Tatu Latvala

KYBERTURVALLISUUS ESINEIDEN INTERNETISSÄ YKSILÖN NÄKÖKULMASTA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2016

TIIVISTELMÄ

Latvala, Tatu
Kyberturvallisuus esineiden internetissä yksilön näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2016, 27 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Koskelainen, Tiina

Tämä tutkielma käsittelee esineiden internetiä, kyberturvallisuutta, sekä miten nämä kaksi toimivat yhdessä. Tutkimuskysymyksinä ovat millaisia kyberturvallisuusriskejä yksilö voi kohdata esineiden internetin palveluissa, sekä miten näiltä riskeiltä voitaisiin suojautua. Esineiden internet on verkko, joka yhdistää miljoonia laitteita yhteen ja antaa niille mahdollisuuden kommunikoida keskenään. Sen tarkoitus on tehdä langattomista ja automatisoiduista toiminnoista arkipäivää ja laajamittaista, ulottuen kodin laitteista terveydenhuoltoon ja jopa elintarvikkeisiin. Ennen kuin esineiden internetin palvelut ja laitteet voivat saavuttaa laajamittaisen ja kokonaisvaltaisen tilan, on ratkaistava lukuisia ongelmia liittyen yksityisyyteen, turvallisuuteen sekä tiedon luottamuksellisuuteen. Tämä tutkielma luo katsauksen esineiden internetin kyberturvallisuusongelmiin yksilön kannalta ja joihinkin esitettyihin ratkaisuihin. Tutkielmassa esiteltävät toiminnot rajautuvat yksilön elämään vaikuttaviin palveluihin. Samalla tarkastellaan, mitä riskejä näiden palveluiden käytöstä voi koitua yksilölle. Aiheen tutkiminen on tärkeää, koska esineiden internet on nopeasti kasvava ja suhteellisen uusi käsite, eikä sen ongelmiin ole vielä puututtu tarpeeksi. Alan tutkimusta esineiden internetistä on paljon ja sitä tehdään jatkuvasti lisää, mutta kaikkiin ongelmiin ei ole vielä löytynyt ratkaisuja. Tutkielma on kirjallisuuskatsaus ja sen aineisto koostuu informaatioteknologian kirjallisuudesta, artikkeleista sekä konferenssijulkaisuista. Tutkimuksen tuloksena löytyi monia yksityisyyttä, turvallisuutta sekä luottamusta uhkaavia ongelmia, mutta hyvin vähän suoria ratkaisuja niihin. On siis todettava, että aihe vaati paljon lisää tutkimusta.

Asiasanat: Esineiden internet, kyberturvallisuus, RFID, yksityisyys, turvallisuus, tiedon luottamuksellisuus

ABSTRACT

Latvala, Tatu
Cyber security in the Internet of things from individual's perspective
Jyväskylä: University of Jyväskylä, 2016, 27 p.
Information Systems, Bachelor's Thesis
Supervisor: Koskelainen, Tiina

This study discusses the internet of things, cyber security and how these two function together. The questions in this study are, what kind of cyber security risks an individual can encounter while using internet of things and is there solutions to prevent these risks. The internet of things is a network connecting millions of devices together and making it possible for them to communicate together. The purpose of the internet of things is to make wireless and automated features a standard and pervasive, reaching from home automation to health care and even food products. Before internet of things, its services and devices, can achieve ubiquitous and pervasive state, a number of issues concerning privacy, security and data confidentiality has to be solved. This study gives a peek to the problems and some of the presented solutions for cyber security in the internet of things from individual's perspective. This study presents internet of things' applications that concern individual, while taking a look at the risks towards the individual from these applications. Studying this subject is important, because the internet of things is rapidly growing and relatively new term, which has many problems that have not been studied enough yet. There is a lot of study from the field and it is studied further all the time, but not all problems have been solved yet. As the result of this study, there is a lot of problems concerning privacy, security and confidentiality, but very little straight solutions for them. Because of this, the subject requires much more studying.

Keywords: Internet of things, cyber security, RFID, privacy, security, data confidentiality

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Esineiden internet on tällä hetkellä kehittyvä käsite, joka on kasvattanut nopeasti jalansijaansa modernin langattoman tietoliikenteen alalla. Perusidea esineiden internetissä on olla kokonaisvaltainen laitteiden ja esineiden verkosto ympärillämme. Se hyödyntää esimerkiksi RFID-tarroja, antureita, erilaisia laitteita, matkapuhelimia ja monia muita välineitä, jotka pystyvät kommunikoimaan ja tekemään yhteistyötä yhteisten tavoitteiden saavuttamiseksi. Esineiden internet tuo uusia ratkaisuja sekä teollisuus- ja palvelualoille, mutta myös kotitalouksiin automaation ja etäkäytön kautta. (Giusto, Iera, Morabito & Atzori, 2010.)

Toinen tärkeä osa tätä tutkielmaa on kyberturvallisuus. Kyberturvallisuus on hyvin laaja käsite, mutta yksinkertaisuudessaan sillä tarkoitetaan kriittisten palveluiden ja toimintojen suojaamista niin verkossa, kuin myös fyysisessä maailmassa (Lehto & Kähkönen, 2015). Kyberturvallisuus liittyy esineiden internetin käyttöön hyvin vahvasti, koska siellä liikkuva data on usein arkaluontoista ja sen kulku täytyy olla suojattu kunnolla, ettei se joutuisi vääriin käsiin. Tässä tutkielmassa keskitytään esineiden internetin kyberturvallisuuteen yksilön kannalta. Tämä tarkoittaa sitä, että tutkielmassa esitellyt riskit ja ratkaisut ovat sellaisia, jotka liittyvät yksilön arkipäivässä käyttämiin toimintoihin ja palveluihin. Näihin toimintoihin lukeutuvat esimerkiksi kotiautomaatio, terveydenhuollon palvelut, ajoneuvot ja monet muut palvelut.

Tutkielman tavoitteena on tutkia esineiden internetin kyberturvallisuutta yksilön kannalta. Keskeisinä tutkimuskysymyksinä tutkielmassa on, millaisia riskejä esineiden internetin käytöstä aiheutuu yksilölle, sekä onko ongelmiin suunniteltu tai kehitetty ratkaisuja. Sen tarkoituksena on lisätä ymmärrystä esineiden internetin käyttöön liittyvistä riskeistä ja puutteista. Aiheen tutkiminen on tärkeää, koska sekä esineiden internet, että kyberturvallisuus ovat ajankohtaisia aiheita. Esineiden internetin uskotaan kasvavan laajamittaiseksi ja kokonaisvaltaisesti laitteiden verkoksi, mutta sitä ei ole kuitenkaan vielä pystytty suojaamaan tarpeeksi hyvin (Gubbi, Buyya, Marusic & Palaniswami, 2013).

