Alina Kyrölä

IOT-LAITTEIDEN KYBERTURVAHAAVOITTUVUUDET ÄLYKOTIYMPÄRISTÖSSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Kyrölä, Alina
IoT-laitteiden Kyberturvahaavoittuvuudet Älykotiympäristössä
Jyväskylä: Jyväskylän yliopisto, 2021, 32 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Kyppö, Jorma

Internet of Things, eli esineiden internet, on viime vuosina yleistynyt teknologia, joka on tarjonnut helpotusta ja mukavuutta niin julkiselle sektorille, kuin yksityishenkilöille. Yksi yksityishenkilöiden käyttöympäristöistä esineiden internetille on sen teknologiaa hyödyntävä älykoti. Käyttäjä voi hallita IoT-älykodin laitteita helposti etäältä käsin, esimerkiksi matkapuhelimensa avulla. Kokonaisuudessaan älykoti voi helpottaa käyttäjänsä arkea säästäen aikaa ja rahaa. Ongelmaksi muodostuu kuitenkin se, että älykotiympäristössä IoT-järjestelmää hallitsevalla henkilöllä harvoin on tietotaitoa ja resursseja ylläpitää asianmukaista kyberturvallisuutta, mikä nostaa kyberturvahaavoittuvuuksien määrää, ja kasvattaa kyberturvariskien toteutumisen todennäköisyyttä.

Älykotien IoT-laitteiden turvallisuus on aiheena tärkeä, sillä pahimmassa tapauksessa turvaton ja epävarma järjestelmä voi aiheuttaa jopa hengenvaarallisia tilanteita. IoT-laitteiden turvallisuus on yleisellä tasolla kehittymässä jatkuvasti, mutta kokonaisuudessaan ne ovat vielä täynnä haavoittuvuuksia. Voidaan myös olettaa, että IoT-laitteet ovat hyökkääjien kohteena vielä vuosien ajan (Noor & Hassan, 2018). Tässä kandidaatintutkielmassa tarkastellaan IoT-laitteiden kyberturvahaavoittuvuuksia älykotiympäristössä, sekä käsitellään niistä johtuvia riskejä käyttäen pohjana tutkimuskysymyksiä *"Mitkä ovat IoT-älykodin keskeisimmät kyberturvahaavoittuvuudet?"* ja *"Mitä kyberturvariskejä IoT-älykodin kyberturvahaavoittuvuuksista voi seurata?"* Tutkielma on toteutettu kirjallisuuskatsauksena. Tutkielman tuloksena syntyi taulukko, jossa määritellään keskeisimmät IoT-älykotien haavoittuvuudet, sekä niihin liittyviä riskejä. Tutkielman tuloksista voidaan todeta, että älykodin IoT-laitteiden haavoittuvuuksia on paljon ja ne voivat altistaa vakavillekin riskeille. Osan näistä haavoittuvuuksista voi kitkeä yksinkertaisillakin menetelmillä, mutta usein jo yksinkertaisiinkin suojauskeinoihin vaaditaan resursseja, joita ei tällä hetkellä ole.

Asiasanat: Tietoturva, Kyberturvallisuus, Esineiden Internet, Älykoti, Haavoittuvuudet

ABSTRACT

Kyrölä, Alina
Vulnerabilities of IoT-Devices in Smart Home Environment
Jyväskylä: University of Jyväskylä, 2021, 32pp.
Information Systems Science, Bachelor's Thesis
Supervisor: Kyppö, Jorma

Internet of Things (IoT) is a technology that has become popular in the last years and has provided convenience for both public sector and private persons. One of the use environments of IoT for a private person is a modern smart home. The user can effortlessly control the devices of their IoT smart home with, for example, their smart phone. Overall a smart home can make the life of its user easier by saving time and money. The problems form when the person controlling the IoT system in a smart home environment does not have the proper knowledge or resources to maintain adequate security, which increases the amount of cyber security vulnerabilities and makes cyber security risks more likely to happen.

The security of IoT-devices in smart homes is a relevant topic because in the worst-case insecure systems can even lead to life-threatening situations. The security of IoT is constantly developing, but overall, they are still full of vulnerabilities. This Bachelor's thesis focuses on the cyber security vulnerabilities of IoT devices in smart homes and covers the risks that result from those vulnerabilities. The research is based on two research questions:" What *are the crucial cyber security vulnerabilities in an IoT-smart home?"* and *"What cyber security risks result from the vulnerabilities of IoT-smart homes?"*. This study has been carried out as a literature review. As the result of this study was created a table that defines the main cyber security vulnerabilities of IoT-smart homes and the risks that result from those. The results of this study show that smart home IoT-devices have plenty of vulnerabilities which can lead to serious risks. However, there are easy solutions to prevent and fix the vulnerabilities, although the resources needed do not exist.

Keywords: Information Security, Cyber Security, Internet of Things, Smart Home, Vulnerabilities

TAULUKOT

SISÄLLYS

1 JOHDANTO

Internet of Things (IoT), eli esineiden internet, on teknologia, jonka uskotaan olevan internetin seuraava sukupolvi (Li, Tryfonas & Li, 2016). Se tarjoaa ihmisille helpotusta ja mukavuutta niin yritysympäristöissä, kuin kotona, ja se on tänä päivänä kriittinen osa autonomisia kokonaisuuksia, esimerkiksi ajoneuvoja sekä armeijajärjestelmiä (Liu ym., 2020). IoT-teknologia lisää tietokoneälyn kodin laitteisiin, mikä mahdollistaa kodin olosuhteiden mittaamisen ja kodin laitteiden toimintojen seuraamisen (Domb, 2019, s. 1). Älykodin IoT -teknologiaa hyödyntävää järjestelmää voidaan hallita esimerkiksi matkapuhelimen tai tabletin avulla, ja parhaimmillaan se tarjoaa käyttäjälle mukavuutta ja turvallisuutta, sekä mahdollisuuden ekologisempaan arkeen. Käyttäjä voi esimerkiksi puhelimellaan seurata kodin lämpötilaa, sekä saada hälytyksen päälle jääneestä liedestä.

Älykodin IoT-laitteiden kasvavat markkinat lupaavat käyttäjälle uusia mukavuuksia luoden samalla uusia haasteista kodin yksityisyyden suojaamiselle (Apthorpe, Reisman, Sundaresan, Narayanan & Feamster, 2017, s. 1). Kun tietojenkäsittely otetaan osaksi tavallisia sähkölaitteita, voivat ne vaivihkaa uhata järjestelmien luotettavuutta, tai vaarantaa henkilöiden turvallisuuden (Matwyshyn, 2017, s. 1125). Williams, McMahon, Samtani, Patton ja Chen julkaisivat vuonna 2017 tutkimuksen, jonka mukaan jopa yli neljäkymmentäkaksi prosenttia tutkituista IoT-laitteista sisälsi vakavaksi luokiteltuja haavoittuvuuksia (Williams, McMahon, Samtani, Patton & Chen, 2017, s. 180). Turvallisuutta ja yksityisyyttä pidetäänkin IoT:n suurimpina kompastuskivinä (Li & Tryfonas Li, 2016).

Kuten kaikilla verkossa tapahtuvan tiedonkäsittelyn alueilla, myös IoT-älykodeissa yksi tärkeimmistä edellytyksistä luotettavalle järjestelmälle ovat sen turvallisuus sekä yksityisyys. Ongelmaksi muodostuu kuitenkin se, että usein älykodit ovat suhteellisen tilapäisiä järjestelmiä ilman kunnollisia resursseja asianmukaiseen ylläpitoon, kun taas yritysten IoT-käyttöympäristöissä on paremmat mahdollisuudet panostaa ammattitasoiseen tietoturvaan. (Lin & Bergmann, 2016.) Jopa siinä tilanteessa, kun yrityksellä on resursseja tietoturvan ylläpitoon, on käytännössä lähes mahdotonta paikata kaikki IoT-laitteiden

haavoittuvuudet (George & Thampi, 2018). Tämän lisäksi älykodin käyttäjille mukavuus on usein korkeammalla prioriteeteissa, kuin turvallisuus (Zheng, Apthorpe, Chetty & Feamster, 2018.), minkä vuoksi älykodit ovat erittäin alttiita haavoittuvuuksien muodostumiselle. Vuonna 2014 paljastui laaja-alainen hyökkäys, jossa hyökkääjien uskotaan hakkeroineen yli 100 000 jokapäiväiskäytössä oleviin kuluttajien laitteisiin (Sivaraman, Gharakheili, Vishwanath, Boreli & Mehani, 2015).

Tämä kandidaatintutkielma on toteutettu kirjallisuuskatsauksena ja sen tarkoituksena on selvittää älykodin keskeisimmät kyberturvahaavoittuvuudet ja -riskit. Tutkielman tutkimuskysymyksiksi muodostuivat seuraavat:

1. Mitkä ovat IoT-älykodin keskeisimmät kyberturvahaavoittuvuudet?
2. Mitä tietoturvariskejä IoT-älykodin kyberturvahaavoittuvuuksista voi seurata?

Tutkielman tuloksena syntyi tutkijan itsensä luoma taulukko, joka on perusteltu lähdekirjallisuudella. Kirjallisuutta etsittäessä on käytetty hakusanoja ”IoT”, ”Smart home”, ”Cyber security”, ”Vulnerability”, sekä erilaisia muunnelmia edellä mainituista. Kirjallisuutta etsittäessä nousi esille, että IoT-laitteiden yleistason tieto- tai kyberturvallisuutta koskevaa tieteellistä kirjallisuutta on ilmestynyt enemmän vasta muutaman viime vuoden aikana, mutta IoT-älykotien turvallisuutta koskevaa kirjallisuutta on edelleen erittäin vähän. Kirjallisuutta älykodeista puolestaan löytyi pitkältäkin aikaväliltä, mutta koska tässä tutkielmassa keskitytään perinteisen älykodin sijaan modernimpiin IoT-älykoteihin, tuli kirjallisuutta rajata tarkasti perustuen sekä julkaisuvuosiin, että termistön vastaavuuteen.

