Sami Jylhä

Loppukäyttäjän yksityisyys IoT-perustaisessa älykodissa

Tietotekniikan kandidaatintutkielma

29. marraskuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Sami Jylhä

Yhteystiedot: sami.j.jylha@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Loppukäyttäjän yksityisyys IoT-perustaisessa älykodissa

Title in English: Privacy of end user in IoT-based smart home

Työ: Kandidaatintutkielma

Sivumäärä: 31+0

Tiivistelmä: Älykotien tietoturva ja loppukäyttäjän yksityisyyden suojaaminen on nykyyhteiskunnassa tärkeässä asemassa Esineiden Internetin (IoT) yleistyessä ja älykodeissakin käytettävien IoT-laitteiden heterogeenisyyden kasvaessa. Tutkimuksen tavoitteena on sekä sovellustoimittajien, valmistajien että käyttäjien kannalta selvittää, millä toimintamalleilla loppukäyttäjän yksityisyyttä voidaan älykodissa vahvistaa. Varsinkin valmistajien kohdalla löytyy monia hyödyllisiä toimintamalleja, jotka olisi tärkeää standardoida yleisesti älykotijärjestelmiin. Esille tuodaan myös hyödyllisiä loppukäyttäjien toimintamalleja, joita noudattamalla heidän yksityisyytensä pysyisi paremmin turvassa.

Avainsanat: Esineiden Internet, älykoti, yksityisyys

Abstract: Information security of smart homes and protection of end user's privacy is essential in modern society while Internet of Things (IoT) is becoming more common and heterogeneity of IoT-devices used in smart homes is growing. The aim of the study is to find out how would it be possible to strengthen the privacy of end user in smart home in the point of view of application providers, manufacturers and users. Especially concerning manufacturers many beneficial procedures that would be important to standardize to smart home systems in general are discovered. Beneficial procedures for end users which would help to protect their privacy are also presented.

Keywords: Internet of Things, smart home, privacy

Kuviot

Sisällys

1 Johdanto

Tutkimus älykotien tietoturvasta ja yksityisyyden suojaamisesta on nyky-yhteiskunnassa tärkeää Esineiden Internetin (Internet of Things, IoT) yleistyessä kovaa vauhtia. Sen lisäksi, että IoT-laitteiden määrä kasvaa, myös niiden heterogeenisyys kasvaa. Laitteiden sekä niiden käyttämien ohjelmistojen ja ohjelmistoarkkitehtuurien tullessa yhä monimuotoisemmiksi, paljastuu jatkuvasti myös uusia tapoja, joilla hyökkääjät voivat käyttää hyväkseen älykotien käyttämiä järjestelmiä. IoT-teknologian heterogeenisyyden ja standardoimattomuuden vuoksi myös aivan tahattomat tietovuodot ovat mahdollisia.

Älykotien pääasiallinen tarkoitus on tehdä elämisestä helpompaa, sujuvampaa ja turvallisempaa, mikä mahdollistuu osaltaan pienten tietoa keräävien sensorien ja laitteiden avulla. Esimerkiksi kotiin asennettujen valvontakameroiden ja liiketunnistinten tarkoitus on turvata käyttäjän omaisuus, ja oikein asennettuna ja oikein käyttämällä tavoitteessa voidaan hyvinkin onnistua. Käyttäjän kannalta on oleellista, että laitteiden ja ohjelmistojen valmistaja on mahdollisimman luotettava, laitteet ovat oikein asennettu, ja ohjelmistojen päivitykset sekä asetukset ovat kunnossa. Tällöin tietoturva-aukkojen mahdollisuus onkin minimoitu, ja käyttäjän omaisuus turvattu tehokkaasti. Näin ollen älykodin käyttäjän yksityisyyttä turvatessa on otettava huomioon sekä valmistajan, että käyttäjän näkökulma. Tärkeää on myös saada valmistajan ja käyttäjän kommunikaatio toimimaan sillä tavalla, että käyttäjä osaisi käyttää älykotinsa laitteita tehokkaasti ja ennen kaikkea turvallisesti vaarantamatta yksityisyyttään. Monesti älykotiympäristössä helppouden ja sujuvuuden parantuessa turvallisuus ja yksityisyys saattaa kuitenkin kärsiä.

On huomattava, että jos älykotijärjestelmässä on tietoturva-aukkoja, niin käyttäjän yksityisyys ja pahimmassa tapauksessa omaisuus saattaa olla jopa enemmän uhattuna, kuin ilman älykotijärjestelmää. Hyökkääjä voi edetä monilla erilaisilla strategioilla, joilla hän pyrkii hyötymään uhristaan. Hyökkääjällä voi esimerkiksi olla fyysinen pääsy älykodin laitteelle ja hän voi tällä tavoin tunkeutua järjestelmään. Fyysinen pääsy laitteelle voi tapahtua joko silloin, kun laite on jo käyttäjän käytössä, mutta se voi tapahtua myös jo ennen laitteen myymistä käyttäjälle. Tällöin hyökkääjä voi hyödyntää hyökkäyksessään laitteistotroijalaista, jonka aktivoituessa laite ei enää toimikaan aivan kuten sen pitäisi. Hyökkääjä voi myös

kohdistaa hyökkäyksensä verkko- ja kuljetuskerrokseen ja kaapata dataa. Sekä salaamattomasta että salatusta datasta voi olla hyökkääjälle hyötyä. Salaamattomasta datasta saatu hyöty on yksiselitteistä, mutta myös salatun datan metadatasta saatu hyöty voi olla merkittävää. Sovelluskerroksen kautta etenevä hyökkäys voi tapahtua esimerkiksi suoraan epäluotettavan kolmannen osapuolen sovalluskehittäjän toimesta, mutta jo mobiililaitteessa valmiina oleva haittaohjelma voi aiheuttaa riskititilanteen älykotisovellusta käytettäessä, vaikka sovellus itsessään olisikin peräisin luotettavalta taholta. Todennuskerroksen kautta hyökätessään hyökkääjä voi edetä esimerkiksi asentamalla laitteeseen tai ohjelmistoon haitallisen päivityksen, jos vaikkapa ohjelmistopäivityksiä ei ole asianmukaisesti todennettu.

Tässä tutkimuksessa kartoitetaan IoT-perustaisten älykotien tuomia haasteita loppukäyttäjän (end user) tietoturvaan ja erityisesti yksityisyyteen, sekä tähdätään siihen, että laite- ja ohjelmistovalmistajat voisivat tehdä entistä turvallisempia järjestelmiä älykoteihin. Tavoitteena on siis selvittää, kuinka valmistajat voisivat kehittää tuotteensa nimenomaan käyttäjää ajatellen, ja mitä toimenpiteitä valmistajat voisivat tehdä, jotta käyttäjän teknisen ymmärryksen ja osaamisen puute ei vaikuttaisi ratkaisevasti siihen, kuinka uhattuna hänen yksityisyytensä älykodissa on.

Loppuosa tekstistä jäsentyy seuraavalla tavalla. Luvussa 2 käsitellään IoT-teknologiaa, sen roolia älykodissa, sen tietoturvan nykyistä tilaa sekä sen tuomia yksityisyyden haasteita. Luvussa 3 käsitellään kerrosteisen järjestelmäarkkitehtuurin mukaan luokiteltuna oleellisimpia seikkoja, jotka liittyvät yksityisyyden uhkien syntymiseen ja toteutumiseen IoT-perustaisessa älykodissa. Luvussa 4 käsitellään aikaisemmin esitellyn teorian pohjalta toimintamalleja, joilla loppukäyttäjän yksityisyyden uhkia voidaan eliminoida, ja niiden toteutumista ehkäistä sekä sovellustoimittajien, valmistajien että loppukäyttäjien toimesta. Lopuksi tehdään yhteenveto luvussa 5.

2 Internet of Things, älykoti ja tietoturva

Tässä luvussa käydään läpi, mitä IoT ja älykoti ovat, sekä pohditaan näiden käsitteiden suhdetta toisiinsa. Lisäksi käsittelyn keskiössä ovat IoT-tietoturvan nykyinen tila sekä erityisesti IoT:n mukanaan tuomat haasteet älykodin loppukäyttäjän yksityisyyteen.

2.1 Internet of Things

IoT on käyttöominaisuuksiltaan ja -tarkoituksiltaan erittäin monipuolinen teknologia. IoT-laitteiksi määritellään Internetiin yhdistetyt laitteet, kuten pienet sensorit ja toimilaitteet, joita voidaan ohjata tai joista voidaan kerätä dataa Internetin välityksellä (Gubbi ym. 2013). Shahin ja Yaqoobin (2016) mukaan IoT-teknologian tarkoitus on yhdistää olemassa olevia teknologian osa-alueita ja näin luoda uusi käyttökelpoinen integraatio. Näin ollen IoT ei sinänsä ole yksittäinen teknologia, ja sen konsepti voi vaihdella paljonkin riippuen käyttöympäristöstä ja tavoitteista.

IoT:n avulla voidaan helpottaa ihmisten elämää tuomalla Internet ja fyysinen maailma lähemmäksi toisiaan. Ali ja Awad (2018) kertovat, että IoT:n tavoitteena on laajentaa perinteisen Internetin toiminnallisuutta yhdistämällä siihen tietokoneiden ja älypuhelinten lisäksi myös lukuisia muita laitteita. Lisäksi he mainitsevat, että IoT:n päätavoite on tehdä laitteisiin pääsystä sekä niiden tunnistamisesta, merkitsemisestä ja hallinnasta mahdollista Internetin välityksellä milloin ja mistä vain.