Tutkielma on toteutettu kirjallisuuskatsauksena. Olen käyttänyt lähteiden etsinnässä enimmäkseen Google Scholar -hakukonetta, jonka kautta olen löytänyt paljon informaatioteknologian artikkeleita, konferenssijulkaisuja sekä kirjallisuutta. Hyvin suuri osa käyttämistäni lähteistä on IEEE:n konferenssijulkaisuja. Olen myös käyttänyt Jyväskylän yliopiston kirjaston verkkopalveluita hyödyksi ja sitä kautta löytänyt muutamia esineiden internetiä käsitteleviä kirjoja. Lähteiden valinnassa olen pyrkinyt panostamaan ajankohtaisuuteen ja suurin osa käyttämistäni lähteistä onkin 2010-luvulta. Olen rajannut hyvin tekniset julkaisut pois lähdemateriaalistani.

Tutkielman tuloksena selvisi, että esineiden internetiin liittyy paljon ominaisuuksia, jotka ovat melko avoimia hyökkäyksille. Laitteiden välisessä yhteydessä käytetään paljon langatonta verkkoa ja toimintoja voidaan tehdä etäältä, jolloin hyökkääjän on mahdollista päästä liikkuvaan dataan käsiksi huomaamattomasti. Langattomia yhteyksiä käytettäessä hyökkääjä saattaa onnistua myös pääsemään kahden päätteen väliin, jolloin hän voi esiintyä toisena päätteistä ja saada näin arkaluontoista tietoa käyttöönsä. Tämän takia palveluista voi koitua suuri riski yksityisyydelle ja luottamukselle. Etäkäytöstä aiheutuu myös fyysisen tason ongelma, koska kaikkia laitteita ei valvota ja siksi niihin on helppo päästä fyysisesti käsiksi ja tehdä vahinkoa. Esineiden internetin turvallisuudesta on paljon puhetta, mutta hyvin suuri osa artikkeleista vaikuttaa vain listaavan vaatimuksia turvallisuudelle. Varsinaisia ratkaisuja ongelmien korjaamiseksi löytyy huomattavasti vähemmän tai ne ovat niin teknisiä ratkaisuja, että täytyy olla alan asiantuntija ymmärtääkseen niitä.

Tutkielma koostuu kolmesta käsittelyluvusta, jotka ovat esineiden internet, kyberturvallisuus sekä kyberturvallisuus esineiden internetissä. Pääpaino tutkielmassa on kuitenkin esiintyvillä kyberturvallisuusriskeillä, eikä niin paljoa ratkaisuissa. Ensimmäisessä luvussa esittelen esineiden internetiä sekä toiminnalliselta, että käyttötarkoitukselliselta kantilta. Tutkielman keskiössä on yksilö, joten tässä luvussa esiteltävät käyttötarkoitukset rajautuvat yksilöä hyödyttäviin laitteisiin ja palveluihin. Toisessa luvussa avaan kyberturvallisuutta käsitteenä. Kyberturvallisuus on merkittävä aihe tämän tutkielman kannalta, koska esineiden internet toimii verkon ja fyysisten laitteiden kautta, mutta sitä ei ole kaikin puolin pystytty vielä suojaamaan. Kolmannessa luvussa päästään itse pääongelmaan, eli käsittelen minkälaisia uhkia yksilö voi kohdata käyttäessään esineiden internetiä. Tarkastelen aihetta kolmen pääongelman kautta, jotka ovat yksityisyys, turvallisuus ja luottamuksellisuus. Tämän jälkeen käsittelen, millaisia toimenpiteitä esineiden internetin kyberturvallisuuden saavuttaminen vaatii ja esitän suunniteltuja ratkaisuja uhkien ehkäisemiseksi.

2 ESINEIDEN INTERNET

Esineiden internet, eli Internet of Things, on fyysisten laitteiden verkko, joka hyödyntää toiminnoissaan erilaisia sensoreita, mittareita, ohjelmistoja, elektroniikkaa sekä internetyhteyttä (Weber, 2010). Esineiden internetin tavoitteena on esimerkiksi edistää toimintojen automatisoitumista sekä etäkäyttöä. Käytännössä se siis tarkoittaa, että yhä useammat laitteet ovat yhteydessä internetiin ja pystyvät kommunikoimaan sen välityksellä keskenään sekä käyttäjän kanssa. (Kopetz, 2011.)

Esineiden internet on tällä hetkellä kasvava trendi informaatio- ja teollisuusaloilla sekä kotitalouksissa (Xia, Yang, Wang & Vinel, 2012). Esineiden internetille on keksitty lukuisia käyttötarkoituksia, eikä sen hyödyntäminen rajoitu pelkkiin laitteisiin, kuten kodin lämpötilasäätimiin tai älyjääkaappeihin. On mahdollista, että esineiden internetin yleistyessä sitä voidaan käyttää myös esimerkiksi vaatteissa tai jopa elintarvikkeissa.

Seuraavissa alaluvuissa kerron ensin yleisellä tasolla, kuinka esineiden internet toimii sekä millaisia teknologioita se hyödyntää toiminnoissaan. Tämän jälkeen tarkastelen, miten esineiden internet vaikuttaa yksilön elämässä, eli millaisia käyttötarkoituksia sillä on yksilön kannalta.

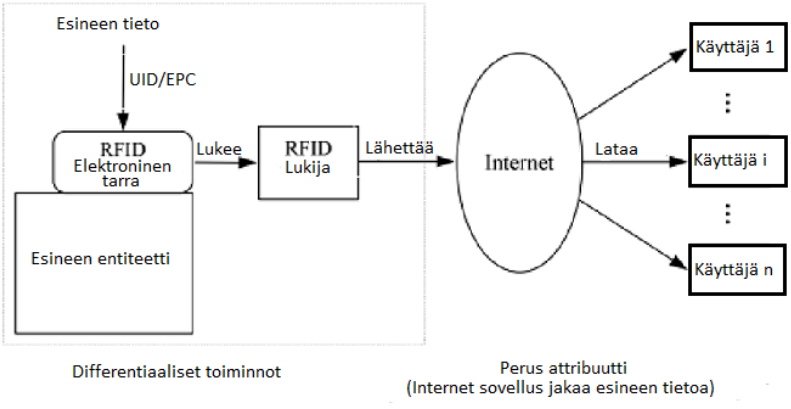
2.1 Toimintaperiaate ja tekniikat

Perusperiaatteeltaan esineiden internet koostuu laitteista, palveluista sekä palveluntarjoajista, ja sen tarkoitus on luoda kommunikointiyhteys kahden laitteen välille. Yksinkertaisesti ajateltuna esineiden internetin applikaatiot toimivat käytännössä seuraavalla tavalla. Käyttäjä haluaa lähettää laitteellaan, esimerkiksi älypuhelimella, toimintapyynnön toiselle laitteelle, jolloin älypuhelin lähettää signaalin eteenpäin. Signaali kulkeutuu langattoman verkkoyhteyden, kuten WiFi:n tai Bluetoothin, välityksellä laitteessa olevalle vastaanottimelle, joka taas välittää toimintopyynnön laitteeseen. Tämän jälkeen laite suorittaa pyydetyn toiminnon. (Zhu, Wang, Chen, Liu & Qin, 2010.)

