Lauri Pimiä

Yksityisyys ja siihen kohdistuvat uhat sekä haasteet IoT-perusteisissa älykodeissa

Tietotekniikan kandidaatintutkielma

30. huhtikuuta 2019

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Lauri Pimiä

Yhteystiedot: lailpimi@student.jyu.fi

Työn nimi: Yksityisyys ja siihen kohdistuvat uhat sekä haasteet IoT-perusteisissa älykodeissa

Title in English: Cybersecurity threats and challenges on privacy in IoT-based smart homes

Työ: Kandidaatintutkielma

Sivumäärä: 26+0

Tiivistelmä: Tutkielmassa perehdytään IoT-perusteisten älykotien tietoturvauhkiiin ja haasteisiin yksilön yksityisyyden näkökulmasta. IoT-älykoti on järjestelmä, joka käyttää useita erilaisia IoT-laitteita toimintojensa suorittamiseen. Tämä useiden heterogeenisten laitteiden määrä aiheuttaa kuitenkin tietoturvauhkia, jotka omassa kodissa ovat varsinkin yksityisyyden kannalta merkittäviä. Tässä tutkielmassa pyritään tunnistamaan näitä uhkia ja haasteita sekä tutustutaan mahdollisiin ratkaisuihin.

Avainsanat: Esineiden internet, Älykoti, Yksityisyys

Abstract: In this thesis we explore different cybersecurity threats and challenges of IoT-based smart homes from the perspective of individual's privacy. IoT-based smart home is a system which uses a group of different IoT devices to perform its functions. However, the number of multiple heterogeneous devices poses security threats which in your own home are especially important concerning privacy. This thesis aims to identify these threats and challenges and to explore possible solutions to them.

Keywords: Internet of Things, Smart home, Privacy

Sisältö

1 Johdanto

Esineiden internetin räjähdysmäisen kasvun jatkuessa yhä useammasta kodista on tulossa niin sanottu älykoti. Älykodeilla on useita määritelmiä, mutta pääsääntöisesti älykoti määritellään järjestelmäksi, jonka tarkoitus on pyrkiä parantamaan elämänlaatua sekä säästämään energiaa.

Tämän hetken älykodit voidaan pääasiassa jakaa raa'asti kahteen ryhmään: valmiiksi rakennettuihin ja jälkikäteen muokattuihin. Valmiiksi rakennetuissa älykodeissa on yleensä syvempi integraatio ja nämä talot voivat älykkäästi esimerkiksi lähettää sähköä takaisin verkkoon, kun sitä ei tarvita. Jälkikäteen muokatut sen sijaan ovat yleisempi ja huomattavasti halvempi ratkaisu, joka toteutetaan useimmiten ostamalla jokin ei niin integroitu valmis laite, kuten esimerkiksi älykaiutin, älyvalot tai älytermostaatti. Nämä laitteet ovat niin sanottuja IoT-laitteita eli jokapäiväisiä tavallisia laitteita, joihin on sisäänrakennettu laskentakapasiteettia ja jokin tapa kommunikoida muiden laitteiden kanssa.

Tavallisten laitteiden yhdistäminen verkkoon avaa kuitenkin suuren määrän erilaisia tietoturvauhkia. Nämä uhat korostuvat varsinkin älykoti-ympäristössä johon on nyt saatavilla enemmän laitteita kuin koskaan aikaisemmin ja näiden laitteiden välisellä turvallisuudella voi olla merkittäviä eroja (Ali ym. 2017). Suurimpiin uhkiin kuuluvat varsinkin henkilön yksityisyyteen kohdistuvat uhat, sillä monet älykoti-laitteet valvovat ympäristöään jatkuvasti ja suuri osa tästä datasta käsitellään jonkin kaltaisessa pilvipalvelussa kuten Amazon AWS, IBM Watson, Microsoft Azure tai Samsung SmartThings (Doan ym. 2018).

Tässä tutkielmassa käsitellään älykodin IoT-laitteiden mahdollistamia turvallisuusuhkia ja haasteita varsinkin yksilön yksityisyyden kannalta. Lisäksi perehdytään ratkaisuihin, joilla näitä uhkia voitaisiin lieventää tai korjata. Esineiden internetin laitteiden turvallisuusongelmista löytyy jo paljon tutkimusta, mutta erityisesti älykoteihin kohdistuvista uhista on vähemmän tutkimusta. Myös yksilön yksityisyys on ajankohtainen puheenaihe, sillä henkilöstä ei koskaan ole pyritty keräämään yhtä paljon dataa. Tämä korostuu varsinkin älykodissa, jossa melkein kaikki data voidaan lähettää jonkin yrityksen käsiteltäväksi.

Tässä tutkielmassa pyritään kuitenkin pysymään uhissa, jotka voidaan Suomen lain mukaan

luokitella rikolliseksi. Esimerkiksi yritysten keräämää dataa ei välttämättä lasketa rikolliseksi toiminnaksi, mutta jos sama data päätyisi yrityksen kautta helposti rikollisten käsiin, olisi yritys myös uhka.

Tutkielma koostuu johdannosta, neljästä eri osiota käsittelevästä luvusta ja yhteenvedosta. Ensimmäisessä osiossa selitetään, mitä IoT-perustaisella älykodilla tarkoitetaan ja mitkä ovat sen keskeiset toimintamallit. Lisäksi tarkastellaan erilaisia älykodin arkkitehtuureita. Seuraavassa osiossa keskitytään turvallisuushaasteisiin, josta siirrytään sitten yleisimpiin turvallisuusuhkiin. Viimeisessä osiossa tarkastellaan erilaisia ratkaisuja edellä mainituissa luvuissa esitettyihin uhkiin.

2 IoT-perusteinen älykoti

Älykodille on useita erilaisia määritelmiä. Esimerkiksi Schiefer (2015) tiivistää älykoti-ekosysteemin määritelmän väljästi kahteen virkkeeseen: ”Älykoti-laite on esine, jonka päätoiminnallisuus on laajennettu verkostointiominaisuuksilla uuden laitteen luomiseksi. Ylimääräinen infrastruktuuri näille laitteille, kuten tukikohta tai ohjauskeskus kuuluvat myös älykotiin” (Schiefer 2015, oma suomennos). Bugeja, Jacobsson ja Davidsson (2016) sen sijaan määrittelevät älykodin asuntona, joka mukautuu käyttäjän tarpeiden mukaisesti erilaisten sensoreiden ja laitteiden avulla.

Älykodin toimintamallit voidaan jakaa neljään eri osa-alueeseen, jotka ovat viihde, energia, turvallisuus ja terveys. Myös Holroyd, Watten ja Newbury (2010) jakavat älykodin hyödyt samankaltaisiin kategorioihin (energiansäästö, käyttäjäkokemus, turvallisuus ja vanhojen ja vammautuneiden henkilöiden tukeminen).

Ensimmäisellä osa-alueella tarkoitetaan toimintojen personalisoimista käyttäjän mukaan. Näytetään esimerkiksi viihdettä, jota käyttäjä voisi halutessaan katsoa sekä muokataan esimerkiksi lämpötilaa tai valaistusta käyttäjän toiminnan mukaan.