Vaikka tässä tutkielmassa käsitellään myös tietoturvahaavoittuvuuksia, tutkimuskysymyksissä käytetään nimenomaan termiä ”kyberturvahaavoittuvuus”, sillä tietoturva ei käsitteenä kata kaikkia tässä tutkielmassa tarkasteltavia haavoittuvuuksia ja riskejä. Tietoturva käsittelee informaatiota ja siihen kohdistuvia uhkia, kun taas kyberturvallisuus kattaa laajemman alueen. Tietoturvan tarkoituksena on suojata kaiken tasoinen informaatio kokonaisuudessaan, kun taas kyberturvallisuuden tavoite ei ole ainoastaan suojata kyberavaruutta ja sen sisällä liikkuvaa informaatiota, vaan myös siinä toimivia yksilöitä, organisaatioita ja valtioita. Solms ja Niekerk esittävätkin esimerkkitapauksena vuonna 2013 julkaistussa tutkimuksessaan tilanteen, jossa hyökkääjä onnistuu luvattomasti hallinnoimaan yksityishenkilön älykodin laitetta ja sammuttamaan kodin turvajärjestelmän murtautuakseen kotiin. Tällaisessa tapauksessa hyökkäyksen uhrin informaatio ei ole välttämättä ainoa vaarantunut asia, vaan hyökkäyksen kohteena voi olla hänen omaisuutensa tai terveytensä. Tämän vuoksi on mielekkäämpää puhua kyberturvallisuudesta. (Solms & Niekerk, 2013).

2 IOT (Esineiden internet) ÄLYKODEISSA

Tässä luvussa tarkastellaan IoT:n ja älykodin käsitteitä tämän tutkielman kannalta oleellisesta näkökulmasta, sekä niiden yhteyttä toisiinsa. On tärkeää erotella, että nämä kaksi termiä eivät tarkoita samaa asiaa, sillä käsitteenä IoT kattaa paljon laajemman alueen, kuin älykoti, kun taas IoT-teknologiaa hyödyntävä älykoti on vain osa IoT:n monimutkaista kokonaisuutta.

Älykoti on kokonaisuudessaan tarpeeksi älykäs tekemään vain hyvin rajattuja toimintoja ihmisen käskystä. IoT-teknologian avulla voidaan kuitenkin mahdollistaa laitteiden koneoppiminen, sekä toimiminen ilman erillistä ohjaamista (Rashidi & Cook 2009). Vuoteen 2025 mennessä ennustetaan olevan 75 miljardia käytössä olevaa IoT-laitetta (Cvitić, Peraković, Periša & Gupta, 2021).

2.1 Esineiden internet (IoT)

Internet of Things, eli esineiden internet on monimutkainen skenaario, minkä vuoksi on hankalaa määritellä mitä se käsitteenä pitää sisällään. Tämän vuoksi eri lähteistä löytyy erilaisia määritelmiä riippuen ympäröivästä kontekstista.

Mainitessaan termin mahdollisesti ensimmäisenä ihmisenä vuonna 1999 Procter & Gamblelle(P&G) laatimassaan esityksessä, Kevin Ashton tarkoitti termillä sitä, että tietokoneet – ja sen myötä internet ovat aina riippuvaisia ihmisistä ja heidän luomastaan informaatiosta (Ashton, 2009). Roberto Minerva, Abyi Biru ja Domenico Rotondi taas kuvailevat teoksessaan *Towards a definition of the Internet of Things (IoT)* IoT:n olevan sovellusala, joka integroi erilaisia teknologisia ja sosiaalisia alueita (Minerva, Biru & Rotondi, 2015, s. 6). Tässä Tutkielmassa IoT:lla tarkoitetaan Internetiin kytkettyjä fyysisiä objekteja, sekä niiden kykyä kommunikoida keskenään ja analysoida dataa.

Lyhyesti selitettynä IoT toimii ympäristöön sijoitettujen sensoreiden avulla, jotka muuttavat fyysisen datan digitaalisiksi signaaleiksi, ja lähettävät ne sitten ohjauskeskukseen. Tämä mahdollistaa IoT-laitteiden monitoroinnin miltä etäisyydeltä tahansa (Suresh, Vijay & Dr.Parhasarathy, 2014), joten käyttäjä voi

esimerkiksi kaupassa asioidessaan saada ilmoituksen pyykinpesuohjelman päättymisestä tai päälle jääneestä kahvinkeittimestä.

2.2 Älykoti

Älykoti on älykkään asumisen ydinosa, jota on kehitetty jo kolmenkymmenen vuoden ajan (Sisavath & Yu, 2021). Perinteinen älykotijärjestelmä koostuu kytkimistä ja sensoreista, jotka ovat yhteydessä keskiöön. Tätä keskiötä asukas hallinnoi seinään asennetun pääteaseman tai pilvipalveluihin kytketyn mobiiliyksikön avulla. (Domb, 2019, s. 2). Kun esitellään IoT teknologiaa älykodin toteutustapana, perinteinen älykoti on usein siihen nähden käsitteenä vanhentunut, sillä IoT kattaa paljon laajemman alueen, kuin vain perinteisen älykodin järjestelmät. IoT-älykoti pitää muun muassa sisällään asukkaiden turvallisuuden, lääketieteellisen hoidon, perheen tietojen prosessoimisen, viihteen sekä liiketoiminnan. (Li & Yu, 2011). IoT-älykoti kykenee myös sensoreiden keräämän informaation pohjalta suorittamaan automaattisia toimintoja (Cook, Crandall, Thomas & Krishnan 2013).

Älykodin IoT-teknologian avulla käyttäjä pääsee etäältä käsiksi kodin turvalaitteistoihin, kuten kameroihin ja palovaroittimiin. IoT-teknologiaa hyödyntävät terveyttä seuraavat laitteet voivat tarvittaessa lähettää viestejä lähimpään sairaalaan, minkä ansiosta lääkäreiden ja hoitajien on helpompi seurata potilaan terveydentilaa. Viihteen näkökulmasta perheen sisäinen data, kuten musiikki, elokuvat ja pelit voidaan varastoida dataservereille, ja IoT-laitteet voivat myös esimerkiksi näyttää säätietoja. Älykodin toiminnallisuudet mahdollistavat myös jokapäiväisten askareiden, kuten ostosten hoitamisen, kotoa käsin. (Li & Yu, 2011).

Jotta voidaan tarkastella IoT-älykodin kyberturvahaavoittuvuuksia ja niiden syitä, on hyvä ymmärtää järjestelmän arkkitehtuuria pääpiirteittäin. IoT-älykodin arkkitehtuuri koostuu useista tasoista, joista Yassein, Shatnawi. Mardini ja Khamayseh luettelevat tärkeimmiksi sovellustason (Application Layer), verkkotason (Network Layer), sekä havaitsemistason (Perceptive Layer) (Yassein, Shatnawi, Mardini & Khamayseh 2019, s. 135). Näiden lisäksi Chong, Zhihao ja Yifeng ovat lisänneet kotiportti (Home Gateway) -kohdan havaitsemis- ja verkkotason välille (Chong, Zhihao ja Yifeng 2011). Tasoja kuvataan **taulukossa 1**.

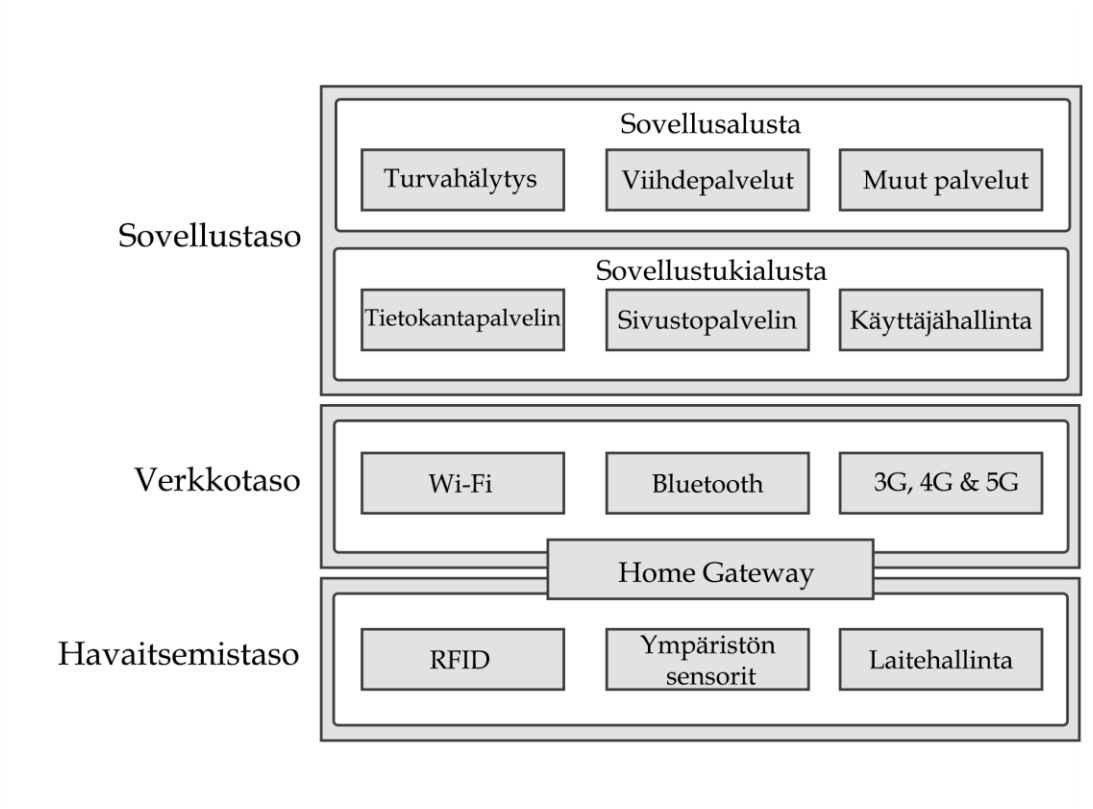
Havaitsemistaso on koko arkkitehtuurirakenteen alin taso. Havaitsemistaso vastaa datan keräämisestä ja sen reaaliaikaisesta monitoroinnista (Chong ym., 2011) esimerkiksi bluetooth-laitteiden, radiotaajuisen etätunnistuksen (RFID), satelliittipaikannusjärjestelmän (GPS), tai ympäristöön sijoitettujen sensoreiden avulla. Havaitsemistaso mittaa esimerkiksi lämpötilaa, kosteutta, tai sydämensykettä. (Yassein, ym., 2019, s. 135). Tässä tasossa tapahtuu myös laitteen hallinnointi ja virransäätely (Li & Yu, 2011).

Home Gateway, eli kotiportti liittää havaitsemistason ja verkkotason toisiinsa keräten datan havaitsemistasolta ja lähettäen sen verkkotasolle (Chong

ym., 2011). Verkkotaso vastaa datan lähettämisestä sitä käsittelevälle tai käyttävälle sovellukselle. Suuri osa IoT-laitteista käyttää datan liikuttamiseen langattomia yhteyksiä, kuten Wi-Fiä tai Bluetoothia. (Yassein ym., 2019, s. 136).

