Teemu Hyytiäinen

KYBERTURVALLISUUS ESINEIDEN INTERNETISSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2017

TIIVISTELMÄ

Hyytiäinen, Teemu
Kyberturvallisuus esineiden internetissä
Jyväskylä: Jyväskylän yliopisto, 2017, 27 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Grahn Hilkka ja Tenkanen Tuomas

Esineiden internetin laitteiden määrä on jatkuvasti kasvussa ja niiden hyödyt koskettavat kaikkia yhteiskuntamme jäseniä. Valitettavasti samanaikaisesti myös onnistuneiden kyberhyökkäysten määrä on kasvussa ja se uhkaa esineiden internetin luotettavuutta. Tämän takia onkin tärkeää tutkia, minkälaisia uhkia esineiden internet kohtaa ja kuinka näiltä uhkilta voitaisiin suojautua. Tutkielmassa käsitellään esineiden internetin laitteita, mitä kyseiset laitteet ovat, kuinka ne toimivat ja miten ne ovat suojattu. Tutkielma toteutettiin kirjallisuuskatsauksena ja sen lähteinä on käytetty pääsääntöisesti akateemisten julkaisujen artikkeleita. Tutkielmassa selvisi esineiden internetin kyberturvallisuuden erityispiirteitä. Näitä ovat fyysisten laitteiden fyysinen suojaamattomuus, langattoman kommunikoinnin tuomat ongelmat, sekä useiden esineiden internetin laitteiden heikko laskentateho. Vaikka kirjallisuuden avulla löydettiinkin useita erilaisia uhkia esineiden internetille, ei näille uhkille löytynyt samassa mittakaavassa ratkaisuja.

Asiasanat: Esineiden internet, kyberturvallisuus, tietoturva

ABSTRACT

Hyytiäinen, Teemu
Cybersecurity in the Internet of Things
Jyväskylä: University of Jyväskylä, 2017, 27 p.
Information systems science, Bachelor's Thesis
Supervisor(s): Grahn Hilkka and Tenkanen Tuomas

Internet of things is constantly growing and benefits from internet of things is helping every member of our society. Unfortunately, succeeded cyberattacks are also on the rise and that is risk for reliability of internet of things. Therefore, it is important to study what kind of threats internet of things faces and how we can protect it better. This thesis concerns how internet of things works, what kind of threats they face and how they are made secure. Thesis is made by literature review and sources are mostly academic peer reviewed articles. In the thesis multiple cybersecurity threats, that internet of things faces, were found. These threats are physical vulnerability from physical attacks, wireless communication and low amount of computing power in the devices of internet of things. Even though many threats were found, it became clear that there are not as many direct answers on how to solve these threats.

Keywords: Internet of things, cybersecurity, information security

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Esineiden internet-termiä (Internet of Things, IoT) käytetään kuvaamaan internetin ja Webin laajentumista fyysiseen maailmaan. Tämä toteutuu erilaisten laitteiden avulla, joihin on upotettu tunnistautumisominaisuus, sekä kyky havainnoida ympäröivää fyysistä maailmaa ja/tai vaikuttaa fyysiseen maailmaan. (Miorandi, Sicari, De Pellegrini & Chlamtac, 2012.) Esineiden internet on leviämässä yhä laajemmalle ja internettiin liittyy kiihtyvään tahtiin uusia laitteita. Ciscon tuottaman tutkimuksen mukaan vuoteen 2020 mennessä internetiin on liittynyt yli 50 miljardia laitetta (Evans, 2011). Eikä ihme. Esineiden internetin avulla on mahdollista helpottaa huomattavasti jokapäiväistä elämäämme automatisoimalla erilaisia tapahtumia. Esineiden internet voidaan yksinkertaisuudessaan jakaa kolmeen osaan. Ensinnäkin esineiden internet havainnoi ympäröivää fyysistä maailmaa ja mittaa haluttuja asioita, kuten lämpötilaa. Toiseksi esineiden internet voi vaikuttaa fyysiseen maailmaan automaattisesti. Esimerkiksi järjestelmän huomatessa lämpötilan nousevan haluttua korkeammaksi, säätää se lämpötilaa alemmaksi. Kolmanneksi esineiden internet pystyy tuottamaan palautetta ja lokitiedostoja järjestelmän hallinnoijalle. Kyseisiä palautteita voidaan tuottaa mitatusta datasta sekä kaikista automatisoiduista toimista. (Khan, Khan, Zaheer & Khan, 2012.)

Ongelman kuitenkin luo erilaiset kyberhyökkäykset näitä järjestelmiä vastaan. Yhä useampi kyberhyökkäys pääsee kohdejärjestelmään (Fonash & Schenck, 2015) eli ohittaa järjestelmien kaikki suojaukset. Usein huomaamattomasti. Tämän seurauksena informaatiota pääsee vuotamaan järjestelmien ulkopuolelle ja hyökkääjä voi vääristää dataa sekä esineiden internetin kohdalla hyökkääjä voi jopa vaikuttaa fyysiseen maailmaan.

Kyberhyökkääjän mahdollinen vaikuttaminen fyysiseen maailmaan on pelottava ajatus, sillä se mahdollistaa jopa verkon kautta tehdyn murhan. Esimerkiksi sydänvikaiselle ihmiselle asennettuun sydämentahdistimeen olisi mahdollista vaikuttaa verkon kautta. Potilaalle asennettu sydämentahdistin pystyy yhdistymään verkkoon WiFi:n avulla. Tämä mahdollistaa sen, että lääkäri pystyy seuraamaan potilaan tilaa etänä ja tekemään hätätilanteessa muutoksia sydä-

mentahdistimen toimintaan. Myös kyberhyökkääjä voi päästä tahdistimeen käsiksi, joka mahdollistaa esimerkiksi laitteen kytkemisen pois päältä etänä. Tämän seurauksena potilas saattaa kuolla. Onkin tärkeätä kartoittaa esineiden internetin kohtaamat uhkat sekä tämänhetkisten turvallisuusratkaisuiden heikkoudet. Näiden kartoitusten pohjalta esineiden internetiä voidaan kehittää toimivammaksi kokonaisuudeksi, jota on turvallista käyttää.

Tutkielman tarkoitus onkin aiempaa kirjallisuutta tutkimalla, kirjallisuuskatsauksen menetelmillä, koota kattava kuva uhkista ja riskeistä, joita esineiden internet kohtaa, sekä kartoittaa nykyisiä ratkaisuja. Tämä toteutetaan vastaamalla seuraaviin tutkimuskysymyksiin:

1. Mitä erityispiirteitä esineiden internetissä on kyberturvallisuuden näkökulmasta?
2. Miten näiltä erityispiirteiden aiheuttamilta uhkilta suojaudutaan?

Tutkielma toteutettiin kirjallisuuskatsauksena, joten lähteillä on todella suuri merkitys tutkimuksen luotettavuuteen. Seuraavaksi pyritään kuvaamaan lähteidenhakuprosessia, jotta lukijalle selviää mistä ja miten tutkielmanlähdemateriaali on kerätty.

Tutkielman aikana lähdemateriaaleina käytettyjä artikkeleita arvioitiin aiempien lähdeviittausten, kirjoittajien ja kirjoitusajankohdan mukaan. Hyvinä lähteinä pidettiin sellaisia julkaisuja, jotka olivat alan johtavia, korkean luokituksen julkaisufoorumissa saaneita, paljon viitattuja sekä suhteellisen tuoreita.

Lähteiden etsimiseen tietokannoista käytettiin hakusanoja Internet of things, IoT, cyber sekä security. Lisäksi haussa käytettiin näiden sekä muiden hakusanojen yhdistelmiä. Lähteitä etsittiin myös aikaisemmin hyväksi havaittujen lähteiden lähdeluetteloista.

Tutkielma on jaettu viiteen lukuun, joista tämä johdanto oli ensimmäinen. Tutkielman toinen luku käsittelee esineiden internetiä yleisesti ja kuvaa sen rakennetta ja toiminallisuutta. Tämän luvun tarkoitus on luoda pohjatietämys esineiden internetistä ja sen toiminnasta sekä pohjustaa tutkielmaa. Kolmas luku käsittelee kyberturvallisuutta yleisesti ja kuinka se eroaa tietoturvasta sekä minkälaisia yleisiä kyberuhkia erilaiset laitteet ja järjestelmät kohtaavat. Neljännessä luvussa käsitellään esineiden internetin kyberturvallisuuden erityispiirteitä ja esineiden internetiin kehitettyjä kyberturvallisuusratkaisuja. Tässä luvussa vastataan myös tutkimuskysymyksiin. Tutkielman viimeisessä luvussa kerätään yhteen tutkielman tulokset, sekä pohditaan esineiden internetin tulevaisuutta ja mahdollisia jatkotutkimusaiheita.