Toisella osa-alueella tarkoitetaan energian säästämistä ja mahdollisimman suuren hyötysuhteen saavuttamista esimerkiksi lämpötilan laskemisella, kun käyttäjä ei ole kotona. Mikäli sähköä tuotetaan omavaraisesti ylimääräistä, voidaan ylimääräinen sähkö palauttaa takaisin verkkoon.

Kolmas osa-alue eli turvallisuus tarkoittaa yleisten turvallisuuselementtien kuten hälytysjärjestelmien integrointia Esineiden internettiin. Näillä tarkoitetaan esimerkiksi valvontakameroita ja ovisensoreita. Käyttäjä pystyy myös seuraamaan järjestelmän tilaa esimerkiksi älypuhelimellaan.

Neljännellä ja viimeisellä osa-alueella tarkoitetaan käyttäjän terveyttä seuraavien laitteiden integroimista älykotiin. Tämän kaltaisia laitteita voisivat olla esimerkiksi sykemittarit, älyrannekkeet ja kuntopyörät. Kidd ym. (1999) arvioivat jo vuonna 1999, että yksi suurimmista älykodin hyödyistä voisi olla eläkeikäisten tukeminen. Terveyden valvomisessa on kuiten-

kin huonotkin puolensa ja Bugeja, Jacobsson ja Davidsson (2016) argumentoivatkin, että terveyden osalla on suurimmat riskit käyttäjän yksityisyyden kannalta.

2.1 IoT-älykodin arkkitehtuuri

IoT-perusteisen älykodin arkkitehtuuri voidaan jakaa sekä ulkoiseen että sisäiseen ympäristöön (Ali ym. 2017). Ulkoiseen ympäristöön kuuluvat esimerkiksi älykkään sähköverkon toiminnot, kun taas sisäiseen kuuluvat kaikki älykodin laitteet ja järjestelmät. Samaa jaottelua voidaan käyttää myös uhkien määrittämiseen, jossa älykodin sisäiset uhat tulevat älykodin sisältä eli toisin sanoen sisäverkosta ja ulkoiset uhat älykodin ulkopuolelta eli ulkoverkosta.

Kodin sisäinen arkkitehtuuri voidaan määritellä ”ikään kuin usean heterogeenisen laitteen symbioosiksi” (Geneiatakis ym. 2017, oma suomennos). Koska IoT-laitteilla ei vielä ole kovin vahvoja standardeja yhteistoiminnan takaamiseksi, vaativat ne yleensä jonkin kolmannen laitteen tietojen käsittelyyn ja siirtämiseen internetiin. Tämänkaltainen keskuslaite varmistaa, että laitteet pysyvät erossa toisistaan ja ulkoverkosta sekä mahdollistaa yhteyden pilvipalveluun jokaiselle laitteelle. Malli on myös hyödyllinen siksi, että se pystyy standardoimaan ulospäin vietävän datan eri sensoreilta.

Tämänkaltainen laite-keskuslaite-pilvi toimintaperiaate onkin yksi yleisimmistä älykodin arkkitehtuureista, jota kutsutaan usein myös Gateway-malliksi (Mocrii, Chen ja Musilek 2018). Erilaiset arkkitehtuurit syntyvät erilaisten vaatimusten perusteella, jonka vuoksi tähän malliin menevistä erilaisista toteutuksista löytyy varsin paljon aikaisempaa tutkimusta.

Yksi toteutus Gateway-mallista on esimerkiksi Jie ym. (2013) kehittämä viiden tason malli. Tässä mallissa pyritään maksimoimaan käytettävyys ja yhteensopivuus luomalla jokaiselle laitteelle oma samankaltainen rajapinta, jonka kautta tietoa siirretään. Jie ym. (2013) jakavat mallin viiteen eri tasoon, jotka ovat:

- Resurssitaso. Tähän kuuluvat erilaiset laitteet ja sensorit
- Rajapintataso. Tämä tarjoaa laitekohtaiset rajapinnat.
- Käsittelijätaso. Jokaisella laitteella on oma käsittelijä, joka voi sitten kommunikoida toisten laitteiden kanssa erilaisten tehtävien suorittamiseksi.

- Ydintaso, joka on yksi tärkeimmistä tasoista. Sen tehtävänä on ohjata käsittelijöitä, siirtää dataa, hoitaa tunnistaminen ja valtuudet sekä monitoroida koko järjestelmän tilaa.
- Käyttäjätaso. Ylin taso, johon kuuluu käyttäjän toiminnot kuten käyttöliittymä.

Edellä mainitussa toteutuksessa keskuslaite hoitaa siis ainakin rajapinta-, käsittelijä- ja ydintason toiminnot. Koska käsittelijätasolla toimivat käsittelijät voivat kommunikoida jokaisen järjestelmässä olevan laitteen kanssa, voidaan järjestelmästä poistaa laitteita tai lisätä uusia laitteita hyvinkin vaivattomasti.

Kaikki toteutukset eivät kuitenkaan seuraa täysin sensori-keskuslaite-pilvi mallia. Soliman ym. (2013) kehittämässä arkkitehtuurissa sensoreilla ja laitteilla on omat mikro-ohjaimet, jotka mahdollistavat suoran yhteyden pilvipalveluihin ilman erillistä laitetta. Pilveen lähetettävä data ei ole raakaa, vaan se prosessoidaan jo osittain datan keränneen sensorin mikro-ohjaimessa. Data voidaan myös tallentaa erilliseen keskuslaitteeseen, jossa datalle voidaan tehdä lisää käsittelyä ennen pilveen lähettämistä. Keskuslaitteen ja pilven välillä toimii erillinen rajapinta, jonka avulla voidaan myös vastaanottaa käyttäjän käyttöliittymästä käsin antamia komentoja.

Edellä mainitussa toteutuksessa käytetään hyödyksi niin sanottua Fog-pilviparadigmaa. Koska dataa voidaan prosessoida ja analysoida myös ilman pilvipalveluita, laskee riippuvuus pilveen ja näin parantaa käyttäjän yksityisyyden suojaa. Toisaalta, koska kaikki laitteet voivat nyt olla yhteydessä ulkoverkkoon, aukeaa mahdolliselle hyökkääjälle useampia hyökkäysvektoreita. Tässä toteutuksessa käytetty esiprosessointi on myös tärkeää pilven suorituskyvyn kannalta, jonka ongelmiin tutustutaan seuraavassa luvussa.