IoT-teknologia yleistyy jatkuvasti valtavalla nopeudella, sillä vuonna 2012 käytössä olevia IoT-laitteita oli maailmassa noin 8,7 miljardia ja vuonna 2018 määrä oli kasvanut noin 34,8 miljardiin (Burhan ym. 2018). Määrä on näin ollen nelinkertaistunut kuudessa vuodessa. Burhan ym. (2018) arvioivat, että vuonna 2020 käytössä olevia IoT-laitteita on jo noin 50 miljardia. IoT-laitteiden hinta markkinoilla on pudonnut huomattavasti samalla, kun niiden käyttömahdollisuudet ovat monipuolistuneet muisti- ja laskentakapasiteetin kasvun seurauksena (Geneiatakis ym. 2017). Tämä voidaan nähdä merkittävänä syynä IoT:n yleistymiseen ja näin valtaisaan laitteiden määrän kasvuun.

IoT-teknologialla on runsaasti erilaisia sovelluskohteita, ja niitä löytyy lisääntyvässä määrin lähes jokaiselta elämän osa-alueelta. Sitä käytetään esimerkiksi potilaiden elintoimintojen seuraamiseen sairaaloissa, eläinten GPS-paikannukseen tai kodinkoneiden automatisointiin älykodeissa (Burhan ym. 2018). Tässä tutkimuksessa keskitytään viimeisimpänä mainittuun eli IoT-perustaisiin älykoteihin.

2.2 IoT:n rooli älykodissa

Älykodin käsitettä voidaan lähestyä useammasta suunnasta. Fabi, Spigliantini ja Corgnati (2017) esimerkiksi kertovat, että yleinen älykodin konsepti on yhdistää erilaisia sensoreita, kodinkoneita ja älylaitteita toisiinsa Internetin välityksellä, jotta pystytään valvomaan ja hallitsemaan niitä sekä päästään niihin käsiksi etäältä. Harperin (2003) näkökulma on taas hieman erilainen. Hän ajattelee älykodin olevan koti, joka on automatisoitu ja näin ollen pystyy vastaamaan asukkaiden tarpeisiin mahdollisuuksien mukaan sekä tuomaan kotiin viihtyisyyttä ja turvaa. Geneiatakis ym. (2017) määrittelevät älykodin erilaisten elementtien, kuten sensorien, yhteyksien ja sovellusten, symbioosiksi, joka synnyttää dynaamisen ja heterogeenisen arkkitehtuurin, jonka tavoitteena on tehokas laitteiden hallinta sekä edistyneiden toimintojen tarjoaminen. Näin ollen älykodille ei voida sanoa olevan yhtä ainoaa määritelmää, vaan määritelmiä on olemassa monia. Älykodit voidaan kuitenkin jakaa kahteen erilaiseen päätyyppiin, jotka ovat hubiin perustuvat sekä pilvipalveluun perustuvat älykodit (Zeng, Mare ja Roesner 2017).

IoT:n sekä älykodin konseptit ovat erittäin vahvasti yhteydessä toisiinsa. Tämä johtuu siitä, että älykoti on lupaavin IoT-teknologian sovelluskohde (Lee ym. 2014). Toisaalta IoT-teknologia on taas pääasiallinen edellytys älykotien kehittymiselle (Ali ja Awad 2018). Älykodeissa käytettävän IoT-teknologian tarkoitus on useimmiten auttaa asukkaita varmistamaan heidän hyvinvointinsa, tehostaa arkipäivän tehtävien toteuttamista sekä yleisesti ottaen tavalla tai toisella helpottaa asukkaiden elämää, ja näin ollen parantaa elämänlaatua (Laplante ja Laplante 2016; Kraijak ja Tuwanut 2015; Ali ja Awad 2018). IoT:n sovelluskohteita älykodissa ovat muunmuassa viihde-elektroniikka, turvajärjestelmät, esteettömyysratkaisut sekä valaistuksen, ilmastoinnin ja kodinkoneiden hallinta (Lee ym. 2014). Näin ollen IoT-teknologia mahdollistaa erittäin monipuolista laitteistoa älykotiin, ja sovelluskohteita on lä-

hes rajattomasti.

2.3 IoT:n tietoturvan tila

Yleisesti ottaen IoT-tietoturvan tila on erittäin huonoissa kantimissa (Ali ja Awad 2018), sillä ei ole olemassa standardeja, joita noudattamalla, pystyttäisiin suojautumaan älykoteihin kohdistuvilta hyökkäyksiltä (Zeng, Mare ja Roesner 2017). Lisäksi suurin osa IoT-laitteista on helppo hakkeroida muun muassa niiden rajoittuneiden resurssien vuoksi (Khan ja Salah 2018), josta kerrotaan tarkemmin luvussa 3.1. Tietoturvaongelmia nousee esille jatkuvasti liittyen langattomiin sensoriverkkoihin (Wireless Sensor Networks, WSN), laitteiden väliseen viestintään (Machine-to-Machine, M2M) ja kyberfysikaalisiin järjestelmiin (Cyber-Physical Systems, CPS), jotka kaikki hyödyntävät tavallista Internet-yhteyttä (IP-protokolla) tietojen välittämiseen (Khan ja Salah 2018). Tietoturvan ja yksityisyyden turvan kehittämiseen ja toteuttamiseen vaadittavat valmistajien taloudelliset resurssit vaihtelevat hyvin paljon erilaisten IoT-sovellutusten välillä (Lin ja Bergmann 2016). Tämän lisäksi vaihtelua esiintyy paljon myös käyttäjälähtöisissä resursseissa, kuten käyttäjän teknisessä osaamisessa, ja kotiympäristössä käyttäjälähtöiset ongelmat voivat olla aivan yhtä vakavia, kuin tekniset ongelmat (Lin ja Bergmann 2016).

IoT-teknologian arkkitehtuurin voi jakaa kolmeksi kerrokseksi, jotka matalimmalta korkeimmalle tasolle lueteltuna ovat fyysinen kerros, verkko- ja kuljetuskerros sekä sovelluskerros (Khan ja Salah 2018). Mainittujen kerrosten lisäksi on vielä neljäs, todennuskerros, joka liittyy kaikkiin kolmeen muuhun kerrokseen, ja kommunikoi suoraan niiden kanssa (Khan ja Salah 2018). Kaikista näistä kerroksista löytyy tietoturva-aukkoja, joista kerrotaan tarkemmin luvussa 3.

2.4 IoT:n tuomat haasteet yksityisyyteen

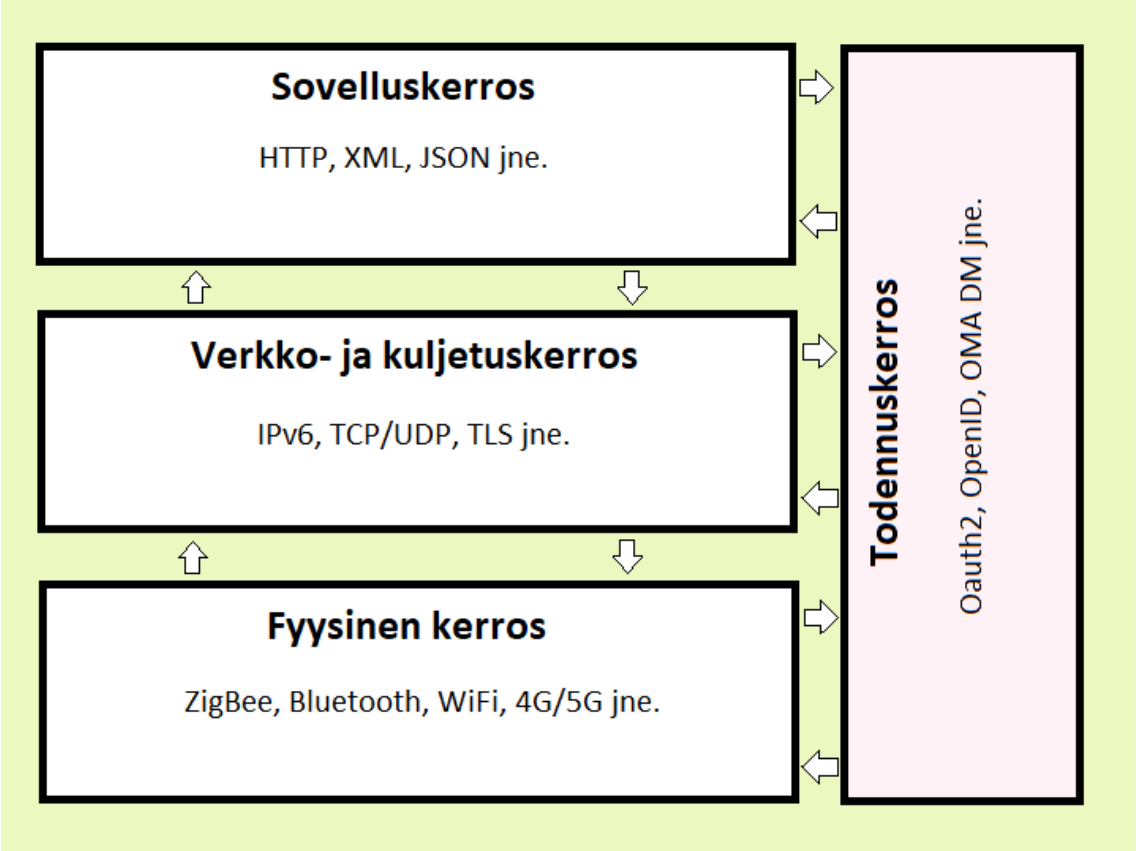
Oman kotinsa varustaminen IoT-laitteilla ei vielä nykyään ole kaikissa tapauksissa yksiselitteisen kannattavaa, sillä tuodessaan hyötyjä ja helpotusta elämään, tuo se mukanaan myös huomattavia riskejä. Bruhanin ym. (2018) mukaan suurimmat IoT:n tuomat ongelmat ja haasteet liittyvät turvallisuuteen ja yksityityyteen. Ali ja Awad (2018) kertovat, että tuotaessa

IoT-teknologiaa kotiin on tehtävä ”vaihtokauppa” sellaisten asioiden välillä, kuten sujuvuus, hallinta, turvallisuus ja yksityisyys. Se, kuinka aiheellista tämän vaihtokaupan tekeminen on, ja voittaako vai häviääkö siinä, riippuu paljon käyttäjästä. Älykodit ovat usein ad hoc -tyyppisiä luomuksia, ja useinkaan käyttäjällä ei ole tarvittavaa teknistä tietämystä ja osaamista luoda yksityisyyden ja turvallisuuden varmistamisen kannalta toimivaa ratkaisua (Lin ja Bergmann 2016). Käyttäjän tekninen tietämys ja osaaminen eivät ole kuitenkaan ainoat muuttujat yksityisyyden suojaamisen suhteen, sillä Linin ja Bergmannin (2016) mukaan älykoti ilman luotettavaa, intuitiivista ja automatisoitua järjestelmää tietoliikenteen käsittelyä varten voi aiheuttaa sen, että yksityisyys- ja turvallisuusuhat peittoavat älykodin hyödyt.