2 ESINEIDEN INTERNET

Tässä luvussa käsitellään esineiden internetiä yleisesti ja määritellään sen rakenne sekä sen toiminnallisuus. Luvun tarkoitus on luoda perustietämys esineiden internetistä, joka mahdollistaa tutkimuskysymyksiin vastaamisen. Luvussa määritellään myös tutkielman kannalta tärkeitä käsitteitä

2.1 Esineiden internetin rakenne

Kevin Ashton (2009) käytti ensimmäisenä sanaa ”Internet of Things” vuonna 1999 Procter and Gamblen järjestämässä tapahtumassa. Ashton (2009) kuvaili tulevaisuutta, jossa radiotaajuuksilla toimiva tunnistaminen ja sensoriteknologia mahdollistavat tietokoneiden informaation keräämisen fyysisestä maailmasta ilman, että ihmisen tarvitsee manuaalisesti kirjata dataa talteen. Ashtonin (2009) kuvailema tulevaisuus on nyt. Esineiden internet mahdollistaa fyysisen maailman mittaamisen ja tarkkailemisen ja jopa joissakin määrin vaikuttaa fyysiseen maailmaan.

Vaikka Ashtonin (2009) kuvailema esineiden internet on jo laajassa käytössä, sekä yksityisillä että erilaisilla organisaatioilla, ei sille ole vielä määritelty yleistä ja kaiken kattavaa mallia. Järjestelmien rakenteita tulee määrittää mahdollisimman tarkasti, sillä valmiin rakenteen pohjalta on helpompi kehittää järjestelmää eteenpäin. Seuraavaksi esitellään esineiden internetin kolme- ja viisikerroksiset mallit (Kuvio 1). Nämä mallit ovat yleisimmin käytetyt ja parhaiten esineiden internetin rakennetta kuvaavat.

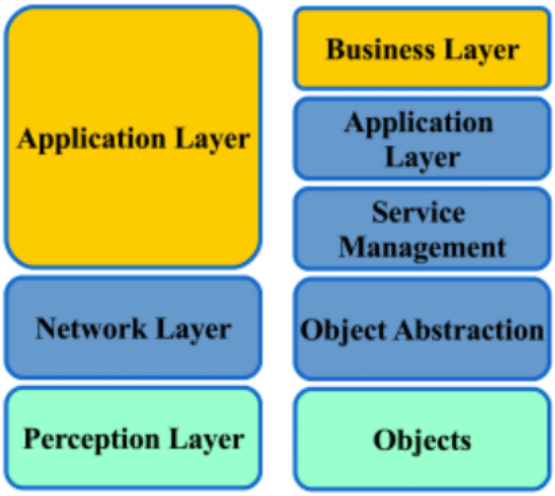
Kaikista teoreettisemmassa mallissa on vain kolme kerrosta, jotka ovat havaintokerros (perception layer), verkkokerros (network layer) ja sovelluskerros (application layer) (Al-Fuqaha ym., 2015). Kolmikerroksinen malli on yleisin käytetty esineiden internetiä kuvaava malli sen yksinkertaisuuden takia. Al-Fugahan ym. (2015) mukaan havaintokerroksella tapahtuu fyysisen maailmaan havainnointi ja datan muuttaminen digitaaliseen muotoon, lisäksi kyseisellä tasolla tapahtuu mahdollinen fyysiseen maailmaan vaikuttaminen. Käytännössä laite saattaa mitata fyysisestä maailmasta vaikkapa lämpötilaa tai ilmankosteutta, ja

muuttaa sen samanaikaisesti digitaaliseen muotoon. Lisäksi fyysiseen maailmaan vaikuttaminen voi olla esimerkiksi saunan päälle laittaminen etänä. Verkkokerroksen tehtävä on siirtää data turvallisesti havaintokerrokselta sovelluskerrokselle. Verkkokerros voi käyttää datan siirtämiseen muun muassa WLAN- tai 3G-yhteyttä. Lisäksi, laitteen tarvitessa ulkoista laskentatehoa, toteutetaan se myös tällä tasolla. Viimeinen eli kolmas kerros on sovelluskerros. Sovelluskerroksen tehtävänä on tuoda käyttäjälle hänen tarvitsemansa tiedot verkon kautta sensoreilta.

Vaikka kolmikerroksinen malli on yleisimmin käytetty esineiden internetiä kuvaava malli, ei se kuitenkaan pysty kuvaamaan edes kaikkia nykyisiä teknologioita. Kolmikerroksisen mallin vajaisuus tulee toisesta kerroksesta eli verkkokerroksesta. Verkkokerros ei käsitä kaikkia esineiden internetin tapoja välittää dataa toimijalta toiselle, vaan painottaa liikaa internetin kautta käytävää datan välitystä. (Al-Fugaha ym., 2015.) Tästä syystä onkin kehitetty hieman laajempi viisikerroksinen malli.

Viisikerroksinen malli on hyvin samankaltainen kolmekerroksisen kanssa. Alimpana kerroksena viisikerroksisessa mallissa on objekti- tai havaintokerros. Tällä kerroksella, kuten kolmikerroksisessakin mallissa, tapahtuu fyysisen maailman havainnointi, kerätyn datan muuttaminen digitaaliseen muotoon, sekä mahdollinen fyysiseen maailmaan vaikuttaminen. Tämän jälkeen mallien rakenne hieman eroaa toisistaan.

Viisikerroksisessa mallissa on jaettu verkkokerros kolmeen kerrokseen, jotka ovat objektin abstrahointi (object abstraction) ja palvelun hallintakerros (service management layer). Lisäksi sovelluskerros (application layer) nähdään viisikerroksisessa mallissa osaksi kolmikerroksisenmallin verkkokerrosta. Objektin abstrahointi-kerroksen tarkoitus on siirtää objektikerroksen tuottama data turvallisesti palvelun hallintakerrokselle. Toteuttaakseen tehtävänsä se saattaa käyttää useita erilaisia viestintäkeinoja, kuten GSM, WiFi, Bluetooth, infrapuna tai 3G. Palvelun hallintakerroksen tehtävä on yhdistää palvelu käyttäjä laitteeseen. Tämän kerroksen tarkoituksena on mahdollistaa sovelluskehittäjien työskentely heterogeenisessä ympäristössä ottamatta huomioon laitteistojen erilaisuutta. Sovelluskerros tarjoaa käyttäjille informaatiota pyydettäessä, kuten esimerkiksi lämpötilan tai ilmankosteuden. Sovelluskerroksen tarkoitus molemmissa malleissa onkin hyvin samankaltainen. Viimeisenä kerroksena viisikerroksisessa mallissa on liiketoimintakerros, joka kontrolloi esineiden internetiä kokonaisuutena. Se on vastuussa erilaisten bisnesmallien ja graafien luomisesta, jonka datan se kerää sovelluskerrokselta. Lisäksi liiketoimintakerros seuraa ja vertaa aiempien neljän kerroksen lähettämää dataa kerrosten oletettuun lähettämään dataan. (Al-Fuqaha ym., 2015.)



KUVIO 1 Esineiden internetin arkkitehtuuri. Kolmikerroksinen ja viisikerroksinen malli (Al-Fugaha ym., 2015)

Käytämme sitten esineiden internetin rakenteen kuvaamiseen mitä tahansa mallia, on sen taustalla useimmiten kuitenkin RFID-tunnisteiden käyttö, sekä sensoriteknologia ja langaton sensoriverkosto (WSN) (Gubbi, Buyya, Marusic & Palaniswami, 2013). RFID-tunnisteet ovat mikropiirejä, joilla on antenni. Ne ovat usein niin pieniä, että niitä on helppo liittää kaikenlaisiin objekteihin. RFID-tunnisteiden ansiosta voimme tunnistaa niihin kytkettyjä laitteita ja ne toimivat kuin elektroninen viivakoodi (Christensson, 2009). Passiivisilla RFID-tunnisteilla ei ole omaa virtalähdettä, vaan ne lähettävät tunnisteensa lukijalaitteelle lukijan lukusignaalin avulla (Gubbi ym., 2013). Tämän ansiosta RFID-tunnisteita voidaan käyttää pankkikorteissa ja julkisen liikenteen lipuissa nopeuttamassa maksamista. Esineiden internetissä niitä käytetään yleisesti identifioimaan sensoreita, minkä ansiosta tiedämme miltä sensorilta mikäkin data on tulossa (Gubbi ym., 2013).