Seuraavissa kappaleissa käydään läpi hieman tarkemmin erilaisia tekniikoita, joita esineiden internetin toiminnoissa hyödynnetään. Näitä toimintoja ovat esimerkiksi RFID-teknologia (radio frequency identification), elektroninen tuotekoodi, eli EPC (eletronic product code), sensoriverkot sekä erilaiset langattomat yhteydet. Jotta kommunikointi laitteiden ja asioiden välillä sekä niiden etäkäyttö olisi mahdollista, tarvitaan jonkinlainen lähetin sekä vastaanotin. Laitteiden välistä kommunikointia varten on otettu käyttöön muutamia erilaisia tekniikoita. Laitteiden välistä signaalia täytyy pystyä lähettämään, vastaanottamaan sekä lukemaan. Esimerkiksi RFID-teknologia pystyy tarjoamaan ratkaisun kommunikaatioon.

RFID-teknologia perustuu siihen, että laitteeseen tai esineeseen asennetaan pieni mikrosiru, joka sisältää sekä lähettimen että vastaanottimen. RFID-teknologian etu on esimerkiksi siinä, ettei lähettimen ja vastaanottimen välillä tarvitse olla suoraa ja esteetöntä yhteyttä. (Kopetz, 2011.) Tämän ominaisuuden ansiosta RFID-teknologia mahdollistaa etäkäytön ja automaattiset toiminnot. RFID-teknologia mahdollistaa myös esineiden tarkan paikkakohtaisen seurannan. Jotta laite tai asia voisi olla osa esineiden internetiä, vaaditaan siis jonkinlainen linkki, tässä tapauksessa RFID-mikrosiru. Kun RFID-mikrosiru tarvitaan jokaiseen esineiden internetin laitteeseen, niiden menekki kasvaa valtavasti, ja tästä johtuen RFID-sirujen hinnoittelu onkin varsin vaikeaa. (Kopetz, 2011.)

Esineen tieto ja sen tunniste voi olla tallennettuna koodina, esimerkiksi EPC:nä (electronic product code), joka kulkeutuu vastaanottimelle, joka voi olla esimerkiksi RFID-tarra. RFID-tarrasta tieto kulkeutuu eteenpäin, kun se luetaan RFID-lukijalla. Tämän jälkeen lukija siirtää tiedon verkkoon, jonka kautta käyttäjä pääsee siihen käsiksi omalla laitteellaan. (Huang & Li, 2010.) Seuraavassa kuviossa (kuvio 1) on esitettynä edellä mainittu esineiden välillä tapahtuva tiedon kulku:



KUVIO 1 Signaalin kulku RFID-teknologialla (Huang & Li, 2010, 485)

Esineiden toiminnoissa hyödynnetään myös monia muita tekniikoita, kuten langattomia sensoriverkkoja, eli WSN:iä (wireless sensor network). Sensoriverkkojen avulla pystytään esimerkiksi seuraamaan ja keräämään erilaista dataa laitteesta ja sen ympäristöstä, sekä prosessoimaan ja analysoimaan sitä. Sen-

soriverkot koostuvat useista solmukohdista, jotka toimivat verkon tiedonkerääjinä ja välittäjinä. Langattomat sensoriverkot ovat myös tehokkaita, halpoja sekä käyttävät vähän energiaa. (Gubbi ym., 2013.) Tästä syystä ne ovat erinomaisia esimerkiksi kodin energiankulutuksen seurannassa. Sensoreilta saatujen tietojen perusteella käyttäjä voi esimerkiksi säätää etäältä kodin lämpötilaa pienemmäksi kun ketään ei ole kotona, jotta energiaa säästyisi. Vastaavasti kun ollaan palaamassa kotiin, lämpötila voidaan nostaa sopivalle tasolle.

Esineiden internetin verkkoyhteystekniikoita perinteisten WiFi- sekä Bluetooth-yhteyksien rinnalla ovat myös ZigBee sekä Z-Wave. Nämä kaksi yhteyttä ovat tällä hetkellä merkittävimpiä kodin automaation verkkotekniikoita. Molemmat yhteystyypit sisältävät useita keinoja välittää viestejä kodin laitteiden välillä. Z-Wave-yhteys perustuu siihen, että se laskee algoritmin avulla nopeimman reitin välittää viesti laitteelle. ZigBeessä taas ajatuksena on, että lähtevät viestit ovat kuin parvi mehiläisiä, jotka sinkoilevat eri suuntiin etsien parasta reittiä laitteelle. (Robles & Kim, 2010.)

2.2 Miten esineiden internet näkyy yksilön elämässä

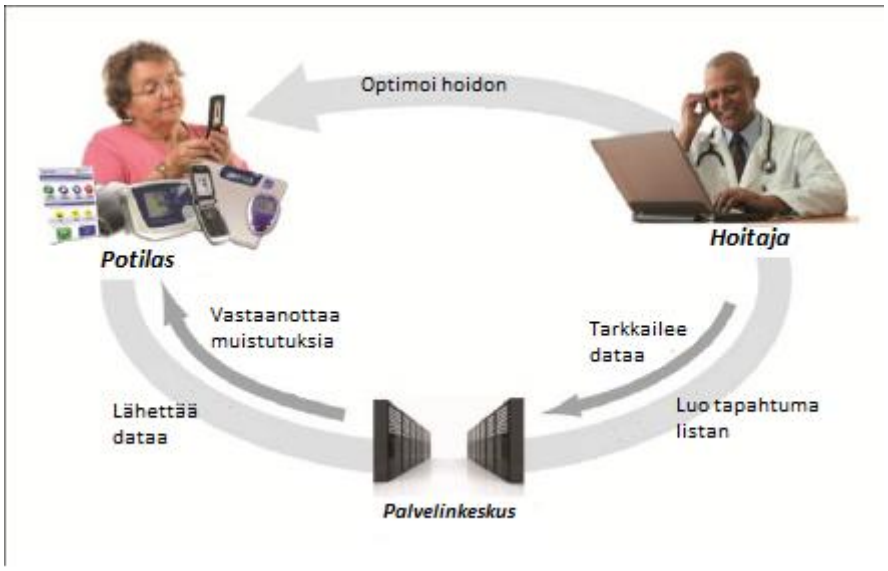
Esineiden internet tulee mullistamaan elämäämme monella tapaa. Sen ratkaisut tarjoavat ihmisen elämään muun muassa lisää mukavuutta, helppoutta, turvallisuutta sekä taloudellisuutta. Tässä alaluvussa käsitellään pintapuolisesti esineiden internetin tarjoamia toimintoja yksilön käyttöön. Esiteltäviin toimintoihin lukeutuu älykoteihin, turvajärjestelmiin, terveydenhuoltoon, ajoneuvoihin sekä energian hallintaan ja sen säästöön liittyviä ratkaisuja.

