä terveydenhuoltoa pystytään kehittämään (Kaw, Loan, Parah, Muhammad, Sheikh & Bhat 2019, 262–263.) Sähköiset terveystiedot muodostuvat monitasoisesta tietomassasta, joka sisältää tietoja esimerkiksi apteekeista, potilaan kuvantamisista ja sairasvakuutuksista. Sähköiset terveystiedot sisältävät dataa myös potilaan verenpaineesta ja sykkeestä. (Williams & Boren 2008, 503.) Näitä tietoja hyödyntäen pystytään tehostamaan terveydenhuollon tarpeita ja kohdistamaan resursseja oikein sekä synnyttämään täysin uusia tapoja palvella terveydenhuollon asiakkaita.

Yhteiskunnallisten uudistusten lisäksi IoT-laitteiden käyttö on levinnyt myös kansalaisten koteihin ja työympäristöihin. Arkipäiväisten asioiden yhdistäminen internetiin on tuonut mahdollisuuden kehittää yhä älykkäämpiä palveluja kotioloissa. Informaation kerääminen ja yhdistäminen on luonut mahdollisuuden kehittää palveluita eteenpäin ja antaa näin ollen asiakkaille enemmän vastuuta päätöksenteossa. (Malek, Kharbouch, Khoukhi, Bakhoya, Florio,

Quadghiri & Blondia 2017, 429.) Yleisesti ottaen älykkäät IoT-järjestelmät ovat auttaneet kansalaisia niin kotona kuin työpaikallakin. Kotona käytettävät IoT:n pienlaitteet ovat saavuttaneet valtavan suosion. Tämän lisäksi yhteiskunnallisella mittakaavalla älykkäiden järjestelmien sulauttamisesta saadut hyödyt ovat valtavan suuria.

3 TIETOTURVAONGELMAT

Tässä luvussa tulen esittelemään IoT: n yleisimpiä tietoturvaongelmia. Ongelmat voidaan karkeasti jakaa kahteen luokkaan: teknisiin haasteisiin sekä muihin turvallisuushaasteisiin. Teknisiin haasteisiin lukeutuvat laitteissa ne asiat, jotka liitetään arkkitehtuurin rakenteellisiin ongelmiin. Teknisten haasteiden lisäksi käsittelen arkkitehtuurirakenteeseen liittymättömiä riskejä, kuten päivityksiä, sääntelyn puutoksia ja heterogeenisuutta. IoT-laitteiden tietoturvaongelmia koskevassa teoksessa on luonnehdittu IoT-tietoturvan vaativan kaikkia samoja perusperiaatteita kuin tietokoneiden tietoturvassa ja verkkoihin liittyvässä tietotekniikassa (Gilchrist 2017, 26).

3.1 Riskit ja haavoittuvuudet

IoT-laitteeseen liittyy monenlaisia riskejä. Laitteita ja teknologiaa integroidaan yhä enemmän älykkäisiin verkkoihin, joten tietoturvaongelmat kasvavat samaan tahtiin (Kondoro, Dhaou, Tenhunen & Mvungi 2021, 1). Hankalimmat riskit liittyvät käyttäjien inhimillisiin erheisiin, kuten saman salasanan asettaminen useaan eri laitteeseen. Useimmissa tapauksissa kuluttaja kyllä tietää ostaessaan riskit, mutta luottaa liikaa laitteen palveluntarjoajaan. Esimerkiksi Wi-Fi reitittimen ostaja varmasti tietää turvallisuusongelmat, mutta päättää silti olla ottamatta käyttöön minkäänlaista salausta (Gilchrist 2017, 10). Tämä johtuu usein joko tiedon puutteesta tai välinpitämättömyydestä. Vastuu laitteiden suojauksesta tulisi olla laitteen tarjoajalla, mutta käytännössä kuluttajan on oltava valveutunut suojaamaan laitteensa oikein. Ongelmana on kuitenkin se, että kaikilla kuluttajilla ei ole tietämystä siitä, kuinka käsitellä ja ylläpitää omaa tietoturvaansa (Hyppönen 2021.)

Useimmat IoT-laitteet eivät pysty käsittelemään tietoa suojatusti. Tästä johtuen mikä tahansa internetiin yhdistetty esine saattaa sisältää haavoittuvuuksia,

jotka voivat asettaa käyttäjän datan, laitteiston, tietosuojan, verkon ja yksityisyydensuojan vaaraan. (Watts 2016, 58.)

IoT-laitteet keräävät valtavan määrän tietoa ja siksi näissä piilee suuri riski yksityistietoihin pääsyyn. Laitteita käytetään yhä laajemmin eri aloilla ja erilaisiin tarkoituksiin, joten laitteet tallentavat usein vaikkapa yksityishenkilön terveystietoja. IoT-laitteet keräävät tietoja eri kohteista ja yhdistelevät näitä massadatan avulla. Näin henkilöstä saadaan tehtyä ikään kuin profiili, jonka tiedot voidaan kommunikoida eteenpäin pilvipalvelimille. (Weber 2015, 619.)

Sellaiset IoT-laitteet, jotka keräävät ja prosessoivat tietoja ovat alttiimpia haavoittuvuuksille. Näiden avulla pystytään identifioimaan ja profiloimaan yksityishenkilön käyttäytymistä. Henkilöstä louhittu informaatio pystytään myymään usein kolmansille osapuolille, kuten kaupoille ja muille yrityksille, jotka saavat näin tietoja kuluttajan kulutustottumuksista, terveydestä ja sijainnista. (Watts 2016, 58.) Tämä tarkoittaa sitä, että kuluttajan käyttäytymistä on helppo ennakoida ilman, että kuluttaja edes tietää tai tunnistaa tietojensa menevän kolmansien osapuolien tarkoituksiin.

Muita IoT:n haasteita on sääntelyn puutos. Sääntelyä on vaikea saavuttaa tekniikan nopean edistymisen vuoksi. Laki kyllä kieltää henkilökohtaisten tunnistettavien tietojen keruun, mutta IoT:ssä tämä pykälä on kierrettävissä niin, että tiedot ovat henkilökohtaisia, mutta eivät kuitenkaan koske tiettyä henkilöä. (Ahlmeyer & Chircu 2016, 22–23.) Kuitenkin valmistettaessa IoT-laitteita fyysisesti on laitteiden sisällettävä asianmukaisten tunnisteiden turvallinen määrittäminen ja rekisteröinti jokaiselle laitteelle. Laitteiden ohjelmistojen testaus ja turvaominaisuuksien tarkastus on keskeinen osa valmistus- ja toimitusvaiheita. (Ahlmeyer ym., 2016, 25.)