2.2 Pilvipalvelut

B. L. R. Stojkoska ja K. V. Trivodaliev (2017) toteavat pilvipalveluiden olevan yksi älykodin monimutkaisimmista osista. Pilvessä toteutettu datan käsittely on käyttäjälle helppoa sekä mahdollistaa dataan käsiksi pääsyn melkein mistä tahansa. Tämä on toisaalta yksi syy, miksi datan säilöminen pilvessä voisi olla käyttäjän tietoturvan kannalta vaarallista. Koska kerättävän ja prosessoitavan datan määrä on yhä kasvussa, tulee pilvipalveluiden jatkuvasti kehittää

uusia toimintatapoja vaatimusten täyttämiseksi. Varsinkin koneoppiminen ja kehittyneet analysointialgoritmit ovat tarpeellisia resurssipulan ratkaisemiseksi (B. L. R. Stojkoska ja K. V. Trivodaliev 2017).

Pilvessä data tulisi prosessoida tilannekohtaisesta kyseltävään muotoon (B. L. R. Stojkoska ja K. V. Trivodaliev 2017). Tällä tarkoitetaan, että vastaanotetusta datasta erotellaan erilaisiin ryhmiin kuuluvat osat, kuten tapahtuma-aika ja mitä tapahtui. Näitä ryhmiä voidaan sitten helposti yhdistää toisiin ryhmiin tai luoda kokonaan uusia ryhmityksiä. Tämä ryhmittely tehostaa ja yksinkertaistaa datan hakemista pilvestä, kun voidaan lähettää vain tarpeellinen tieto.

Toinen ratkaisu pilvipalveluiden resurssipulaan ovat erilaiset laskentaparadigmat. Tällaisia ovat mallit kuten Fog tai Edge, joiden tarkoitus on siirtää laskentaa pois pilvestä. Näihin kahteen laskentamalliin tutustutaan tarkemmin seuraavissa luvuissa.

2.2.1 Fog-pilvilaskenta

”Fog” tai ”sumu” on yksi pilvilaskentaparadigma, jonka avulla pyritään vähentämään pilven resurssitaakkaa (B. L. R. Stojkoska ja K. V. Trivodaliev 2017). Tässä paradigmassa oletetaan, että dataa on jo alettu prosessoimaan ja ryhmittelemään ennen pilveen saapumista.

Datan prosessoiminen lähellä luojaa (eli laitetta joka datan on kerännyt) on halvempaa kuin pilvessä laskeminen ja vähentää lisäksi merkittävästi energiankulutusta (B. R. Stojkoska ja K. Trivodaliev 2017). Koska dataa prosessoidaan vähemmän pilvessä, on se myös käyttäjän yksityisyyden kannalta turvallisempaa. Näin lähetettävän datan määrä vähenee myös IoT-laitteiden välillä, joka parantaa suorituskykyä varsinkin langattomissa verkoissa. Datan määrää pyritään myös vähentämään esimerkiksi datan kompressoimisella ja ennustamisella (Risteska Stojkoska 2012).

2.2.2 Edge-pilvilaskenta

”Edge” on toinen pilvilaskentaparadigma, joka on tavoitteiltaan hyvin samankaltainen kuin Fog. Edgen tarkoituksena on pilven resurssitaakan vähentämisen lisäksi myös anonymisoida

pilveen lähetettävää dataa. Näin yksilön yksityisyydensuojaa voidaan parantaa, kun pelkkää dataa ei voida kohdentaa suoraan käyttäjään (Garcia Lopez ym. 2015).

Edgessä laskentaa suoritetaan vielä enemmän datan luojan lähellä, jonka lisäksi jokaisella laitteella on myös kyky päättää, tulisiko kerätty data säilöä pilvessä vai ainoastaan paikallisena kopiona. Garcia Lopez ym. (2015) argumentoivat myös, että koska jokainen laite on kykenevä tekemään päätöksiä datasta, on järjestelmä nyt hajautetumpi, jolloin järjestelmän luotettavuus paranee. Järjestelmä voisi jopa toimia ilman pilveä, mikäli tarpeeksi laskentaa saadaan hajautettua laitteiden välillä. Edgen hyötyihin palataan myöhemmin, kun tutkitaan ratkaisuja tietoturvauhkiin.

3 Yksityisyys ja sen haasteet IoT-älykodeissa

Tietoturvaongelmat ovat yksi älykodin suurimmista haasteista, jonka vuoksi uhkien tunnistaminen on oleellista (B. L. R. Stojkoska ja K. V. Trivodaliev 2017). Tässä luvussa käymme läpi erilaisia haasteita ja turvallisuustavoitteita yksityisyyden näkökulmasta. Käymme myös yksityisyyttä läpi älykodin käyttäjän näkökulmasta.

3.1 Yksityisyys käyttäjän näkökulmasta

Vaikka yksityisyyden varmistaminen onkin yksi IoT-perusteisten älykotien suurimmista haasteista, on monille asiakkaille usein tärkeämpää, että järjestelmä toimii hyvin. Tutkimuksessaan Zheng ym. (2018) havaitsivat, että käyttömukavuus sekä helppokäyttöisyys olivat suurimpia prioriteetteja älykotien omistajille. Järjestelmän toimivuudella oli suora yhteys siihen, miten huolissaan asiakkaat olivat siitä kuka dataan pääsisi käsiksi tai miten data kulki järjestelmässä.

Käyttäjien mielipiteet siitä, kuka saisi hallita älykodista kerättyä dataa riippui siitä, olisiko tästä käyttäjälle mahdollista hyötyä. Varsinkin internet-palveluntarjoajiin luotettiin todella vähän, koska tutkimuksen osallistujat eivät nähneet internet-palveluntarjoajien voivan tuottaa mitään näkyviä etuja. Sen sijaan järjestelmän valmistajille, jotka tuottivat sovelluspäivityksiä, oltiin dataa luovuttamassa paljon helpommin.

Kenties paljon huolestuttavampaa oli, että monet asiakkaat olivat skeptisiä yksityisyysriskeistä mikäli älykoti ei nauhoittanut ääntä tai videota. Tämä on ongelma, sillä esimerkiksi älytermostaateista tai älyvaloista pystytään erilaisten algoritmien avulla keräämään monenlaista dataa. Tähän dataan kuuluvat esimerkiksi, onko käyttäjä kotona, mikä hänen päivärytminsä on tai jopa minkälainen hänen unenlaatunsa on (Srinivasan, Stankovic ja Whitehouse 2008).

3.2 Tietoturvan tavoitteita yksityisyyden kannalta

Tietoturvasta on usein mahdotonta tehdä täydellinen, mutta sille voidaan asettaa tavoitteita suurimpien uhkien torjumiseksi. Omassa katsauksessaan Ali ym. (2017) jakoivat älykodin tietoturvan tavoitteet viiteen osa-alueeseen:

- Autentikointi. Pyritään varmentamaan laitteet joiden välillä kommunikoidaan sekä mihin todennetulla käyttäjällä on oikeudet ja mihin ei.
- Valtuutus. Asetetaan käyttäjille oikeanlaiset valtuudet. Tällä tarkoitetaan, että valtuuksia ei saa olla liikaa tai liian vähän. Pyritään asettamaan niin, että kukin käyttäjä pystyy hyödyntämään ominaisuuksia niin paljon kuin turvallista.
- Luottamuksellisuus. Varmistetaan, että vain valtuutetut henkilöt pääsevät käsiksi yksityiseen dataan. Tämä on yksi tärkeimmistä tavoitteista yksityisyyden kannalta.
- Integraatio. Varmistetaan, että kerättyä dataa pystytään käyttämään sujuvasti eri tietokantojen ja laitteiden välillä ilman että dataa katoaa, tai sitä pystytään keräämään luvattomasti.
- Saatavuus. Varmistetaan, että jokaiselle valtuutetulle käyttäjälle on aina saatavilla kaikki mahdolliset ominaisuudet. Eli järjestelmät pysyvät ylhäällä, vaikka kohdattaisiin hyökkäys.