Datan kerääminen tapahtuu yksittäisillä sensoreilla. Sensorit voivat olla aktiivisia tai passiivia, riippuen siitä onko niihin asennettu virtalähdettä. Esimerkiksi sensorit kuten kamerat tarvitsevat virtalähdettä toimiakseen ja ovat aktiivisia, kun taas lämpömittarit ovat passiivia (Ning Liu & Yang, 2013). Datan kerättyään sensorit välittävät sen yhdyskäytävän kautta eteenpäin ja lopulta käyttäjälle. Monet esineiden internetin laitteet tarvitsevat kuitenkin useita sensoreita toimiakseen. Esimerkiksi kasvihuoneissa seurataan jokaisen kasvin mullan kosteutta ja tämän takia sensoreille luodaan usein itseorganisoituva verkosto, jolloin jokainen sensori välittää datan yhdyskäytävälle tai tarvittaessa välittävät datan toisen sensorin kautta yhdyskäytävälle (Stankovic, 2008). Tätä sensorien luomaa verkostoa kutsutaan langattomaksi sensoriverkostoksi eli WSN:ksi. Sen avulla esineiden internetiin voidaan kerätä todella suuret määrät dataa useista eri sensoreista samanaikaisesti ja näin ollen tarjota käyttäjälle mahdollisimman hyvä kuva fyysisesti maailmasta, jota sensorit mittaavat (Stankovic, 2008).

2.2 Haasteita esineiden internetissä

Esineiden internet mahdollistaa fyysisten objektien, kuten tuolien tai television nähdä, kuulla, ajatella ja tehdä tehtäviä ”keskustelemalla” toistensa kanssa (Al-Fuqaha ym., 2015). Esineiden internet muuttaa nämä perinteiset objektit älykkäiksi antamalla niille tietoa niitä ympäröivästä fyysisestä maailmasta, antamalla niille mahdollisuuden välittää ja vastaanottaa dataa sekä mahdollisuuden käsitellä tätä dataa palvelimilla.

Tulevaisuudessa esineiden internetin odotetaan parantavan huomattavasti sekä yksityisten ihmisten että yritysten arkea. Esimerkiksi älykodit tulevat avaamaan autotallin ovet älypuhelimen käskystä ja laittamaan kahvin samalla tippumaan. Kolmivuorotyöläiset taas löytävät työpaikallaan esineiden internetistä hyötyä, sen säätäessä työolosuhteita, kuten valoja ja ilmankosteutta, kellonajan mukaan. Tämän seurauksena työntekijät pysyvät virkeinä töissä myös yövuorojen aikana. Esineiden internetin suurista mahdollisuuksista huolimatta, on siinä edelleen huomattavan paljon erilaisia ratkaisemattomia ongelmia. Suurimmat ongelmat esineiden internetin toimivuuden suhteen, ovat tällä hetkellä niiden saatavuus, toimintavarmuus, datan omistajuus, dynaamisuus ja yhteensopivuus sekä hallinta (Al-Fugaha ym., 2010). Tämän lisäksi haasteita herättää turvallisuus, jota käsitellään muun muassa luvussa 4.

Saatavuudella tarkoitetaan esineiden internetin palveluiden tarjoamista kaikkialle kaikkina aikoina. Tämä täytyy huomioida sekä laitteistojen että ohjelmistojen osalta. Laitteistojen osalta tulisi huomioida niiden yhteensopivuus protokollien kanssa ja kaikkiin laitteisiin tulisikin liittää muun muassa IPv6-protokolla. (Al-Fuqaha ym., 2015.) IPv6:n etu verrattuna IPv4:ään on huomattavasti suurempi määrä IP-osoitteita identifioimaan internetiin liittyviä laitteita. IP-protokollan tarkoitus on antaa jokaiselle internetin laitteelle oma uniikki tunniste, jotta data välitetään oikealle laitteelle (Christensson, 2016). On yleisesti tiedossa, että IPv4-osoitteita ei riitä identifioimaan kaikkia laitteita, jotka ovat ja tulevat liittymään esineiden internetiin. IPv6:ssa on $7{,}9 \times 10^{28}$ kertaa enemmän IP-osoitteita (Christenssson, 2016) ja näin ollen se olisi toimiva ratkaisu pitkäksi aikaa. Tämän lisäksi saatavuus tulisi huomioida ohjelmistoissa, jotta kaikilla olisi yhtenäinen mahdollisuus asentaa tarvitsemiaan sovelluksia (Al-Fuqaha ym., 2015). Ratkaisuksi tähän on ehdotettu tarjottavaksi päällekkäisiä sovelluksia ja laitteistoja (Macedo, Guedes & Silva, 2014). Tällöin yhden laitteen tai sovelluksen mennessä toimintakyvyttömäksi, esimerkiksi liian suuren työtaakan takia, voidaan tilalle ottaa saumattomasti varakappale.

Toimintavarmuudella tarkoitetaan, että järjestelmä toimii halutulla ja kuvatulla tavalla (Macedo ym., 2014). Toimintavarmuus ja saatavuus pyrkivät molemmat takaamaan palvelun ja laitteiden käytön ajankohdasta ja paikasta riippumatta. Erona on kuitenkin, että toimintavarmuuden takaamisella mahdollistetaan käyttäjän käyttää palveluita ja laitteita myös poikkeustilanteissa. Erittäin kriittistä on huomioida verkon toimivuus ja sen resilienssi poikkeustilanteissa, jotta voidaan taata datan jatkuva välitys ja järjestelmän toiminta. Tämä täytyykin

huomioida esineiden internetin jokaisella tasolla, sillä epäluotettavan järjestelmän seurauksena voi olla vääristynyttä dataa, datan välityksen hidastuminen ja datan häviäminen. (Kempf, Arkko, Behesthi & Yedavalli, 2011.) Näiden seurauksena käyttäjä saattaa tehdä vääriä ratkaisuja, jotka voivat johtaa katastrofaalisiin seurauksiin ja näin ollen tehdä esineiden internetistä epäluotettavan.

Datan omistajuus tuottaa esineiden internetissä ongelmia. Koska esineiden internetin laitteilla on hyvin vähän laskentatehoa, joudutaan lisätehoa ja/tai tallennustilaa ostamaan erilaisista pilvipalveluista. Pilvipalveluita valittaessa olisikin tärkeää perehtyä yrityksen toimitusehtoihin, sillä joissakin tilanteissa yritys omistaa kaiken datan joka kulkee heidän servereidensä kautta (Gray, 2014). Dataa voi suojata myös salaamalla sitä, mutta laadukas salaus vaatisi useimmiten reilusti laskentatehoa (Bandyopadhyay & Sen, 2011), johon esineiden internetin laitteilla ei usein ole mahdollisuutta.

Dynaamisuus on myös yksi esineiden internetin erityisistä haasteista, koska suurin osa palvelunkäyttäjistä olettavat saavansa palvelut mobiililaitteisiin. Käyttäjät haluavat käyttää palveluita jatkuvasti liikkeessä ollessaan. Mobiililaitteen siirtyessä yhdestä yhdyskäytävästä toiseen, saattaa se aiheuttaa palvelun keskeytymistä. (Al-Fuqaha ym., 2015). Eräänä ratkaisuna tähän on ehdotettu käyttäjien yhteistä verkkoa (Misra & Agarwal, 2011). Esimerkiksi autot, jotka voivat käyttää sensoreiden tuottamaa dataa ennustaen ruuhkia ja näin ollen ehdottaa ajajalle vaihtoehtoisia reittejä, voisivat kommunikoida keskenään ja jakaa tietoja. Tämän ansiosta yhden auton menettäessä verkkoyhteyden, se voisi kommunikoida viereisen auton kanssa ja saada siltä tarvitsemansa tiedon. Näin voitaisiin estää esimerkiksi tunneleissa yhteyden katoaminen.

Päästä-päähän-yhteensopivuus on myös ongelmallista esineiden internetissä suuren heterogeenisuuden takia. Sekä ohjelmisto- että laitekehittäjien tulisi huomioida työssään yhteensopivuus, jolloin käyttäjät voisivat käyttää heidän palveluitaan käyttämästään alustasta riippumatta. Toinen yhteensopivuuden ongelma on, että vaikka käytettäisiin samoja protokollia, niin useiden eri tulkintojen takia eivät sovellukset ja laitteet välttämättä toimi keskenään (Al-Fuqaha ym., 2015). Olisi kuitenkin tärkeää ratkaista sekä skaalautuvuus että päästä-päähän-yhteensopivuus järjestelmässä, koska silloin voitaisiin taata käyttäjälle paremmin toimivat laitteet ja palvelut.