Hyvin suuri osa esineiden internetin ratkaisuista yksilön kannalta näkyy kotiautomaatiossa. Kotiautomaation avulla pystymme muuttamaan tavallisen kotitalouden älykodiksi, jossa asukas pystyy hoitamaan päivittäisiä askareitaan muun muassa langattomien laitteiden ja äänikomentojen avulla. Älykotien perimmäisenä tavoitteena on tehdä asukkaan elämästä vaivattomampaa ja mukavampaa. Älykotien ratkaisut voivat helpottaa erityisesti liikuntarajoitteisten henkilöiden ja vanhusten elämää. (Dohr ym., 2010). Monet toiminnot, jotka ennen edellyttivät fyysisiä toimia, pystytään nyt hoitamaan etäkomennoilla. Laitteiden etäkäyttöön voi hyödyntää esimerkiksi älypuhelinta tai erillistä kaukoohjainta. Älypuhelin on kuitenkin erittäin kätevä, koska ne ovat nykyään hyvin yleisiä ja kulkeutuvat minne tahansa henkilön mukana. Tällöin henkilö pystyy laittamaan esimerkiksi saunan lämpenemään ollessaan poissa kotoa tai laittamaan talon lämmityksen päälle palatessaan matkalta. Älykodin laitteet pystyvät kommunikoimaan myös keskenään. Tämä mahdollistaa joidenkin toimintojen automatisoitumisen. (Kumar, 2014.)

Älykodit tarjoavat myös turvallisuutta älykkäiden turvajärjestelmien avulla. Kotiin ja pihaan voidaan asentaa esimerkiksi valvontakameroita, liiketunnistimia, varoittimia sekä älylukkoja. Älykodin valvontakamerajärjestelmät valvovat kodin ympäristöä ja toimivat jopa pilkkopimeässä. Ulko-oveen voidaan

myös liittää kamera, joka välittää asukkaalle kuvan ovella olevasta henkilöstä. Normaalit lukot voidaan korvata älylukoilla, jotka toimivat esimerkiksi jollain biometrisellä tunnistuksella, kuten sormenjäljellä, silmällä tai äänellä, tai koodilla. Pihaan voidaan myös asentaa liiketunnistimia, jotka pystyvät jopa erottamaan eläimet ja ihmiset. (Robles & Kim, 2010.)

Esineiden internet tarjoaa myös terveydenhuollon palveluita. Sen ansiosta on mahdollista seurata elintoimintoja esimerkiksi erilaisilla sensoreilla ja mittareilla. Esimerkiksi vanhuksille tai jostain sairaudesta kärsivälle henkilölle voidaan tarjota langattomia sensoreita, jotka seuraavat hänen terveydentilaansa. Sensorit pystyvät tarvittaessa lähettämään ilmoituksen hätäkeskukselle sekä läheisille, mikäli henkilölle tulee sairaskohtaus tai muuta vastaavaa. (Bandyopadhyay & Sen, 2011.) Sensorit voivat ilmoittaa henkilölle, milloin tulisi ottaa lääkkeet. Tämä on erityisen hyvä ominaisuus esimerkiksi muistisairaille tai vanhuksille. Myös terveyskeskuksissa asioinnista tulee paljon helpompaa, kun henkilöä hoitava lääkäri pystyy sensorien keräämien tietojen avulla arvioimaan henkilön terveydentilaa, sekä ylläpitämään aktiivista yhteyttä, kuten seuraavassa kuviossa esitetään (kuvio 2). (Dohr ym., 2010.)



KUVIO 2 Terveydenhuollon kehä (Dohr, Modre-Osprian, Drobics, Hayn & Schreier, 2010, 4)

Myös tulevaisuuden autot voivat olla osa esineiden internetiä. Suurin osa uusista autoista sisältää langattomia ominaisuuksia ja kyvyn kerätä, varastoida sekä lähettää kuljettajan dataa, sijainti mukaan lukien. (Fink, Zarzhitsky, Carroll & Farquhar, 2015.) Tämän datan avulla pystytään esimerkiksi seuraamaan ajoneuvon suorituskykyä sekä ajohistoriaa. Nykyaikaisissa autoissa saattaa olla myös sisäänrakennettu puhejärjestelmä, johon kuljettaja voi kytkeä älypuhelimensa langattomasti. Esineiden internetin ansiosta on mahdollista parittaa älypuhelin ja auto siten, että jatkossa kuljettajan astuessa autoon, puhelin yhdistyy automaattisesti järjestelmään. Kuljettaja saa järjestelmän kautta myös tietoa reitiltään. Järjestelmä pystyy ilmoittamaan, mikäli reitillä on esimerkiksi huono

kuntoinen tie, ruuhkaa, tietöitä tai kolari. (Ghose, Biswas, Bhaumik, Sharma, Pal & Jha, 2012.) Autoilijoiden elämä helpottuu myös parkkeerauksen suhteen, sillä tulevaisuudessa auton on mahdollista etsiä itse vapaa parkkipaikka hyödyntäen sensoreita ja esineiden internetiä (Chou, Sheu & Chen, 2006).