Kuten edellä nähdään, on suurin osa tavoitteista valtuuttamiseen ja salaukseen liittyviä. Oikeanlainen valtuutus on erityisen tärkeää varsinkin älykodeissa, koska pilven vuoksi dataan voidaan päästä käsiksi mistä tahansa.

Valitettavasti IoT-laitteilla on usein rajoitteita, jotka voivat hankaloittaa näihin tavoitteisiin pääsyä. Esimerkiksi heikko laskentakapasiteetti voi estää vahvemman salauksen käyttämisen, jonka vuoksi data voi liikkua laitteiden välillä jopa salaamattomana.

3.3 Tietoturvan haasteita yksityisyyden kannalta

IoT-perusteiset älykodit koostuvat usein joukosta erilaisia langattomia laitteita. Laitteiden langattomuus tekee muutoksista helpompaa, mutta avaa uusia haasteita ollessaan turvattomampi kuin vastaava kaapelilla kytketty laite. Bugeja, Jacobsson ja Davidsson (2016) jaka-

vat IoT-perusteisen älykodin suojaamisen haasteet kolmeen ryhmään, jotka ovat:

- Laitteiden haasteet
- Kommunikoinnin haasteet
- Palveluiden ylläpidon haasteet

Laitetasolla suurimpiin haasteisiin kuuluvat IoT-laitteille ominainen laskentakapasiteetin vähyys. Tämä on suurempi ongelma varsinkin pelkissä sensoreissa, jotka usein toimivat vähäisellä virralla, tehden laskentakapasiteetista niin vähäisen, että salaus ei aina ole mahdollinen. Tässä tapauksessa mahdollinen hyökkääjä voisi poimia datan eri laitteiden väliltä hyvinkin helposti. Toinen yksityisyyden kannalta merkittävä seikka on, että laitteita käytetään usein jonkin toisen laitteen läpi. Tämä tarkoittaa, että ei voida varmasti tietää mitä dataa laitteelle kuljetetaan, tai onko komentojen joukossa jotain mitä ei pitäisi olla.

Kommunikointi on varsinkin IoT-älykotien ongelma verrattuna tavallisiin älykoteihin. Laitteiden langattomuus luo verkon erilaisia laitteita erilaisilla protokollilla, jotka pitää heterogeenisuudestaan huolimatta saada toimimaan yhdessä. Bugeja, Jacobsson ja Davidsson (2016) argumentoivat, että tämä standardien puute aiheuttaa usein vahvemmista suojauksista luopumisen suuremman yhteensopivuuden saavuttamiseksi. Kun otetaan huomioon, että salaus voi olla jo laitteen heikon laskentakapasiteetin vuoksi huono, ovat heikosti salatut langattomat tiedonsiirrot hyvä kohde mahdolliselle salakuunteluhyökkäykselle. Tähän yksityisyyden kannalta vaaralliseen hyökkäystyyppiin palataan myöhemmin luvussa 4.1.

Palveluiden ylläpito on myös merkittävä tekijä laitteiden pitkäikäisyyden kannalta. Vaikka laite olisi ostettaessa turvallinen, ei se välttämättä ole sitä enää muutaman kuukauden päästä. Ilman turvallisuuspäivityksiä laitteet voivat muuttua turvattomiksi, mikä on suurempi uhka varsinkin laitteissa, joiden on tarkoitus toimia useita vuosia ilman mitään muutoksia. Esimerkki tällaisesta laitteesta on älytermostaatti, joita asiakkaat eivät luvussa 3.1 mainitusti näe kovin suurena yksityisyysuhkana. Asiakas ei välttämättä koskaan tule edes ajatelleeksi, että joku voi kerätä hänestä dataa laitteen kautta, joka oli turvallinen vielä puoli vuotta sitten.

Lee ja Zappaterra (2014) havaitsivat tutkimuksessaan samankaltaisia haasteita IoT-älykodille. Heidän mukaansa yksi haaste tulee myös siitä, kuinka suuri osa älykotilaitteista on hyvin helposti muokattavissa, mikäli hyökkääjä pääsisi niihin fyysisesti käsiksi. Hyökkääjä voisi myös

päästä käsiksi salausavaimiin, joita voitaisiin sitten käyttää yksityisen datan kaappaamiseen.

Mielenkiintoisesti, Bugeja, Jacobsson ja Davidsson (2016) tai Lee ja Zappaterra (2014) eivät nähneet pilven osuutta IoT-älykodissa suurena haasteena. Pilven haasteet ovat toisaalta hyvin riippuvaisia käytetystä laitekokoonpanosta eivätkä siksi ole niin helposti yleistettävissä.

4 Uhat yksityisyyden kannalta IoT-älykodeissa

Kuten edellisessä luvussa mainittiin, on IoT-perusteisilla älykodeilla useita erilaisia tietoturvahaasteita eri tasoilla. Nämä heikkoudet mahdollistavat suuren joukon eri tyyppisiä hyökkäyksiä, joiden vakavuus voi vaihdella laitekohtaisesti (Geneiatakis ym. 2017). Koska erilaisia IoT-älykotilaitteita on todella paljon, pyritään tässä luvussa keskittymään vaan suurimpiin ja yleistettävimpiin uhkiin yksityisyyden kannalta. Ei siis keskitytä vain yhteen tiettyyn laitteeseen tai uhkaan, joka koskee vain yhtä tiettyä laitetta.

Seuraavat uhat ovat yhdistelmä Ali ym. (2017), Lee ja Zappaterra (2014) ja Geneiatakis ym. (2017) tekemistä tutkimuksista löytyneistä havainnoista.

4.1 Salakuuntelu

Salakuuntelu (*engl.* Eavesdropping) on yksi yksityisyyden kannalta vakavimmista uhista. Tässä hyökkäyksessä hyökkääjä pyrkii kuuntelemaan ja kaappaamaan dataliikennettä älykodin eri laitteiden välillä. Dataliikenteellä ei kuitenkaan yleensä tarkoiteta sensorien keräämää dataa kuten videota tai lämpötiloja vaan dataa, jota voitaisiin hyödyntää vaikeammassa hyökkäyksessä. Tämänkaltaista dataa ovat esimerkiksi esiasennetut salausavaimet ja laitteiden tunnisteet (Lee ja Zappaterra 2014). Varsinkin älykodit, joissa laitteiden välinen kommunikointi on heikosti salattua, ovat tämän uhan alaisena (Geneiatakis ym. 2017).