Vaikka esineiden internet toimiikin jo melko hyvin, on sen kehittämisessä edelleen työtä, jotta se saadaan toimimaan parhaalla mahdollisella tavalla. Olisikin tärkeää kehittää yleisiä toimivia malleja ja toimintatapoja, jotta laitteet ja palvelut voisivat toimia paremmin toistensa kanssa. Tämän hyötynä olisi, että käyttäjä voisi halutessaan itse lisätä sensoreita ja toimintoja käyttämiinsä palveluihin (Ning ym., 2013).

3 KYBERTURVALLISUUS

Tässä luvussa määritellään kyberturvallisuus sekä erotetaan se tietoturvallisuudesta. Määrityksen tarkoitus on mahdollistaa kyberturvallisuuden käsitteleminen seuraavassa luvussa ilman, että sitä sekoitetaan tietoturvallisuuteen. Luvussa käsitellään myös järjestelmien yleisesti kohtaamia kyberturvallisuusuhkia. Tämän tiedon avulla voidaan seuraavassa luvussa esitellä, minkälaisia erityispiirteitä esineiden internetissä on.

3.1 Tietoturvasta kyberturvallisuuteen

Usein varsinkin arkikielessä tietoturvallisuutta käytetään kyberturvallisuuden synonyyminä. Näillä kahdella on kuitenkin huomattavan suuria eroja toisiinsa. Seuraavaksi avataan tietoturvallisuuden ja kyberturvallisuuden eroja.

Ymmärtääksemme kyberturvallisuutta on ensin ymmärrettävä kyberavaruus käsitteenä. Kuehl (2009) on jakanut kyberavaruuden neljään kerrokseen: 1) operationaalinen paikka, 2) elektroniset laitteet, 3) informaatio ja 4) verkkojen yhteenliittymä. Kyberavaruus on operationaalinen paikka, jossa ihmiset ja heidän organisaationsa käyttävät tarvittavia teknologioita vaikuttaakseen kyberavaruudessa tai fyysisessä maailmassa. Tämän takia se voidaankin nähdä samankaltaisena kuin neljä muuta ympäristöä jossa toimimme. Nämä neljä ympäristöä ovat maa, ilma, vesi ja avaruus. Toiseksi kyberavaruus koostuu elektronisista laitteista, joiden avulla voimme luoda tai ”siirtyä” kyberavaruuteen. Nämä laitteet luovat monimuotoisen ja alati muuttuvan kyberavaruuden, sillä jokainen laite tuo mukanaan omat uniikit piirteensä. Tästä pääsemmekin kolmanteen kerrokseen. Näiden elektronisten laitteiden avulla voimme luoda, tallentaa, muokata, vaihtaa ja hyödyntää informaatiota. Viimeiseksi kyberavaruus on itsenäisten ja yhdistyneiden verkkojen yhteenliittymä. Kyberturvallisuus pyrkii suojaamaan tätä maailmaa kaikilla neljällä eri tasolla. Sen tarkoituksena on luoda kai-

kille turvallinen kyberavaruus, jossa järjestelmät ja infrastruktuuri toimivat moitteettomasti, jossa informaatio on oikeaa ja luotettavaa sekä ympäristö jossa käyttäjän on turvallista toimia. (Kuehl, 2009.)

Tietoturvallisuudella tarkoitetaan eheyden, luottamuksellisuuden ja informaation saatavuuden turvaamista (Solms & Niekerk, 2013). Tämän lisäksi tietoturvallisuudella tarkoitetaan informaation ja sen kriittisten elementtien, kuten järjestelmien ja laitteiden suojaamista. Nämä laitteet käyttävät, säilyttävät ja välittävät informaatiota (Whitman & Mattord, 2009). Tietoturva pyrkiikin turvaamaan informaatiota ja sitä tallentavia sekä käyttäviä laitteita. Tällöin informaatiota sisältävän tietokoneen tuhoaminen fyysisin keinoin on tietoturvariski. Koska kyberturvallisuus taas pyrkii suojaamaan kybermaailmassa tapahtuvia hyökkäyksiä, ei fyysinen hyökkäys laitetta kohtaan ole kyberturvallisuusuhka. Vastaavasti tietoturva ei suojaa käyttäjää, kun taas kyberuhkissa käyttäjä nähdään osana kyberavaruutta ja näin ollen myös hänen turvallisuutensa on kyberturvallisuudessa huomioitava. (Solms & Niekerk, 2013.)

Yksinkertaisuudessaan voitaisiinkin todeta, että kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa on turvauduttu kaikilta kyberavaruudesta tulevilta hyökkäyksiltä. Tietoturvallisuus taas kattaa turvautumisen kaikilta hyökkäyksiltä, joiden kohteena ovat tietojärjestelmät tai niihin tallennettua data. Näin ollen voidaankin todeta, että kyber- ja tietoturvallisuus eivät ole toistensa synonyymejä, vaikka ne osittain turvaavatkin samoja asioita (Solms & Niekerk, 2013).

3.2 Kyberavaruuden uhkat

Nykyään kohtaamme hyvin erilaisia kyberuhkia ja hyökkäysten tekijät ovat innovatiivisia toteuttaessaan hyökkäyksiään. Vuosien 2004 – 2013 aikana hyökkääjät ovat kasvattaneet onnistumistaan kyberhyökkäyksissään 75 prosentista noin 90 prosenttiin. Samaan aikaan järjestelmiä valvovien tahojen kyky huomata käynnissä olevat hyökkäykset muutamien päivien aikana hyökkäyksen alusta on kasvanut vain 13 prosentista 20 prosenttiin. (Fonash & Schenck, 2015.) Hyökkääjien ja järjestelmiä valvovien tahojen välillä onkin huomattava innovaatiokuilu ja tämän kuilun takia yhä suurempi osa hyökkäyksistä pääsee järjestelmiin huomaamattomasti. Fonashin ja Schneckin (2015) mukaan syynä tähän on ihminen, joka valvoo järjestelmän toimintaa ja pyrkii korjaamaan sitä poikkeustilanteessa. Heidän mielestään ihminen on liian hidas ja kykenemätön huomaamaan käynnissä olevia hyökkäyksiä. He ehdottavatkin ratkaisuksi osana aktiivista järjestelmää toimivan ihmisen korvaamista automaattisilla laitteilla. Ongelmana tässä on, että vaikka koneet ovatkin toisissa tehtävissä ihmistä huomattavasti nopeampia, eivät ne silti ole yhtä tehokkaita tunnistamaan epäilyttävää toimintaa. Esimerkiksi Googlen kehittämä tekoäly pystyi tunnistamaan kissan YouTube-videoista 74,8 prosentin todennäköisyydellä (Clark, 2012). Tämä voi aluksi kuulostaa todella tehokkaalta, mutta on yleisesti tiedossa, että ihminen pystyy tunnistamaan kissan lähes 100 prosentin tarkkuudella (Thiel & Masters, 2014). Tietojärjestelmiä

suunniteltaessa tulisikin huomioida ihmisen mahdollisuus toimia osana järjestelmää.

PayPal kohtasi alkuaikoinaan ongelmia väärennöksiin ja huijauksiin liittyen. Tämän seurauksena PayPal teki huomattavia tappioita. PayPal yritti luoda ohjelmaa, joka tunnistaisi väärennökset sekä huijaukset. Rikolliset kuitenkin vaihtoivat taktiikkaansa muutaman tunnin sisällä eikä ohjelmisto pysynyt muuttuneiden taktiikoiden perässä. Tämän seurauksena PayPal kehitti ohjelmiston, joka liputti kaikki epäilyttävät tapahtumat. Liputuksen jälkeen työntekijä kävi tapahtuman läpi ja päätti toimenpiteistä. Yhdistämällä ihmisen tietojärjestelmän tärkeäksi osaksi, yritys sai tiputettua onnistuneiden huijausten määrää. (Thiel & Masters, 2014.) Onkin huomioitava, että vaikka monia kyberuhkia voidaan ratkoa automaattisella valvonnalla, on ihminen kuitenkin edelleen ylivertainen koneeseen verrattuna toisilla aloilla. Tämän takia emme pysty vielä automatisoimaan kaikkia tehtäviä ja useat automatisoidut tehtävät vaativat edelleen ihmisen valvontaa toimiakseen parhaalla mahdollisella tavalla.