Yksi tärkeä asia, johon esineiden internet vaikuttaa positiivisesti, on energian käyttö kodissa. Esineiden internet mahdollistaa energiatehokkuuden maksimoimisen esimerkiksi valaisimien käytössä. On hyvin yleistä, että ihmiset pitävät turhia valoja päällä kotonaan ja tämä kuluttaa energiaa turhaan. Esineiden internetin ansiosta valaisimista voidaan tehdä automaattisia liiketunnistimien avulla tai esimerkiksi ääniohjauksella toimivia. Liiketunnistimilla toimivat valaisimet sammuvat automaattisesti henkilön poistuessa huoneesta. (Robles & Kim, 2010.) Tämän ansiosta valoja ei tule jätettyä vahingossa päälle. Samantyylisiä ratkaisuja voidaan soveltaa myös moniin muihin laitteisiin valaisimien lisäksi. Langattomien sensoriverkkojen ansiosta asukkaan on myös mahdollista seurata omaa energian kulutustaan. Sensorit mittaavat paljonko energiaa kuluu milloinkin ja asukas voi seurata kulutusta siihen tarkoitetun sovelluksen kautta. (Gomez & Paradells, 2010.) Kun asukas näkee konkreettisesti, paljonko energiaa kuluu, hänen on helpompaa hallita kulutusta.

3 KYBERTURVALLISUUS

Kyberturvallisuus on ollut viime aikoina paljon esillä ja sen merkitystä on korostettu. Niin valtiot kuin myös yritykset ympäri maailman ovat alkaneet panostamaan kyberturvallisuuteen. Tähän mennessä jopa yli 50 valtiota on julkaissut oman kyberturvallisuusstrategiansa (Von Solms & Van Niekerk, 2013). Tässä luvussa aion avata käsitettä kyberturvallisuus ja samalla vertaan sitä tietoturvaan, tarkoituksena selittää miten nuo kaksi termiä eroavat. Lisäksi tämän tutkielman kannalta on tärkeää, että luodaan vielä tarkempi katsaus kyberturvallisuuden yhteen osa-alueeseen, kyberrikollisuuteen.

3.1 Kyberturvallisuus ja miten se eroaa tietoturvasta

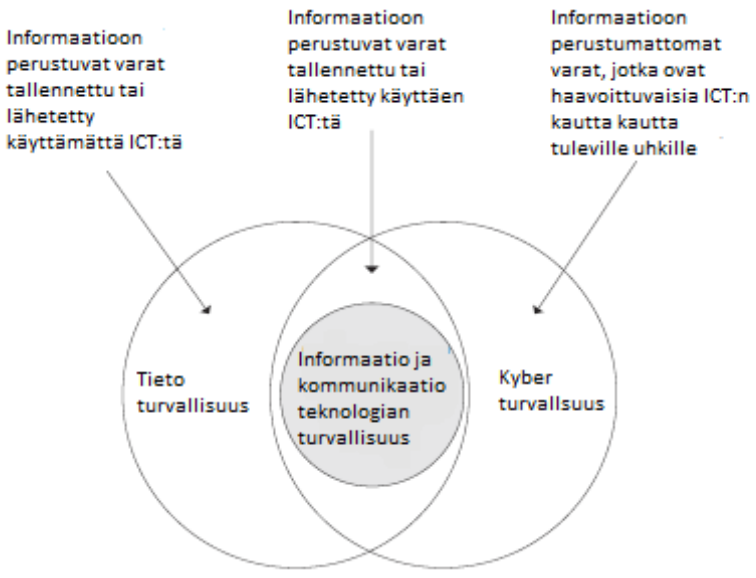
Puhuttaessa kyberturvallisuudesta, tulee ensin ymmärtää kybermaailman käsite. Kybermaailma koskettaa sekä yksittäistä kansalaista, elinkeinoelämää, että julkista sektoria. Kybermaailma voidaan jakaa viiteen eri kerrokseen (Libicki 2007). Nämä kerrokset ovat fyysinen, syntaktinen, semanttinen, palveluntarjonta sekä kognitiivinen kerros. Fyysiseen kerrokseen kuuluu fyysiset elementit, jotka ovat yhteydessä verkkoon, kuten verkkolaitteet, reitittimet, kytkimet, kiinteät ja langattomat verkkoyhteydet. Syntaktinen kerros koostuu erilaisista järjestelmän ohjaus- ja hallintaohjelmista, verkkoprotokollista sekä virheiden korjauksesta. Semanttinen kerros on hyvin tärkeä osa kybermaailmaa. Se on kerros, jossa käyttäjä tulee mukaan kuvioon, ja se käsittää muun muassa käyttäjän päätelaitteissa olevan informaation, tietosisällöt sekä erilaiset käyttäjän hallinnassa olevat toiminnot. Palvelukerros on nimensä mukaisesti kerros, johon kuuluvat kaikki julkiset ja kaupalliset verkkopalvelut. Kognitiivinen kerros on abstraktimpi käsite, sillä se käsittää ihmisen ymmärryksen ja tulkinnan informaation merkityksestä. Siihen katsotaan myös kuuluvan inhimillinen ongelmanratkaisu. (Libicki 2007.)

Kyberturvallisuuden tarkoitus on turvata tämän kybermaailman toiminta. Kansainvälisen kyberturvallisuusstrategian mukaan kyberturvallisuuden tavoi-

te on suojata elintärkeät toiminnot haitalta ja vaaroilta, tarjota tila, jossa kaikki toimijat voivat toimia järkevästi, luoda ympäristö, johon toimijat voivat luottaa, kyetä vastustamaan hyökkäyksiä sekä edistää lainsäädäntöä, jolla pyritään aikaansaamaan kyberympäristön turvallisuus. (International strategy for cyberspace, 2011.)

Suomen kyberturvallisuusstrategian (2013) mukaan suurin syy kyberhaavoittuvuuksille on liian huono suojautuminen sekä vähäinen tieto ja ymmärrys kyberuhkista. Kyberturvallisuutta ajateltaessa lähtökohta on se, että hyökkäys pääsee aina läpi. Sellaista järjestelmää ei voida luoda, joka pystyisi estämään kaikki hyökkäykset, vaan järjestelmän pitää ennemmin pystyä sietämään hyökkäyksiä, pystyä toipumaan niistä ja kyetä rajaamaan vahinkoja sekä toimimaan niistä huolimatta. Turvallisuus muodostuu siitä, että tiedostetaan uhkat ja haavoittuvuudet, osataan arvioida riskit ja suhtautua niihin vaadittavalla vakavuudella sekä osataan varautua ja toimia tilanteen mukaan. (Suomen kyberturvallisuusstrategia, 2013.)