Hyökkääjä voi toteuttaa hyökkäyksen kahdella tavalla: salakuuntelemalla dataa suoraan langattomien laitteiden väliltä esimerkiksi lähellä sijaitsevalla vastaanottimella tai käyttämällä jotain muuta laitetta salakuuntelun suorittamiseksi. Näitä laitteita voivat olla esimerkiksi muut huonosti suojatut älykotilaitteet tai jopa käyttäjän oma älypuhelin (Geneiatakis ym. 2017).

Salakuuntelu on yleensä passiivinen hyökkäys (Ali ym. 2017). Tämä tarkoittaa, että hyökkäys pyritään tekemään huomaamatta ja ilman, että laitteet lakkaavat toimimasta. Tämä toisaalta tekee hyökkäyksen havaitsemisesta hankalaa. Salakuuntelu on varsinkin IoT-älykotien ongelma, koska perinteisissä älykodeissa laitteet ovat useammin fyysisesti kytkettynä toisiinsa, mikä poistaa langattomat yhteydet laitteiden väliltä. Hyökkääjä voisi kuitenkin yhä kuun-

nella dataa, mikäli hän saa yhteyden kiinteään verkkoon esimerkiksi toiseen laitteen kautta.

4.2 Imitaatio

Imitaatio (*engl.* Impersonation) on uhka, jonka aikaisemmin mainittu salakuuntelu mahdollistaa. Hyökkäys on myös mahdollinen ilman salakuuntelua, mutta useimmiten hankala toteuttaa ilman salakuuntelussa esiintyviä tietoturvapuutteita (Geneiatakis ym. 2017). Hyökkäyksessä hyökkääjä pyrkii esittämään oikeaa käyttäjää hyödyntämällä esimerkiksi hänen tunnuksiaan tai salausavaimia, jonka seurauksena hän voi tehdä järjestelmään muutoksia.

Imitaatioksi voidaan laskea myös mahdollisen pilvipalvelun tunnusten käyttäminen, mutta tässä tapauksessa imitaatiolla tarkoitetaan älykodin laitteeseen kohdistuvaa hyökkäystä. Jos hyökkääjä kuitenkin saisi pilvipalvelun tunnukset, ovat riskit yksityisyyden kannalta suuret, koska pilvipalveluissa usein säilötään enemmän dataa kuin älykodissa olevissa laitteissa (B. L. R. Stojkoska ja K. V. Trivodaliev 2017).

Salakuuntelulla hyökkääjä saa pilvipalvelun tunnusten sijaan yleisemmin jonkin salausavaimen, jota laite käyttää itsensä identifioimiseen toiselle laitteelle (Geneiatakis ym. 2017). Pelkän laitteen avain voi tosin olla hyödytön, ellei hyökkääjä halua lähettää väärää dataa. Hyökkääjä on kuitenkin voinut saada käsiinsä esimerkiksi älypuhelimen salausavaimen, jota käyttämällä älykotia ohjataan. Tämänkaltainen salausavain antaa hyökkääjälle mahdollisuuden tehdä muutoksia esimerkiksi järjestelmän asetuksiin.

Yksi uhka olisi, että hyökkääjä ohjaa kaiken kerättävän yksityisen datan myös hänen hallitsemalle palvelimelle. Näin hyökkääjä pääsisi käsiksi kaikkeen jatkossa kerättävään dataan ja voi käytännössä vakoilla kohdettaan. Lisäksi koska älykotilaitteiden käyttäjät eivät yleensä tutki laitteiden asetuksia alkuasennuksen jälkeen, voisi tämänkaltainen muutos helposti jäädä huomaamatta (Zheng ym. 2018).

Imitaation uhkaavuus riippuu paljon käytetystä järjestelmästä. Mikäli salakuuntelu laitteiden välillä on mahdotonta, on hyökkääjän hankala saada salausavaimia jotain muuta kautta. Tämä tekee imitaatiosta hankalasti toteutettavan, mutta mikäli se pystytään toteuttamaan, ovat seuraukset vakavat. Varsinkin koska hyökkäys voidaan toteuttaa passiivisesti, ei käyttä-

jä välttämättä koskaan huomaa, että mikään on muuttunut. Mikäli hyökkääjä haluaisi, voisi hän toteuttaa myös aktiivisen hyökkäyksen, jossa toiminnallisuutta rikotaan.

4.3 Yleisten tietoturvapuutteiden hyödyntäminen

Yleisten tietoturvapuutteiden hyödyntäminen (*engl.* Software exploitation) on yleisin älykoteihin kohdistuva uhka. Näihin tietoturvapuutteisiin kuuluvat yleensä joko ihmisen aiheuttamat ongelmat tai laitteen valmiiksi heikko suojaus. Yksi yleisimmistä tietoturvapuutteista onkin laitteiden käyttäminen oletusasetuksilla yhdistettynä internetiin (Geneiatakis ym. 2017).

Kun käyttäjä ostaa esimerkiksi verkkoon kytketyn kameran, on mahdollista, että käyttäjä ei asentamisen jälkeen halua koskea laitteen asetuksiin, vaan antaa sen toimia oletusasetuksilla. Tämä voi aiheuttaa sen, että laitteeseen jää käyttöön esiasennetut oletustunnukset. Nyt hyökkääjän on hyvin helppo päästä laitteeseen käsiksi. Hyökkääjä voi sitten suorittaa laitteella edellä mainittuja salakuunteluun tai imitaatioon liittyviä operaatioita. Tässä tapauksessa laite on myös näkyvissä ulkoverkkoon, joten mahdollisen keskuslaitteen suojauksista ei ole apua.

Toinen yleisin tietoturvapuute on laitteen jo valmiiksi epäilyttävä suojaus. Käyttäjä on voinut hankkia laitteen mahdollisimman halvalla, jolloin laitteessa ei välttämättä ole mitään suojauksia tehdasasetuksilla (Geneiatakis ym. 2017). Laitteessa voi myös olla hyvä suojaus, mutta se ei saa turvallisuuspäivityksiä, jotka ylläpitävät turvallisuutta. Joissain tapauksissa hyökkääjä on jopa uudelleenmyynyt laitteita, joihin on asennettu jo valmiiksi turvallisuusaukko. Tällainen hyökkääjän asentama takaovi (*engl.* Backdoor) mahdollistaa hyökkääjälle luvattoman pääsyn laitteeseen ohittaen todennuksen.

Edellä mainitut puutteet ovat ylivoimaisesti yleisimpiä uhkia (Geneiatakis ym. 2017). Tämä on harmillista, sillä ainakin oletusasetusten aiheuttamat ongelmat ovat helposti estettävissä. Esimerkiksi oletustunnusten tapauksessa valmistajat voisivat tuottaa laitteita, joihin asetetaan tehtaalla satunnainen käyttäjätunnus ja salasana. Saastutettujen laitteiden ongelma sen sijaan on hankalampi, sillä monet ihmiset arvostavat laitteen alhaista hintaa enemmän kuin omaa yksityisyyttään (Zheng ym. 2018).