Kyberavaruudessa on myös useita muita uhkia kuin vain haavoittuvuuksien löytäminen ja hyödyntäminen. Näitä uhkia ovat esimerkiksi hyökkäyksien hajauttamisen mahdollisuus. Kyberavaruudessa yksittäisenkin henkilön on mahdollista toteuttaa hyökkäys, joka tapahtuu samanaikaisesti useasta IP-osoitteesta ja samalla säilyttäen anonymiteetin (Lau, Rubin, Smith & Trajkovic, 2000). Lisäksi taito kyberhyökkäyksiin on erittäin helppo hankkia, sillä verkossa myydään ohjelmistoja, jotka toteuttavat halutun kaltaisia hyökkäyksiä lähes automaattisesti. Tästä hyvänä esimerkkinä ovat bottiverkot. Bottiverkko on useiden internetiin liittyneiden laitteiden joukko, jota voidaan kontrolloida yhdellä laitteella (Christensson, 2010). Hyökkääjä voi bottiverkon luodakseen esimerkiksi lähettää exe-tiedoston uhrin laitteeseen. Tiedosto reagoi hyökkääjän komentoihin ja näin ollen hyökkääjä voi käskeä uhrin laitetta toteuttamaan hänen komentojaan. (Liu, Xiao, Ghaboosi, Deng & Zhang, 2009.) Usein bottiverkkoja käytetään palvelunestohyökkäyksiin (Denial of Sevice, DoS). Palvelunestohyökkäyksen tarkoitus on ruuhkauttaa kohdepalvelu hitaammaksi tai pahimmillaan saattaa se käyttökelvottomaksi. Sen toimintatapa on erittäin yksinkertainen. Hyökkääjä lähettää suuren määrän pyyntöjä kohdepalveluun, jolloin palvelu ei ehdi vastaamaan näihin kaikkiin. Tämän takana voi olla yksi tai useampia hyökkääjiä. Jos hyökkäys tapahtuu useasta IP-osoitteesta, kutsutaan hyökkäystä hajautetuksi palvelunestohyökkäykseksi (Distributed Denial of Service, DDoS). Samoin, jos yksittäinen henkilö toteuttaa hyökkäyksen useasta IP-osoitteesta, kutsutaan hyökkäystä hajautetuksi palvelunestohyökkäykseksi. (Altiparmak, Tekeoglu & Tosun, 2011; Peng, Leckie & Ramamohanarao, 2007.)

DoS-hyökkäyksiä voidaan toteuttaa useilla eri keinoilla, joiden monimuotoisuudesta kolme seuraavaa esimerkkiä ovat 1) SYN-hyökkäys (SYN flood attack), 2) PING-hyökkäys ja 3) smurffihyökkäys (smurf attack). SYN-hyökkäyksessä hyökkääjä käyttää hyväkseen tiedonsiirtoyhteyden varmistavaa kolmiosaista kättelyä. Kättelyssä käyttäjä lähettää ensin palvelulle SYN-pyynnön, johon palvelu vastaan SYN-ACK -vastauksella, jonka jälkeen käyttäjä viimeistelee

kättelyn vastaamalla ACK. SYN-pyyntö tarkoittaa TCP/IP-protokollassa tahdistuslippua (syncronize flag) eli se ilmoittaa palvelulle, että kyseinen käyttäjä haluaisi käyttää palvelua. ACK-viesti tarkoittaa kuittauslippua (acknowledge flag) eli SYN-ACK-viestin tarkoitus on ilmoittaa käyttäjälle, että hän voi käyttää palvelua ja viimeinen ACK-viesti ilmoittaa palvelulle käyttäjän saaneen SYN-ACK-viestin. Jos palvelu ei vastaanota määritetyn ajan sisällä ACK-viestiä, lähettää se käyttäjälle uuden SYN-ACK-viestin. SYN-hyökkäyksen tarkoituksena onkin tuottaa palvelulle, niin paljon keskeneräisiä kättelyitä, ettei se voi vastata muille käyttäjille. Keskeneräisiä kättelyitä syntyy, kun hyökkääjä ei koskaan lähetä palvelulle ACK-viestiä. (Nakashima & Oshima, 2006.)

Toinen mahdollinen DoS-hyökkäystapa on hyödyntää ping-komentoa. Tämä komento mahdollistaa käyttäjän tiedustelun kohdelaitteelta tämän yhteydestä lähettäjään. Hyökkääjä käyttää useita väärennettyjä IP-osoitteita, joista lähettää komentoa kohdelaitteelle (Udhayan & Anitha, 2009). Tämän ansiosta kohdelaite vastaa epäröimättä komentoon, kunnes hukkuu komentotulvaan, eikä enää pysty vastaamaan käyttäjille.

Kolmatta DoS-hyökkäystapaa kutsutaan smurffihyökkäykseksi (Smurf attack) tai vahvistushyökkäykseksi (amplification attack). Tässäkin hyökkäyksessä hyökkääjä käyttää usein hyödykseen ping-komentoa ja lisäksi verkon muita laitteita. Hyökkääjä muokkaa ensin ping-komentoon uhrin IP-osoitteen ja sen jälkeen lähettää ping-komennon useille eri verkon laitteille. Laitteet vastaavat komentoon lähettämällä datan uhrin koneeseen. Näin ollen mitä useammalle laitteelle hyökkääjä lähettää ping-komentoja, sitä hitaammaksi uhrin laite muuttuu, kunnes siitä tulee käyttökelvoton. (Kumar, 2007.)

Kuten edeltä käy ilmi, on kyberavaruudessa useita erilaisia uhkia. Yllä kuvatut uhkat eli järjestelmän heikkouksien etsiminen ja hyödyntäminen, hyökkäysten hajauttaminen, bottiverkot, sekä DoS-hyökkäykset koskettavat kaikkia palveluita, jotka toimivat kyberavaruudessa. Kuvattujen uhkien lisäksi verkossa voi toteuttaa useita erilaisia hyökkäyksiä, jotka koskettavat kaikkia kyberavaruuden laitteita sekä järjestelmiä. Näiden lisäksi erilaiset laitteet ja järjestelmät, sekä muun muassa esineiden internet kohtaavat niille erityisiä uhkia. Seuraavassa kappaleessa käydäänkin läpi minkälaisia uhkia esineiden internet kohtaa yleisten kyberturvallisuusuhkien lisäksi.

4 ESINEIDEN INTERNETIN KYBERTURVALLISUUS

Tässä sisältöluvussa vastataan tutkimuskysymyksiin ja käsitellään esineiden internetin kyberturvallisuuden erityispiirteitä ja minkälaisia uhkia esineiden internet kohtaa jatkuvasti kasvavassa verkossa. Tämän lisäksi tarkastellaan erilaisia kyberturvallisuusratkaisuja, joilla näitä uhkia pyritään ehkäisemään.

4.1 Kyberturvallisuusuhkat esineiden internetissä

Esineiden internetissä on aivan uudenlaisia kyberturvallisuusriskejä, sillä ne toimivat suuremmassa yhteistyössä fyysisen maailman kanssa kuin perinteiset järjestelmät. Niiden kyberturvallisuudessa on kuitenkin huomattavan suuria aukkoja, joita hyökkääjät voivat käyttää hyödykseen. Tämä johtuu osittain kehittäjien virheellisestä ajatusmaailmasta, että käyttäjät käyttäisivät laitteitta poikkeuksetta yksityisissä verkoissa ja näin ollen vastaisivat itse laitteiden turvallisuudesta (Tuen, 2015).

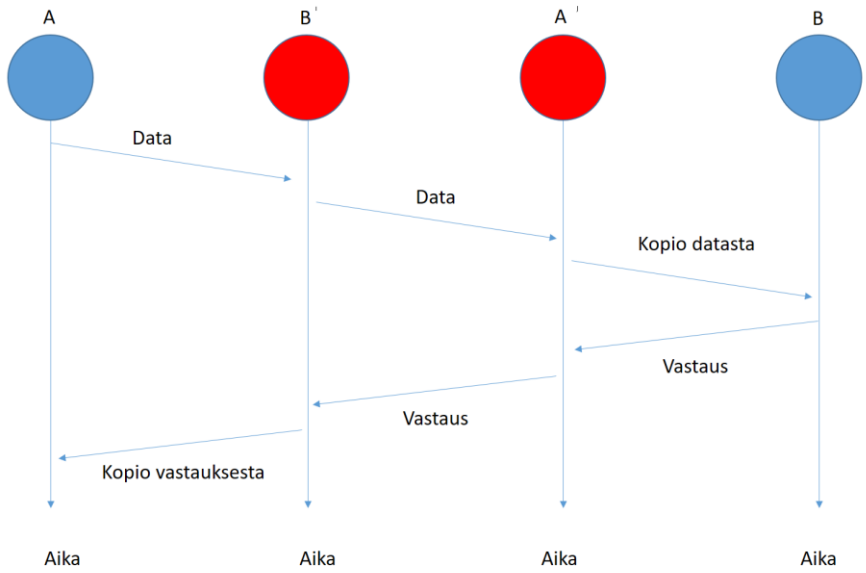
Fyysisen maailman yhteydestä esimerkkinä toimivat lääketieteelliset laitteet. Kyberturvallisuusyritys Cylance on löytänyt yli 300 lääketieteellistä laitetta, jotka ovat haavoittuvaisia kyberhyökkäyksille (Solms & Niekerk, 2013). Tämän kaltaisia laitteita ovat esimerkiksi insuliinipumppu, joka hyökkääjän halutessa voisi tappaa käyttäjän pumppaamalla käyttäjän täyteen insuliinia. Esineiden internetin kyberturvallisuus onkin erittäin tärkeä, koska sillä voi olla hyvinkin merkittäviä fyysisiä maailman uhkia ja se mahdollistaa jopa verkon kautta tehdyn murhan.