Viimeisenä data tavoittaa sovellustason, joka on täysin riippuvainen loppukäyttäjästä (Yassein ym., 2019, s. 136). Sovellustaso koostuu sovellustukialustasta ja konkreettisista sovelluksista, ja se toimii rajapintana käyttäjän ja älykotijärjestelmän välillä (Chong ym., 2011). Sovellustason laitteet, kuten älypuhelin tai kannettava tietokone, kommunikoivat suoraan loppukäyttäjän kanssa (Yassein ym., 2019, s. 136). Sovellustasolla käyttäjä pääsee käsiksi esimerkiksi sensoreiden avulla mitattuun tietoon, tai voi hallinnoida älykodin laitteistoa, jolloin käyttäjähallintadata lähetetään aina takaisin havaitsemistasolle asti.

TAULUKKO 1 Älykodin tasoarkkitehtuuri (mukaelma Lin & Yun (2011) sekä Chongin, Zhihaon & Yifengin (2011) taulukoista).



3 HAAVOITTUVUUDET

Tämän luvun ensimmäisessä alaluvussa avataan kyberturvahaavoittuvuuksien kannalta oleellista termistöä, jonka jälkeen toisessa alaluvussa tarkastellaan OWASP:in listaamia IoT-laitteiden haavoittuvuuksia. Jotta voidaan tarkastella ja ymmärtää IoT- laitteiden kyberturvahaavoittuvuuksia älykotiympäristöissä, on niitä hyvä käsitellä ensin yleisellä tasolla.

Kolmannessa alaluvussa käsitellään IoT-älykotien kyberturvahaavoittuvuuksia verraten niitä myös IoT-laitteiden yleisiin haavoittuvuuksiin. Tässä alaluvussa esitetään myös mahdollisia haavoittuvuuksista aiheutuvia riskejä.

3.1 Haavoittuvuuden ja riskin määritelmät

Kyberturvahaavoittuvuuksien ja tietoturvahaavoittuvuuksien, sekä niistä aiheutuvien riskien ymmärtämisen kannalta on tärkeää ensin määritellä haavoittuvuus, kyberturvallisuus sekä tietoturva erillisinä käsitteinä. Haavoittuvuus terminä riippuu paljon ympäröivästä kontekstista, eivätkä tutkijat ole päässeet yksimielisyyteen sen määritelmästä vuosikymmenienkään tutkimisen jälkeen. Lyhyesti tiivistettynä haavoittuvuuden voidaan katsoa tarkoittavan vahingon tai haitan mahdollisuutta tulevaisuudessa (Wolf ym., 2013). Yhdysvaltain kansallinen standardien ja teknologian instituutti on määritellyt tietokoneturvallisuuden yhteydessä haavoittuvuuden tarkoittavan heikkoutta tietojärjestelmässä, järjestelmäturvallisuusmenetelmissä, sisäisessä hallinnassa, tai toteutuksessa, jota uhan aiheuttaja voi hyödyntää (NIST, 2020). Hyökkääjän näkökulmasta haavoittuvuus tarkoittaa heikkoa kohtaa järjestelmässä, sovelluksessa tai palvelussa, joka hyökkääjän hyväksikäyttäessä johtaa laitteen kehittäjän silmissä tarkoituksenvastaiseen lopputulemaan (Kennedy, O'Gorman, Kearns & Aharoni, 2011, s. 8).

Tietoturva ja kyberturvallisuus ovat käsitteitä, joita käytetään usein limittäin. Vaikka niissä on päällekkäisyyksiä, ne eivät silti määritelmiltään täysin vastaa toisiaan (Solms & Niekerk 2013). Kyberturvallisuus ei kokonaisuudes-

saan keskity ainoastaan tekniseen näkökulmaan (Craigen, Diakun-Thibault & Purse, 2014), vaan pitää sisällään myös muita alueita, kuten käyttäjän, ympäristön ja organisaation (Schatz, Bashroush & Wall, 2017). Kansainvälinen Telekommunikointiyhdistyksen (ITU) mukaan kyberturvallisuus koostuu muun muassa laitteista, käytännöistä, turvallisuuskonsepteista, ohjenuorista, riskinhallintakäytännöistä, henkilöstöstä, palveluista sekä teknologioista, joita voidaan hyödyntää organisaatioiden ja henkilöiden sekä heidän omaisuutensa tai tietojensa turvaamisessa (ITU, 2020).

Kyberturvallisuuden lailla tietoturvakin on käsite, jolla ei ole yksiselitteistä määritelmää; joissakin lähteissä tietoturvalla viitataan tietojärjestelmien turvallisuuteen, kun taas muissa lähteissä siitä saatetaan puhua digitaalisena turvallisuutena, tai jopa turvallisuutena yleisellä tasolla. Tietoturva on termin muuttumisesta huolimatta historiallisesti määritelty kolmeen osaan, joista käytetään lyhennettä CIA. Nämä kolme osaa tarkoittavat informaation luotettavuuden (Confidentiality), yhtenäisyyden (Integrity) ja saatavuuden (Availability) varmistamista. (Torres, Sarriegi & Santos, 2006). On tärkeää mainita, että tietoturva ei ole tuote tai teknologia, vaan prosessi (Solms & Niekerk, 2013). Tärkein ero kyberturvallisuuden ja tietoturvan välillä on se, että kyberturvallisuuden tavoite on turvata kyberavaruuden ja sen sisällä liikkuvan informaation lisäksi myös kyberavaruudessa toimivia yksilöitä, organisaatioita ja valtioita, kun taas tietoturva keskittyy suojaamaan informaatiota sen kokonaisuudessaan (Solms & Niekerk, 2013).

Kyberturvallisuuden ja tietoturvan määritelmien perusteella voidaan päätellä, että myös kyberturvahaavoittuvuus ja tietoturvahaavoittuvuus eroavat termeinä toisistaan. Tässä tutkielmassa kyberturvahaavoittuvuudella tarkoitetaan heikkoutta tietojärjestelmässä, fyysisessä turvallisuudessa, järjestelmäturvallisuusmenetelmissä, sisäisessä hallinnassa, tai toteutuksessa, joita hyödyntämällä uhan aiheuttaja voi aiheuttaa vahinkoa tai haittaa. Tietoturvahaavoittuvuudella tarkoitetaan tässä tutkielmassa nimenomaan informaation vaarantumiseen johtavaa heikkoutta. Riskillä tarkoitetaan vaaraa aiheuttavaa tilannetta, joka johtuu kyberturva- tai tietoturvahaavoittuvuudesta. Kuten jo aiemmin mainittiin, tässä tutkielmassa on mielekkäämpää joissakin tapauksissa puhua kyberturvahaavoittuvuuksista tietoturvahaavoittuvuuksien sijaan, sillä tutkielmassa käsitellään haavoittuvuuksia myös muusta kuin informaation ja sen suojaamisen näkökulmasta.

3.2 IoT:n haavoittuvuudet OWASP:in mukaan

The Open Web Application Security Project (OWASP) on maailmanlaajuinen voittoa tavoittelematon organisaatio, joka keskittyy kehittämään sovellustietoturvaa. Organisaation tavoite on tehdä sovellustietoturvasta näkyvämpää organisaatioita ja yksityishenkilöitä varten. (OWASP, 2020).

OWASP on päivittänyt vuonna 2018 verkkosivuillaan ylläpitämäänsä listausta IoT-teknologian päähaavoittuvuuksista, ja asettanut ne seuraavaan vakavuusjärjestykseen:

1) Heikot, arvattavat tai kovakoodatut salasanat
Kun käytetään kirjautumistietoja, jotka ovat yleisessä käytössä, yleisesti saatavilla tai helposti hankittavissa brute-force-hyökkäyksen avulla, on suuri riski, että hyökkääjä pääsee luvattomasti käsiksi IoT-järjestelmään.

2) Epävarmat rajapintapalvelut
Epävarmoilla rajapintapalveluilla tarkoitetaan etenkin internetille altistuneita tarpeettomia, tai epävarmoja rajapintapalveluita, jotka pyörivät itsestään taustalla. Ne saattavat vaarantaa IoT-laitteen tai järjestelmän luotettavuuden, yhtenäisyyden, ja tiedon saavutettavuuden, tai jopa sallia laitteen luvattoman etähallinnoinnin.

3) Epävarmat ekosysteemirajapinnat
Turvattomat verkko-, taustajärjestelmän API-, pilvi- tai mobiilirajapinnat laitteen ulkopuolella olevassa ekosysteemissä voivat vaarantaa laitteen tai sen osia. Usein tähän haavoittuvuuteen sisältyy myös puutteellinen tunnistautuminen, puuttuva tai heikko salaus, tai syötteen ja tulosteen suodattamisen puuttuminen.

4) Turvallisen päivitysmekanismin puuttuminen
Turvallisen päivitysmekanismin puuttuminen tarkoittaa tilannetta, jossa laitetta ei ole mahdollista päivittää turvallisesti esimerkiksi laiteohjelman vahvistamisen puuttumisen, epäturvallisen toimittamisen, anti-rollback-mekanismin puuttumisen, tai turvallisuusmuutosilmoitusten vajavaisuuden vuoksi.

5) Epävarmojen ja vanhentuneiden komponenttien käyttö
Epävarmojen ja käytöstä poistuneiden komponenttien tai kirjastojen käyttö vaarantaa IoT-laitteen. Tämä koskee myös huolimattomasti toteutettua käyttöjärjestelmäalustojen kustomointia ja epäluotettavan jakeluketjun tarjoamaa kolmannen osapuolen laitteistokomponenttien ja ohjelmistojen käyttöä.

6) Riittämätön yksityisyyden suojaaminen
Yksityisyyttä katsotaan suojattavan riittämättömästi, kun esimerkiksi käyttäjän henkilökohtaista dataa on tallennettu laitteelle tai ekosysteemiin, jota käytetään väärin tai luvatta.

7) Epäturvallinen datan siirto- ja säilytys
Epäturvallinen datan siirto ja säilytys tarkoittaa tilannetta, jossa missä tahansa kohtaa ekosysteemiä salaus on puutteellista tai sensitiiviseen dataan pääsee käsiksi.

8) Laitehallinnoinnin puutteellisuus
Laitehallinnoinnin puutteellisuudella tarkoitetaan tuotantokäytössä olevien laitteiden tietoturvaa tukevien toimintojen, kuten päivitystenhallinnan, turvallisen käytöstä poiston, järjestelmänvalvonnan ja palautumiskyvykkyyden puutteellisuutta.

9) Epävarmat oletusasetukset
Laitteissa tai järjestelmissä voi olla epävarmoja oletusasetuksia tai ne voivat olla kyvyttömiä estämään oletusasetusten muuttamista.

10) Fyysinen suojaaminen
Fyysiset suojausmenetelmät voivat olla puutteellisia, mikä mahdollistaa sen, että potentiaalinen hyökkääjä voi saavuttaa laitteen hallinnan paikallisesti. Hyökkääjä voi myös päästä sensitiiviseen dataan käsiksi, mikä mahdollistaa tulevaisuudessa hyökkäyksen etäältä. (OWASP, 2020).