Tutkimuksessaan Geneiatakis ym. (2017) painottavat, että useat valmistajat jättävät tietoturvan taka-alalle sillä oletuksella, että älykodissa on jokin vahvemmilla suojauksilla varusteltu keskuslaite tai reititin. Näin laitteet eivät tarvitsisi vahvaa suojausta, koska niihin ei pitäisi päästä käsiksi suoraan ulkoverkosta. Tämä ei kuitenkaan ole riittävää, koska hyökkääjillä on usein mahdollisuuksia hyökätä laitteisiin myös sisäverkosta käsin esimerkiksi toisen laitteen kautta.

Tutkimuksessaan Sivaraman ym. (2016) todistivat, kuinka laitteisiin voitaisiin päästä käsiksi saastutetun älypuhelimen kautta. Tässä tapauksessa keskuslaitteesta tai reitittimestä ei olisi mitään hyötyä, koska hyökkäys tulee sisäpuolelta. Keskuslaite voi siis suojella vain ulkoverkosta tulevia uhkia ja valmistajien tulisi ottaa vastuuta asettaa laitteisiinsa tarpeeksi vahvat suojaukset jo yksinäänkin.

Kuten luvussa 3.1 mainittiin, Zheng ym. (2018) havaitsivat, että käyttäjät olivat skeptisiä yksityisyysuhista laitteilla, jotka eivät nauhoittaneet kuvaa tai ääntä. Vaikka laite itsessään ei pystyisikään keräämään mitään yksityistä dataa, voidaan sitä käyttää toisiin laitteisiin hyökkäämiseen. Tämä mahdollistaa pahimmassa tapauksessa sen, että yksi laite voi tuoda kaikki muut älykodin laitteet uhan alaisiksi. Siksi on tärkeää, että laitteiden suojausta ei keskitä vain yhteen laitteeseen. Mikäli keskittäminen on välttämätöntä, niin käyttäjän ei kannata ostaa yhtä huonosti suojattua laitetta sillä periaatteella, että varsinaiset nauhoittavat laitteet kuten älykaiuttimet ja valvontakamerat ovat turvallisia.

5 Ratkaisut

Tässä luvussa tutustumme mahdollisiin ratkaisuihin edellisessä luvussa esitettyihin ongelmiin. Koska erilaisia IoT-älykotilaitteita on erittäin paljon, ovat esitetyt ratkaisut mahdollisimman helposti yleistettäviä. Valitettavasti monet ratkaisut ovat hyvin riippuvaisia laitteen valmistajasta.

5.1 Laitetaso ja kommunikointi

Edellisessä luvussa salakuuntelun suorittaminen mahdollisti aktiivisemmat hyökkäykset kuten imitaation. Salakuuntelu on kuitenkin mahdollista vain ympäristöissä missä laitteiden välistä liikennettä pystytään kuuntelun lisäksi myös lukemaan. Helpoin tapa välttyä tältä olisi salata kaikki liikenne mahdollisimman aikaisin.

Tutkimuksessaan Bugeja, Jacobsson ja Davidsson (2016) esittävät, että jokaisessa laitteessa tulisi olla toimintoja datan salaamiseen keräämisestä saakka. Laite ei saa hajotessaan rikkoa salausta ja myös kaikki muut laitteet, joille dataa lähetetään, tulee valtuuttaa erikseen. Bugeja, Jacobsson ja Davidsson (2016) myös argumentoivat, että laitteiden tulisi kommunikoidessaan käyttää yhtä hyvin suojattua langatonta protokollaa, usean eri tarkoitukseen luodun protokollan sijaan. Mikäli liikennettä siirretään verkon yli, tulisi data siirtää VPN-yhteyden lävitse.

Ylivoimaisesti suurin este tämän salauksen toteuttamiseen laitteissa ja niiden välisessä kommunikoinnissa, on IoT-laitteiden pieni laskentakapasiteetti (Geneiatakis ym. 2017). Varsinkin patterilla toimivissa sensoreissa on mahdotonta suorittaa vahvaan salaukseen vaadittavia laskentoja. Tämänkaltaisissa laitteissa myös vahvasti suojattu langaton protokolla voi viedä liian paljon virtaa, vaikka itse salaus voitaisiin suorittaa.

5.2 Arkkitehtuurilliset ratkaisut

Kun laitetasolla keskityttiin kaiken kerätyn datan salaamiseen, niin arkkitehtuurillisissa ratkaisuissa pyritään etsimään vaihtoehtoja siihen, kuinka dataa kerätään ja kuljetetaan järjes-

telmässä. Yksi tapa vähentää lähetettävää yksityistä dataa on käyttää Edge-pilvilaskentaa.

Edge-pilvilaskennassa dataa pyritään prosessoimaan mahdollisimman lähellä datan keränyttä laitetta. Tämän lisäksi kaikille datan keränneille laitteille pyritään antamaan mahdollisuus päättää, pitäisikö dataa lähettää pilveen tai tallentaa ollenkaan (Garcia Lopez ym. 2015). Näin käyttäjä voisi esimerkiksi määrittää, että tietyissä huoneissa sensorit voivat lähettää dataa pilveen, kun taas toisissa kaikki data käsiteltäisiin paikan päällä. Tosin myös Edge on hyvin riippuvainen laitteiden suoritustehosta ja jos tehoa ei löydy laitteista, on data pakko käsitellä pilvessä.

Tutkimuksessaan Edgcomb ja Vahid (2012) etsivät keinoja, kuinka käyttäjästä nauhoitettua videota voitaisiin anonymisoida ja samalla säilyttää laitteiden toiminnallisuus. Parhaaksi tavaksi paljastui käyttäjän sensurointi erilaisilla maskeilla, jotka peittivät miltä käyttäjä näytti tai mitä hän teki, mutta antoivat tarpeeksi dataa esimerkiksi siitä missä käyttäjä oli huoneessa.

Tämän kaltaista sensurointia voitaisiin soveltaa esimerkiksi pilveen lähetettävän datan kanssa, mutta maskin lisääminen jälkeenpäin tai reaaliajassa vaatii jälleen suoritustehoa.

5.3 Toimintatapoihin perustuvat ratkaisut

Yksi yleisimmistä turvallisuusuhista oli jo valmiiksi huonosti suojatun laitteen ostaminen. Vaikka tästä olisi helppo syyttää käyttäjää, on syyllinen usein myös valmistaja, joka ei tuota turvallisuuspäivityksiä laitteelle (Geneiatakis ym. 2017).

Tutkimuksessaan Geneiatakis ym. (2017) kritisoivat useiden valmistajien välinpitämättömyyttä laitteiden tietoturvasta. Tehdasasetusten tulisi jo valmiiksi olla niin, että käyttäjältä vaaditaan mahdollisimman vähän toimia. Oletustunnuksia ei pitäisi olla, vaan jokaisella laitteella pitäisi olla oma satunnainen salasana, jotta vältyttäisiin yhdeltä yleisimmältä käyttäjän aiheuttamalta turvallisuusuhalta.