Esineiden internet on erittäin haavoittuvainen erilaisille hyökkäyksille neljästä eri syystä. Ensinnäkin useat komponentit, kuten sensorit, viettävät pitkiäkin aikoja ilman valvontaa. Tämän takia sensorit ovat erittäin alttiita luonnonvoimille sekä fyysiselle ilkivallalle. Toiseksi kaikki komponentit kommunikoivat pääsääntöisesti langattomasti ja tästä syystä ovat alttiita salakuuntelulle. Kolmanneksi suurin osa esineiden internetin komponenteista on melko tehottomia sekä virran että laskentatehon suhteen. Tämän takia niille on mahdotonta luoda

monimutkaisia turvallisuusratkaisuja. (Atzori, Iera & Morabito, 2010; Sayana & Joshi, 2016.) Neljänneksi heterogeenisen ympäristön takia ohjelmistoissa saattaa olla heikkouksia ja takaovia (Zhang, Cho, Wang, Hsu, Chen & Shieh, 2014). Seuraavaksi kuvataan esineiden internetin kyberuhkia hieman enemmän.

Esineiden internet kerää jatkuvasti dataa fyysisestä maailmasta lukemattomilta sensoreilta. Nämä sensorit ovat usein ilman valvontaa ja tästä syystä luonnonvoimat, sekä fyysiset hyökkäykset voivat häiritä tai rikkoa laitteet helposti (Atzori ym., 2010). Hyökkääjä voi helposti, vaikka tuhota sensorin, jos se on esillä. Toisaalta, jos sensori käyttää aurinkoenergiaa toimiakseen, on suhteellisen helppo estää auringonsäteitä pääsemästä sensorille asti ja näin ollen sammuttaa laite. Tämän lisäksi myös sensorin lukemaa dataa on yksinkertaista muokata vääräksi vaihtamalla sen paikkaa tai muokkaamalla sen mittamaa ympäristöä. Esimerkiksi, jos sensori mittaa ilmankosteutta ja se upotetaan veteen, tuottaa se jatkuvasti väärää dataa käyttäjälle. Toisaalta sensorit ovat myös luonnonvoimien armoilla, joten niiden tulisikin kestää aina paikastaan riippuen vallitsevia olosuhteita.

Toinen esineiden internetin kohtaama kyberturvallisuusuhka on langattomien verkkojen yksinomainen käyttäminen. Sensorien lähettäessä dataa yhdyskäytävälle, on hyökkääjien mahdollista salakuunnella tätä liikennettä esimerkiksi man-in-the-middle-hyökkäyksen muodossa. Tässä hyökkäyksessä kaikki sekä sensorin että käyttäjän lähettämä data kulkee aina hyökkääjän kautta eteenpäin. Kuviosta 2 huomataan, kuinka sensorin A lähettäessä dataa yhdyskäytävälle B, kulkee viesti ensin hyökkääjälle, joka sitten välittää datan yhdyskäytävälle. Hyökkäyksen toteuttamiseen hyökkääjä tarvitsee kaksi komponenttia. Ensimmäinen sijoitetaan lähelle alkuperäistä lähettäjää ja toinen lähelle alkuperäistä vastaanottajaa. Tarkoituksena on luoda sekä lähettäjälle että vastaanottajalle kuva, että ne kommunikoivat oikean tahon kanssa. Todellisuudessa, kun lähettäjä A lähettää dataa, ei sen vastaanottaja ole B, vaan hyökkääjän B’. Tämän jälkeen hyökkääjä siirtää datan A’ lähettimelleen ja sieltä datan vastaanottajalle B. (Atzori ym., 2010.)



KUVIO 2 Man-in-the-middle-hyökkäys (Atzori ym., 2010)

Atzorin ym. (2010) kuvaama hyökkäys siis mahdollistaa hyökkääjän saavan kaiken sensorien ja yhdyskäytävän välisen datan omaan käyttöönsä. Tämän lisäksi jopa suurempi uhka kyseisessä hyökkäyksessä on datan luotettavuus. Kun data kulkee ulkopuolisen kautta, ei voida varmistua datan oikeellisuudesta, sillä hyökkääjä saattaa muuttaa hänen kauttaan kulkemaa dataa.

Kolmanneksi esineiden internetissä laitteet ovat pääsääntöisesti varustettu hyvin pienellä virralla sekä laskentateholla. Tämän takia niiden suojaamiseen on käytettävä kevyitä ratkaisuja, verrattuna perinteisessä internetissä toimiviin laitteisiin kuten tietokoneisiin ja puhelimiin, joissa on huomattavasti enemmän laskentatehoa. Tietokoneita ja puhelimia voidaan suojata huomattavasti vahvemmilla ratkaisuilla, koska niillä on suurempi laskentateho. (Jing, Vasilakos, Wan, Lu & Qiu, 2014.) Tietokoneiden ylivertainen laskentateho verrattuna esineiden internetin laitteisiin tekee myös mahdolliseksi ja toisinaan jopa helpoksi murtaa esineiden internetin kevyet suojaukset.

Neljäs suuri ongelma esineiden internetissä on suuri heterogeenisuus, joka vallitsee varsinkin RFID:n ja WSN:n välillä. Näiden välillä ja jopa niiden sisällä saattaa olla käytössä erilaisia protokollia, joista seuraa yhteensopivuusongelmia. Ne saattavat käyttää erilaisia tallennusformaatteja ja erilaisia turvallisuusratkaisuja. Lisäksi erilaisten tallennusformaattien takia ne käyttävät erilaisia metodeja datan prosessoimiseen. (Jing ym., 2014.) Tämän seurauksena dataa ei välttämättä saada siirrettyä sensorilta käyttäjän laitteelle tai data saattaa vääristyä matkan varrella. Jos järjestelmä ei osaa ilmoittaa puuttuvasta tai vääristyneestä datasta, käyttäjä saattaa tehdä virheellisiä päätöksiä puutteellisen datan seurauksena.

Kuten tutkielmassa esille tulleista uhkista huomataan, voi niillä toteutuessaan olla suuriakin vaikutuksia sekä laitteiden luotettavuuteen, että toimintaan. Seuraavassa luvussa perehdytään ratkaisuihin, joita näihin uhkiin on tällä hetkellä kehitetty.

4.2 Uhkilta suojautuminen – ratkaisuja kyberturvallisuusuhkiin

Esineiden internetin kohtaamiin fyysisiin uhkiin, kuten sensoreiden tuhoamiseen ja häiritsemiseen ei ole vielä juurikaan löydetty ratkaisuja. Aina kun laite jätetään luontoon ilman valvontaa, on mahdollista, että joku pahantahtoinen henkilö löytää laitteen ja tekee sille ilkivaltaa. Tätä estääkseen laitteet pyritään sijoittamaan paikkoihin, josta niitä ei löydettäisi yhtä helposti ja jos mahdollista suojaamaan paremmalla kuorella. (Jing ym., 2014.) On kuitenkin huomioitava, että laitteen piilottaminen tai sen parempi muu suojaaminen ei saa vaikuttaa laitteen tekemiin mittauksiin.