Kyberturvallisuus ja tietoturvallisuus eivät siis ole täsmälleen sama asia. Näiden käsitteiden välillä on toki jonkin verran päällekkäisyyttä, mutta käytännössä kyberturvallisuus on paljon laajempi käsite, kuin tietoturva, sillä tietoturva koskettaa yleensä ainoastaan tietojärjestelmien kestävyyttä hyökkäyksiä kohtaan. Kyberturvallisuuteen taas liittyvät myös fyysiset elementit. Von Solmsin ja Van Niekerkin (2013) mukaan kyberturvallisuus ja tietoturvallisuus eroavat esimerkiksi siltä osin, että kyberturvallisuushyökkäykset voivat suoraan vahingoittaa sekä ihmisiä, että yhteiskuntaa, mutta tietoturvahyökkäyksissä vahingon teko on aina epäsuoraa. Tietoturvallisuuden ja kyberturvallisuuden välimaastoon jää vielä kolmas käsite, eli ICT-turvallisuus, joka tarkoittaa informaatio- ja kommunikaatioteknologian turvallisuutta. Alla olevassa kuviossa (kuvio 3) on esitettynä Von Solmsin ja Van Niekerkin (2013) näkemys tietoturvallisuuden ja kyberturvallisuuden eroista.



KUVIO 3 Tietoturvallisuuden, ICT-turvallisuuden ja kyberturvallisuuden erot (Von Solms & Van Niekerk, 2013, 101)

Kyberturvallisuuteen liittyy paljon käsitteitä, jotka tulisi tietää pystyäkseen ymmärtämään, mitä kyberturvallisuus on. Tästä johtuen asian pystyy avaamaan helpoiten taulukon avulla. Seuraavassa taulukossa (taulukko 1) avataan kyberturvallisuuteen liittyviä tärkeimpiä käsitteitä. Taulukon tiedot perustuvat Suomen kyberturvallisuusstrategiaan (2013).

TAULUKKO 1 Kyberturvallisuuden käsitteitä. (Suomen kyberturvallisuusstrategia, 2013, 12-13)

Kyber-	Sanan merkityssisältö liittyy yleensä sähköisessä muodossa olevan informaation (tietojen) käsittelyyn: tietotekniikkaan, sähköiseen viestintään (tiedonsiirtoon), tieto- ja tietokonejärjestelmiin.
Kyberriski	Kyberriskillä tarkoitetaan kybertoimintaympäristöön kohdistuvaa vahinkomahdollisuutta tai haavoittuvuutta, joka toteutuessaan tai jota hyväksi käyttäen kybertoimintaympäristön toiminnasta riippuvalle toiminnolle voi aiheutua vahinkoa, haittaa tai häiriötä.
Kybertoimintaympäristö	Kybertoimintaympäristö on sähköisessä muodossa olevan informaation käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö. Ympäristöön kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet.
Kyberuhka	Kyberuhka tarkoittaa mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon.
Tietoturvallisuus	Tietoturvallisuudella tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus.
Kyberturvallisuus	Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen informaation käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle. Luottamus kybertoimintaympäristöön perustuu siihen, että sen toimijat toteuttavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenettelyjä. Menettelyjen avulla pystytään estämään tietoturvauhkien toteutuminen, ja niiden mahdollisesti toteutuessa estämään, lieventämään tai sietämään niiden vaikutuksia. Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa valtiolle tai sen väestölle.

3.2 Kyberrikollisuus

Informaatioteknologian ja internetin merkitys on kasvanut merkittävästi viime vuosina. Tämä räjähdysmäinen kasvu on vaikuttanut myös siihen, että rikolliset ovat alkaneet omaksumaan yhä enemmän informaatioteknologiaa käyttöönsä.

Informaatioteknologia on mahdollistanut rikollisille uuden toimintaympäristön, joka ei edellytä fyysistä läsnäoloa kohteessa ja näin heidän on helppoa tehdä kohdennettuja hyökkäyksiä huomaamattomasti. Internetin välityksellä rikollinen tai mikä tahansa muu toimija pystyy hyökkäämään minne tahansa rajoista riippumatta. (Richardson, 2008.) Valtioiden erilaiset lainsäädännöt hankaloittavat kyberrikollisten kiinniottamista, koska hyökkäys voidaan tehdä toisen valtion alueelta. Tällaisissa tilanteissa hyökkääjän kiinnisaamiseen ei aina voida käyttää kohdemaan lakia ja siitä syystä kyberrikollisia saadaan hyvin harvoin vastuuseen teoistaan. (Smith, Grabosky & Urbas, 2004.)

Yksi puhutteleva uhka liittyen kybermaailmaan on kyberrikollisuus. Kyberrikollisuudella tarkoitetaan rikoksia, jotka tehdään sähköisiä viestintäverkkoja ja tietojärjestelmiä hyödyntäen, tai jotka kohdistuvat mainittuihin verkkoihin ja järjestelmiin. Kyberuhkien suurimmat motiivit ovat valta, vahingonteko ja taloudellinen etu, joista valta on tärkeintä valtiollisille toimijoille, kun taas kyberrikollisille raha tai vahingonteko on yleensä valtaa tärkeämpi motiivi. (Suomen kyberturvallisuusstrategia, 2013.)

Kyberrikollisuuden määrä on kasvanut merkittävästi 2000-luvulta eteenpäin. Vuonna 2010 julkaistussa Yhdysvaltain-Kiinan talouden ja turvallisuuden arviointi komission (US-China Economic and Security Review Commission) raportissa todettiin, että rikollinen kyberaktiivisuus Yhdysvaltain turvallisuusministeriötä kohtaan on lisääntynyt vuodesta 2000. Seuraavassa taulukossa (taulukko 2) on esitettynä raportin tulokset. Taulukon perusteella voidaan todeta, että rikollinen kyberaktiivisuus on noususuhdanteessa. (Choo, 2011.)

TAULUKKO 2 Kyberrikollisuuden lisääntyminen (Choo, 2011, 720)

Vuosi	**Kyberhyökkäysten määrä**	**Prosentuaalinen kasvu edellisestä vuodesta**
2000	1415	-
2001	3651	158.02 %
2002	4352	19.2 %
2003	9919	127.92 %
2004	16110	62.42 %
2005	23031	42.96 %
2006	30215	31.19 %
2007	42880	45.23 %
2008	54640	24.52 %
2009	71661	31.15 %

4 ESINEIDEN INTERNETIN KYBERTURVALLISUUS

Esineiden internet mahdollistaa monien asioiden automatisoitumisen ja siten helpottaa ja muuttaa elämäämme suuresti. Siitä on paljon hyötyä monilla aloilla ja myös yksittäisen ihmisen elämässä, mutta siihen sisältyy myös varjopuoli. Uusien teknologioiden myötä myös rikollisille aukeaa uusi kanava tehdä rikoksia. Kyberrikollisuus on ollut paljon esillä viime aikoina ja se on lisääntynyt. (Choo 2011) Mitä kaikkea voi seurata siitä, kun yhdistämme kotiemme laitteet verkkoon? Tässä luvussa käsitellään esineiden internetin ongelmakohtia kyberturvallisuuden kannalta yksilön näkökulmasta. Tarkastellaan, kuinka esineiden internet vaikuttaa yksilön elämään negatiivisesti. Tämän lisäksi luodaan katsaus siihen, miten näitä ongelmia on pyritty korjaamaan tai ennaltaehkäisemään.