3.3 IoT-laitteiden haavoittuvudet kotiympäristössä

Tässä alaluvussa käsitellään älykodin IoT-laitteiden kyberturva- ja tietoturvahaavoittuvuuksia heijastaen niitä myös edellisessä alaluvussa käsiteltyihin OWASPin listaamiin yleisiin IoT:n ongelmiin. Koska moderni IoT-teknologiaa hyödyntävä älykotijärjestelmä on kytköksissä internetiin, kasvaa sen hyökkäyspinta-ala huomattavasti. Fyysisten haavoittuvuuksien lisäksi laitteisiin voidaan tehdä hyökkäyksiä etäältä joko rajapintojen kautta, tai ladaten haittaohjelmia laitteistoon. (Lin & Bergmann, 2016.)

Vaikka älykoti ympäristönä on hyvin ainutlaatuinen verrattuna muihin IoT:n käyttöympäristöihin, ovat sen haavoittuvuudet teoriassa hyvin samankaltaisia. Älykoti eroaa muista IoT-ympäristöistä kuitenkin siten, että usein älykoteja hallinnoi yksityishenkilö, jolla ei ole samanlaisia resursseja ylläpitää IoT-järjestelmän tietoturvallisuutta, kuten yrityksillä ja muilla oikeushenkilöillä. (Lin & Bergmann, 2016.) Tämä johtaa siihen, että tieto- ja muiden kyberturvahaavoittuvuuksien kirjo kasvaa ja niihin liittyvät riskit voivat moninkertaistua.

Tässä tutkielmassa löydetyt keskeisimmät haavoittuvuudet, sekä niistä johtuvat riskit esitellään **taulukossa 2**, jonka jälkeen haavoittuvuuksia avataan alaluvuissa. Taulukossa käytetään neljää astetta, joilla esitetään todennäköisyys haavoittuvuuden esiintymiselle. Lisäksi taulukossa käytetään sanaa *välitön* kuvaamaan tilannetta, jolloin riski johtuu suoraan kyseisestä haavoittuvuudesta, kun taas sanaa *välillinen* käytetään tapauksessa, jossa haavoittuvuus voi johtaa toiseen, riskille mahdollisuuden luovaan haavoittuvuuteen. Mikäli riski katsotaan mahdottomaksi, tai vain heikosti välillisenä mahdolliseksi, on sen kohdalle merkitty *ei huomattavaa riskiä*.

TAULUKKO 2 IoT-laitteiden kyberturvahaavoittuvuudet älykotiympäristössä

4 = kriittinen
3 = suuri
2 = kohtalainen
1 = matala

	haavoittuvuuden todennnäköisyys	Riskin toteutumisen mahdollisuus		
		Laite tai Järjestelmä	Informaatio	Henkilö-turvallisuus
Luvaton pääsy	4	Välitön	Välitön	Välitön
Asiantuntemuksen puute	4	Välitön	Välillinen	Välillinen
Epävarmat rajapinnat ja rajapintapalvelut	3	Välillinen	Välitön	Välillinen
Fyysinen turvallisuus	2	Välitön	Välitön	Välitön
Epävarmat ohjelmistot ja puutteelliset tietoturva-asetukset	2-3	Välitön	Välitön	Välillinen
Järjestelmien heterogeenisyys	4	Välillinen	Välillinen	Ei huomattavaa riskiä
Tietosuoja ja yksityisyys	3	Ei huomattavaa riskiä	Välitön	Ei huomattavaa riskiä

3.3.1 Luvaton pääsy

OWASP on listannut vuonna 2018 heikot, arvattavat tai kovakoodatut salasanat suurimmaksi ja vuonna 2014 riittämättömän todentamisen toiseksi suurimmaksi IoT-teknologian haavoittuvaisuuksista. (OWASP, 2020). Usein todentamiseen liittyvät haavoittuvuudet johtuvat heikoista salasanoista (Lin & Bergmann, 2016), minkä vuoksi tässä tutkielmassa ne luetaan yhden kyberturvahaavoittuvuuden alle, josta käytetään nimeä *luvaton pääsy*.

Luvaton pääsy voi johtaa siihen, että ulkopuolinen pääsee käsiksi sensitiiviseen informaatioon, kuten havaitsemistietoihin tai hallintajärjestelmään, ja voi näin ollen peukaloida dataa ja asetuksia. (Lin & Bergmann, 2016). Se altistaa useille erilaisille hyökkäyksille, kuten laiteskannaukselle, brute-force-hyökkäyksille, sekä haittaohjelmille (Ling ym., 2017). Luvaton pääsy kohdistuu sovellustasoon ja voi pahimmillaan johtaa jopa hengenvaarallisiin tilanteisiin, mikäli ulkopuolinen onnistuu säätämän lääketieteellisten laitteiden asetuksia, tai kytkemään päälle elektronisia laitteita, kun älykodin asukkaat eivät ole paikalla.

Luvattomaan pääsyyn voi johtaa hyvin moni tekijä, esimerkiksi aiemmin mainitut heikot salasanat tai heikko tunnistautumisen vaatiminen. Edellä mainittujen lisäksi myös äänikomento-ominaisuus lisää riskiä luvattomalle pääsylle. Hyökkääjät ovat tutkitusti pystyneet luomaan äänikomentoja, jotka eivät ole edes ihmiskorvaan kuultavia tai ymmärrettäviä, ja näin ollen saavuttaneet luvattoman pääsyn laitteisiin. (Meng, Zhang, Zhu & Shen, 2018). Muut haavoittuvuudet voivat myös välillisesti altistaa luvattomalle pääsylle, mikä tekee sen

esiintymisen todennäköisyydestä kriittisen. Luvattomasta pääsystä aiheutuvat riskit ovat myös välittömiä sekä pahimmassa tapauksessa erittäin vaarallisia, minkä vuoksi se on asetettu taulukossa 2 kaikista suurimmaksi haavoittuvuudeksi.

Luvattoman pääsyn riskit vähenisivät huomattavasti, mikäli IoT-laitteiden valmistajat asettaisivat tiukemmat tunnistautumisvaatimukset, mikä estäisi liian heikkojen salasanojen käytön. On kuitenkin huomioitava, että myös käyttäjällä on vastuu laatia mahdollisimman turvalliset salasanat hallinnoimiinsa IoT-laitteisiin. Myös kodin verkko tulisi suojata asianmukaisella tavalla, sillä ulkopuolinen taho voi päästä käsiksi älykodin laitteisiin myös yhdistämällä oman laitteensa verkkoon, jota kodin IoT-laitteisto käyttää. (Lin & Bergmann, 2016).

3.3.2 Asiantuntemuksen puute

Lin ja Bergmann määrittävät artikkelissaan *IoT Privacy and Security Challenges for Smart Home Environments* tietoturvan tuntemisen puutteen olevan suurin älykodin ongelmista, eli sen esiintymistodennäköisyyden voidaan katsoa olevan kriittinen. Ammattitasoisia ja omistautuneita henkilöitä, jotka hallitsevat älykodin monimutkaisen tietoverkon tuntemisen, on hyvin vähän. Usein älykodin omistajalla ei ole resursseja saada ammattitasoista avustusta laitteiston ylläpitoon, mikä johtaa siihen, että älykodin turvallisuutta ylläpitää usein aiheeseen perehtymätön henkilö. (Lin & Bergmann, 2016). Asiantuntemuksen puutteen vuoksi käyttäjä saattaa esimerkiksi tietämättään käyttää laitetta väärin, mikä voi johtaa sen toimimattomuuteen.

Asiantuntemuksen puute johtaa helposti siihen, että muiden kyberturvahaavoittuvuuksien riski tulla hyödynnetyksi kasvaa; esimerkiksi tehdasasetusten mukaisia salasanoja ei välttämättä muuteta ollenkaan, eikä fyysistä tietoturvaa osata ottaa huomioon. Se voi välillisesti johtaa esimerkiksi luvattomaan pääsyyn, epävarmojen ohjelmistojen käyttöön, tai kykenemättömyyteen ylläpitää älykodin heterogeenistä järjestelmää. Asiantuntemuksen puute voi johtaa myös siihen, ettei käyttäjä edes tiedosta, että laitteeseen on kohdistunut kyberhyökkäys (Shouran, Ashari, Priyambodo, 2019).

Asiantuntemuksen puutteen esiintymistodennäköisyyden vuoksi voidaan päätellä, että siihen liittyvät riskit ovat myös hyvin todennäköisiä. Tämän vuoksi se on todettu taulukossa 2 toiseksi suurimmaksi haavoittuvuuksista.

3.3.3 Epävarmat rajapinnat ja rajapintapalvelut

OWASP:in mukaan epävarmat rajapintapalvelut ja ekosysteemirajapinnat ovat korkealla tasolla IoT:n haavoittuvuuksien listalla. IoT:n kommunikaatioprotokollat eivät pohjaudu salaustekniikkamekanismeihin (Ling ym., 2017) ja usein IoT-laitteet käyttävät erilaisia teknisiä rajapintoja (Mahmoud, Yousuf, Aloul & Zualkernan, 2015), joten edellä mainittujen esiintyvyys on yleistä. Järjestelmän taustalla saattaa pyöriä internetille altistuneita tarpeettomia, tai epävarmoja

rajapintapalveluita samalla vaarantaen IoT-laitteen tai järjestelmän luotettavuuden, yhtenäisyyden sekä tiedon saavutettavuuden. Laitteen ulkopuolella olevassa ekosysteemissä saattaa myös esiintyä turvattomia verkko-, taustajärjestelmän API-, pilvi, tai mobiilirajapintoja (OWASP, 2020).

IoT-laitteet vaativat jatkuvaa kommunikointia pilvipalveluiden kanssa. IoT-laitteesta pilvipalveluun kulkevaa reittiä voi tutkitusti vääristää tai tuhota, ja reittiä pitkin siirrettävän datan kulkua voidaan estää. (Buinevich, Fabrikantov, Stolyarova, Izrailov & Vladyko, 2017). Turvattomat rajapinnat ja rajapintapalvelut lisäävät kyseisen riskin muodostumista ja altistavat tiedon vuotamiselle sekä salakuuntelulle (Ling ym., 2017). Pelkkä liikenteen salaus(encryption) ei tutkitusti riitä turvaamaan tietoa (Apthorpe, Reisman, Feamster, 2017.).

Mikäli vuotanut tieto on järjestelmien kannalta sensitiivistä, altistuu älykoti myös luvattomalle pääsylle. Koska epävarmojen rajapintojen ja rajapintapalvelujen voidaan katsoa aiheuttavan suurta uhkaa informaatiolle, ja niiden voidaan todeta esiintyvän IoT-laitteissa paljon, on ne lueteltu kolmanneksi suurimmaksi haavoittuvuudeksi taulukossa 2.