Turvallinen toimitusketju muodostuu haasteeksi IoT-laitteiden muodostaessa yhä suurempaa yhteysverkkoa internetiin. Mahdolliset haavoittuvuudet kasvavat, sillä suuri osa tästä vuorovaikutuksesta on näkymätöntä, mikä tekee riskien tunnistamisesta entistä hankalampaa. Sekä IoT-laitteen tarjoaja että käyttäjä saattavat olla tietämättömiä puuttuvasta suojauksesta. Ongelmaksi tämä muodostuu silloin, kun laitteiston päivitykset eivät ole enää ajan tasalla. Päivitysten ajantasaisuus on olennaista yksityisyydensuojan takaamiseksi. (Folk, Hurley, Kaplow & Payne 2015, 4.)

3.1.1 Huolenaiheet IoT:n eri sovelluskerroksilla

IoT sisältää monia erilaisia riskejä sovelluskerroksilla. Jotta olisi helpompi havainnollistaa tietoturvahuolenaiheita, tarkastellaan seuraavaksi yleisimpiä haavoittuvuuksia neljällä eri IoT:n kerroksella: rajapinta-, prosessointi-, verkko- ja havainnointikerroksella. Jokaisella kerroksella on omat haavoittuvuutensa, vaikkakin ne ovat keskenään lähes samoja tietoturvaan liittyviä ongelmia. Jokainen edellä mainituista kerroksista pystyy tarjoamaan myös rajattuja suojaustoimintoja, kuten tietojen eheyden, todennuksen ja tietojen luottamuksellisuuden. (Li ym. 2017, 28–29.) IoT:n turvallisuuden huolenaiheet ovat tiivistetty seuraavassa

taulukossa (taulukko 1), joka on suomennettu mukaelma Lin & Xun (2017) kirjasta.

TAULUKKO 1 Yleisimmät haavoittuvuudet IoT:n eri kerroksilla. (Li & Xu 2017, 31.)

Tietoturvahuolet	Rajapinta-kerros	Prosessointi-kerros	Verkkoker-ros	Havainnoin-tikerros
Epävarma käyttöliittymä	x	x	x	
Riittämätön todennus	x	x	x	x
Turvattomat verkkopalvelut		x	x	
Tietoliikenteen salauksen puutteet		x	x	
Yksityisyydensuojan huolet		x	x	x
Epävarma pilvikäyttöliittymä	x			
Epävarma mobiilikäyttöliit-tymä	x		x	x
Epävarmat suojausasetukset	x	x	x	
Epävarma ohjelmisto	x		x	
Heikko fyysinen suojaustaso			x	x

Rajapintakerros neljän kerroksen arkkitehtuurissa yhdistää aiemmin esitellyn sovellus- ja liiketoimintakerroksen. Havainnointikerroksella huolenaiheita ovat riittämätön todennus, yksityisyydensuoja, epävarmat mobiilikäyttöliittymät ja heikko fyysinen suojaus. IoT-laitteiden on esimerkiksi kyettävä todentamaan käyttäjän henkilöllisyyden aitous. (Li ym., 2017, 30–32.) Verkkokerroksen ongelmia taas ovat salaushaasteet laitteilla, joiden kapasiteetti on liian pieni. Tällä kerroksella huolenaiheita on lähes jokaisella osa-alueella. Prosessointi- ja rajapintakerroksien huolenaiheita ovat yksityisyydensuojan turvallisuusvaatimukset, kuten riittämättömät todennukset ja epävarmat käyttöliittymät. (Li ym. 2017, 32–34.)

Jokainen kerroksista tarjoaa erilaisia toimintoja, mutta jokaisella on myös omat uhkansa. Kaikki kerrokset ovat tekemisissä toistensa kanssa, joten jokaisen kerroksen on luotettava toiseen kerrokseen toimiakseen. Sitä varten kaikkien kerrosten tulee olla turvallisia. (Rizvi, Pfeffer, Kurtz & Rizvi 2018, 164.)

3.2 Tekniset haasteet

Osa laitteistojen valmistajista myy sellaisia laitteita, joiden tietoturvaominaisuudet eivät ole riittävällä tasolla. Tämä aiheuttaa haittaa niin globaalille kuin yksilöidenkin taloudelle. (Corser 2017, 1.) Tietoturvaominaisuudet jäävät keskeneräiseksi sen vuoksi, että yritykset myyvät laitteita markkinoille niin nopeasti kuin pystyvät, koska laitteiden kysyntä on suuri. Tällöin laitteiston fyysisten riskien huomioiminen jää vähäiseksi. IoT:n turvallisuuden huomioiminen teknisessä toteutuksessa on tärkeä osa-alue, mutta tämä unohdetaan usein (Weinberg,

Milne, Andonova & Hajjat 2015, 616). Karkeasti voisi sanoa, että tuotteiden saaminen markkinoille nopeasti on useasti tärkeämpää kuin käyttäjien tietosuoja ja turvallisuus.

Yksi tärkeimmistä ongelmista on IoT-laitteiden rajoitettu laitteiston kapasiteetti. Laitteiden on oltava tehokkaita ja yksinkertaisia, jonka vuoksi niihin suunnitellaan vain rajoitettu verkkokapasiteetti. Suunnittelu ja toteutus vie paljon aikaa, mutta laitteistojen vieminen markkinoille on nopeaa, mikä asettaa nämä vakavien turvallisuusriskien alaiseksi. Lisäksi laitteita asetetaan usein turvattomiin ja helppoihin fyysisiin ympäristöihin. Vaikka tietoturvarike näissä ympäristöissä huomattaisiin, ei edullisia laitteita todennäköisesti koskaan korjata ja huolleta niin kuin pitäisi. Korjauskulut ovat usein suuremmat kuin uuden laitteen hankkimiskustannukset. (Wheelus & Zhu 2020, 260–261.) Tämä muodostaa todellisen tietoturvauhan laitteiden fyysiselle rakenteelle.