Älykodissa IoT:n vaikutus yksityisyyteen riippuu käyttäjän kyvystä hallita kompleksista ympäristöä. Lisäksi yksityisyyteen vaikuttaa IoT:n mahdollistama useiden eri tietolähteiden yhdisteleminen. Dataa voivat yhdistellä niin sovellustoimittajat, luvallisesti, kuin haavoittuvuuksia hyödyntävät hyökkääjätkin. Ali ja Awad (2018) kertovat, että yhdistämällä IoT-laitteita Internetiin luodaan uusia turvallisuus- ja yksityisyyshaasteita liittyen tietosuojaan sekä sensorien avulla kerätyn, ja yhteyksien avulla jaetun datan todentamiseen ja eheyteen. Heidän mukaansa IoT-perustaiset älykodit tarvitsevat nykyistä korkeamman tason tietoturvaratkaisuja, sillä älykotiympäristöstä on saatavilla erittäin yksityistä ja arkaluontoista tietoa käyttäjistä, ja IoT-teknologia luo uusia riskejä ollessaan haavoittuva Internetin kautta tehdyille hyökkäyksille. Jos älykoti tai jokin kodin IoT-laitteista hakkeroidaan, Bingin ym. (2011) mukaan hyökkääjällä on mahdollisuus päästä rikkomaan käyttäjän yksityisyyttä, varastamaan henkilökohtaisia tietoja sekä tarkkailemaan älykodissa asuvia henkilöitä. Fernandes, Jung ja Prakash (2016) kertovat, että kolmannen osapuolen kehittämät IoT-sovellukset ovat yleistyneet, joka omalta osaltaan tarjoaa käyttäjille mahdollisuuksia, mutta tuo mukanaan myös merkittäviä tietoturvariskejä. Näihin kolmansien osapuolten sovelluksiin liittyviin riskeihin ja niiden hallintaan perehdytään tarkemmin luvussa 4.1.

3 Yksityisyyden uhat

Tässä luvussa kartoitetaan oleellisimpia uhkia yksityisyyden suojalle älykodeissa ja jäsennetään niitä Khanin ja Salahin (2018) esittämän kerrosteisen IoT-arkkitetuurin (Kuvio 1) avulla. Arkkitehtuuri jaetaan yhteensä neljään eri kerrokseen: Fyysiseen kerrokseen, verkko- ja kuljetuskerrokseen, sovelluskerrokseen sekä todennuskerrokseen. Näin ollen tässä luvussa selitetään näiden kerrosten toimintaa sekä käydään läpi yksityisyyden uhkia nimen omaan näiden kerrosten kautta muun muassa kuhunkin kerrokseen kohdistetun esimerkkihyökkäyksen avulla.



Kuvio 1. IoT:n kerrosteinen arkkitehtuuri sekä kerroksissa yleisesti käytettäviä protokollia Khanin ja Salahin (2018) mukaan.

3.1 Fyysinen kerros

Fyysinen kerros koostuu itse IoT-laitteista sekä niiden komponenteista ja se kommunikoi sekä verkko- ja kuljetuskerroksen että todennuskerroksen kanssa. Fyysiseen kerrokseen liittyvät uhat ja haavoittuvuudet johtuvat pääsääntöisesti siitä, että IoT-laitekanta on erittäin heterogeeninen ja laitteet ovat resursseiltaan rajoittuneita. Lisäksi on mahdollista, että epäluotettavilla tahoilla, kuten asuinkumppanilla tai vierailijoilla on fyysinen pääsy laitteille. Toisaalta laitteita saatetaan jo lähtökohtaisesti ostaa epäluotettavilta tahoilta, joista kerrotaan tarkemmin luvussa 4.3. Tällöin esimerkiksi laitteistotroijalaisten uhka on olemassa.

Geneiatakiksen ym. (2017) mukaan IoT-laitekanta on hyvin heterogeeninen. Tästä johtuen kunnollisten tietoturvastandardien luominen on ollut haastavaa, eikä sellaisia ole kyetty muodostamaan. Standardien puuttuminen taas johtaa siihen, että hyökkääjät voivat löytää paljon erilaisia tietoturva-aukkoja. Laitteiden heterogeenisyyden vuoksi laitteet eivät myöskään osaa kommunikoida keskenään, joten älykodeissa on yleensä käytössä hubi, johon laitteet on yhdistetty ja jonka kautta ne voivat kommunikoida (Geneiatakis ym. 2017). Hubi on taas yhdistettynä reitittimeen, ja tätä kautta Internetiin (Geneiatakis ym. 2017). Markkinoilla olevista sensoreista suurimman osan valmiuksiin ei kuulu suora Internet-yhteys, vaan hubi on vastuussa tästä (Geneiatakis ym. 2017). Yhteys IoT-laitteen ja hubin välillä on yleensä langaton, ja yleisimmät protokollat, joita yhteyden muodostamiseen käytetään ovat Zigbee ja Z-wave (Geneiatakis ym. 2017).

IoT-laitteet ovat resursseiltaan erittäin rajoittuneita, mistä syntyy monenlaisia ongelmia. Resursseista kriittisiä ovat usemmiten laskentateho ja tallennuskapasiteetti sekä joskus myös kaistanleveys (Khan ja Salah 2018). Lisäksi laitteita ei ole välttämättä kytketty verkkovirtaan, vaan toimivat akulla tai saavat tarvitsemansa virran signaalista, ja ovat tästä syystä pakostikin rajoittuneita. Rajoittuneet resurssit aiheuttavat sen, että IoT-laitteiden välillä kulkevan tietoliikenteen salaamiseen ei voida käyttää kovinkaan raskaita salausalgoritmejä, jolloin myös salauksen pitävyys kärsii. Resursseiltaan rajoittuneille laitteille suuria ongelmia tuottavat myös esimerkiksi laitteistotroijalaiset (Hardware Trojan, HT) (Singh ym. 2017). Sekä rajoittuneisiin resursseihin, heterogeenisyyteen että tuntemattomiin valmistajiin liittyviin ongelmiin auttaa kuitenkin yhdyskäytäväarkkitehtuuri, johon syvennytään tarkemmin luvussa 4.2.

Integroitujen piirilevyjen (IC board) tarpeen lisääntyminen on pakottanut yhtiöitä ulkoistamaan erilaisten komponenttien valmistuksen halvemmille tehtaille ympäri maailmaa, mikä korottaa esimerkiksi laitteistotroijalaisten uhkaa (Sidhu, Mohd ja Hayajneh 2019). Laitteistotroijalainen on jonkin laitteen mikropiiriin pahantahtoisesti tehty muunnos (Venugopalan ja Patterson 2018). On olemassa laitteistotroijalaisia, joissa ei ole herätettä (trigger) ja jotka ovat jatkuvasti aktiivisia, mutta yleensä laitteistotroijalainen on passiivinen, eikä aiheuta harmia ennen, kuin siihen kehitetty heräte laukeaa (Venugopalan ja Patterson 2018). Tämän jälkeen laitteistotroijalainen aktivoituu ja alkaa sabotoimaan laitteen tai järjestelmän toimintaa jollakin tavalla (Venugopalan ja Patterson 2018). herätteitä on sekä sisäisiä että ulkoisia. Sisäinen heräte aktivoituu, kun järjestelmässä toteutuu tiettyjen tapahtumien kombinaatio tietyssä järjestyksessä, joten oikeanlaisen sisäisen herätteen kehittäminen vaatii hyökkääjältä hyvää tuntemusta kyseessä olevasta järjestelmästä (Venugopalan ja Patterson 2018). Sisäisen herätteen laukeamiseen voi johtaa esimerkiksi jonkin sensorin lähtö (output) tai laitteen komponentin logiikkatila (Wang, Tehranipoor ja Plusquellic 2008). Ulkoinen heräte voi aktivoitua milloin vain, kun se aktivoidaan jostain ulkoisesta lähteestä (Venugopalan ja Patterson 2018). Ulkoinen heräte voi olla esimerkiksi laitteeseen sulautettu antenni, johon tietyn signaalin lähettäminen aktivoi herätteen (Wang, Tehranipoor ja Plusquellic 2008). Ulkoinen heräte voi laueta myös I/O-porttien välityksellä, jolloin ulkoinen laite kommunikoi laitteistotroijalaisen kanssa (Jin, Kupp ja Makris 2009).