3.3.4 Fyysinen turvallisuus

Fyysistä turvallisuutta pidetään usein toissijaisena puhuttaessa tietoturvasta ja kyberturvallisuudesta. Palomuurit ja muut salaustekniikat ovat kuitenkin hyödyttömiä siinä vaiheessa, kun fyysinen turvallisuus laiminlyödään ja hyökkääjä pääsee fyysisesti käsiksi laitteisiin. (Hutter, 2016, s. 1). OWASP on listannut puutteellisen fyysisen suojaamisen kymmenenneksi suurimmaksi IoT-teknologian haavoittuvuuksista (OWASP, 2020). Älykotiympäristössä fyysiseen turvallisuuteen liittyvät riskit ovat kuitenkin suurempia verrattuna esimerkiksi toimisto- tai tehdasympäristöihin, sillä liikkumista ei välttämättä ole rajoitettu yhtä paljon, eikä fyysiseen turvallisuuteen ole asianmukaista ohjeistusta (Lee, Zappatera, Choi & Choi, 2014).

Älykotiympäristössä fyysinen turvallisuus voidaan nähdä haavoittuvuutena esimerkiksi silloin, kun IoT-laitteita kontrolloiva väline on asetettu huolimattomasti niin, että ulkopuolinen voi päästä siihen käsiksi. Mikäli älykodissa asuu useampi henkilö, myös salasana on voitu kirjoittaa näkyvälle paikalle muistiin. Kodissa saattaa liikkua asukkaiden lisäksi myös ulkopuolisia henkilöitä, joilla on rajoittamaton pääsy älykodin laitteistoon, mikä mahdollistaa esimerkiksi USB-liitännän kautta tehtävät hyökkäykset. Myös sensorit ja muut havaitsemiseen käytetyt laitteet tulisi fyysisesti suojata, sillä niihin kohdistuvat hyökkäykset voivat johtaa laitteiden toimimattomuuteen (Amadeo, Campolo, Iera & Molinaro, 2015).

Puutteellinen fyysinen turvallisuus altistaa älykodin vahvasti muun muassa luvattomalle pääsylle, josta johtuvat riskit voivat pahimmassa tapauksessa olla jopa hengenvaarallisia. Vakavista riskeistä huolimatta voidaan kuitenkin olettaa, että koska yleensä älykoteihin on integroitu hälytys- ja valvontajärjestelmiä (Lee, Zappatera, Choi & Choi, 2014), ei täysin tuntematon hyökkääjä

pääse hyödyntämään fyysisen turvallisuuden haavoittuvuutta kovin helposti. Älykodin turvajärjestelmä voi esimerkiksi tunnistaa tuntemattoman kodissa liikkuvan ihmisen kasvot ja lähettää hyökkääjästä videokuvaa älykodin asukkaalle (Robles & Kim, 2010). Täytyy kuitenkin ottaa huomioon, että hyökkääjä voi myös etäältä hyökätä laitteisiin fyysisesti, esimerkiksi käyttämällä häiritseviä radiosignaaleja sekoittaakseen älykodin järjestelmän kommunikaatiota (Lee, Zappatera, Choi & Choi, 2014). Edellä mainittujen seikkojen vuoksi fyysinen turvallisuus on tässä tutkielmassa määritelty neljänneksi suurimmaksi haavoittuvuudeksi.

3.3.5 Epävarmat ohjelmistot ja puutteelliset tietoturva-asetukset

OWASP listaa epävarmat epävarmojen ja vanhentuneiden komponenttien käytön, laitehallinnoinnin puuttumisen, sekä epävarmat oletusasetukset IoT-teknologian haavoittuvuuksiksi (OWASP, 2020). Kun käytetään epävarmoja ja käytöstä poistuneita komponentteja tai kirjastoja, tai kustomoidaan laite epäturvallisella tavalla, muuttuvat IoT-laitteet turvattomiksi. Näiden ongelmien ratkaisemiseksi on otettu käyttöön automaattista järjestelmähaavoittuvuuksien tunnistamista varten koneoppiminen osana IoT-laitteita. Koneoppiminen on kuitenkin suunniteltu tunnistamaan haavoittuvuuksia ainoastaan lähdekooditasolla. (Liu ym., 2020), minkä vuoksi myös ohjelmistojen tarkka testaaminen on tärkeää (Khan & Salah, 2018). IoT-laitteet käyttävät usein myös ohjelmistoja, joissa on yleisesti tunnettuja haavoittuvuuksia; esimerkiksi osassa IoT-laitteita on käytössä pelkistetty versio Linux OS:stä, joka on riskialtis sensitiivisen informaation, kuten kirjautumistietojen, vuotamiselle (Costa, Barros, Tavares, 2019).

OWASP listaa turvallisen päivitysmekanismin puuttumisen neljänneksi suurimmaksi IoT:n haavoittuvuuksista (OWASP, 2020). Kiinteät laiteohjelmat ovat haavoittuvaisia, sillä vain harvalle älykodin käyttöön suunnitellulle laitteelle on tarjolla säännöllisiä ohjelmistopäivityksiä. Lin Ja Bergmann epäilevät, että valmistajilla on hyvin vähän motivaatiota tarjota jatkuvia päivityksiä edullisten laitteiden järjestelmien ylläpitoa varten. Tämä on erittäin ongelmallista, sillä vaikka valmistushetkellä laite olisikin turvallinen, ei se ilman päivityksiä pysy turvallisena. Kyberrikolliset löytävät jatkuvasti uusia haavoittuvuuksia ja kehittävät uusia hyökkäysmenetelmiä, joten päivittämättömät laitteet ovat haavoittuvaisempia hyökkäyksille. (Lin & Bergmann, 2016). Tarjoamalla laitteisiin päivityksiä ja muistuttamalla käyttäjää niistä, voitaisiin parantaa niiden turvallisuutta huomattavasti (Simpson, Roesner & Kohno, 2017).

Koska kiinteät ohjelmistot sisältävät paljon puutteellisia tietoturva-asetuksia, eikä niihin usein edes tarjota päivitysmahdollisuutta, esiintyy IoT-älykodeissa kohtalaisen paljon epävarmoja ohjelmistoja ja puutteellisia tietoturva-asetuksia. Luonnollisesti nämä haavoittuvuudet lisäävät riskiä kyberhyökkäyksen toteutumiselle ja tietojen vuotamiselle, mikä voi altistaa järjestelmän

luvattomalle pääsylle. Edellä mainittujen seikkojen vuoksi epävarmat ohjelmistot ja puutteelliset tietoturva-asetukset on luettu viidenneksi suurimmaksi haavoittuvuudeksi taulukossa 2.

3.3.6 Järjestelmien heterogeenisyys

Älykoti on hyvin heterogeeninen järjestelmä, jolle on ominaista monentyyppiset laitteet, erilaiset liitäntäteknologiat, sovellukset ja palvelumallit (Amadeo, Campolo, Iera & Molinaro, 2015). Älykodin laitteet voivat esimerkiksi käyttää keskenään eri radioteknologioita, kuten Bluetoothia ja Wi-Fiä (Sarijari, Lo, Abdullah, Groot, Niemegeers & Rashid, 2013). Suurimmassa osassa älykodeista älylaitteet on integroitu pala palalta jo olemassa olevaan ympäristöön, jossa ei ole mahdollisuutta ammattitasoiseen asennukseen, tai resursseja järjestelmän ylläpitoon. Vaikka älykotien IoT-laitteiden asennus hoidettaisiinkin ammattitasoisesti, herää kuitenkin kysymys siitä, voiko aiheeseen perehtymättömän älykodin omistajan olettaa ylläpitävän moniprotokollaista heterogeenistä verkkoa tehokkaasti ja turvallisesti. (Lin & Bergmann, 2016.)

Kuten jo aiemmin mainittu, älykodin IoT-laitteita on vielä nykypäivänä harvoin asennettu älykotiin rakennusvaiheessa. Järjestelmien heterogeenisyys on muodostunut ongelmaksi, sillä etenkin edellä mainituissa älykodeissa IoT-laitteet tulevat usein eri valmistajilta, joilla on käytössä hyvin erilaiset tietoverkkostandardit, sekä päivitysmahdollisuudet. Usein laitteissa on myös hyvin vähän, tai ei ollenkaan dokumentaatiota sisäiseen ohjelmistoon asennetuista turvallisuusmekanismeista. (Lin & Bergmann, 2016).

Järjestelmien heterogeenisyys on erittäin todennäköistä, ja se altistaa älykodin erityisesti verkkotason tietoturvahaavoittuvuuksille, kuten epävarmojen rajapintojen esiintymiselle, mikä voi johtaa laitteiden ja järjestelmän toiminnan vaarantumiseen ja informaation vuotamiseen (Lee, Zappatera, Choi & Choi, 2014). Koska järjestelmien heterogeenisyys ei suoranaisesti aiheuta välitöntä uhkaa, on se listattu tässä tutkielmassa kuudenneksi suureksi IoT-älykodin haavoittuvuuksista.

3.3.7 Tietosuoja ja yksityisyys

OWASP listaa riittämättömän yksityisyyden suojaamisen, sekä epäturvallisen datan siirron ja -säilytyksen IoT-laitteiden tietoturvahaavoittuvuuksiksi (OWASP, 2020). Tietosuojan ongelmilla viitataan tilanteisiin, joissa sensitiivinen informaatio vaarantuu tai pääsee vuotamaan tarkoituksetta, esimerkiksi laitteen väärinkäytön seurauksena (Lin & Bergmann, 2016). Monissa älykodeissa on koko ajan päällä olevia sensoreita, jotka keräävät ja kuljettavat dataa käyttäjästä ja hänen liikkeistään (Apthorpe ym. 2017, s. 1). Mikäli tällainen data säilytetään tai siirretään väärin, on riski sen vuotamiselle suuri. Esimerkkitapauksena voidaan pitää tilannetta, jossa henkilökohtaisia sairastietoja vuotaa kotiympäristöön integroitujen lääketieteellisten IoT-laitteiden kautta. (Lin & Bergmann, 2016).