Teknisten toimintojen osalta tärkein laillinen näkökulma on toiminnan avoimuus. Teknologian tuottajan, joka on aiheuttanut vahinkoa käyttäjälle, on osoitettava, että toiminta on ollut kohtuullista ja oikeudenmukaista. Vaikka teoriassa teknologian tuottaja on vastuussa siitä, jos teknologia ei toimi oikein, vastuu siirtyy silti usein käyttäjälle. Usein käyttäjät ovat tietämättömiä tekniikasta, joten heidän ainoa keinonsa on valita, luottavatko he tekniikan sääntelyyn vai eivät. Lain mukaan tekniikan tuottajat ovat kuitenkin velvoitettuja tekemään tietyt testausprosessit ennen käyttöönottoa, mutta useat viat saatetaan löytää vasta epäonnistumisen yhteydessä. (Singh, Millard, Reed, Cobbe & Crowcroft 2018, 55.)

Teknisemmät hyökkäykset suoritetaan fyysisesti joko langallisen tai langattoman verkon kautta. Hyökkäykset suoritetaan käyttämällä laitteita väärin tarkoituksena vahingoittaa laitetta tai siinä olevia tietoja. Hyökkäyksen ideana on tallentaa, estää tai lähettää haitallisia viestejä eteenpäin muihin IoT-laitteisiin. (Rizvi ym. 2018, 165.) Tietoturvahaavoittuvuudet ja päivitysten puutokset vaikkapa Android-käyttöliittymässä saattavat sallia virusohjelman näppäinpainallusten tallentamiseen. Näppäinpainalluksista on saatavissa kaikki tärkeä tunnistetieto käyttäjästä, minkä avulla voidaan saada IoT-laite hallintaan. Tämänkaltaiset tapaukset aiheuttavat merkittävän identiteettivarkauden uhan käyttäjälle. (Folk ym. 2015, 13–14.)

Vähintään 70 prosentissa tämän päivän IoT-laitteita on fyysisiä riskejä. Nämä haavoittuvuudet laitteissa ovat syy siihen, miksi hyökkäyksiä pystytään tekemään. Esimerkiksi Mirai-haittaohjelma vuonna 2016 pystyi bottiverkon avulla tekemään laajan palvelunestohyökkäyksen. Haavoittuvuudet eivät yksinään aina mahdollista hyökkäyksen tekemistä, vaan fyysinen turvallisuusympäristö sekä fyysiset laitteistojen vauriot ovat myös hyökkäysten riskitekijöitä. (Mustapha & Alghamdi 2018, 2.)

Tietoturvariskit johtavat usein samankaltaisiin tietoturvauhkiin, vaikka laitteiden tietoturvapuutokset ovat harvemmin tarkoituksellisesti tehtyjä. Tässä luvussa tarkasteltiin sitä, kuinka suuri vaikutus käyttäjälähtöisillä inhimillisillä erheillä on riskien kasvamiseen. Monet käyttäjät luottavat laitevalmistajiensa tarjoamaan suojaan eivätkä koe sen olevan puutteellista. Tutkielmassa esitetyt esimerkit hyökkäyksistä ovat kuitenkin erittäin vakavia tietoturvaongelmia

yksityisyyden turvaamiselle. Tarkoituksellisten hyökkäysten tavoitteena on lähes aina jokin hyöty. Oli motiivina sitten raha tai käyttäjän tietoihin pääseminen, on hyökkäys aina otettava vakavasti. Tahalliset hyökkäykset keskittyvätkin juuri sellaisiin laitteisiin, joissa suojaus on puutteellinen. Tulevaisuuden IoT:n turvaamiseksi on otettava mallia menneisyyden erheistä, jotta nämä voidaan välttää jatkossa (Gilchrist 2017, 26). Seuraavassa luvussa tarkastellaan sitä, millaisia eri suojausmenetelmiä tulisi tulevaisuudessa käyttää riskien minimoimiseksi.

4 IOT-LAITTEIDEN SUOJAAMISTAPOJA

Tässä luvussa kerron, millaisia tapoja IoT-laitteiden suojaamiseen on ja miten näitä pystytään hyödyntämään. Lähestyn suojaamista kolmesta eri näkökulmasta: käyttäjälähtöinen suojaus, laitevalmistajien fyysinen suojaus sekä nykyisin yleistyneet tietoturvatuotteet suojauksen apuna. Käyttäjällä on suuri vaikutus oman laitteensa tietoturvalliseen käyttöön, mutta kuitenkin vastuu salauksesta on lähtökohtaisesti IoT-laitteen valmistajalla. Tutkin näiden kahden osapuolen välistä yhteyttä siinä, millainen ratkaisu antaisi laitteelle tarpeeksi tehokkaan suojan. Käsittelen myös suhteellisen uutta IoT-maailman aihealuetta, joka koskee tietoturvayritysten myymien tietoturvatuotteiden käyttöä laitteiden ongelmien ehkäisemiseksi.

4.1 Käyttäjälähtöinen suojaaminen

Suuri osa kuluttajista omistaa nykyään IoT-laitteita, mutta ovat myös yhä valveutuneempia siitä, millainen suojaus näissä tulisi olla. Käyttäjien huoli laiteturvallisuudesta ei vastaa heidän kykyjään huolehtia tästä kuitenkaan itse. Kuluttajien huolta lisää yksittäisten laitteiden haavoittuvuus sekä tieto suuremmista kyberhyökkäyksistä suojaamattomia IoT-laitteita kohtaan. (Hosein & Badran 2019, 133.)

Joka tapauksessa käyttäjällä on suuri vaikutus omien laitteidensa tietoturvalliseen käyttöön. Laitteita käytetään usein myös fyysisesti suojaamattomissa ympäristöissä. Käyttäjät eivät usein tiedä tai välitä laitteidensa suojauksesta. Jos laite toimii niin kuin on tarkoitus, käyttäjät eivät ehkä ymmärrä sitä, että turvallisuudesta täytyy huolehtia. (Rizvi ym. 2018, 166.) Tietoturvallisen käytön lähtökohdat on jokaisen käyttäjän hyvä tiedostaa. Maailmanlaajuinen tietoturvayhtiö Kaspersky luonnehtii verkkosivuillaan muutamia tärkeimpiä asioita oman tietoturvan toteuttamiseksi. Näitä ovat esimerkiksi vahvan arvaamattomissa olevan salasanan asettaminen jokaiseen laitteeseen, julkisten Wi-Fi verkkojen

välttäminen, vahvojen salausmenetelmien käyttö sekä todentamisen varmistaminen. (Kaspersky, 2017.)