Laitteistotroijalaisella voidaan tehdä hyökkäys esimerkiksi seuraavanlaiseen Mohammedin ym. (2018) esittelemään älykotiin, joka koostuu etäluettavasta sähkömittarista sekä kodinkoneista, jotka kommunikoivat sähkömittarin kanssa. Mohammed ym. (2018) esittelevät myös kolme erilaista hyökkäystyyppiä, jotka älykodin laitteeseen, kuten kodinkoneeseen sijoitettu laitteistotroijalainen voi aiheuttaa. Nämä hyökkäystyypit ovat Excess ARQ Traffic, Denial-of-Service ja RSSI Effect. Näistä kaksi ensiksi mainittua voivat aiheuttaa verkon ylikuormittumisen, jolloin osa tärkeistä datapaketeista voi jäädä matkan varrelle. Näistä esimerkiksi Excess ARQ Traffic -hyökkäyksen toimintamalli on seuraavanlainen (Mohammed ym. 2018). Laitteistotroijalaisen saastuttama kodinkone lähettää ensin normaalina datapaketin sähkömittarille, jonka jälkeen sähkömittari lähettää kuittauksen (ACK-paketti) kodinkoneelle. Laitteistotroijalainen kuitenkin aiheuttaa sen, että kodinkone jättää tämän kuittauksen huomiotta, jonka vuoksi se lähettää toistuvasti samaa datapakettia sähkömittarille lyhyen ai-

kaa, jolloin verkko saattaa ylikuormittua. Tämän tyyppisessä hyökkäyksessä keskeistä on se, että laitteistotroijalainen asettaa kodinkoneen hyökkäystilaan vain ajoittain, jolloin ongelman havaitseminen ja sen alkuperän selvittäminen on haastavaa.

3.2 Verkko- ja kuljetuskerros

Verkko- ja kuljetuskerros kommunikoi sovelluskerroksen, fyysisen kerroksen sekä todennuskerroksen kanssa. Sen keskeinen tehtävä on huolehtia tietoliikenteestä laitteiden, sovellusten ja muiden IoT-järjestelmän komponenttien välillä. Jotta arkaluontoinen tietoliikenne pysyisi suojassa urkkijoilta, tärkeänä osana siihen kuuluu tietoliikenteen salaus sekä salausta tehostavia menetelmiä. Tietoliikenteen salaus edesauttaa myös datan eheyden säilyttämistä, joka on tietoturvan kannalta oleellista. Perinteisesti verkkoliikenteen perusteella on pystynyt päättelemään ainoastaan käyttäjien online-käyttäytymistä, mutta älykotien tapauksessa siitä pystytään päättelemään myös offline-käyttäytymistä (Apthorpe, Reisman ja Feamster 2017). Tästä syystä tietoliikenteen salaus ja sitä tehostavat menetelmät ovat entistä tärkeämpiä.

Sen lisäksi, että riskejä syntyy sen vuoksi, että laitteet keräävät käyttäjistä arkaluontoisia tietoja ja lähettävät niitä mahdollisesti epäluotettaville kolmansille osapuolille, myös ylipäätään tällaisen arkaluontoista dataa sisältävän tietoliikenteen olemassaolo voi jo paljastaa yksityistä tietoa käyttäjien tekemisistä (Apthorpe ym. 2019). Tässä viitataan datan rakenteellisiin ominaisuuksiin liittyvään tietoon, jota kutsutaan metadataksi. Se koostuu muun muassa tietoliikenteen määrästä, ajoituksesta ja kohteista. Metadata sisältää siis itse datan erinäisiä ominaisuuksia, mutta ei itse dataa. Datan salaaminen ei näin ollen yksin riitä suojaamaan käyttäjän yksityisyyttä, sillä metadatasta voi olla pahantahtoisille tahoille yllättävän suurta hyötyä. Näin ollen tietoliikenteen salauksella ei yksin saada piilotettua kaikkea toimintaa, jota käyttäjä IoT-laitteidensa välityksellä potentiaalisesti Internetin kautta lähettää.

Salatun datan metadatasta voi olla hyötyä passiivisille verkkoliikenteen tarkkailijoille, joista osa saattaa olla pahantahtoisia. Vaikka itse data olisikin salattua, ja esimerkiksi Internet-palveluntarjoajalla ei ole salauksen ansiosta pääsyä itse dataan, sillä on kuitenkin pääsy datan salattuun versioon, ja näin ollen myös metadataan (Apthorpe, Reisman ja Feamster 2017). Käyttäjän lähettämään ja vastaanottamaan dataan liittyvästä metadatasta taas voi päätellä eri-

näisiä asioita käyttäjän toimista ja esimerkiksi päivittäisistä rutiineista (Apthorpe, Reisman ja Feamster 2017).

Apthorpen, Reismanin ja Feamsterin (2017) mukaan DNS-kyselyitä (DNS-query) tarkkailemalla saadaan selville verkkotunnuksia (domain), joihin kyselyitä lähetetään. Verkkotunnuksista taas voidaan päätellä, mikä laite tai kenen valmistama laite kulloinkin dataa lähettää. Tämän jälkeen hyökkääjän helpoin tapa päätellä metadatasta käyttäjän toimia on hankkia itselleen IoT-laitteita, joita käyttäjällä älykodissaan on, ja niitä itse käyttämällä tutkia, millaista niiden lähettämä metadata on. Näin ollen hyökkääjä saa selville esimerkiksi käyttäjän rutiineja ja voi hyödyntää näitä tietoja monilla tavoilla edeten hyökkäyksessään. Esimerkiksi koneoppiminen, ja useiden laitteiden lähettämän datan käyttäminen saattaa auttaa metadatan hyödyntämisessä, kun päätellään monimutkaisempia käyttäjän toimia (Apthorpe, Reisman ja Feamster 2017). Tämä hyökkäysstrategia on mahdollinen, sillä IoT-laitteet ovat käyttötarkoitukseltaan suurimmaksi osaksi hyvin rajoittuneita, joten lähetetty data ei useinkaan ole kovin monimutkaista (Apthorpe ym. 2019). Strategia ei ole kuitenkaan taloudellisesti tehokkain, sillä hyökkääjältä kuluu rahaa laitteiden hankkimiseen. Joka tapauksessa Internet-palveluntarjoajan pystyessä päättelemään käyttäjän toimia metadatan perusteella, on se uhka käyttäjän yksityisyydelle (Apthorpe, Reisman ja Feamster 2017). Datan salaaminen ei siis itsessään suojaa tarpeeksi käyttäjän yksityisyyttä tämän kaltaisissa tilanteissa.

On olemassa keinoja, joilla metadata saadaan sellaiseksi, että hyökkääjän on sitä vaikea hyödyntää. Esimerkiksi tietoliikenteen muotoilun (traffic shaping) avulla voidaan peittää todellinen lietoliikenteen määrä ja luonne (Apthorpe, Reisman ja Feamster 2017). Tällöin metadata ei kerro datan todellisesta luonteesta merkittävästi, jolloin siitä saatavat hyödyt hyökkääjälle jäävät vähäisiksi. VPN-tunnelointi (VPN-tunneling) taas tekee yksittäisten laitteiden tunnistamisesta haastavampaa (Apthorpe, Reisman ja Feamster 2017). Traffic shapingiin syvennytään tarkemmin luvussa 4.2.

On olemassa julkisia ja täysin laillisia työkaluja, joiden käyttämisestä on hyötyä hyökkäysten toteuttamisessa. Tällaisia työkaluja ovat esimerkiksi Internet device-scanning -tyyppiset hakukoneet, kuten Shodan ja Censys. Tällaiset hakukoneet poikkeavat Googlesta ja muista tavanomaisista hakukoneista sillä tavalla, että ne eivät etsi Internet-sivuja, vaan Internetiin yhdistettyjä laitteita, kuten reitittimiä ja web-kameroita (Lin ja Bergmann 2016). Tämä

tapahtuu skannaamalla avoimia portteja protokollien kuten FTP, SSH, DNS, SIP ja RTSP avulla tavanomaisten hakukoneiden käyttämien HTTP:n ja HTTPS:n sijaan (Lin ja Bergmann 2016). Jotta hyökkääjä voi toteuttaa hyökkäyksensä, on hänen tietysti löydettävä internetiin yhdistetty laite, jota hän käyttää hyökkäyksessä hyväkseen. Esimerkiksi Shodanin avulla haavoittuvaisten laitteiden löytäminen on yllättävän helppoa. Hyökkääjän saadessa yhteys älykodin keskeisiin komponentteihin, kuten ADSL-reitittimeen, on hänellä mahdollisuus kaapata kaikki tietoliikenne, joka älykodissa yleensä käytössä olevan smart hubin ja käyttäjien välillä kulkee (Geneiatakis ym. 2017). Tietoliikenteen kaappaukseen hyökkääjä voi käyttää ohjelmia, kuten Wireshark ja Tcpdump (Geneiatakis ym. 2017). Tietoliikenteen ollessa langatonta, voi hyökkääjä käyttää laitteistoa, kuten WiFi Pineapple, jonka avulla on mahdollista väärentää (spoof) tukiasemia ja näin siepata laitteiden välinen langaton kommunikaatio (Geneiatakis ym. 2017).

3.3 Sovelluskerros

Sovelluskerros kommunikoi sekä verkko- ja kuljetuskerroksen että todennuskerroksen kanssa. Sen tarkoitus on toimia alustana IoT-järjestelmien käyttöliittymille, joiden avulla käyttäjät voivat verkko- ja kuljetuskerroksen kautta konfiguroida fyysisiä laitteita sekä ottaa vastaan niiden keräämää informaatiota.