Käyttäjät eivät usein osaa ajatella sellaisten laitteiden yksityisyyden ongelmia, jotka eivät tallenna kuvaa tai ääntä (Zheng ym., 2018). Älykotien omistajat saattavat olettaa, että laitevalmistajat voivat seurata kuinka käyttäjä käyttää laitteita, mutta usein älykodin verkkoliikenne on altis muiden osapuolien, kuten internet-palveluntarjoajien ja luvattomasti Wi-Fiä käyttävien henkilöiden salakuuntelulle. (Apthorpe ym. 2017, s. 1). Vuotaneita ja salakuuntelun avulla hankittuja tietoja voidaan väärinkäyttää, ja niiden avulla voidaan muun muassa profiloida käyttäjää, mikä avaa mahdollisuuksia laajempaan haitantekoon tulevaisuudessa. Koska suuri osa älykodin laitteista ei toimi ilman verkkoyhteyttä, ei tietosuojan ja yksityisyyden ongelmilta voida välttyä (Apthorpe ym. 2017, s. 15). Tämän vuoksi niiden voidaan katsoa olevan kohtalaisen yleisiä. Tietosuoja ja yksityisyys ei tietoturvahaavoittuvuutena kuitenkaan kohdista välitöntä uhkaa laitteelle ja järjestelmälle, tai henkilöille, joten se on määritelty seitsemänneksi suureksi keskeisimmistä IoT-kyberhaavoittuvuuksista.

4 TULOSTEN ANALYSOINTIA

Tutkimuksen tuloksena syntynyt **taulukko 2** on kehitetty perustuen useisiin eri lähteisiin, joista tuoreimmille tutkimuksille on annettu enemmän painoarvoa. Aineistoa kerätessä tuli ilmi, että IoT-älykotien haavoittuvuuksista on edelleen suhteellisen vähän akateemista tutkimustietoa, vaikka IoT ei teknologiana olekaan enää uusi käsite. Empiirisiä tutkimuksia löytyi jonkun verran, ja niitä on hyödynnetty tämän tutkimuksen tulosten luonnissa.

Pohjalähteenä on käytetty kahta viimeisintä OWASP:in (The Open Web Application Security Project) luomaa top 10 IoT-laitteiden haavoittuvuuslistausta vuosilta 2014 ja 2018. OWASPin listaamia IoT:n yleisiä haavoittuvuuksia verrattiin älykotien turvallisuuteen painottuvissa lähteissä esiintyviin haavoittuvuuksiin. Vertailun tuloksena osa haavoittuvuuksista on nimetty yhdeksi kokonaisuudeksi, mikäli niiden on voitu katsoa kuuluvan samaan kategoriaan. Esimerkiksi OWASPin listaamat heikot, arvattavat tai kovakoodatut salasanat (2018), ja riittämättömän todentaminen (2014) (OWASP, 2020) on nimetty haavoittuvuudeksi *Luvaton pääsy*, sillä usein todentamiseen liittyvät ongelmat johtuvat heikoista salasanoista (Lin & Bergmann, 2016).

Aineistoa tutkiessa otettiin huomioon *aktiiviset* ja *passiiviset* kyberhyökkäykset. Passiivinen kyberhyökkäys tarkoittaa tilannetta, jossa hyökkääjä pyrkii esimerkiksi salakuuntelemalla, tai verkkoliikennettä tutkimalla keräämään informaatiota, vaikuttamatta kuitenkaan laitteiden käyttäytymiseen. Passiivisessa hyökkäyksessä hyökkääjä yleensä pyrkii oppimaan uutta tietoa, jota voidaan käyttää hyödyksi aktiivisessa hyökkäyksessä. Aktiivisen hyökkäyksen tarkoituksena on vaikuttaa laitteiden toimintaan, joko estämällä tai muuttamalla sitä. (Ali, Dustgeer, Awais & Shah, 2017). Tuloksia analysoidessa on arvioitu lähdekirjallisuuteen pohjautuen, kohdistuuko **taulukossa 2** esiintyviin haavoittuvuuksiin enemmän aktiivisia, vai passiivisia hyökkäyksiä. Esimerkiksi luvaton pääsy johtuu suurimmaksi osaksi aktiivisista hyökkäyksistä, kun taas rajapintojen salakuunteluun, tai tietosuojaan ja yksityisyyteen liittyvät hyökkäykset ovat useammin passiivisia.

On otettava huomioon, että haavoittuvuuksia hyödyntävien hyökkäysten vakavuus riippuu paljon siitä, millaiseen laitteeseen ne kohdistuvat. Esimerkiksi uloskirjautumisen pakottava hyökkäys ei aiheuta epäkäytännöllisyyttä suurempaa haittaa useimmissa viihdetarkoitukseen suunnitelluissa laitteissa, mutta voi riskeerata ihmisen hengen esimerkiksi lääketieteellisissä IoT-laitteissa. (Anthi, Williams, Slowinska, Theodorakopoulos, Burnap, 2019.) Tämän vuoksi tässä tutkimuksessa suurimmaksi haavoittuvuudeksi listattu luvaton pääsy, voi joissakin tapauksissa johtaa pienempään vahinkoon, kuin tiedon vuotaminen, riippuen hyökkääjän tarkoitusperästä. Vaikka hyökkääjä saavuttaisikin luvattoman pääsyn, hän ei välttämättä kohdista laitteisiin hengenvaaraa aiheuttavaa toimintaa, vaan voi haluta tehdä vain kiusaa esimerkiksi sammuttamalla älykodin valot. Toisaalta taas sensitiiviseen informaatioon käsiksi päässyt henkilö voi kiristää informaatiolla älykodin omistajaa.

Hyökkääjien tarkoitusperää on hankalaa, ellei mahdoton mitata, minkä vuoksi tässä tutkielmassa on tuloksia analysoidessa otettu huomioon vakavin seuraus, mikä haavoittuvuudesta voi seurata, jonka jälkeen sitä on verrattu haavoittuvuuden esiintymisen todennäköisyyteen. Esimerkiksi, vaikka fyysinen turvallisuus haavoittuvuutena voi pahimmillaan johtaa henkilövahinkoon, on epätodennäköistä, että tuntematon hyökkääjä pääsee sitä hyödyntämään kovinkaan helposti. Fyysinen turvallisuus on poikkeus siinä tilanteessa, kun oletetaan ulkopuolisen henkilön pääsevän asukkaan luvalla sisään älykotiin: tällöin kyseessä on yleensä asukkaan ystävä, sukulainen tai ammattihenkilö, joiden voidaan harvoin olettaa tahtovan aiheuttaa vahinkoja. Tässä tilanteessa ei siis ole loogista yleisellä tasolla puhuttaessa ottaa huomioon vakavinta seurausta.

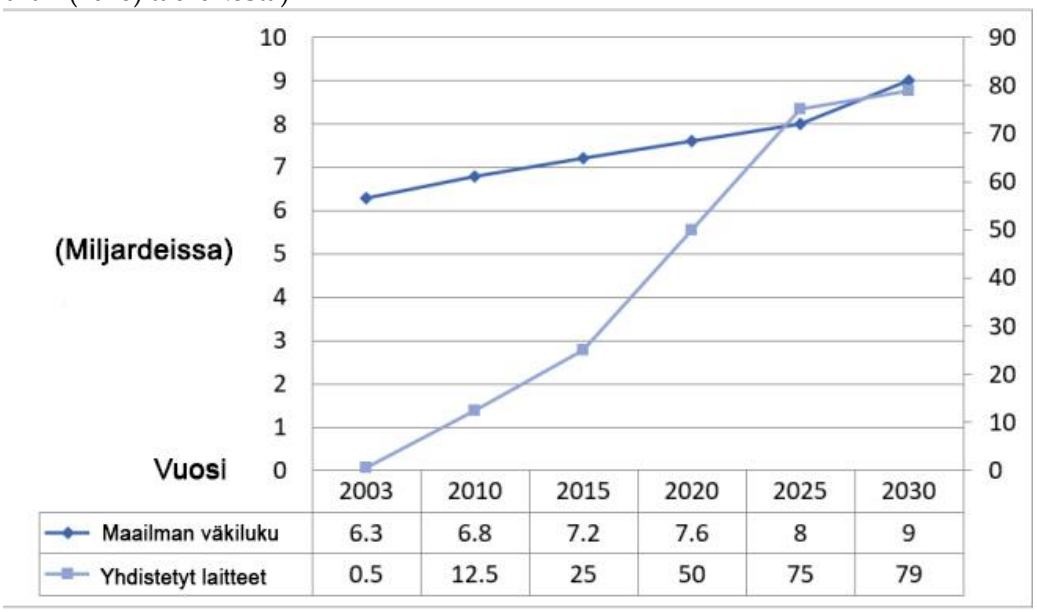
Tutkimustuloksena syntynyttä **taulukkoa 2** rakentaessa on verrattu seuraavia ominaisuuksia lähdekirjallisuuteen pohjaten:

1. Esiintymistodennäköisyys
2. Hyödyntämistodennäköisyys
3. Vaikutusten vakavuus
4. Vaikutusten laajuus

Esiintymistodennäköisyys ja hyödyntämistodennäköisyys on yhdistetty **taulukossa 2** kohdaksi *haavoittuvuuden todennäköisyys*, ja vaikutusten vakavuus sekä laajuus on yhdistetty kohdaksi *riskin toteutumisen mahdollisuus.* Kyseisen kohdan alle on listattu kolme kohdetta, joita ovat laite ja järjestelmä, informaatio, sekä henkilöturvallisuus. Henkilöturvallisuudelle annetaan myös enemmän painoarvoa, kuin laitteelle ja järjestelmälle, jolle puolestaan annetaan enemmän painoarvoa, kuin informaatiolle. Mikäli haavoittuvuuden voidaan katsoa olevan välitön riski jokaiselle kohteelle, voidaan haavoittuvuuden vaikutukset arvioida erittäin laajoiksi ja vakaviksi. Jos haavoittuvuus on välitön riski vain informaatiolle, mutta vain välillinen riski laitteelle ja järjestelmälle sekä henkilöturvallisuudelle, voidaan sen vaikutusten vakavuuden katsoa olevan keskivakavat, mutta laajat.

Vaikka IoT-laitteiden määrä kasvaa jatkuvasti (**taulukko 3**), ei suurinta osaa näistä laitteista, tai niiden sovelluksista, olla suunniteltu tavalla, joka ottaisi huomioon tämänhetkiset ja tulevaisuudessa ilmaantuvat turvallisuusongelmat (Ammi, Alarabi & Benkhelifa, 2021). Vaikka saataisiinkin aikaan yleinen turvallisuusprotokolla kaikille laitteille, on kyseenalaista, pystyvätkö IoT-laitteiden kevyet käyttöjärjestelmät kuitenkaan käsittelemään sitä (Jia ym. 2018). Vuonna 2018 tehdyn tutkimuksen mukaan IoT:n keskeisimmistä turvallisuusprotokollista löytyi useita tunnettuja haavoittuvuuksia. Tämän lisäksi turvallisimmin rakennettu protokolla, Z-Wave, oli pitkään yksityisomistuksellinen, minkä vuoksi se on vielä hyvin harvassa IoT-laitteessa käytössä. (Marksteiner, Jimenez, Vallant & Zeiner, 2017). Näiden seikkojen valossa tämän tutkimuksen tulosten voi olettaa olevan valideja vielä vuosien jälkeen tulevaisuudessa, ellei IoT-laitteiden valmistuksessa tai käytössä tapahdu ennusteista poikkeavaa, radikaalia muutosta.