Erilaisia suojausmenetelmiä yhdistämällä saadaan kattavampi suojaus kuin yhdellä menetelmällä. Esimerkiksi pelkkä salasana yksinään ei ole tarpeeksi vahva suojaus (Aqrawal & Mishra 2012, 877). Varmistuaksemme siltä, että tiedostoihin eivät pääse käsiksi sinne kuulumattomat henkilöt, voimme käyttää tähän kahdenlaista salaamismenetelmää: symmetrinen ja epäsymmetrinen. Symmetrinen salaus sisältää salauksen avaamiseen ja purkamiseen saman salausavaimen. Epäsymmetrinen salaus poikkeaa symmetrisestä siinä, että salausavain on eri avaamiseen ja purkamiseen. Oikein tehtynä kumpikin salaus tarjoaa miltei läpäisemättömän suojan. Salaus on tehokas tapa saavuttaa tietoturva, sillä salauksen voivat purkaa vain ne henkilöt, joilla on pääsyavain kyseiseen aineistoon. (Aqrawal ym., 2012, 877.)

Tämän lisäksi suuri haaste käyttäjän suojaamiseksi on todennuksen puuttuminen. Tietoja lähetetään liian herkästi varmistamatta sitä, ketkä tietoja tosiasiassa saavat. Todennus on kahden osapuolen välillä tietoliikenteessä kulkevan informaation turvaamiseksi käytettävä tapa. Todennusta tarvitaan, jotta IoT-laitteista saa turvallisemman käyttäjälleen. Todennusta voi olla yksi-, kaksi- tai kolmipuolista. Tällä tarkoitetaan osapuolten määrää, jotka todentavat toisensa keskinäisessä tiedonvälityksessä. (Ali, Dustgeer, Awais & Shah 2017, 1–2.)

Todennuksen ja salaamismenetelmän lisäksi yksi tehokas tapa suojata itsensä tietoturvahaavoittuvuuksilta on valtuutus, jonka avulla jokaisen tiedostoihin käsiksi pääsevän käyttöoikeudet on määritelty tarkasti. Luottamuksellisuus varmistaa sen, että vain valtuutetut käyttäjät voivat päästä tiedostojen yksityistietoihin. Tämä tarkoittaa myös sitä, että liian vähäiset käyttöoikeudet eivät aina ole käytön resursseja varten parhaimmat, vaan nämä on määritettävä järkevällä ja suotuisalla tavalla. Valtuutukseen liitetään myös usein integrointi- ja saatavuusperiaatteet. Tietoja on säilytettävä johdonmukaisesti ja tarkasti, sekä varmistettava turvallinen tietojen saatavuus. (Ali ym., 2017, 2.)

4.2 Laitevalmistajien vastuu suojauksesta

IoT-laitteistojen valmistajilla on päävastuu laitteiden turvallisesta toiminnasta. Ihanteellinen ratkaisu voisi korjata nopeasti haavoittuvuudet laitteista. Tämä ei kuitenkaan ole niin yksinkertaista. Erityisesti IoT-laitteiden ohjelmistopäivitykset ovat ongelmallisia. Toisilla laitteilla päivitysmahdollisuudet puuttuvat kokonaan, kun taas toiset laitteet ovat liian vanhoja uusille päivityksille. Päivitysten ajantasaisuus puuttuu yleensä niissä tapauksissa, joissa laitteet on hankittu moneksi vuodeksi, kuten vaikkapa älyjääkaappi, jonka päivitykset saattavat olla vain muutaman ensimmäisen vuoden ajan tasalla. Vaikka päivityksiä vanhempiin laitteisiin olisi vielä saatavilla, on niiden soveltaminen haastavaa. Toiset laitteet vaativat käyttäjiä päivittämään itse laitteensa, kun taas toiset ovat automaattisesti asennettuja lataamaan uudet ohjelmistopäivitykset. (Simpson, Roesner & Kohno 2017, 551.)

Verkon turvallisuus riippuu myös sen infrastruktuurin rakenteesta. Ongelmat juontuvat usein muuttuvista teknologioista. Uudet IoT-laitteet eivät ole välttämättä suojattuja ollenkaan. Turvallisuusmekanismien eteen on tehty valtavasti töitä, ja eri laitevalmistajat ovat alkaneet luoda omia tietoturvastandardejaan esimerkiksi yksityisyydensuojan turvaamiseksi. Uusia tietoturvalaajennuksia on alettu lisäämään myös jo markkinoilla oleviin IoT-laitteisiin. Näiden suojausprotokollien lisääminen vanhoihin laitteisiin on kuitenkin niin monivaiheinen prosessi, että se hidastaa uusien laitteiden tuloa markkinoille. (Kondoro ym. 2021, 1.)

Laitteiden hyvällä fyysisellä turvallisuudella voidaan estää erityisesti havainnointikerroksen hyökkäykset. Fyysisen turvallisuuden parantamiseksi laitteiden komponenttien, kuten vaikkapa radiotaajuuden, on oltava korkealla suojaustasolla. (Rao & Haq 2018, 33.) Tekniset haasteet liittyvätkin suurelta osin tietoturvaongelmiin IoT-laitteita suunniteltaessa ja valmistettaessa. Turvallisuus tulisi huomioida sovelluksen jokaisella arkkitehtuurikerroksella. Teknisten tietoturvavaatimusten täyttämiseksi IoT-laitteiden suojaustoimintojen on oltava luottamuksellisia, eheitä ja saatavilla olevia. IoT-laitteiden heterogeenisuutta tulisi välttää, jotta turvallisuusuhkat lievenisivät. Laitteiden turvallisuuden takaamiseksi ne on valmistettava asianmukaisia turvatoimenpiteitä noudattaen. (Duc, Jabangwe, Paul & Abrahamsson 2017, 1–4.)