Geneiatakis ym. (2017) mukaan valmiiksi saastutetut laitteet ovat myös osittain valmistajien vastuulla. Valmistaja voisi esimerkiksi pyrkiä tekemään laitteista mahdollisimman suljettuja, jotta hyökkääjä ei pystyisi asentamaan laitteisiin omaa ohjelmistoaan. Toisaalta, koska saas-

tutettuja laitteita on suhteessa melko vähän, eivät valmistajat ehkä näe tarpeellisena lisätä näin vahvoja sovellussuojauksia.

Keshavarz ja Anwar (2018) esittävät tutkimuksessaan erilaisen tavan suojata yksilön yksityisyyttä. Heidän kehittämässä ratkaisussa käyttäjälle esitetään selvästi mitä dataa kerätään, miksi ja kenelle. Käyttäjä voi sitten helposti valita mitä haluaa varmasti jakaa tai kerätä. Näin voidaan estää tarpeetonta yksityisen datan keräämistä, mutta lisäksi myös saada käyttäjälle lisää informaatiota siitä mitä hänestä kerätään.

Edellä mainittua ratkaisua voitaisiin myös soveltaa esimerkiksi Edge-pilvilaskennan kanssa. Tällöin parhaassa tapauksessa käyttäjästä kerättäisiin ja lähetettäisiin vain sitä dataa mihin hän suostuu ja tietää suostuneensa. Toisaalta yritykset, joiden toimintamalli perustuu kerätyn datan analysointiin eivät ehkä koskaan suostuisi lisäämään käyttäjälle vaihtoehtoa kieltäytyä.

6 Yhteenveto

Tässä tutkielmassa käytiin läpi tietoturvan näkökulmasta, mitä yksityisyyteen kohdistuvia haasteita IoT-perusteisilla älykodeilla on, mitä uhkia nämä haasteet mahdollistavat ja miten näitä voitaisiin ratkaista. Kaikista osa-alueista pyrittiin myös esittämään selkeitä ja konkreettisia esimerkkejä.

IoT-perusteisen älykodin haasteet voitiin pääasiassa jakaa kolmeen osa-alueeseen:

- Laitteiden haasteet
- Kommunikoinnin haasteet
- Palveluiden ylläpidon haasteet

Varsinkin IoT-laitteille ominainen laskentakapasiteetin puute aiheutti ongelmia vahvan salauksen luomiseksi laitetasolla ja laitteiden välisessä kommunikoinnissa. Ylläpitoon kuuluivat valmistajien välinpitämättömyys tietoturvaa kohtaan tekemällä joko valmiiksi huonosti suojattuja laitteita tai jättämällä laitteet ilman turvallisuuspäivityksiä. Yksi yllättävämpi tekijä oli myös ihmisten skeptinen suhtautuminen yksityisyysuhkiin laitteissa, jotka eivät nauhoittaneet ääntä tai videota.

Koska erilaisia IoT-älykotilaitteita on valtava määrä, pyrittiin uhissa pysymään mahdollisimman yleistettävissä ja suurimmissa yksityisyyden kannalta. Pääasiassa uhat menivät pyramidina, jossa alimmalla tasolla olivat erilaiset yleiset tietoturvapuutteet, sitten laitteiden datan salakuuntelu ja päällimmäisenä imitaatio.

Yleisiin tietoturvapuutteisiin kuuluivat valmiiksi huonosti suojatut halvat laitteet sekä käyttäjän tekemät inhimilliset virheet, jotka aiheuttivat tietoturvan heikkenemisen. Koska useat laitevalmistajat olettavat, että laitteet ovat jonkin paremmin suojatun keskuslaitteen takana, saattoi yksittäisissä laitteissa olla hyvinkin heikko suojaus. Tämä yhden laitteen heikko suojaus saattoi avata takaoven, jolla mahdollinen hyökkääjä pystyi ohittamaan suurimman osan suojauksista ja pystyi siten hyökkäämään muihinkin älykodin laitteisiin.

Salakuuntelu tarkoitti pääasiassa laitteiden välisen liikenteen salakuuntelemista, josta pyrittiin saamaan jokin salausavain tai tunniste. Tätä avainta hyödynnettiin sitten aktiivisemman

imitaatiohyökkäyksen tekoon. Salakuuntelua voitiin toteuttaa lähellä olevalla vastaanottimella, mutta hyökkääjä voisi myös halutessaan käyttää esimerkiksi heikosti suojattua laitetta tai jopa käyttäjän älypuhelinta.

Mikäli salakuuntelu onnistui, on mahdollisella hyökkääjällä nyt kyky tehdä muutoksia järjestelmään. Tämä on yksityisyyden kannalta pahin tilanne, koska hyökkääjä voi nyt päättää mitä dataa hän haluaa laitteilla kerätä tai vaikka vain vakoilla käyttäjää kaikilla mahdollisilla sensoreilla. Hyökkääjä voisi myös rikkoa toiminnallisuuden, mutta yksityisyyden kannalta pahin on, jos hyökkääjä ei riko mitään, sillä useimmat käyttäjät eivät käy tutkimassa laitteittensa asetuksia niiden toimiessa.

Ratkaisut jaettiin salauksen parantamiseen laitteessa ja laitteiden välisessä kommunikoinnissa, arkkitehtuurillisiin muutoksiin, jotka koskivat koko järjestelmää ja toimintatapoihin perustuviin ratkaisuihin, jotka pyrkivät ratkaisemaan varsinkin yleisimpiä tietoturvapuutteita. Suurin vastuu turvallisuuden ja samalla yksityisyyden parantamisessa oli selvästi laitteen valmistajalla.

IoT-perusteisen älykodin yksityisyysuhat johtuivat pääasiassa laitteiden heikosta laskentakapasiteetista ja valmistajien heikoista suojauksista. Voidaan silti esittää kysymys: ovatko IoT-älykotiin kohdistuvat yksityisyysuhat uhka satunnaiselle henkilölle? Esimerkiksi yleisten tietoturvapuutteiden hyödyntäminen ja salakuuntelun tekeminen olisi helppo automatisoida, mutta imitaatio on jo niin kohdistettu hyökkäys, että en näe sitä kovin todennäköisenä satunnaiselle henkilölle. Kenties tähän vastaamiseksi tulisi toteuttaa enemmän tutkimusta siitä, mitä käyttäjä näkee yksityiseksi dataksi ja mikä on se raja, jonka kohdalla oltaisiin valmis maksamaan paremmasta laitteesta.

Tällä hetkellä IoT-perusteiset älykodit kuitenkin jatkavat yleistymistään uhista huolimatta ja paras tapa suojata itsesi, on olla luottamatta täysin valmistajaan ja välttää liian hyvältä ja liian halvalta kuulostavan laitteen hankkimista.

Lähteet

Ali, W., G. Dustgeer, M. Awais ja M. A. Shah. 2017. “IoT based smart home: Security challenges, security requirements and solutions”. Teoksessa *2017 23rd International Conference on Automation and Computing (ICAC),* 1–6. Syyskuu. doi:10.23919/IConAC.2017.8082057.