TAULUKKO 3 Arvio verkkoon yhdistettyjen IoT-laitteiden kasvusta (mukaelma Guptan & Quamaran (2018) taulukosta)



5 YHTEENVETO JA POHDINTA

Tämän tutkielman tarkoituksena oli selvittää IoT-laitteiden keskeisimmät kyberturvahaavoittuvuudet älykotiympäristössä. Tutkielma toteutettiin kirjallisuuskatsauksena. Lähdekirjallisuuden pohjalta analysoitiin IoT:n yleisiä haavoittuvuuksia peilaten niitä muista IoT:n käyttöympäristöstä melkoisesti poikkeavaan älykotiympäristöön käyttäen apuna tutkimuskysymyksiä *"Mitkä ovat IoT-älykodin keskeisimmät kyberturvahaavoittuvuudet?"* ja *"Mitä kyberturvariskejä IoT-älykodin kyberturvahaavoittuvuuksista voi seurata?"*. Tutkielman tuloksena syntyi taulukko, jossa esiteltiin myös haavoittuvuuksien todennäköisyyttä, sekä haavoittuvuuksista syntyviä riskejä ja niiden esiintymisasteita.

Suurimmiksi haavoittuvuuksiksi listattiin tässä tutkielmassa niiden vakavuusjärjestyksessä seitsemän seuraavaa kyberturvahaavoittuvuutta:

1. Luvaton pääsy
2. Asiantuntemuksen puute
3. Epävarmat rajapinnat ja rajapintapalvelut
4. Fyysinen turvallisuus
5. Epävarmat ohjelmistot ja puutteelliset tietoturva-asetukset
6. Järjestelmien heterogeenisyys
7. Tietosuoja ja yksityisyys

Vakavuusjärjestys perustuu haavoittuvuuden esiintymisen todennäköisyyteen, siitä aiheutuvien uhkien vakavuuteen, sekä siihen, ovatko haavoittuvuudesta johtuvat riskit välillisiä vai välittömiä.

IoT-älykotijärjestelmässä suurimmaksi ongelmaksi muodostuu se, että suurin osa haavoittuvuuksista liittyy alueisiin, joihin tavallinen älykodin omistaja ei ole perehtynyt. Vaikka on olemassa erilaisia standardeja, joita voidaan hyödyntää älykotien turvallisuuden varmistamisessa (IEEE SA, 2020), on niissä jokaisessa myös omat heikkoutensa. Älykodeissa olevat laitteistot, laitesuunnittelu ja asennukset saattavat olla ammattitasoisia, jos ne on sisälletty kotiin rakennusvaiheen yhteydessä. Vaikka älykotien IoT-laitteiden asennus hoidettaisiinkin ammattitasoisesti, herää kuitenkin kysymys siitä, voiko aiheeseen pe-

rehtymättömän älykodin omistajan olettaa ylläpitävän moniprotokollaista heterogeenistä verkkoa tehokkaasti ja turvallisesti. (Lin & Bergmann, 2016.)

IoT-teknologian turvallisuus on vielä kehitysvaiheessa, ja vaikka olemassa on jo menetelmiä sen parantamiseksi, ei resursseja niiden toteuttamiseen käytännössä ole tällä hetkellä tarpeeksi; IoT:n Asiantuntijoita on vähän, ja IoT-älykodin turvallisuuden asiantuntijoita vielä vähemmän.

Valmistajien alhainen motivaatio tarjota jatkuvia ohjelmistopäivityksiä edullisiin laitteisiin on ongelma, joka hankaloittaa ratkaisujen toteuttamista käytännössä. Päivitysten tarjoaminen on luontaisesti kallista, joten niiden lisääminen tarkoittaisi myös IoT-laitteiden hintojen nousua. Niin kauan kuin käyttäjät priorisoivat mukavuutta ja luottavat IoT-laitteiden valmistajiin, eikä lainsäädännössä vaadita tiukempia tietoturvastandardeja, tulee harva valmistaja pitämään paremman tietoturvan tarjoamista taloudellisesti kannattavana (Zheng ym., 2018,). Tulevaisuudessa tulisi olla kansainväliset raamit, jotka pakottavat minimi-turvastandardien käytön heterogeenisissä IoT-laitteissa ja -sovelluksissa (Anand ym., 2020).

Osavastuu IoT-maailman turvallisuudesta on myös kuluttajilla; mikäli kuluttajat valitsisivat kalliimpia, mutta tietoturvallisempia laitteita valmistavien yritysten tuotteita, nostaisi tämä muidenkin valmistajien motivaatiota kehittää tuotteidensa turvallisuutta ja kitkeä haavoittuvuuksia. Ongelmaksi nousee myös se, että käyttäjät usein luottavat älykodin IoT-laitteiden hankinnassa perinteisiä kodinkoneita valmistaviin yrityksiin, vaikka niillä olisi hyvin rajallinen kokemus internetiin kytketyistä tuotteista (Zheng ym., 2018).

Nykyään markkinoilla on myös kolmannen osapuolen tarjoamaa IoT-älykodin turvallisuuden ylläpitoa; esimerkiksi F-Secure tarjoaa ”SENSE”-nimistä palvelukokonaisuutta, joka lupaa suojata IoT-älykodin laitteiston kyberhyökkäyksiltä (F-Secure, 2020). Palvelun heikkous on kuitenkin se, että asiakkaalle ei tarjota suoraa hintaa, vaan hänen täytyy varata aika konsultaatioon, mikä jo itsessään kuulostaa hintavalta ja aikaa vievältä. Lisäksi ulkopuolisen IoT-turvausjärjestelmän haasteena on aidosti toimivan kokonaisuuden rakentaminen jo olemassa olevaan sovellusinfrastruktuuriin (Chifor, Bica, Patriciu & Pop, 2017).

Kokonaisuudessaan vastuu kodin IoT-laitteiden haavoittuvuuksien kitkemisestä on sekä valmistajilla, että käyttäjillä. Valmistajien tulisi tarjota paremmat mahdollisuudet ylläpitää laitteita turvallisesti, esimerkiksi automaattisilla ohjelmistopäivityksillä. Käyttäjien taas tulisi omalla toiminnallaan pyrkiä pitämään älykoti turvallisena, esimerkiksi käyttämällä vahvoja salasanoja, sekä perehtymällä paremmin tietoturvaan. Käyttäjien kannattaisi myös perehtyä eri IoT-laitteiden valmistajiin ennen ostopäätöksen tekoa.

Vaikka haavoittuvuuksia on paljon, voi IoT-teknologian käyttö kotiympäristössä parhaimmillaan olla ekologista, parantaa turvallisuutta, sekä tarjota mukavuutta käyttäjälle. Hyvin toteutettuina ja ylläpidettyinä IoT-laitteet ja -järjestelmät eivät muodosta älykodeissa huomattavaa riskiä.

Älykotien IoT-laitteiden kyberturvahaavoittuvuuksista tehtyä tutkimusta on vielä tällä hetkellä suhteellisen vähän. Vaikka teknologioina IoT ja älykoti

eivät ole enää kovin uusia, on niiden yhdistelmä vielä kehitysvaiheessa oleva aihealue. Tulevaisuudessa IoT-laitteita koskeva lainsäädäntö tulee oletettavasti muuttumaan ja tiukentumaan, ja haavoittuvuudet tulevat elämään sen mukana. IoT-älykotien yleistyessä käyttäjien tietotaito sekä prioriteetit saattavat muuttua, minkä myötä sekä käyttäjät, että valmistajat alkavat kiinnostua enemmän haavoittuvuuksien kitkemisestä. Jatkotutkimuksessa olisi siis mielekästä tutkia menetelmiä, joilla IoT-älykodin kyberturvallisuutta voitaisiin parantaa. Muita mahdollisia tutkimusaiheita voisivat olla esimerkiksi:

1. IoT-laitteiden kyberturvahaavoittuvuudet yritysympäristöissä
2. Miten halpatuotettujen IoT-laitteen turvallisuus eroaa luotettujen valmistajien laitteesta?
3. IoT-älykotien kyberturvallisuus Suomessa
4. Heterogeenisen ja homogeenisen älykotijärjestelmän turvallisuuserot
5. IoT-älykotien tietoturvahaavoittuvuudet käyttäjän psykologiseen käyttäytymiseen perustuen

LÄHTEET

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

Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S. & Kumar, N. (2020). IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges. *IEEE Access*, 8, 168825-16885. doi: 10.1109/ACCESS.2020.3022842.

Anthi, E., Williams, L., Slowinska, M., Theodorakopoulos, G. & Burnap, P. (2019). A Supervised Intrusion Detection System for Smart Home IoT Devices. EEE INTERNET OF THINGS JOURNAL, 6(5). 9042-9053. doi:10.1109/JIOT.2019.2926365

Amadeo, M., Campolo, C., Iera, A. & Molinaro, A. (2015) Information Centric Networking in IoT scenarios: the Case of a Smart Home. Teoksessa *IEEE International Conference on Communications,* London, (s. 648–653). doi: 10.1109/ICC.2015.7248395.

Ammi, M., Alarabi, S. & Benkhelifa, E. (2021) Customized blockchain-based architecture for secure smart home for lightweight IoT. Teoksessa J.Jansen, B.He & T.Jiang (toim.), *Information Processing and Management* (s.1-22). Elsevier Ltd. doi:10.1016/j.ipm.2020.102482

Apthorpe, N., Reisman, D. & Feamster, N. (toim.). (2017). *A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic*. Cryptography and Security. Cornell University.

Apthorpe, N., Reisman, D.M Sundaresan, S.M Narayanan, A. & Feamster, N. (toim.). (2017). *Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic*. Cryptography and Security. Cornell University.

Ashton, K. (2009). That 'Internet of Things' Thing. *RFID JOURNAL, 22(7)*, 97–114. Haettu osoitteesta http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

Buinevich, M., Fabrikantov, P., Stolyarova, E., Izrailov, K. & Vladyko, A. (2017) Software Defined Internet of Things: Cyber Antifragility and Vulnerability Forecast. Teoksessa *IEEE 11th International Conference on Application of Information and Communication Technologies*, Moscow, Russia, (s. 1–5). doi: 10.1109/ICAICT.2017.8687021.