Asianmukaisten menetelmien käytöllä laitevalmistajat varmistavat sen, että he saavat asiakkaita, joilla tietoturvatietous on hallussa. Tämä auttaa myös muita asiakkaita määrittämään laitteidensa hinta-laatusuhdetta ja tarkastamaan laitteidensa riskit ennen ostopäätöstä. Tämä pakottaa laitevalmistajat valmistamaan tulevaisuudessa paremmin suojattuja IoT-laitteita. Tämä tekee myös IoT-laitteiden valmistuksesta kustannustehokasta, sillä haluttuja ominaisuuksia ja tuotteita on helpompi tuoda markkinoille ympäri maailmaa. (Megas, Cuthill & Gupta 2021, 7.)

4.3 Tietoturvatuotteet suojaamisen apuna

Viime vuosina kysymyksiä herättänyt IoT-laitteiden yksityisyydensuoja on saanut yritykset kehittämään uusia suojaa tukevia alustoja. Tietoturva-alustat pystyvät suojaamaan käyttäjän yksityisyyttä, mutta tietoturvayritysten on päästävä käyttäjän laitteiden käyttöoikeuksiin käsiksi. Käyttäjät pystyvät määrittelemään sen, mitä he haluavat jakaa tietoturvayrityksille sovelluksen kautta. (Torre, Koceva, Sanhez & Adorni 2016, 384.) Tietoturva-alustat pystyvät seuraamaan mahdollisia tietosuojaongelmia ja tekemään tarvittavia johtopäätöksiä toimenpiteitä vaativista ongelmista (Torre ym., 2016, 390).

Tietoturvayritysten kehittelemät tietoturvatuotteet IoT-laitteiden suojaamiseen ovat kuitenkin suhteellisen uusi tapa suojata omia laitteita hyökkäyksiltä. Olemme kyllä tottuneet tietoturvasovellusten käyttöön esimerkiksi tietokoneellamme, mutta nyt tämän kaltaiset tietoturvatuotteet ovat tulleet avuksi myös

muissa IoT-laitteissa, sillä kuluttajat eivät useinkaan hallitse suojauksen ylläpitoa. Tietoturvatuotteet ovat apuna heille, jotka eivät luota laitevalmistajiensa tekemiin suojauksiin eivätkä itse syystä tai toisesta ylläpidä korkeaa suojaustasoa laitteissaan.

Tietoturvaratkaisuja myyvä suomalaisyhtiö F-secure on kehitellyt muutama vuosi takaperin Sense-nimisen reitittimen, joka lupaa estää laitteisiin kohdistuvat hyökkäykset. Laite mukautuu sen mukaan, millainen hyökkäystapa missäkin tilanteessa on, sillä laitteet tarvitsevat usein hyvin erilaista suojausta keskenään. Tämän laitteen toimintaperiaate on, että se havaitsee heti tekoälyn avulla, kun suojattavissa IoT-laitteissa tapahtuu jotain epätavallista. Tällä tavoin voidaan suojata myös niitä laitteita, joista suojaus puuttuu kokonaan. Sense-reititin lupaa päivittää ohjelmistonsa säännöllisesti sekä automaattisesti. Reititin lupaa suojata hyökkäyksiltä kaikkia kodin IoT-laitteita. (F-Secure 2021.)

Ratkaisua IoT-laitteiden suojaamisen on ehdotettu myös amerikkalaisomisteisen ohjelmistoyritys CUJO AI:n toimesta. Yritys tarjoaa tuotetta nimeltä Sentry, joka on kuluttajille sekä yrityksille suunnattu digitaalinen tietoturvapalvelu. Se käyttää tekoälyä havaitakseen verkkoon kohdistuvat uhat ja estääkseen mahdolliset hyökkäykset. Tarkoitus on sama kuin F-Securen Sensellä, eli suojata loppukäyttäjää ja tämän yksityisyyttä. Sentry voidaan ottaa käyttöön missä vain laajakaistareitittimessä, eikä se vaadi lisäohjelmistoja. Laite lupaa myös suojata jokaista kodin IoT-laitetta. Sentry käyttää tiedon käsittelemiseen koneoppimisalgoritmeja, jotka luovat turvallisemman ympäristön loppukäyttäjälle ja suojaavat mahdollisilta uusilta hyökkäyksiltä. (CUJO AI 2021.)

Paras tapa suojautua IoT-laitteisiin kohdistuvilta tietoturvauhilta on käyttää vain sellaisia laitteita, jotka ovat riittävän hyvin suojattuja. Valmistajan täytyisi kertoa selkeästi laitteisiin tehdyistä tietoturvatoimenpiteistä ja päivityksistä. Arkkitehtuuriltaan turvallisen laitteen käyttö yhdessä käyttäjän suojaamistoimenpiteiden, kuten vahvan salasanan ja kaksivaiheisen todennuksen kanssa, pitäisi tuoda riittävää suojaa laitteen käyttäjälle. Tietoturvatuotteiden käyttäminen suojaamisen apuna on luultavasti yleistymässä, sillä käyttäjät eivät aina välttämättä halua tai ehdi itse tehdä tarvittavia suojaustoimenpiteitä. Jokainen käyttäjän kodissa oleva verkkoon kytketty IoT-laite sisältää niin paljon tietoa, että puutteellinen suojaus ajaa käyttäjän yksityisyyden todelliseen vaaraan. Johtopäätöksenä voidaan todeta, että hyvin tehty suojaus on tarpeellinen eikä suojaukseen voi suhtautua milloinkaan välinpitämättömästi.