Bugeja, J., A. Jacobsson ja P. Davidsson. 2016. “On Privacy and Security Challenges in Smart Connected Homes”. Teoksessa *2016 European Intelligence and Security Informatics Conference (EISIC),* 172–175. Elokuu. doi:10.1109/EISIC.2016.044.

Doan, Tam Thanh, Reihaneh Safavi-Naini, Shuai Li, Sepideh Avizheh, Muni Venkateswarlu K. ja Philip W. L. Fong. 2018. “Towards a Resilient Smart Home”. Teoksessa *Proceedings of the 2018 Workshop on IoT Security and Privacy,* 15–21. IoT S&P ’18. Budapest, Hungary: ACM. ISBN: 978-1-4503-5905-4. doi:10.1145/3229565.3229570. http://doi.acm.org.ezproxy.jyu.fi/10.1145/3229565.3229570.

Edgcomb, Alex, ja Frank Vahid. 2012. “Privacy Perception and Fall Detection Accuracy for In-home Video Assistive Monitoring with Privacy Enhancements”. *SIGHIT Rec.* (New York, NY, USA) 2, numero 2 (syyskuu): 6–15. ISSN: 2158-8813. doi:10.1145/2384556.2384557. http://doi.acm.org/10.1145/2384556.2384557.

Garcia Lopez, Pedro, Alberto Montresor, Dick Epema, Anwitaman Datta, Teruo Higashino, Adriana Iamnitchi, Marinho Barcellos, Pascal Felber ja Etienne Riviere. 2015. “Edge-centric Computing: Vision and Challenges”. *SIGCOMM Comput. Commun. Rev.* (New York, NY, USA) 45, numero 5 (syyskuu): 37–42. ISSN: 0146-4833. doi:10.1145/2831347.2831354. http://doi.acm.org/10.1145/2831347.2831354.

Geneiatakis, D., I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri ja G. 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. Toukokuu. doi:10.23919/MIPRO.2017.7973622.

Holroyd, Patrick, Phil Watten ja Paul Newbury. 2010. “Why Is My Home Not Smart?” Teoksessa *Aging Friendly Technology for Health and Independence,* toimittanut Yeunsook Lee, Z. Zenn Bien, Mounir Mokhtari, Jeong Tai Kim, Mignon Park, Jongbae Kim, Heyoung Lee ja Ismail Khalil, 53–59. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-13778-5.

Jie, Y., J. Y. Pei, L. Jun, G. Yun ja X. Wei. 2013. “Smart Home System Based on IOT Technologies”. Teoksessa *2013 International Conference on Computational and Information Sciences,* 1789–1791. Kesäkuu. doi:10.1109/ICCIS.2013.468.

Keshavarz, M., ja M. Anwar. 2018. “Towards Improving Privacy Control for Smart Homes: A Privacy Decision Framework”. Teoksessa *2018 16th Annual Conference on Privacy, Security and Trust (PST),* 1–3. Elokuu. doi:10.1109/PST.2018.8514198.

Kidd, Cory D., Robert Orr, Gregory D. Abowd, Christopher G. Atkeson, Irfan A. Essa, Blair MacIntyre, Elizabeth Mynatt, Thad E. Starner ja Wendy Newstetter. 1999. “The Aware Home: A Living Laboratory for Ubiquitous Computing Research”. Teoksessa *Cooperative Buildings. Integrating Information, Organizations, and Architecture,* toimittanut Norbert A. Streitz, Jane Siegel, Volker Hartkopf ja Shin’ichi Konomi, 191–198. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-48106-5.

Lee, C., ja L. Zappaterra. 2014. “Securing smart home: Technologies, security challenges, and security requirements”. Teoksessa *2014 IEEE Conference on Communications and Network Security,* 67–72. Lokakuu. doi:10.1109/CNS.2014.6997467.

Mocrii, Dragos, Yuxiang Chen ja Petr Musilek. 2018. “IoT-based smart homes: A review of system architecture, software, communications, privacy and security”. *Internet of Things* 1-2:81–98. ISSN: 2542-6605. doi:https://doi.org/10.1016/j.iot.2018.08.009. http://www.sciencedirect.com/science/article/pii/S2542660518300477.

Risteska Stojkoska, Biljana. 2012. “Variable Step Size LMS Algorithm for Data Prediction in Wireless Sensor Networks”. *Sensors and Transducers Journal* 14-2 (maaliskuu): 111–124.

Schiefer, M. 2015. “Smart Home Definition and Security Threats”. Teoksessa *2015 Ninth International Conference on IT Security Incident Management IT Forensics,* 114–118. Toukokuu. doi:10.1109/IMF.2015.17.

Sivaraman, Vijay, Dominic Chan, Dylan Earl ja Roksana Boreli. 2016. “Smart-Phones Attacking Smart-Homes”. Teoksessa *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks,* 195–200. WiSec ’16. Darmstadt, Germany: ACM. ISBN: 978-1-4503-4270-4. doi:10.1145/2939918.2939925. http://doi.acm.org/10.1145/2939918.2939925.

Soliman, M., T. Abiodun, T. Hamouda, J. Zhou ja C. Lung. 2013. “Smart Home: Integrating Internet of Things with Web Services and Cloud Computing”. Teoksessa *2013 IEEE 5th International Conference on Cloud Computing Technology and Science,* 2:317–320. Joulukuu. doi:10.1109/CloudCom.2013.155.

Srinivasan, Vijay, John Stankovic ja Kamin Whitehouse. 2008. “Protecting Your Daily In-home Activity Information from a Wireless Snooping Attack”. Teoksessa *Proceedings of the 10th International Conference on Ubiquitous Computing,* 202–211. UbiComp ’08. Seoul, Korea: ACM. ISBN: 978-1-60558-136-1. doi:10.1145/1409635.1409663. http://doi.acm.org/10.1145/1409635.1409663.

Stojkoska, B. R., ja K. Trivodaliev. 2017. “Enabling internet of things for smart homes through fog computing”. Teoksessa *2017 25th Telecommunication Forum (TELFOR),* 1–4. Marraskuu. doi:10.1109/TELFOR.2017.8249316.

Stojkoska, Biljana L. Risteska, ja Kire V. Trivodaliev. 2017. “A review of Internet of Things for smart home: Challenges and solutions”. *Journal of Cleaner Production* 140:1454–1464. ISSN: 0959-6526. doi:https://doi.org/10.1016/j.jclepro.2016.10.006. http://www.sciencedirect.com/science/article/pii/S09596526161589X.

Zheng, Serena, Noah Apthorpe, Marshini Chetty ja Nick Feamster. 2018. “User Perceptions of Smart Home IoT Privacy”. *Proc. ACM Hum.-Comput. Interact.* (New York, NY, USA) 2, numero CSCW (marraskuu): 200:1–200:20. ISSN: 2573-0142. doi:10.1145/3274469. http://doi.acm.org.ezproxy.jyu.fi/10.1145/3274469.