Toinen esineiden internetin kyberturvallisuusuhka on langattoman kommunikoinnin tuomat heikkoudet. Ratkaisuna tähän on kommunikoinnin salaaminen, joka voidaan toteuttaa joko symmetrisillä avaimilla tai julkisilla avaimilla (Zhang ym., 2014). Symmetrisillä avaimilla salatessa molemmilla osapuolilla on sama salausavain ja lähetetyt viestit salataan aina kyseisellä salausavaimella. Vastaanottajan saadessa salatun viestin, hän käyttää samaa salausavainta purkaakseen viestin (Delfs & Knebl, 2007, s. 11-12). Julkisilla avaimilla salatessa molemmat osapuolet jakavat toiselle osapuolelle oman julkisen avaimen ja säilyttävät itsellään salatun avaimen. Viestit salataan aina vastaanottajan julkisella avaimella ja niiden purkaminen vaatii vastaanottajan salaista avainta (Rivest, Shamir & Adleman, 1978). Julkisilla avaimilla datan suojaaminen on symmetrisiä avaimia tehokkaampi tapa. Suurin syy tähän on, että symmetrisillä avaimilla salatessa datan vastaanottajan täytyy luottaa toiseen osapuoleen, ettei tämä jaa suojausavainta. Julkisilla avaimilla suojaaminen vaatii kuitenkin huomattavasti enemmän laskentatehoa ja näin ollen esineiden internetissä tämä ei aina ole mahdollista (Zhang ym., 2014). Esineiden internet vaatiikin edelleen parempia kevyitä salausmenetelmiä, jotka laitteet pystyvät toteuttamaan ja jotka ovat tarpeeksi tehokkaita salatakseen datan ulkopuolisilta.

Kolmantena uhkana esineiden internetin kyberturvallisuuteen on sen useiden laitteiden heikko laskentateho sekä virta. Tämän takia laitteita on suojattu kevyillä turvallisuusratkaisuilla. Ongelmaksi nousee kuitenkin edelleen, että usein joudutaan tasapainottelemaan turvallisuusratkaisun ja laskentatehon käytön välillä. (Jing ym., 2014.) Verrattuna perinteisiin internetin laitteisiin, kuten tietokoneisiin, joissa voidaan yhdistellä kevyitä ja muita turvallisuusratkaisuja, on esineiden internetin turvallisuusratkaisut auttamatta heikompia (Atzori, 2010). Heikon laskentatehon takia esineiden internetin on myös käytettävä pilvilaskentaa. Sensorit siirtävät jatkuvasti dataa pilvipalveluihin tallennettavaksi sekä laskentaa varten. Tästä seuraa hitaita päätöksiä esineiden internetin datan perusteella, sillä datan siirtäminen pilvilaskentakeskukseen vie aikaa, sekä datakaistaa. Ratkaisuna tähän olisi sumulaskenta (fog computing). Sumulaskenta toisi laskentatehon lähemmäksi itse sensoreita ja näin ollen vähentäisi kommunikoinnin tarvetta pilvipalveluihin. Sumulaskennassa sensorin lähettäessä datan

yhdyskäytävällä, ei yhdyskäytävä lähetäkään dataa pilvilaskentaan, vaan käyttää esimerkiksi yhdyskäytävän omaa laskentatehoa tai joitain muuta lähellä sijaitsevaa laitetta, tehdäkseen tarvittavat laskut. (Shi, Cao, Zhang, Li, Xu, 2016.)

Vanhat yhdyskäytävät ovat suhteellisen helppo korvata uusilla, joissa on parempi laskentatehoa ja näin esineiden internet saadaan jo toimimaan huomattavasti paremmin. Muiden laitteiden liittäminen sumulaskentaan onkin hieman haastavampi tehtävä. Lohkoketjusovellutus IOTA on kuitenkin kehittämässä tähän ratkaisua. IOTA tarjoaa esineiden internetille hajautettua verkkoa, johon kuka vain voi liittää laitteita ja näin ollen tarjota esineiden internetille kaivattua laskentatehoa korvausta vastaan (IOTA, 2017). Tämä sovellutus on kuitenkin vasta kehitysasteella, eikä vielä ole minkäänlaista informaatiota sen valmistumisajankohdasta.

Neljäntenä uhkana on heterogeenisuus. Tämän seurauksena dataa saattaa kadota siirrettäessä sitä sensorilta eteenpäin. Toisaalta heterogeenisuuden takia sovelluskehittäjien on vaikea toteuttaa sovelluksia, joissa ei ole takaovia, eikä muita selkeitä turvallisuusriskejä. Tämä voitaisiin ratkaista dynaamisella analyysilla, jossa ohjelmistoa käytetään reaaliajassa ja ohjelmistoa tutkitaan samalla tavalla kuin hyökkääjä tutkii ohjelmistoa. Tarkoituksena on löytää kaikki ohjelmiston heikkoudet, jotka hyökkääjä voisi löytää ja sen jälkeen paikata kyseiset aukot. Esineiden internetin laitteiden heikon laskentatehon takia dynaaminen analyysi esineiden internetissä ei kuitenkaan ole aina mahdollista ja siksi analyysi tulisikin suorittaa tehokkaammilla laitteilla käyttäen emulaattoria (Zhang ym., 2014.) Emulaattori on laite tai ohjelmisto, jolla voidaan mallintaa haluttu järjestelmä toisessa laitteessa (Christensson, 2008). Tämän ansiosta esineiden internetin laitteita voitaisiin testata tietokoneella, jolloin useampia ongelmia voitaisiin löytää ennen tuotteen julkaisemista käyttäjille. Ongelmaksi nousee emulaattorin ja esineiden internetin mahdollinen eroavaisuus. Toimivan emulaattorin tekeminen on haastavaa ja kallista, koska esineiden internetissä toimii useita erilaisia laitteita, kuten GPS ja RFID (Zhang ym., 2014). Tämän takia toimivan emulaattorin luominen on mahdotonta varsinkin pienille toimijoille, joilla ei ole vaadittuja resursseja. Esineiden internetille tulisikin kehittää toimiva ja kaikkien saatavilla oleva emulaattorialusta, jonka avulla laitteille voitaisiin toteuttaa dynaaminen analyysi, ilman laitteiden eroavaisuuksien tuottamia ongelmia.

Ning ym., (2013) ovat ehdottaneet ratkaisuksi esineiden internetin ongelmiin the Unit and Ubiquitous IoT:n (U2IoT) kehittämistä. Tässä ratkaisussa salakuunteluyritykset estettäisiin tietojen salaamisella ja man-in-the-middle-hyökkäykset erilaisilla aikaleimoilla ja käyttäjien tunnistamisella, jolloin järjestelmä havaitsisi hyökkääjän. Lisäksi asennettaisiin useita palomuureja, virustorjuntaohjelmia, tunkeutujan tunnistamisohjelmia sekä häirinnän estolaitteita, kuten Faradayn häkki. Tämäkään malli ei kuitenkaan ota huomioon fyysisten laitteiden turvattomuutta valvomattomissa sijainneissa. U2IoT:n käyttöönotto vaatisi kuitenkin todella paljon jatkotutkimuksia ennen kuin se olisi mahdollista.

Taulukosta 1 huomataan, että kaikkiin kyberturvallisuusuhkiin on jonkin asteisia ratkaisuja. Kaikissa näissä ratkaisuissa on kuitenkin ratkaisemattomia

ongelmia ja nämä ongelmat tuleekin ottaa huomioon kyseisiä ratkaisuja käytettäessä.

TAULUKKO 1 Kyberturvallisuus uhkien ratkaisut

Kyberturvallisuusuhka	**Ratkaisu**	**Ongelma ratkaisussa**
Fyysiset uhkat	Laitteen piilottaminen tai parempi suojakuori	Suojaus ei saa vaikuttaa mitattaviin arvoihin
Langaton kommunikointi	Salaaminen symmetrisillä tai julkisilla avaimilla	Näistä vaihtoehdoista julkisilla avaimilla on tehokkaampaa, mutta esineiden internetin laskentateho ei tähän aina riitä
Heikko laskentateho	Pilvilaskenta	Vie aikaa ja datakaistaa
Heikko laskentateho	Sumulaskenta	Käytännön toteutus vaatii jatkotutkimuksia
Heterogeeniset laitteet	Dynaaminen testaus emulaattorissa	Emulaattorin luominen todella hidasta ja kallista. Tämän seurauksena sen luominen on mahdotonta varsinkin pienille toimijoille
Langaton kommunikointi, heikko laskentateho ja heterogeeniset laitteet	Uusi esineiden internet nimeltä U2IoT	Vaatii lisää tutkimusta, sillä kehitys on vasta suunnitteluasteella

Kuten uhkilta suojautumisratkaisuista huomataan, aihetta on tutkittu, mutta ratkaisujen toteuttaminen vaatisi esineiden internetiltä suuria muutoksia sekä laitteissa että verkossa. Monille uhkille on teoreettisia ratkaisuja, sekä useita kehitteillä olevia ratkaisuja. Useat näistä ratkaisuista eivät kuitenkaan vielä ole valmiita yleiseen käyttöön ja aihe vaatiikin tästä syystä vielä lisätutkimuksia.