5 YHTEENVETO

Tämän kirjallisuuskatsauksena suoritetun tutkimuksen tavoitteena oli vastata kahteen tutkimuskysymykseen *"Millaisia tietoturvariskejä IoT-laitteet pitävät sisällään?"* ja *"Miten näiltä riskeiltä tulisi suojautua?"*. Kirjallisuuden tutkimuksen kautta päästiin siihen tulokseen, että riskit laitteissa ja näiden käytössä ovat hyvin moninaisia. Suurimpiin tietoturvaongelmiin tutkimuksessa johtivat saadun informaation väärinkäyttö ja käyttäjien inhimillisistä erheistä johtuvat suojaamistason puutteet (ks. Gilchrist 2017). Myös IoT-laitteiden tietoturvaominaisuuksien sääntelyn puute on suuri ongelma. Tietoturvaominaisuudet on testattava uusissa laitteissa, mutta ominaisuuksien ylläpito jää huomiotta. (ks. Ahlmeyer ym., 2016.) IoT-laitteet pyritään saamaan mahdollisimman nopeasti markkinoille, minkä vuoksi laitevalmistajien paine tietoturvan nopeasta integroinnista laitteisiin kasvaa. (ks. Weinberg ym., 2015.)

Kirjallisuuskatsauksesta kävi ilmi, että laitteet sisältävät monenlaisia teknisiä riskejä myös eri sovelluskerroksilla. Tutkimuksessa tarkasteltiin arkkitehtuuria neljällä eri sovelluskerroksella. Lähes jokaisen sovelluskerroksen riskit olivat riittämätön todennus, epävarmat käyttöliittymät ja huoli yksityisyydensuojasta. Jokainen kerros pystyi kuitenkin tarjoamaan myös joitakin suojaustoimenpiteitä. (vrt. Li ym., 2017.)

Riskeiltä suojautumiseen liittyen tuli tehdyssä kirjallisuuskatsauksessa ilmi suojautumistapojen moninaisuus. Suojaamistapoja on sekä käyttäjille, kuin laitevalmistajille, mutta konkreettista näkökulmaa siihen, kuka oikeasti on vastuussa suojauksesta ja millainen sen pitäisi olla, ei ole löytynyt. Tehokas suojaamistapa vaatii laitevalmistajan tekemien päivitysten rinnalle käyttäjän omaa havainnointia laitteensa tilasta (ks. Simpson ym., 2017). Hyvä fyysinen turvallisuus tulisi olla aina peruslähtökohtana laitteiden markkinoille viemisessä (ks. Mustapha ym., 2018). Laitteen käyttäjälle on annettava kaikki tietous siitä, miten hänen tulee toimia pitääkseen laitteitaan turvassa yksityisyydensuojansa tueksi.

Tehdystä tutkimuksesta päätellen IoT-laitteet ovat tulleet jäädäkseen. IoT on noussut teknologian alana nopeasti, sillä se tarjoaa valmiudet kommunikoida verkossa erilaisten laitteiden avulla. Sillä, millainen laite on, ei ole enää merkitystä. Tämä tarkoittaa sitä, että teknologia on mahdollistanut älykkään

järjestelmän sulauttamisen puettavasta vaatteesta isoihin laitteistoihin ja kokonaisiin älykaupunkeihin asti. Tulevaisuudessa ne vain muotoutuvat uudelleen ja laitteista halutaankin yhä älykkäämpiä ja omatoimisempia. Tämä on mahdollista toteuttaa nykyisen tekniikan myötä, mutta haasteita on ratkaistava etenkin turvallisuuspuolella. (Reyna, Martin, Chen, Soler & Diaz 2018, 173.)

Vaikka IoT-tietoturvaongelmiin liitettyjä tutkimuksia on tehty erityisesti viime vuosina paljon, eivät ne ole saaneet heräteltyä riittävästi laitevalmistajien ja kuluttajien huolta tietoturvasta. Motiiveja ongelmien ratkomiseen pitäisi löytyä, mutta toteutus on vielä keskeneräistä. Tämä saattaa osittain johtua IoT-järjestelmien monimutkaisuudesta. Ensinnäkin voi olla vaikea havaita IoT-laitteisiin kohdistuvia hyökkäyksiä. Hyökkäystä tarkastellessa on erotettava, onko käyttäjän tiedot laittomasti hankittu vai onko itse IoT-laite heikon arkkitehtuurin vuoksi vuotanut käyttäjän tietoja esimerkiksi pilveen. Jotta voimme tulevaisuudessa taata, että IoT-laitteet ovat turvallisia, meidän on otettava käyttöön useampi tutkimuksessa esitellyistä suojaustekniikoista. (Yang, Peng, Li & Niu 2016, 592.)

Tulevaisuuden tutkimuksissa voitaisiin keskittyä enemmän siihen, kuinka laitteisiin saataisiin riittävä suoja niin, että käyttäjät pystyvät luottamaan enemmän laitevalmistajien tarjoamaan suojaan. Tällä hetkellä käyttäjillä on usein tietämättään suurin vaikutus omien IoT-laitteidensa turvallisuuteen kotiympäristöissä. Käyttäjien tietämättömyys omien laitteidensa tietoturvasta vaikuttaa osaltaan puutteelliseen suojaukseen. Yksi ratkaisu suojaamisen lisäämiseksi voisi olla tutkimuksessa esitellyt tietoturvayritysten tietoturvatuotteet. Nämä ovat kuitenkin suhteellisen uusi alue IoT:n maailmassa, joten niiden kehittämiseen tarpeeksi tehokkaiksi saattaa kulua vielä aikaa. IoT:n suojaamisen vakavasti ottamisessa tarvittaisiin myös lainsäädäntötoimia, joita uskoisin tehtävän tulevina vuosina. Aihepiiri on sellaisenaan kuitenkin niin uusi, että lainsäädäntö ei ole kyennyt mukautumaan samaan tahtiin.

Täytyy kuitenkin muistaa, että IoT-teknologiat ovat nopeasti muuttuvia, joten tutkimusten tulisi keskittyä tulevaisuudessa yhä enemmän vallitsevan ajan kontekstiin. Tulevaisuudessa kehitysnäkymät saattavat mennä eri suuntaan kuin mitä on kuviteltu. Tähän vaikuttavat monet tekijät, kuten tietoturvaoppiminen, uudet lainsäädännöt ja laitevalmistajien uudet tuotteet. Jatkotutkimusaiheita voisi kuitenkin esittää esimerkiksi seuraavista aiheista:

1. IoT-laitteiden riittävä suoja yritysympäristössä.
2. Käyttäjien keskinäiset tietotaidot tietoturvallisessa käytettävyydessä.
3. IoT:n käytettävyyden yleistymisen aiheuttamat ongelmat.
4. Markkinoille tulevien IoT-teknologioiden päivitysten ylläpito.