4.1 Esineiden internetin kyberturvallisuusriskit

Esineiden internet laajenee jatkuvasti. Covingtonin ja Carskaddenin (2013) mukaan vuonna 2003 internetiin liittyneitä laitteita oli noin 500 miljoonaa. Vuoteen 2010 mennessä tämä luku kasvoi 12,5 miljardiin ja arvio vuodelle 2020 on jopa 50 miljardia laitetta. Näiden esineiden valtava määrä, niiden liikkuvuus sekä levinneisyys tarjoavat hyökkääjille monia mahdollisuuksia ilman pelkoa kiinni jäämisestä. Esineiden internet on erittäin arvokas ja helppo kohde kyberrikollisille. Ensimmäinen haavoittuvuus liittyy verkonvalvontaan tai paremminkin sen puutteeseen. Koska esineet toimivat ilman ihmisen valvontaa esineiden internetissä, hyökkääjän on helppo päästä niihin käsiksi kenenkään tietämättä sekä verkon kautta että fyysisesti. Toinen haavoittuvuus liittyy kommunikointiin langattomien verkkojen välityksellä. Langattomiin verkkoihin on varsin helppo päästä luvattomasti ja niiden kautta pystyy esimerkiksi urkkimaan luottamuksellisia tietoja. Kolmas haavoittuvuus liittyy esineiden heikkoon suojaukseen, mikä johtuu puutteellisista resursseista. (Atzori, Iera & Morabito, 2010.) Voidaan ajatella, että esineiden internetin kyberturvallisuusriskit yksilön kan-

nalta koostuvat kolmesta pääongelmasta. Nämä ongelmat ovat henkilöiden yksityisyys, turvallisuus sekä prosessien luottamuksellisuus. (Abomhara & Koien 2015.)

Jokaisella ihmisellä on oikeus yksityisyyteen ja omien tärkeiden tietojensa salassapitoon. Jotkin esineiden internetin ominaisuudet saattavat kuitenkin vaikuttaa ihmisten yksityisyyteen negatiivisesti. Henkilöstä pystytään keräämään paljon yksityisiä tietoja hänen tietämättään. Informaatiota on niin paljon, että sen hallinta ja turvaaminen on täysin mahdotonta nykyisillä tekniikoilla. Yksityisyyteen liittyvät riskit ovatkin yksi ihmisiä eniten askarruttava asia esineiden internetissä. (Atzori ym., 2010.) Seuraavissa kappaleissa perehdytään esineiden internetin yksityisyydensuojaan liittyviin ongelmiin.

Esineiden internetin laitteiden yksi ominaisuus on laitteiden ääniohjauskomennot. Laitteiden ääniohjauskomentoihin sisältyy hieman kyseenalaisuuksia yksityisyyden kannalta. Esimerkiksi Fink, Zarzhitsky, Carroll ja Farquhar (2015) kertovat artikkelissaan, että laitteiden ääniohjauskomennot voivat antaa laitevalmistajille ja kolmansille osapuolille mahdollisuuden käyttäjän kuunteluun. Esimerkiksi Samsung on kertonut avoimesti, että heidän älytelevisionsa ääniohjausjärjestelmä kuuntelee ihmisten puhetta laitteen läheisyydessä ja välittää sitä eteenpäin laitevalmistajalle sekä kolmansille osapuolille. Tämä ei suinkaan rajoitu ainoastaan älytelevisioihin vaan myös monet muut laitteet ja laitemerkit tekevät samaa. Toiminnon tarkoituksena pitäisi olla palveluiden kehittäminen, mutta ongelmatilanne koituu siitä, että laitteet keräävät äänidataa läheisyydestään, vaikka kyseinen ääni ei olisikaan laitteelle kohdistettu komento. Tämä johtuu siitä, että laitteet eivät pysty erottamaan mikä ääni on komento ja mikä ei. Tämän takia on mahdollista, että kotona käydyt keskustelut eivät välttämättä olekaan niin yksityisiä, kuin voisi olettaa ja laitteiden äänikomennot saattavat vaikuttaa yksityisyyteen negatiivisesti.

Henkilön yksityisyyttä uhkaavat toki myös muut tahot, kuin laitevalmistajat, sillä myös kyberrikolliset saavat tehokkaita keinoja tietojen kalasteluun esineiden internetin avulla. Esineiden internetin kautta pystyy helposti selvittämään henkilön sijainnin, missä hän on käynyt, salakuuntelemaan, keräämään arkaluontoista dataa sekä kalastelemaan salasanoja. (Abomhara & Koien 2015)

Monet esineiden internetin palvelut toimivat sensoriverkkojen avulla. Sensoriverkkojen käytössä on esimerkiksi se ongelma, että itsenäisiä sensoreita voi olla käytössä niin paljon, ettei niiden suojaukseen tarvittavia resursseja pystytä tarjoamaan. Tarvittavan suojauksen puute aiheuttaa sen, että kyberhyökkäyksen toteuttaminen on erittäin helppoa. Chanin ja Perrigin (2003) mukaan sensoriverkon kautta hyökkääjän on erittäin helppo päästä käsiksi joko sensoriin tallennettuun dataan tai ”salakuuntelemaan” liikkuvaa dataa. Hyökkääjän ei tarvitse päästä käsiksi kuin yhteen sensoriverkon solmukohtaan, sillä kun data kulkee tämän saastuneen solmukohdan lävitse, hyökkääjä pääsee dataan käsiksi. Hyökkääjä voi hyödyntää useitakin sensoreita, kuten kodin ulko- ja sisäsensoreita kerätäkseen tietoja asukkaiden yksityisistä aktiviteeteista. Hyökkääjien ei myöskään tarvitse olla fyysisesti paikan päällä, vaan tietojen keruu

onnistuu täysin langattomasti, jolloin riski kiinnijäämisestä on pieni. (Chan & Perrig, 2003.)