Nykyään yleisin tapa hallita IoT-laitteita on käyttää tähän tarkoitukseen mobiilisovellusta, jollaisen lähes kaikki valmistajat tarjoavat (Geneiatakis ym. 2017). Vaihtoehtoisesti usein on käytössä myös jokin kolmannen osapuolen kehittämä sovellus. Molempiin tapauksiin liittyy riskejä, sillä tämä kolmas osapuoli saattaa olla epäluotettava, jolloin sen kehittämä sovellus mahdollisesti käyttää saamiaan oikeuksia vääriin tarkoituksiin. Toisaalta myös jo mobiililaitteessa valmiina oleva haittaohjelma voi aiheuttaa riskitilanteen sovelluksen kautta IoT-järjestelmään (Geneiatakis ym. 2017).

Sovelluskerrokseen liittyy vahvasti datan eheys ja eheyden varmistus. Datan eheyden varmistamisen tarkoitus on selvittää se, että data on lähtöisin nimenomaan oletetulta lähettäjältä ilman, että kukaan on päässyt luvattomasti muokkaamaan sitä (Pöhls 2015). Kun datan eheys on varmistettu, pystytään suojautumaan esimerkiksi man-in-the-middle -hyökkäyksiltä

(MITM-hyökkäys), joissa hyökkäjä asettuu kahden solmun välille kaappaamaan, muokkaamaan ja lähettämään dataliikennettä (Murtonen 2016). Älykotiin kohdistetussa MITM-hyökkäyksessä voidaan hyödyntää esimerkiksi haavoittuvuutta, jollainen on löydetty Google-kalenteria käyttävän Samsung RF28HMELBSR-älyjääkaapista (Cekerevac ym. 2017). Se ei vahvista SSL-varmennetta, joten MITM-hyökkäyksellä hyökkääjän on periaatteessa mahdollista saada käsiinsä loppukäyttäjän Google-tunnukset (Cekerevac ym. 2017).

3.4 Todennuskerros

Todennuskerros kommunikoi kaikkien muiden kerrosten kanssa, ja toimii eräänlaisena vartijana näiden välillä. Sen tehtävänä on varmistaa, että jokainen toimenpide muiden kerrosten välillä tapahtuu luotettavasti, ja että sellaisia toimenpiteitä ei tehdä, jotka eivät ole tulleet luotettavalta ja tunnistettavalta taholta. IoT-järjestelmässä on sen toimivan tietoturvan kannalta tavoitteena päästä päähän -todennus (end-to-end authentication). Jotta se saataisiin toteutettua vaaditaan useimmiten monivaiheinen todennus, toisin sanoen vähintään kaksivaiheinen todennus (Shivraj ym. 2015).

Mikäli todennuskerros ei toimi toivotulla tavalla, voi syntyä vaaratilanne esimerkiksi automaattisten päivitysten tullessa siihen tarkoitetun tahon sijaan pahantahtoiselta taholta. Näin ollen, jos ohjelmistopäivityksiä ei ole asianmukaisesti todennettu (authenticate), on se tietoturvauhka (Lin ja Bergmann 2016). Esimerkkinä tällaisesta uhasta on tunnettu Mirai malware -tapaus, jossa hyökkääjät pääsivät tunkeutumaan miljooniin IoT-laitteisiin, joissa oli käytössä oletussalasana (Geneiatakis ym. 2017). Tämän jälkeen näihin laitteisiin pystyttiin hyökkääjän toimesta tekemään haitallinen laiteohjelmiston päivitys, jolloin mahdollistui laitteiden käyttäminen hajautetuissa palvelunestohyökkäyksissä (Distributed Denial of Service, DDoS) (Geneiatakis ym. 2017).

4 Yksityisyyden turvaaminen

Tässä luvussa käsitellään eri tahojen kautta toimintamalleja, jotka voivat vaikuttaa joko positiivisesti tai negatiivisesti älykodin loppukäyttäjän yksityisyyden turvaamiseen. Näihin tahoihin kuuluvat erilliset sovellustoimittajat, IoT-järjestelmien valmistajat, itse käyttäjät sekä poliittiset vaikuttajat. Tässä tutkimuksessa keskitytään kolmeen ensinnä mainittuun, mutta poliittisiin vaikuttajiin ei syvennytä. Tässä luvussa esitellään näiden tahojen toimintamalleja, joita tulisi soveltaa IoT-perustaisiin älykoteihin sekä toimintamalleja, joita tulisi välttää. Näitä toimintamalleja peilataan luvussa 3 esitettyihin uhkiin sekä hyökkääjien strategioihin, toimintamalleihin ja hyökkäystyyppeihin.

4.1 Sovellustoimittajat

Sovellustoimittajat ovat oleellinen osa älykotien luomisessa, sillä sovellukset toimivat usein käyttöliittymänä älykodin toiminnoille ja toimivat näin älykotia sujuvoittavana elementtinä. Kolmannen osapuolen sovellustoimittajiin liittyy kuitenkin myös tietoturvariskejä (Fernandes ym. 2016). Näitä riskejä esiintyy erityisesti mobiililaitteiden ja näihin asennettavien sovellusten oikeuspolitiikkaan liittyen. Älykoteja varten kehitetyt älypuhelinsovelluksien käyttöoikeudet datanlähteisiin ovat nimittäin hyvin usein ylimitoitettuja (Zeng, Mare ja Roesner 2017). Tämä on huolestuttavaa, sillä hyvin usein älykodin sujuva toiminta vaatii älypuhelinsovelluksen käyttämistä.

Fernandesin ym. (2016) mukaan nämä kolmannen osapuolen kehittämät sovellukset käyttävät yleisesti älypuhelimista tuttua käyttöoikeuksienhallintakäytäntöä, jossa sovellus pyytää käyttäjältä käyttöoikeuksia tiettyyn datanlähteeseen sovelluksen ensimmäisen käynnistyksen yhteydessä (permission-based access control), mutta käyttäjä ei käyttöoikeuden antamisen jälkeen enää hallitse tästä lähteestä sovellukselle kulkeutuvaa datavirtaa. Heidän mukaansa käyttöoikeuden antamisen jälkeen on vain toivottava, ettei sovellus käytä tai kerää dataa enempää, kuin on järjestelmän toiminnan ja käyttäjän kannalta tarpeellista. Tällainen käyttöoikeuksienhallintakäytäntö on siis tietoturvaominaisuuksiltaan huono ja riittämätön (Fernandes ym. 2016). .

Eräs mahdollinen ratkaisu, joka auttaisi suojaamaan loppukäyttäjän henkilökohtaista dataa on Momenin, Bockin ja Fritschin (2020) esittämä malli, jossa mobiilisovelluksen ladatessaan ja sen käynnistäessään käyttäjältä kysyttäisiin käyttöoikeutta tiettyyn datanlähteeseen. ”kyllä”- ja ”ei”-vaihtoehtojen lisäksi tässä mallissa olisi myös vaihtoehto ”ehkä”. Käyttäjän ollessa epävarma käyttöoikeuden antamisesta datalähteeseen, hän voi valita ”ehkä”-vaihtoehdon, joka tarkoittaisi sitä, että sovellus saisi käyttöoikeuden datalähteeseen vain tietyn ajanjakson ajaksi, esimerkiksi 24 tunniksi.

Kolmansina osapuolina toimivien sovelluskehittäjien oikeuspolitiikka suhteessa laitteiden toimintoihin ja käyttäjästä saatavaan dataan ei ole nykyisen kaltaisena hyväksi käyttäjän yksityisyyden nimissä, joten tilanteeseen tulisi puuttua. Tärkeää se olisi siksi, että kolmannet osapuolet eivät pystyisi käyttämään hyväkseen näitä oikeuksia.

4.2 Valmistajat

Valmistajilla on hyvin tärkeä rooli älykotien tietoturvaan ja yksityisyyteen liittyen, sillä he voivat oikeilla keinoilla, kuten automaattisella konfiguraatiolla sekä automaattisilla päivityksillä ohjata käyttäjiä huolehtimaan paremmin yksityisyydestään. Yhtenä suurimmista haasteista valmistajilla kuitenkin on yhdistää monta erillistä puolustusstrategiaa yhdeksi käyttäjäystävälliseksi ja helposti toteutettavaksi ratkaisuksi älykodeille (Apthorpe, Reisman ja Feamster 2017). Älykodit myös kehittyvät kovaa vauhtia jatkuvan IoT:n monimuotoisuuden lisääntyessä ja uusien laitteiden tullessa markkinoille, jolloin herää kysymys siitä, onko tällainen standardisointi kovin laajamittaisesti edes toteutettavissa.

IoT-laitteiden resurssien kuten laskentatehon ja muistin rajoittuneisuuden ollessa eräs suurimmista haasteista älykotien tietoturvassa, tulisi sen aiheuttamiin ongelmiin löytää ratkaisu. Jos ongelmia ei voida suorasti ratkaista lisäämällä IoT-laitteiden resursseja, ne pitäisi ratkaista epäsuorasti esimerkiksi yhdyskäytäväarkkitehtuurin (gateway architecture) avulla, jonka on osoitettu sopivan laitteille, joiden resurssit, ovat hyvin rajalliset (Lin ja Bergmann 2016). Sen toiminta perustuu siihen, että älykodin kaikilla IoT-laitteilla on yhteinen yhdyskäytävä (Lin ja Bergmann 2016). Yhdyskäytävän resurssit ovat suuret verrattuna IoT-laitteiden resursseihin, minkä vuoksi IoT-laitteet voivat antaa paljon muistia ja laskentatehoa vaativia

tehtäviä yhdyskäytävän suoritettavaksi (Lin ja Bergmann 2016). Sen lisäksi, että yhdyskäytäväarkkitehtuuri on hyväksi resurssien rajoittuneisuuden kannalta, se auttaisi myös osaltaan ratkaisemaan IoT-laitteiden heterogeenysyyteen liittyviä ongelmia, kunhan vain kaikki älykodissa olevat IoT-laitteet asetetaan toimimaan yhdyskäytävän kautta.