IoT-laitteiden turvallisuutta yrityskäytössä tulisi tutkia lisää, sillä laitteita hyödynnetään yhä enemmän etenkin suurien yrityksien sisällä. Tietojen vuotaminen yrityksen käytössä olevista IoT-laitteista on suuri uhka. Tämä asettaa vaaraan niin työntekijöiden tiedot kuin yrityksen sisäiset asiatkin. Tämä voi

aiheuttaa pahimmassa tapauksessa taloudellista menetystä, mutta myös yrityksen luotettavuuden ja identiteetin heikentymistä.

Käyttäjät ovat yhä valveutuneempia pitämään huolta omasta tietoturvastaan. Jatkossa tulisikin tutkia sitä, millainen vaikutus lisääntyneellä tietoturvatietoudella on laitteiden tietoturvalliseen käyttöön. Käyttäjät oppivat yhä enemmän siitä millainen tietoturva pitäisi saavuttaa, mutta on vielä epäselvää, toteutuuko tämä silti käytännössä. Koska IoT-laitteet yleistyvät jatkuvasti ja uusia tuotteita syntyy markkinoille, on tämä käytettävyyden kannalta haasteellista. Tulisikin tutkia tuoko käytettävyyden yleistyminen yhä enemmän tietoturvaongelmia laitteiden monimutkaisten ohjelmistojen vuoksi.

Jatkotutkimusaiheena voitaisiin tutkia lisäksi uusien laitevalmistajien IoT-teknologioiden päivitysten ylläpitoa. Niin kuin tutkielmassa havaittiin, päivitysten ylläpito on jäänyt taka-alalle, koska uusia laitteita tulee jatkuvasti lisää. Niin sanotut ”vanhat” päivitystä vaativat laitteet unohdetaan usein suojata, koska päivityksiä näihin ei enää ole. On myös tutkittava niiden laitevalmistajien päivitysten ylläpitoa, jotka ovat tulleet juuri markkinoille. Nämä laitevalmistajat saattavat nopeastikin poistua markkinoilta, jos tuote ei ollut kannattava. Tällöin uusia päivityksiäkään ei ilmesty ja laitteesta tulee yhä haavoittuvaisempi.

Laitteiden tietoturvaongelmia tarkasteltaessa tulisi keskittyä erityisesti pyrkimykseen suojata käyttäjää verkossa. IoT-laitteiden luultavasti lisääntyessä tulee esille uusia haavoittuvuuksien muotoja, joihin varautuminen on yhä hankalampaa. Markkinoille saattaa lähivuosina tulla kokonaan uusia tuotekategorioita, joiden suojaustoiminnot ovat keskeneräisiä siksi, että mallia edellisestä vastaavasta laitteesta ei vielä ole. Käyttäjää tulisi kuitenkin aina pitää ajan tasalla omien laitteidensa toiminnoista, päivityksistä ja kaikesta sellaisesta, mikä voi hänen yksityisyyttään loukata. IoT on muuttanut pysyvästi maailmaa ja tuonut meille paljon hyötyä, mutta haasteita on edelleen ratkottavana turvallisuuden ja yksityisyyden turvaamiseksi tulevaisuudessa.

LÄHTEET

Adewale, O. S. (2004). An internet-based telemedicine system in Nigeria. *International journal of Information management*, 24(3), s. 221-234.

Ahlmeyer, M., & Chircu, A. M. (2016). Securing the Internet of Things: A review. *Issues in information Systems,* 17(4), s. 21-28.

Ali, W., Dustgeer, G., Awais, M., & Shah, M. A. (2017). IoT based smart home: Security challenges, security requirements and solutions. *In 2017 23rd International Conference on Automation and Computing (ICAC)*. s. 1-6. IEEE.

Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, s. 8-27.

Badran, H. (2019). Iot security and consumer trust. *In Proceedings of the 20th Annual International Conference on Digital Government Research*. s. 133-140.

Bassi, A. t., Bauer, M. t., Fiedler, M. t., Kramp, T. t., Kranenburg, R. v. t., Lange, S. t. & Meissner, S. t. (2013). Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model. Springer Berlin Heidelberg.

Boos, D., Guenter, H., Grote, G., & Kinder, K. (2013). Controllable accountabilities: The Internet of Things and its challenges for organisations. *Behaviour & Information Technology*, 32(5), s. 449-467.

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management*, 51, 101952. s. 1-17.

Chi, Z., Li, Y., Liu, X., Yao, Y., Zhang, Y., & Zhu, T. (2019, November). Parallel inclusive communication for connecting heterogeneous IoT devices at the edge. *In Proceedings of the 17th conference on embedded networked sensor systems.* s. 205-218.

Collin, J. & Saarelainen, A. (2016). *Teollinen internet*. Helsinki: Talentum.

Corser, G. (2017). Internet Of Things (Iot) Security Best Practices. White Paper. IEEE. s. 1-13.

CUJO AI Sentry (2021). Network Security and Device Protection. White paper. Haettu 21.11.2021 osoitteesta: https://cujo.com/resources/cujo-ai-sentry-whitepaper/

Duc, A. N., Jabangwe, R., Paul, P., & Abrahamsson, P. (2017). Security challenges in IoT development: a software engineering perspective. *In Proceedings of the XP2017 Scientific Workshops.* s. 1-5. ACM.

Folk, C., Hurley, D. C., Kaplow, W. K., & Payne, J. F. X. (2015). The security implications of the Internet of Things. AFCEA International Cyber Committee. Haettu 14.10.2021 osoitteesta: http://www.afcea.org/committees/cyber/documents/InternetofThingsFINAL.pdf

F-Secure (2021). Mikä on F-Secure SENSE? Haettu 7.11.2021 osoitteesta: https://www.f-secure.com/fi/home/products/sense

Geng, H. (2017). *Internet of things and data analytics handbook.* John Wiley & Sons. Incorporated.

Gilchrist, A. (2017). *IoT security issues* (First edition.). De G Press. Boston, [Massachusetts] ; Berlin, [Germany].

Giri, A., Dutta, S., Neogy, S., Dahal, K., & Pervez, Z. (2017). Internet of Things (IoT) a survey on architecture, enabling technologies, applications and challenges. *In Proceedings of the 1st International Conference on Internet of Things and Machine*. Learning Association for Computing Machinery, New York, NY, USA, Article 7, s. 1–12.