Chifor, B-C., Bica, I., Patriciu, V-V. & Pop, F. (2017). A security authorization scheme for smart home Internet of Things devices. Teoksessa M. Taufer, E.Cambria & D.Abramson (toim.), *Future Generation Computer Systems* (s.740-749). Elsevier Ltd. doi:10.1016/j.future.2017.05.048

Chong, G., Zhihao, L. & Yifeng, Y. (2011). The Research and Implement of Smart Home System Based on Internet of Things. Teoksessa *International Conference on Electronics, Communications and Control*, Ningbo, (s. 2944–2947) doi: 10.1109/ICECC.2011.6066672.

Cook, D.J., Crandall A.S., Thomas, B.L. & Krishnan, N.C. (2012) CASAS: A Smart Home in a Box. *Computer, 46(7),* 62–69. Haettu osoitteesta https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6313586

Costa, L.T., Barros, J. & Tavares, M. (2019). Costa, L.T., Barros, J., & Tavares, M. (2019). Vulnerabilities in IoT Devices for Smart Home Environment. ICISSP.

Craigen, D., Diakun-Thibault, N & Purse, R. (2014) Defining Cybersecurity. *Technology Innovation Management Review*, 4(10), 13–21. Haettu osoitteesta http://doi.org/10.22215/timreview/835

Cvitić, I., Peraković, D., Periša, M. & Gupta, B. (2021). Teoksessa Wang, X., Yeung, D.S. (toim.) *International Journal Machine Learning & Cybernetics* Ensemble machine learning approach for classification of IoT devices in smart home. Springer International Publishing https://doi.org/10.1007/s13042-020-01241-0

Domb, M. (toim.). (2019) *Smart Home Systems Based on Internet of Things*. Intechopen.

F-Secure: Enhance your home WiFi proposition (26.10.2020). Haettu osoitteesta https://www.f-secure.com/en/partners/operators/solutions/connected-home-sec§§urity

George, G. & Thampi, S.M. (2018). *A Graph-Based Security Framework for Securing Industrial IoT Networks from Vulnerability Exploitations.* Cochin University of Science and Technology, Kochi 682022, India.

Gupta, B. B. & Quamara, M. (2018). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols, Concurrency Comput., Pract. Exper. (s. e4946). doi: 10.1002/cpe.4946

Hutter, D. (toim.). (2016). *Physical Security and Why It Is Important.* SANS Institute Information Security Reading Room.

IEEE Standards Association: Internet of Things. (27.10.2020). Haettu osoitteesta https://standards.ieee.org/initiatives/iot/stds.html

International Telecommunication Union: Definition of cybersecurity. (27.10.2020). Haettu osoitteesta https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Jia, Y., Xiao, Y., Yu, J., Cheng, X., Liang, Z. & Wan, Z. (2018). A Novel Graph-based Mechanism for Identifying Traffic Vulnerabilities in Smart Home IoT. Teoksessa *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, (s. 1493-1501). IEEE INFOCOM doi:10.1109/INFOCOM.2018.8486369.

Kennedy, D., Gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit: The Penetration Tester's Guide (W. Pollock & T. Ortman, Eds.). San Francisco: No starch press.

Khan, M.J. & Salah, K. (2018) IoT security: Review, blockchain solutions, and open challenges. Teoksessa *Future Generation Computer Systems Vol 82* (s.395-411). doi.org/10.1016/j.future.2017.11.022

Lee, C., Zappaterra L., Choi, K. & Choi, H. (2014). Securing smart home: Technologies, security challenges, and security requirements. Teoksessa *IEEE Conference on Communications and Network Security*, San Francisco (s.67–72). doi: 10.1109/CNS.2014.6997467.

Li, S., Tryfonas, T. & Li, H (2016). The Internet of Things: a security point of view. *Internet Research, 26(2),* 337–359. Haettu osoitteesta: https://www.researchgate.net/publication/299421725_The_Internet_of_Things_a_security_point_of_view

Li, B. & Yu, J. (2011). Research and application on the smart home based on component technologies and Internet of Things. Teoksessa *Procedia Engineering 15, (s.*2087–2092). Elsevier Ltd. doi.org/10.1016/j.proeng.2011.08.390

Lin, H. & Bergmann, N.W. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *MDPI - Information open access journals, 7(3)*, 44. Haettu osoitteesta https://doi.org/10.3390/info7030044

Ling, Z., Luo J., Xu Y., Gao C., Wu K. & Fu, X. (2017). Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System. *IEEE Internet of Things Journal, 4(6)*, s. 1899–1909. Haettu osoitteesta https://ieeexplore.ieee.org/abstract/document/7932855

Liu, S., Dibaei, M., Tai, Y., Chen, C., Zhang, J. & Xiang, Y. (2019) Cyber Vulnerability Intelligence for Internet of Things Binary. *IEEE Transactions on Industrial Informatics, 16(3*), 2154–2163. Haettu osoitteesta: https://ieeexplore.ieee.org/document/8892533

Mahmoud, R., Yousuf, T., Aloul, F., & I. Zualkernan. (2013). Internet of things (IoT) security: Current status, challenges and prospective measures. Teoksessa *10th International Conference for Internet Technology and Secured Transactions*, London (s. 336-341). doi: 10.1109/ICITST.2015.7412116.

Marksteiner, S., Exposito Jimenez, V. J., Valiant H. & H. Zeiner, H. (2017) An overview of wireless IoT protocol security in the smart home domain. *2017 Internet of Things Business Models, Users, and Networks* (s. 1-8). IEEE. doi: 10.1109/CTTE.2017.8260940.

Matwyshyn, A.M. (2017). CYBER!. Teoksessa *Brigham Young University Law Review (*s.1109-1196). Haettu osoitteesta https://digitalcommons.law.byu.edu/lawreview/vol2017/iss5/6

Meng, Y., Zhang, W. , Zhu, H. & Shen, X. S. (2018). Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures. *IEEE Wireless Communications*, 25(6), 53-59 doi: 10.1109/MWC.2017.1800100.

Minerva, R., Biru, A., Rotondi, D. (2015). *Towards a definition of the Internet of Things(IoT)*. Telecom Italia S.p.A.

National Institure of Standards and Technology: vulnerability. (27.10.2020). Haettu osoitteesta https://csrc.nist.gov/glossary/term/vulnerability

Noor, M.M. & Hassan W.H. (2018). Current research on Internet of Things (IoT) security: A survey. Teoksessa *Computer Networks vol 148* (s.283–294). doi.org/10.1016/j.comnet.2018.11.025

OWASP Foundation: Internet of Things (IoT) Top 10 (5.9.2020). Haettu osoitteesta https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

Rashidi, P. & Cook D.J. (2009) Keeping the Resident in the Loop: Adapting the Smart Home to the User. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans 39(5)*, 949–959. Haettu osoitteesta: https://ieeexplore.ieee.org/document/5196706

Robles, R.S. & Kim, T. (2010). A Review on Security in Smart Home Development. *International Journal of Advanced Science and Technology, 15(2), 13*–22. Haettu osoitteesta http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.178.1685&rep=rep1&type=pdf

Sarijari, M.A., Lo, A., Abdullah, M.S., de Groot, S.H., Niemegeers, I.G.M.M. & Rashid, R.A. (2013). *Coexistence of Heterogeneous and Homogeneous Wireless Technologies in Smart Grid-Home Area Network*. International Conference on

Parallel and Distributed Systems (ICPADS). Haettu osoitteesta https://www.researchgate.net/publication/269308891_Coexistence_of_Heterogeneous_and_Homogeneous_Wireless_Technologies_in_Smart_Grid-Home_Area_Network

Schatz, D., Bashroush, R. & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*, *12(2),* 53–74. Haettu osoitteesta https://doi.org/10.15394/jdfsl.2017.1476

Shouran, Z., Ashari, A. & Priyambodo, T.K. (2019). Internet of Things (IoT) of Smart Home: Privacy and Security. *International Journal of Computer Applications 182(39),* 3-8. Haettu osoitteesta https://www.researchgate.net/publication/331133954_Internet_of_Things_IoT_of_Smart_Home_Privacy_and_Security

Simpson, A.K., Roesner F. & Kohno, T. (2017). Securing vulnerable home IoT devices with an in-hub security manager. Teoksessa *2017 IEEE International Conference on Pervasive Computing and Communications Workshops*, Kona (s. 551-556). doi: 10.1109/PERCOMW.2017.7917622.

Sisavath, C. & Yu, L. (2021). Design and implementation of security system for smart home based on IOT technology. Teoksessa *Procedia Computer science 183, (s.*4–13). Elsevier Ltd. doi.org/10.1016/j.procs.2021.02.023

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R. & Mehani, O. (2015) Network-level security and privacy control for smart-home IoT devices. Teoksessa *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (s.163-167), doi: 10.1109/WiMOB.2015.7347956.

Solms, R. & Niekerk. J. (2013). From information security to cyber security. Teoksessa Dimitris G. & Gurvirender T (toim.), *Computers & Security Volume 38: Cybercrime in the Digital Economy* (s 97-102). https://doi.org/10.1016/j.cose.2013.04.004

Suresh, P.J., Vijay, D. & Dr.Parhasarathy, V. (2014). A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. Teoksessa 2014 *International Conference on Science Engineering and Management Research*, Chennai (s. 1–8). doi: 10.1109/ICSEMR.2014.7043637.

Torres, J.M., Sarriegi, J.M., Santos, J. & Serrano, N. (2006). Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness. Teoksessa Katsikas S.K., López J., Backes M., Gritzalis S. & Preneel B (toim.). *Information Security: Lecture Notes in Computer Science, vol 4176* (s.530-545). Springer, Berlin, Heidelberg.

Williams, R., McMahon, E., Samtani, S., Patton M. & Chen, H. (2017). Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach. *IEEE International Conference on Intelligence and Security Informatics*, Beijing, (s. 179-181). doi: 10.1109/ISI.2017.8004904.

Wolf, S., Hinkel, J., Hallier, M., Bisaro, A., Lincke, D., Ionescu, C. & Klein, R.J.T. (2013). Clarifying vulnerability definitions and assessments using formalisation. *International Journal of Climate Change Strategies and Management 5(1),* 54-70. Haettu osoitteesta https://www.emerald.com/insight/content/doi/10.1108/17568691311299363

Yassein, M,B. Hmeidi, I. Shatnawi, F. Mardini W. Khamayseh, Y. (2019). Smart Home Is Not Smart Enough to Protect You - Protocols, Challenges and Open Issues. Teoksessa *Procedia Engineering 160, (s.*134–141). Elsevier Ltd. https://doi.org/10.1016/j.procs.2019.09.453

Zheng, S., Apthorpe, N., Chetty M., & Feamster, N. (2018). User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction, 2(200*), (1–20). Haettu osoitteesta https://dl.acm.org/doi/10.1145/3274469