Zeng, Mare ja Roesner (2017) suosittelevat käyttäjän tietoisuutta lisääviä ja ohjaavia toimia kehittäjiltä hyvän UI/UX designin avulla, joihin voisi kuulua esimerkiksi runsaasti laitteisiin asetettavia fyysisiä nappuloita ja indikaattoreita sekä vaivattomasti tarkasteltavissa olevia käyttölokeja. Tämä auttaisi tilanteeseen, jossa älykotijärjestelmään tunkeutunut hyökkääjä olisi päässyt tekemään vahingollisia toimia. Tällöin loppukäyttäjällä olisi mahdollisuus huomata nämä toimet ja reagoida tilanteeseen nopeasti, ennen kuin hyökkääjä kerkeää hyötyä tilanteesta tai aiheuttaa enempää vahinkoa.

IoT-järjestelmissä ei yleisesti ottaen voida käyttää kovin raskaita salausalgoritmejä johtuen laitteiden resurssien rajallisuudesta. Eräs IoT-laitteille lupaavaksi todettu salausalgoritmi on HLA (hybrid lightweight algorithm), sillä se määrittelee käytettävän salauksen muun muassa laitteen laskentatehon mukaan (Singh ym. 2017). Kuitenkin myös HLA:lla on haavoittuvuuksia, joita voi käyttää hyväksi hyökkäysten, kuten multi-key attack, avulla (Singh ym. 2017). Näin ollen parempia IoT-laitteille keveytensä puolesta soveltuvia salausjärjestelmiä on kehitettävä. Tietoliikenteen salauksella voidaan myös tukea aikaisemmin luvussa 3.3 käsiteltyä datan eheyden varmistamista (Pöhls 2015).

Aiemmin luvussa 3.2 mainitusta tietoliikenteen muotoilusta on hyötyä loppukäyttäjän yksityisyyden turvaamiseen. Tietoliikenteen muotoilu tarkoittaa sitä, että datan rakennetta joko hajotetaan tai homogenisoidaan, jotta metadatan analysoiminen tuottaisi mahdollisimman vähän informaatiota hyökkääjälle käyttäjän toimista. Eräs tähän tarkoitukseen tehty tietoliikenteen muotoilu -algoritmi on Apthorpen ym. (2019) kehittämä STP (stochastic traffic padding). Tämä menetelmä toimii pääpiirteittäin sillä tavalla, että aina, kun varsinaista dataa lähetetään, lähetetään myös täytedataa, jonka avulla saadaan datan kulkemisesta ulkopuolisen silmin monotonista (Apthorpe ym. 2019). Lisäksi täytedataa lähetetään sattumanvaraisina ajankohtina myös silloin, kun varsinaista dataa ei lähetetä lainkaan (Apthorpe ym. 2019). Tällöin ulkopuolinen tarkkailija ei voi olla varma, tapahtuuko oikeasti mitään merkityksellistä, kun dataa kulkee.

Hyvin toteutettuun sovelluskerrokseen liittyy vahvasti se, että käyttäjältä ei vaadittaisi erityisen laajaa tietoteknistä osaamista hänen asentaessa tai ylläpitäessä IoT-järjestelmää. Tähän tavoitteeseen tähdättäessä on pyrittävä toteuttamaan järjestelmän automaattinen käsittely. Sen kaksi tärkeintä osaa ovat järjestelmän automaattinen konfiguraatio sekä tietokone- ja laiteohjelmiston (software ja firmware) säännölliset ja automaattiset tietoturvapäivitykset (Lin ja Bergmann 2016). Järjestelmänvalvoja on vastuussa oletussalasanan vaihtamisesta välittömästi asennuksen jälkeen vahvaan salasanaan (Cobb 2012), mutta IoT-laitteiden käyttäjät eivät varsinkaan älykotiympäristössä ole aina kovin valveutuneita tietoturvan suhteen. Näin ollen valmistajien olisi tärkeää huolehtia siitä, että automaattinen konfiguraatio olisi olemassa. Tällä tavoin pystyttäisiin yksinkertaistamaan laitteiden käyttöönottoa ja ylläpitoa. Jos automaattinen konfiguraatio on laadukkaasti tehty, voidaan välttyä monilta virheiltä, joita ihminen saattaa tehdä konfiguroidessaan manuaalisesti, sillä se on hyvin toisteista ja virheherkkää toimintaa (Lin ja Bergmann 2016). Tietokoneiden ja älypuhelinten käyttöjärjestelmillä on jatkuva tuki päivityksille, ja aina tietoturvahaavoittuvuuden löytyessä pystytään se paikkaamaan päivityksellä (Lin ja Bergmann 2016). Tuki on taloudellisesti mahdollinen, sillä erilaisia käyttöjärjestelmiä on käytössä suhteellisen vähän, jolloin samaa käyttöjärjestelmää käyttävät miljoonat ihmiset. Toisin on IoT-laitteiden kohdalla, sillä niitä on olemassa satoja erilaisia monilta valmistajilta, jolloin jatkuva tuki ei ole valmistajien kannalta taloudellisesti kannattavaa (Lin ja Bergmann 2016).

IoT:n tietoturvaan ja käyttäjän yksityisyyden turvaamiseen liittyy datan eheyden tarkistaminen sekä päästä päähän todennus. Datan eheyden tarkistaminen on yleisesti ottaen mahdollista suorittaa sekä kuljetuskerroksella, esimerkiksi TLS:n (Transport Layer Security) avulla, että sovelluskerroksella esimerkiksi JSS:n (JSON Sensor Signatures) avulla (Pöhls 2015). Murtosen (2016) tekemien testien perusteella sekä TLS että JSS suojasivat täsmälleen samoilta vaaratilanteilta, mutta Pöhlsin (2015) mukaan juuri IoT-ympäristöön sovelluskerroksella toteutettu eheystarkistus on käytännöllisempi, sillä se mahdollistaa datan käsittelyn tarvittaessa ilman eheystarkistuksiakin. Lisäksi kuljetuskerroksen datan eheyden tarkistus ei ole enää datan lähettämisen jalkeen suojelemassa sitä rikkoutumiselta tai estämässä rikkoutuneen datan käyttöä (Pöhls 2015). Päästä päähän -todennukseen tulisi keskittyä, sillä Shivrajin ym. (2015) mukaan nykyisin yleisesti käytössä olevat todennuskäytännöt ovat haavoittuvaisia tietoturvauhille, ja ne vaatisivat monivaiheisen, vähintään kaksivaiheisen, todennus-

menetelmän käyttöä, jotta saavuttaisivat IoT-laitteiden ja -sovellusten välille päästä päähän -todennuksen.

4.3 Käyttäjät

Tässä luvussa käsitellään muun muassa asiantuntijoiden tiedostamia uhkia, joita käyttäjät eivät yleisesti tiedosta. Näitä ovat esimerkiksi epäluotettavat laitteet, yhtiöiden datan keräys, hyökkäykset laitteen käyttövalmiutta vastaan sekä epäluotettavat ja bugiset kolmannen osapuolen sovellukset (Zeng, Mare ja Roesner 2017). Käyttäjien vaillinainen ymmärrys teknologiasta johtaa vaillinaiseen käsitykseen uhista, ja rajoittaa tietoturvaa lisäävien tekniikoiden käyttöä. Tämä asioiden tiedostamattomuus ja huoleton käyttäytyminen taas avaa ovia hyökkääjälle. Nykyään loppukäyttäjän on mahdollista suurenevissa määrin hakea luotettavaa tietoa älykoteihin liittyen. Esimerkiksi voittoa tavoittelematon järjestö, Consumer Reports Advocacy on alkanut arvioida älykoteihin liittyviä tuotteita tietoturvan ja yksityisyyden kannalta, joka on askel oikeaan suuntaan. (Zeng, Mare ja Roesner 2017). Loppukäyttäjien tietoturvastrategioista mikään ei kuitenkaan ole standardisoitunut yleisesti vallitsevaksi strategiaksi (Zeng, Mare ja Roesner 2017).

Merkittävässä osassa loppukäyttäjien yksityisyyden turvaamiseen ovat loppukäyttäjien valmiudet joihin kuuluvat perehtyneisyys IoT-laitteisiin ja niiden käyttämiin järjestelmiin sekä tietotekniikkaan yleensäkin. Jos nämä osa-alueet eivät ole kohtuullisella tasolla, voivat käyttäjien toimintatavat älykotien asennuksessa sekä käytössä olla liian huolettomia ja huolimattomia. Tällaiset toimintatavat taas omalta osaltaan edesauttavat hyökkääjiä löytämään haavoittuvuuksia, ja parantavat heidän mahdollisuuksiaan onnistua haavoittuvuuksien hyödyntämisessä. Tärkeää olisi saada loppukäyttäjien tietämys käyttämästään tekniikasta korkeammalle tasolle, ja asiantuntijoiden tutkima tieto kulkemaan paremmin loppukäyttäjille asti.