Hyppönen, M. (2021). *Internet*. WSOY: Helsinki.

Irmak, E., & Bozdal, M. (2018). Internet of Things (IoT): The most up-to-date challenges, architectures, emerging trends and potential opportunities. *International Journal of Computer Applications*, Volume 179, Volume 40, s. 20-27.

Kaspersky (2017.) Why IoT Security Is Important for Your Home Network. Resource Center. Haettu 20.10.2021 osoitteesta: https://www.kaspersky.com/resource-center/threats/secure-iot-devices-on-your-home-network

Kaw, J. A., Loan, N. A., Parah, S. A., Muhammad, K., Sheikh, J. A., & Bhat, G. M. (2019). A reversible and secure patient information hiding system for IoT driven e-health. *International Journal of Information Management*, 45, s. 262-275.

Kondoro, A., Dhaou, I. B., Tenhunen, H., & Mvungi, N. (2021). Real time performance analysis of secure IoT protocols for microgrid communication. *Future Generation Computer Systems*, 116, s. 1-12.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (2009). A brief history of the Internet. ACM SIGCOMM Computer Communication Review, 39(5), s. 22-31.

Li, S., Xu, L. D. & Romdhani, I. (2017). *Securing the internet of things*. Syngress: Cambridge, MA, United States.

Li, S., Tryfonas, T. and Li, H. (2016). *The Internet of Things: a security point of view. Internet Research*, Vol. 26 No. 2, s. 337-359.

Malek, Y. N., Kharbouch, A., El Khoukhi, H., Bakhouya, M., De Florio, V., El Ouadghiri, D., ... & Blondia, C. (2017). On the use of IoT and big data technologies for real-time monitoring and data processing. *Procedia computer science*, *113*, s. 429-434.

Matthews, Ruth. Mikä on esineiden internet (IoT)? NordVPN 2021. Haettu 26.9.2021 osoitteesta: https://nordvpn.com/fi/blog/mika-on-iot/

Megas, K., Cuthill, B., & Gupta, S. (2021). Establishing Confidence in IoT Device Security: How do we get there? NIST Cybersecurity white paper (draft). s. 1-28. haettu 21.10.2021 osoitteesta: https://doi.org/10.6028/NIST.CSWP.05142021-draft

Mrabet H, Belguith S, Alhomoud A, Jemai A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors*. 2020; 20(13):3625. Haettu 3.10.2021 osoitteesta: https://doi.org/10.3390/s20133625

Mustapha, H., & Alghamdi, A. M. (2018). DDoS attacks on the internet of things and their prevention methods. *In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems* (s. 1-5).

Patel, K. K., & Patel, S. M. (2016). Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing*, *6*(5), s. 6122-6132.

Rao, T. A., & Haq, E. U. (2018). Security challenges facing IoT layers and its protective measures. *International Journal of Computer Applications*, *179*(27), s. 31–35.

Rathore, M. M., Ahmad, A., Paul, A., & Thikshaja, U. K. (2016, May). Exploiting real-time big data to empower smart transportation using big graphs. In *2016 IEEE Region 10 Symposium (TENSYMP),* s. 135-139.

Reggio, G., Leotta, M., Cerioli, M., Spalazzese, R., & Alkhabbas, F. (2020). What are IoT systems for real? An experts' survey on software engineering aspects. *Internet of Things,* 12, 100313, s. 1-14.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, *88*, s. 173-190.

Rizvi, S., Kurtz, A., Pfeffer, J., & Rizvi, M. (2018, August). Securing the internet of things (IoT): A security taxonomy for IoT. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. s. 163-168. IEEE.

Salge, T. O., Cichy, P., & Kohli, R. (2021). Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars. *MIS Quarterly*. Haettu osoitteesta: https://misq.org/privacy-concerns-and-data-sharing-in-the-internet-of-things-mixed-methods-evidence-from-connected-cars.html

Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 2017.

Simpson, A. K., Roesner, F., & Kohno, T. (2017). Securing vulnerable home IoT devices with an in-hub security manager. In 2017 *IEEE International Conference on Pervasive Computing and Communications Workshops*. s. 551-556. IEEE.

Singh, D., Tripathi, G., & Jara, A. J. (2014, March). A survey of Internet-of-Things: Future vision, architecture, challenges and services. *In 2014 IEEE world forum on Internet of Things*, s. 287-292. IEEE.

Singh, J., Millard, C., Reed, C., Cobbe, J., & Crowcroft, J. (2018). Accountability in the IoT: Systems, law, and ways forward. *Computer Society*, *51*(7), s. 54-65. IEEE.

Sinha, S. (2021). State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion. *Market insights for the internet of things.* Haettu 12.10.2021 osoitteesta: https://iot-analytics.com/number-connected-iot-devices/

Suresh, P., Daniel, J. V., Parthasarathy, V., & Aswathy, R. H. (2014, November). A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. *In 2014 International conference on science engineering and management research (ICSEMR*) s. 1-8. IEEE.

Torre, I., Koceva, F., Sanchez, O. R., & Adorni, G. (2016). A framework for personal data protection in the IoT. *In 2016 11th international conference for internet technology and secured transactions (ICITST)*. s. 384-391. IEEE.

Watts, S. (2016). *The Internet of Things (IoT) : Applications, Technology, and Privacy Issues*. Nova Science Publishers.

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review,* 31(5), s. 618-627.

Weinberg, B. D., Milne, G. R., Andonova, Y. G. & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons*, 58(6), s. 615-624.

Wheelus, C., & Zhu, X. (2020). Iot network security: Threats, risks, and a data-driven defense framework. *IoT*, *1*(2), s. 259–285. Haettu 7.11.2021 osoitteesta: https://doi.org/10.3390/iot1020016

Williams, F., & Boren, S. A. (2008). The role of electronic medical record in care delivery in developing countries. *International journal of information management*, 28(6), s. 503-507.

Yang, Y., Peng, H., Li, L., & Niu., X. (2016). General theory of security and a study case in internet of things. *IEEE Internet of Things Journal*, *4*(2), s. 592-600.