5 YHTEENVETO

Tutkielmassa kartoitettiin kirjallisuuskatsauksen menetelmin esineiden internetin kyberturvallisuuden erityispiirteitä ja kyberturvallisuusratkaisuita. Lähdemateriaaleista pyrittiin valitsemaan luotettavimmat ja löydetyt tulokset jaettiin johdantoon, kolmeen sisältölukuun ja yhteenvetoon. Ensimmäisessä sisältöluvussa määriteltiin tärkeitä käsitteitä, kuvattiin esineiden internetin sekä 3-kerroksinen että 5-kerroksinen mallin kautta (Al-Fuqaha ym., 2015). Toisessa luvussa määriteltiin kyberavaruus kolmikerroksiseksi (Kuehl, 2009) ja määriteltiin kyberturvallisuus sekä sen eroavaisuus tietoturvallisuudesta.

Viimeisessä sisältökappaleessa käsiteltiin esineiden internetin kyberturvallisuuden erityispiirteitä ja vastattiin tutkimuskysymyksiin, jotka olivat:

1. Mitä erityispiirteitä esineiden internetissä on kyberturvallisuuden näkökulmasta?
2. Miten näiltä erityispiirteiden aiheuttamilta uhkilta suojaudutaan?

Tutkimuksessa havaittiin neljä erityispiirrettä esineiden internetin kyberturvallisuudelle. Nämä olivat:

1. komponenttien oleminen fyysisessä maailmassa valvomattomissa,
2. komponentit käyttävät lähes yksinomaan langattomia kommunikointitapoja,
3. suuri osa esineiden internetin komponenteista omaavat hyvin vähän virtaa, sekä laskentatehoa (Atzori ym., 2010) ja
4. heterogeenisuuden takia laitteisiin ja ohjelmistoihin jää selkeitä haavoittuvuuksia, sekä takaovia (Zhang ym., 2014).

Tämän lisäksi viimeisessä kappaleessa pyrittiin löytämään ratkaisuita, kuinka näiltä ongelmilta vältytään esineiden internetissä. Tutkimuksessa paljastui, että vaikka asiaa on tutkittu lähiaikoina paljon, ei vieläkään ole löydetty täysin toimivia ratkaisuita, jotka poistaisivat esineiden internetin kyberturvallisuuden ongelma. Lisäksi useissa ratkaisuissa on edelleen ratkaisemattomia ongelmia, jotka

tulisi ratkaista ennen kuin kyseiset kyberturvallisuusratkaisut voidaan ottaa laajamittaisesti käyttöön esineiden internetissä. Ratkaisuksi on ehdotettu koko esineiden internetin uudelleen luomista (Ning ym., 2013), mutta nykyiseen esineiden internetiin ei ole löydetty ratkaisuja kaikkiin sen kyberuhkiin.

Kuten aikaisemminkin on tullut ilmi, oli tutkielma kirjallisuuskatsaus. Siitä johtuen väitteitä ja tuloksia ei ole saavutettu tai testattu käytännössä. Lisäksi tutkielman laajuus on suppeahko, mistä johtuen lähteiden vertailua on rajoitettu ja teknisiä ratkaisuita ei esitelty tarkimmalla mahdollisella tasolla. Tutkielma on myös tekijän ensimmäinen akateeminen tutkimus, jonka tarkoituksena on ollut opettaa akateemisen tutkimuksen tekoa. Tämä saattaa vaikuttaa tutkielmaan valittuihin lähteisiin sekä argumentaatioon.

Jatkotutkimusaiheiksi tutkielmassa nousi esineiden internetin kyberturvallisuus, sekä esineiden internetin järjestelmien toiminta heterogeenisessa ympäristössä. Kyberturvallisuuden osalta olisi tärkeää tutkia, kuinka olisi mahdollista toteuttaa kyberturvallinen esineiden internet huolimatta sen heikosta laskentatehosta. Toisaalta teoriassa olisi myös mahdollista kehittää kokonaan uusi esineiden internet ja näin ollen ratkaista useita nykyisen esineiden internetin kyberuhkia. Tämä kuitenkin vaatisi reilusti jatkotutkimuksia.

LÄHTEET

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*. 17(4), 2347-2376.

Altiparmak, N., Tekeoglu, A., & Tosun, A. Ş. (2011, November). DoS resilience of real time streaming protocol. *Performance Computing and Commu-nications Conference (IPCCC). 2011 IEEE 30th International*, 1-8.

Ashton, K. (2009). That 'internet of things' thing. *RFiD Journal*, 22(7), 97-114.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15), 2787-2805.

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1), 49-69.

Clark, L. (26.6.2012) Google's Artificial Brain Learns to Find Cat Videos. *Wired*. Haettu 28.4.2017 osoitteesta https://www.wired.com/2012/06/google-x-neural-network/

Christensson, P. (2010, June 9). Botnet Definition. Haettu osoitteesta https://techterms.com/definition/botnet

Christensson, P. (2008, June 26). Emulation Definition. Haettu osoitteesta https://techterms.com/definition/emulation

Christensson, P. (2016, September 21). IP Address Definition. Haettu osoitteesta https://techterms.com/definition/ip_address

Christensson, P. (2009, September 4). RFID Definition. Haettu osoitteesta https://techterms.com/definition/rfid

Delfs, H., & Knebl, H. (2007). *Introduction to cryptography*. Berlin: Springer

Evans, D. (2011). The internet of things: How the next evolution of the in-ternet is changing everything. *CISCO white paper*, 1(2011), 1-11.

Fonash, P., & Schneck, P. (2015). Cybersecurity: From months to millisec-onds. *Computer*, 48(1), 42-50.

Gray D. (2014) Data Ownership in the Cloud. *Dataconomy*. Haettu osoitteesta http://dataconomy.com/2014/03/data-ownership-in-the-cloud/

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7), 1645-1660.

IOTA. (13.11.2017) IOTA THE ECONOMY OF THINGS. Haettu osoitteesta https://iota.org/

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, 20(8), 2481-2501.

Kempf, J., Arkko, J., Beheshti, N., & Yedavalli, K. (2011). Thoughts on reli-ability in the internet of things. *Interconnecting smart objects with the Internet workshop*, 1, 1-4.

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: the internet of things architecture, possible applications and key challenges. *Frontiers of Information Technology (FIT), 2012 10th International Conference on*, 257-260.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. *Cyberpower and national security*, 24-42.

Kumar, S. (2007). Smurf-based distributed denial of service (ddos) at-tack amplification in internet. *Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on*, 25-25.

Lau, F., Rubin, S. H., Smith, M. H., & Trajkovic, L. (2000). Distributed denial of service attacks. *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*, 3, 2275-2280.

Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., & Zhang, J. (2009). Botnet: classification, attacks, detection, tracing, and preventive measures. *EURASIP journal on wireless communications and networking*. 2009, 1184-1187.

Macedo, D., Guedes, L. A., & Silva, I. (2014). A dependability evaluation for Internet of Things incorporating redundancy aspects. *Networking, Sensing and Control (ICNSC), 2014 IEEE 11th International Conference on*. 417-422.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), 1497-1516.

Misra, S., & Agarwal, P. (2012). Bio-inspired group mobility model for mobile ad hoc networks based on bird-flocking behavior. *Soft computing*, 16(3), 437-450.

Nakashima, T., & Oshima, S. (2006). A detective method for SYN flood attacks. *Innovative Computing, Information and Control, 2006. ICI-CIC'06. First International Conference on*, 1, 48-51.

Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the internet of things. *Computer*, 46(4), 46-53.

Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR)*, 39(1), 3.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.

Sayana, L. S., & Joshi, B. K. (2016). Security issues in internet of things. Uttarakhand: ICFAI.

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 3(5), 637-646.

Stankovic, J. A. (2008). Wireless sensor networks. *Computer*, 41(10), 92-95.

Masters, B., & Thiel, P. (2014). *Zero to one: notes on startups, or how to build the future*. New York: Crown Business.

Tuen, C. D. (2015) *Security in Internet of Things Systems*. Trondheim: NTNU.

Udhayan, J., & Anitha, R. (2009). Demystifying and rate limiting ICMP hosted DoS/DDoS flooding attacks with attack productivity analysis. *Advance Computing Conference, 2009. IACC 2009. IEEE International*. 558-564.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Boston: Cengage Learning.

Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014). IoT security: ongoing challenges and research opportunities. *Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on*, 230-234.