Zengin, Maren ja Roesnerin (2017) tutkimuksessa haastateltiin viittätoista IoT-perustaisen älykodin käyttäjää. Heistä kolme ei osannut tunnistaa ainuttakaan haavoittuvuutta älykodissaan, kaksi ei osannut tunnistaa ainuttakaan potentiaalista hyökkääjää ja yksi ei osannut tunnistaa ainuttakaan potentiaalista uhkaa. Lisäksi tutkimuksessa kerrotaan, että vaikka osal-

listujat pystyivät tunnistamaan joitakin turvallisuuteen ja yksityisyyteen liittyviä ongelmia, suurin osa heistä ei ollut huolissaan kyseisistä ongelmista päivittäisessä käytössä, joka on jossain määrin huolestuttavaa. Kukaan käyttäjistä ei tunnistanut laitteen käyttövalmiuden olevan potentiaalinen hyökkäyksen kohde. Ennemminkin käyttäjät ajattelivat käyttövalmiuden liittyvän ainoastaan laitteen luotettavuuteen, eikä lainkaan tietoturvaan. Käyttäjät eivät yleensä osanneet tunnistaa potentiaalista hyökkääjää, vaan he viittasivat hyökkääjään sanalla ”joku”. Osa käyttäjistä tunnisti hallituksen tai viranomaiset mahdolliseksi viholliseksi, mutta tästäkään ei oltu kovin huolissaan. Myös uhkien tunnistamisessa oli hajontaa, sillä osa käyttäjistä ei ollut huolissaan hyökkäyksistä, koska eivät tunnistaneet itseään kiinnostavaksi hyökkäyksen kohteeksi. Esimerkiksi DDoS-hyökkääjiä ei kuitenkaan kiinnosta, keiden laitteisiin he hyökkäävät. Tästä hyvänä esimerkkinä on luvussa 3.4 käsitelty Mirai malware -tapaus.

Zengin, Maren ja Roesnerin (2017) mukaan tietoturva-asiantuntijoiden ja älykotien käyttäjien käsitysten välillä on suuri kuilu, kun kyseessä on älykotiin liittyvät tietoturvauhat. Valmistajat saavat usein esimerkiksi pilvipalveluunsa dataa käyttäjästä ja moni käyttäjä tunnistaakin tällaisen valmistajan sellaiseksi tahoksi, jolla on mahdollisuus hyökätä käyttäjää vastaan. Tästä ei kuitenkaan olla käyttäjien keskuudessa yleisesti huolissaan, joten käyttäjien luottamus valmistajaan on melko suuri. Tietoturva-asiantuntijoiden mukaan kuitenkin esimerkiksi sovelluskehittäjät ovat potentiaalisia hyökkääjiä, mikä tulisi ottaa vakavasti huomioon älykotia asennettaessa ja käytettäessä (Zeng, Mare ja Roesner 2017). Sen lisäksi, että asiantuntijoiden ja älykotien käyttäjien näkemyserot ovat suuria, Zengin, Maren ja Roesnerin (2017) tutkimuksessa käy ilmi, että myös itse käyttäjiä löytyy laajalla skaalalla liittyen heidän tekniseen osaamiseen ja käsitykseen tietoturvasta. Heidän mukaansa heikomman käsityksen omaavat saattavat luulla esimerkiksi, että asettamalla vahvan salasanan, he ovat turvassa, eikä sen suurempaa vaivaa tietoturvan eteen ole tarpeen nähdä. Tarkemman käsityksen omaavat tunnistavat kuitenkin haavoittuvuudeksi esimerkiksi sen, että iso osa datasta ei ole salattua (Zeng, Mare ja Roesner 2017).

Huomioon otettavaa on myös se, kuinka ohjelmistot saataisiin toimimaan älykotiympäristöissä, joissa on enemmän, kuin yksi käyttäjä. Usein IoT-järjestelmän asentaneella pääkäyttäjällä on suuremmat käyttöoikeudet, kuin muilla älykodin asukkailla, jonka lisäksi pääkäyttäjä on useimmiten teknisesti taitavampi ja tietää esimerkiksi järjestelmään liittyvästä tekno-

logiasta ja uhista paremmin, kuin muut talon asukkaat (Zeng, Mare ja Roesner 2017). Tällöin voi syntyä muiden talon asukkaiden yksityisyyttä loukkaavia tilanteita tahallisesti tai tahattomasti pääkäyttäjän toimesta, kuten pääsyn rajoittamista tai vakoilua (Zeng, Mare ja Roesner 2017). Tämän johdosta älykotijärjestelmä saattaa vaikuttaa kodinsisäisiin valta-asemiin. Sen vaikuttaessa tasavertaisten aikuisten välisiin valtasuhteisiin koituu se ongelmaksi, mutta esimerkiksi lapsilla ei luonnollisestikaan aina kuulu olla täysin samoja valtuuksia, kuin heidän vanhemmillaan. Zengin, Maren ja Roesnerin (2017) tutkimuksessa ilmeni, että yksi käyttäjä asui älykodissa, joka oli hänen vuokranantajansa asentama. Tällaisessa tapauksessa piilee suuria riskejä liittyen yksityisyyteen, koska se mahdollistaa esimerkiksi vuokralaisen vakoilun vuokranantajan taholta. Myös älykodissa vierailevilla henkilöillä, joilla on fyysinen pääsy laitteille on periaatteessa mahdollisuus päästä vakoilemaan älykodin asukkaita. Tämä onnistuu esimerkiksi sillä tavalla, että vierailija irrottaa laitteen alkuperäisestä älykodin hubista ja liittää sen omaan hubiinsa (Zeng, Mare ja Roesner 2017).

Käyttäjien olisi tärkeää olla perillä, mitä laitetta ollaan hankkimassa ja keneltä. Esimerkiksi erilaisista huutokauppapalveluista yksityisiltä henkilöiltä IoT-laitteen käytettynä ostamisessa on omat riskinsä. Ostettaessa laitetta muulta, kuin luotettavaksi tiedetyltä laitteiden valmistajalta tai jälleenmyyjältä, riskinä voi olla se, että laitteeseen on asennettu haittaohjelma jo ennen sen myymistä uudelle käyttäjälle (Geneiatakis ym. 2017).

Yleisiä syitä älykodin asentamiseen on fyysisen turvallisuuden lisääminen, kodin automatisoiminen ja etäohjaus (Zeng, Mare ja Roesner 2017). Näistä suurin asia, joista käyttäjät ovat huolissaan on fyysinen turvallisuus, joka on luonnollista, koska juuri siksi yleensä älykoteja luodaan (Zeng, Mare ja Roesner 2017). Vaikka laitteiden etäkäyttö/ohjaus saattaa vaarantaa tietoturvan ja yksityisyyden, se on silti käyttäjien mukaan yksi tärkeimmistä ominaisuuksista, joka älykodilta vaaditaan (Zeng, Mare ja Roesner 2017). Zengin, Maren ja Roesnerin (2017) tutkimuksessa automaatiota esiintyi kolmella eri tavalla toteutettuna: laitteen graafiselta käyttöliittymältä ohjelmoituna, kolmannen osapuolen sovelluksilla ohjelmoituna ja komentosarjoilla (script) toteutettuna. Komentosarjoilla toteutettuna käyttäjät toimivat keskenään hieman eri tavalla. Osa käyttäjistä automatisoi kotiansa kirjoittamalla itse komentosarjoja Raspberry-Pi -pohjaisille controllereille. Osa käytti muiden tekemiä komentosarjoja, joko esimerkiksi samassa asunnossa asuvan puolison kirjoittamia tai foorumeilta ladattuja.

Eräs käyttäjä sai jopa pyydettyä toiveidensa mukaisia komentosarjoja muilta, mutta tällainen toiminta saattaa aiheuttaa tietoturva-aukkoja (Zeng, Mare ja Roesner 2017). Mahdollisuuksien mukaan sovellusten ynnä muun siirtäminen pilvipalvelusta käyttäjän omaan paikalliseen hubiin toimisi tietoturvaa vahvistavana tekijänä, mutta se heikentää käytettävyyttä (Zeng, Mare ja Roesner 2017). Monet mieltävätkin älykodin eräänlaisena vaihtokauppana yksityidyyden ja sujuvuuden välillä (Zeng, Mare ja Roesner 2017).

5 Yhteenveto

Sovellustoimittajiin liittyen nykyisestä älypuhelimissa vallalla olevasta käyttöoikeuksienhallintakäytännöstä tulisi luopua, sillä se mahdollistaa hyökkääjille liian helpon kanavan käyttäjien dataan käsiksi pääsemiseen. Tilalle tulisi ottaa esimerkiksi Momenin, Bockin ja Fritschin (2020) esittämä malli, jossa käyttöoikeus datanlähteeseen on mahdollista antaa sovellukselle rajoitetuksi ajaksi.

Valmistajilla on erittäin tärkeä rooli älykotien käyttäjien yksityisyyteen liittyen, joten älykotien IoT-laitteille tulisi luoda yleisiä standardeja, joita noudattamalla tietoturva saataisiin kohtuulliselle tasolle ja voitaisiin välttää monesta suunnasta tulevia uhkia. IoT-laitteiden resurssien rajoittuneisuuden sekä niiden heterogeenisyyden ollessa eräitä suurimmista haasteista älykotien tietoturvassa, tulisi yhdyskäytäväarkkitehtuurista tehdä standardi älykodeille. Myös käyttäjän tietoisuutta lisääviä ja ohjaavia toimia hyvän UI/UX designin avulla tulisi lisätä. Niihin kuuluu esimerkiksi laitteisiin asetettavat fyysiset nappulat ja indikaattorit sekä vaivattomasti tarkasteltavissa olevat käyttölokit. Salaukseen tulisi panostaa nykyistä enemmän, ja IoT-laitteille soveltuvia keveitä salausalgoritmejä tulisi kehittää. Hyvän tietoliikenteen salauksen lisäksi tulisi huolehtia myös salatun tietoliikenteen muotoilusta esimerkiksi STP-algoritmin avulla. Myös älykotijärjestelmien automaattisesta käsittelystä olisi hyvä tehdä standardi. Varsinkin automaattinen konfiguraatio olisi mahdollista standardoida, mutta automaattisten tietoturvapäivitysten kohdalla saattaa ilmetä monilla valmistajilla taloudellisia haasteita. Datan eheyden tarkistamisesta tulisi huolehtia, ja päästä päähän -todennus tulisi toteuttaa muun muassa monivaiheisen todennusmenetelmän avulla.

Käyttäjiä ajatellen olisi tärkeää, että järjestöt, kuten Consumer Reports Advocacy saisivat enemmän näkyvyyttä, jolloin käyttäjät olisivat paremmin perillä teknologiasta, jota he käyttävät. Kun asiantuntijoiden tieto saataisiin kulkemaan loppukäyttäjille, liika huolettomuus ja tästä seuraava huolimattomuus vähenisi loppukäyttäjien keskuudessa. Käyttäjien tulisi olla perillä siitä, että laitteita ja järjestelmiä tulisi ostaa ainoastaan luotettavilta valmistajilta ja jälleenmyyjiltä. Myös asennus tulisi teettää joko luotettavalla taholla tai tehdä asennus itse, jos tietotekniset kyvyt ovat riittävän hyvät. Myös älykotia automatisoitaessa ja komentosarjoja käytettäessä käyttäjän tulisi aina olla itse perillä siitä, mitä komentosarjat tulevat tekemään,

eikä vain sokeasti luottaa siihen, että komentosarja tekee sen, mitä joku taho on sen kertonut tekevän. Mahdollisuuksien mukaan sovellusten ynnä muun siirtäminen pilvipalvelusta käyttäjän omaan paikalliseen hubiin toimisi myös tietoturvaa vahvistavana tekijänä, mutta se toisaalta heikentää käytettävyyttä.

Älykodit myös kehittyvät kovaa vauhtia jatkuvan IoT:n monimuotoisuuden lisääntyessä ja uusien laitteiden tullessa markkinoille, jolloin herää kysymys siitä, onko riittävä standardisointi kovin laajamittaisesti edes toteutettavissa. Eräs keino voisi olla poliittinen vaikuttaminen ja lainsäädäntö, jolla voitaisiin painostaa valmistajia yhtymään hyödyllisiksi todettuihin standardeihin. Myös sitä tulisi miettiä, että pitäisikö esimerkiksi internet-palveluntarjoajien kayttäjädatan keräämiseen ja käyttöön lisätä nykyistä suurempia rajoitteita, jotta pystyttäisiin turvaamaan käyttäjien yksityisyyttä. Poliittisia vaikuttajia ja lainsäädäntöä ei kuitenkaan tässä tutkimuksessa käsitelty, mutta jatkotutkimuksen kannalta se olisi tarpeellista.

Lähteet

Ali, Bako, ja Ali Ismail Awad. 2018. “Cyber and physical security vulnerability assessment for IoT-based smart homes”. *Sensors* 18 (3): 817.

Apthorpe, Noah, Danny Yuxing Huang, Dillon Reisman, Arvind Narayanan ja Nick Feamster. 2019. “Keeping the smart home private with smart (er) iot traffic shaping”. *Proceedings on Privacy Enhancing Technologies* 2019 (3): 128–148.

Apthorpe, Noah, Dillon Reisman ja Nick Feamster. 2017. “A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic”. *arXiv preprint arXiv:1705.06805.*

Bing, Kang, Liu Fu, Yun Zhuo ja Liang Yanlei. 2011. “Design of an internet of things-based smart home system”. Teoksessa *2011 2nd International Conference on Intelligent Control and Information Processing,* 2:921–924. IEEE.

Burhan, Muhammad, Rana Asif Rehman, Bilal Khan ja Byung-Seo Kim. 2018. “IoT elements, layered architectures and security issues: a comprehensive survey”. *Sensors* 18 (9): 2796.

Cekerevac, Zoran, Zdenek Dvorak, Ludmila Prigoda ja Petar Cekerevac. 2017. “Internet of things and the man-in-the-middle attacks–security and economic risks”. *MEST Journal* 5 (2): 15–25.

Cobb, M. 2012. *Password security best practices: Change passwords to passphrases. 12 June.* https://www.computerweekly.com/tip/Password-security-best-practices-Change-passwords-to-passphrases.

Fabi, Valentina, Giorgia Spigliantini ja Stefano Paolo Corgnati. 2017. “Insights on smart home concept and occupants’ interaction with building controls”. *Energy Procedia* 111:759–769.

Fernandes, Earlence, Jaeyeon Jung ja Atul Prakash. 2016. “Security analysis of emerging smart home applications”. Teoksessa *2016 IEEE Symposium on Security and Privacy (SP),* 636–654. IEEE.

Fernandes, Earlence, Justin Paupore, Amir Rahmati, Daniel Simionato, Mauro Conti ja Atul Prakash. 2016. “Flowfence: Practical data protection for emerging iot application frameworks”. Teoksessa *25th {USENIX} Security Symposium ({USENIX} Security 16),* 531–548.

Geneiatakis, Dimitris, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri ja Gianmarco Baldini. 2017. “Security and privacy issues for an IoT based smart home”. Teoksessa *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),* 1292–1297. IEEE.

Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic ja Marimuthu Palaniswami. 2013. “Internet of Things (IoT): A vision, architectural elements, and future directions”. *Future generation computer systems* 29 (7): 1645–1660.

Harper, Richard. 2003. “Inside the Smart Home: Ideas, Possibilities and Methods”. Teoksessa *Inside the Smart Home,* toimittanut Richard Harper, 1–13. London: Springer London. ISBN: 978-1-85233-854-1. https://doi.org/10.1007/1-85233-854-7_1. https://doi.org/10.1007/1-85233-854-7_1.

Jin, Yier, Nathan Kupp ja Yiorgos Makris. 2009. “Experiences in hardware Trojan design and implementation”. Teoksessa *2009 IEEE International Workshop on Hardware-Oriented Security and Trust,* 50–57. IEEE.

Khan, Minhaj Ahmad, ja Khaled Salah. 2018. “IoT security: Review, blockchain solutions, and open challenges”. *Future Generation Computer Systems* 82:395–411.

Kraijak, Surapon, ja Panwit Tuwanut. 2015. “A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends”. Teoksessa *11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015).* IET.

Laplante, Phillip A, ja Nancy Laplante. 2016. “The internet of things in healthcare: Potential applications and challenges”. *It Professional* 18 (3): 2–4.

Lee, Changmin, Luca Zappaterra, Kwanghee Choi ja Hyeong-Ah Choi. 2014. “Securing smart home: Technologies, security challenges, and security requirements”. Teoksessa *2014 IEEE Conference on Communications and Network Security,* 67–72. IEEE.

Lin, Huichen, ja Neil W Bergmann. 2016. “IoT privacy and security challenges for smart home environments”. *Information* 7 (3): 44.

Mohammed, Hawzhin, Jimmy Howell, Syed Rafay Hasan, Nan Guo, Faiq Khalid ja Omar Elkeelany. 2018. “Hardware trojan based security issues in home area network: A testbed setup”. Teoksessa *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS),* 972–975. IEEE.

Momen, Nurul, Sven Bock ja Lothar Fritsch. 2020. “Accept - Maybe - Decline: Introducing Partial Consent for the Permission-Based Access Control Model of Android”. Teoksessa *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies,* 71–80. SACMAT ’20. Barcelona, Spain: Association for Computing Machinery. ISBN: 9781450375689. https://doi.org/10.1145/3381991.3395603. https://doi.org/10.1145/3381991.3395603.

Murtonen, Henri. 2016. “Datan eheyden varmistaminen IoT-ympäristössä ja siitä johtuvat tietoturvavaikutukset”, https://jyx.jyu.fi/bitstream/handle/123456789/52455/1/URN%5C%3ANBN%5C%3Afi%5C%3Ajyu-201612195173.pdf.

Pöhls, Henrich C. 2015. “JSON Sensor Signatures (JSS): end-to-end integrity protection from constrained device to IoT application”. Teoksessa *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing,* 306–312. IEEE.

Shah, Sajjad Hussain, ja Ilyas Yaqoob. 2016. “A survey: Internet of Things (IOT) technologies, applications and challenges”. Teoksessa *2016 IEEE Smart Energy Grid Engineering (SEGE),* 381–385. IEEE.

Shivraj, VL, MA Rajan, Meena Singh ja P Balamuralidhar. 2015. “One time password authentication scheme based on elliptic curves for Internet of Things (IoT)”. Teoksessa *2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW),* 1–6. IEEE.

Sidhu, Simranjeet, Bassam J Mohd ja Thaier Hayajneh. 2019. “Hardware security in IoT devices with emphasis on hardware Trojans”. *Journal of Sensor and Actuator Networks* 8 (3): 42.

Singh, Saurabh, Pradip Kumar Sharma, Seo Yeon Moon ja Jong Hyuk Park. 2017. “Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions”. *Journal of Ambient Intelligence and Humanized Computing,* 1–18.

Wang, Xiaoxiao, Mohammad Tehranipoor ja Jim Plusquellic. 2008. “Detecting malicious inclusions in secure hardware: Challenges and solutions”. Teoksessa *2008 IEEE International Workshop on Hardware-Oriented Security and Trust,* 15–19. IEEE.

Venugopalan, Vivek, ja Cameron D Patterson. 2018. “Surveying the hardware trojan threat landscape for the internet-of-things”. *Journal of Hardware and Systems Security* 2 (2): 131–141.

Zeng, Eric, Shrirang Mare ja Franziska Roesner. 2017. “End user security and privacy concerns with smart homes”. Teoksessa *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017),* 65–80.