Kun rikolliset saavat käyttöönsä tällaisia keinoja, voidaankin alkaa miettiä myös yksilön turvallisuutta. Vaikka esineiden internetin povataan lisäävän ihmisen ja kodin turvallisuutta tarjoamalla ratkaisuja, kuten valvontakamerajärjestelmiä, liiketunnistimia ja lukitusjärjestelmiä, myös ne voivat olla purettavissa taitavan kyberrikollisen käsissä (Notra, Siddiqi, Gharakheili, Sivaraman & Boreli, 2014). Suurin kysymys kuuluukin, voidaanko verkkoon yhdistyneiden turvajärjestelmien turvallisuuteen luottaa? Pahin mahdollinen tilannehan olisi se, että kotiin asennetut turvajärjestelmät olisivatkin purettavissa kyberrikollisten toimesta. Dlamini, Eloff ja Eloff (2009) kertovat artikkelissaan toisenlaisen esimerkin siitä, miten kodin turvallisuus saattaa olla uhattuna. Heidän mukaansa hyökkääjän olisi mahdollista kaapata esimerkiksi kodista löytyvä älyliesi, jolloin hän voisi kytkeä sen päälle tai pois ja säätää sen lämpöä haluamallaan tavalla. Tämän johdosta hyökkääjä voisi säätää lieden täydelle teholle, kun ketään ei ole kotona aiheuttaen tulipalovaaran. (Dlamini, Eloff & Eloff, 2009.)

Tulevaisuuden autoissakin alkaa olla yhä enemmän elektroniikkaa, ja ne voivat olla osa esineiden internetiä, mutta kuinka turvallista se loppujen lopuksi on, että kuljettamasi ajoneuvo on linkitettynä verkkoon? Wired-lehden (2015) uutisessa kerrotaan, kuinka hakkerit Charlie Miller ja Chris Valasek suorittivat kokeen, jossa he ottivat ajossa olevan jeepin haltuunsa etäältä täysin langattomasti. Hakkerit ovat jo nyt pystyneet ottamaan ajoneuvon haltuunsa etäältä käyttäen ainoastaan kannettavaa tietokonetta, puhumattakaan siitä, kuinka helppoa auton GPS-järjestelmän kautta on selvittää auton sijainti. Miller ja Valasek onnistuivat kokeessa esimerkiksi säätämään auton tuuletusjärjestelmää, ajotietokonetta, radiota sekä lopulta sammuttamaan moottorin auton ollessa keskellä moottoritietä. Auton kuljettaja menetti kaiken hallinnan hakkeroiduista järjestelmistä, eikä pystynyt säätämään itse radiota tai muita järjestelmiä, eikä käynnistämään autoa uudestaan. (Wired, Andy Greenberg, 2015.)

Esineiden internetin monissa palveluissa käyttäjä luovuttaa itsestään tärkeitä ja henkilökohtaisia tietoja. On erittäin tärkeää, että tieto on silloin luottamuksellista. Palveluntarjoajien pitää pystyä tällöin takaamaan käyttäjälle, ettei hänen tietonsa joudu vääriin käsiin. Tiedon luottamuksellisuus on tutkijoiden mielestä kolmas suurimmista haasteista esineiden internetin laajamittaisessa käyttöönotossa. Luottamuksellisuuden takaaminen ja käyttäjien luottamuksen ansaitseminen on ongelmallista ja siksi suuri este sille, ettei esineiden internet ole vielä niin laaja, kuin olisi mahdollista. (Miorandi, Sicari, Pellegrini & Chlamtac, 2012.)

Luottamuksellisuuden takaaminen on erittäin tärkeää esimerkiksi terveydenhuollon palveluissa. Kuten todettu esineiden internet mahdollistaa monia toimintoja terveydenhuollon palveluihin, esimerkiksi terveydentilan seurantaan tarkoitettuja sensoreita. Miorandi, Sicari, Pellegrini ja Chlamtac (2012) toteavat kuitenkin artikkelissaan, että terveydenhuollon palvelut ovat merkittävin esineiden internetin kehityskenttä, josta puuttuu tarvittavat työkalut ihmisten yksityisten ja arkaluontoisten tietojen suojaamiseksi. Lisäksi tiedonsiirto ter-

veydenhuollon palveluissa tulisi olemaan suurelta osin langattomien verkkojen varassa, jolloin riski ulkopuolisten tahojen tekemälle salakuuntelulle ja tiedon kalastelulle kasvaa. Ulkopuolinen tekijä voi myös onnistua pääsemään potilaan ja lääkärin tiedon kulun väliin, jolloin hänen on mahdollista esiintyä vastapuolena, potilaan tai lääkärin tietämättä. Tätä kutsutaan ”man-in-the-middle” hyökkäykseksi. Niin kauan, kuin tällaiset riskit ovat mahdollisia tai jopa todennäköisiä, esineiden internetiä tuskin voidaan käyttää laajamittaisesti terveydenhuollossa. Tästä syystä on erittäin tärkeää, että terveydenhuollon, sekä myös muissa palveluissa pystytään takaamaan tiedon luottamuksellisuus. (Miorandi ym., 2012.)

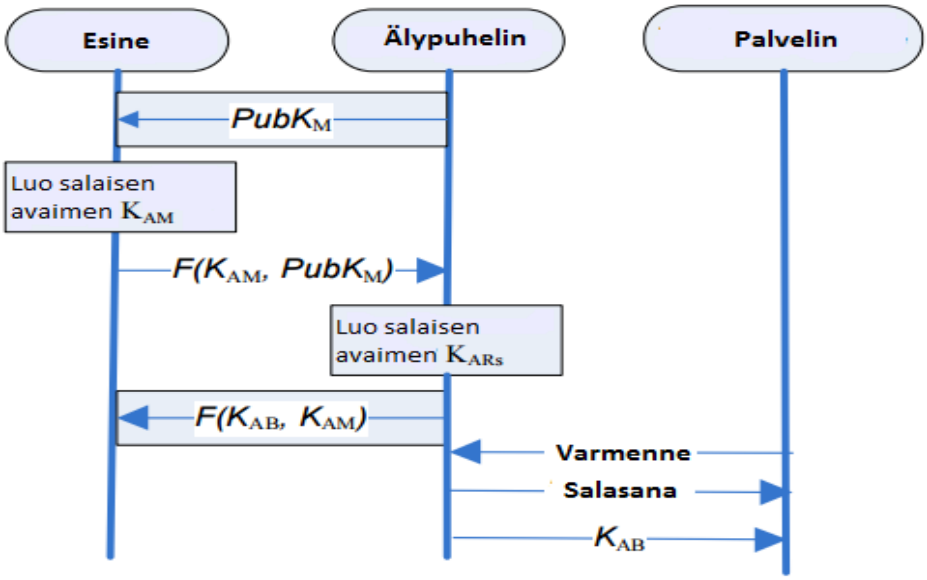
4.2 Esineiden internetin kyberturvallisuusratkaisuja

Esineiden internetin kyberturvallisuuden kannalta palveluiden tulee pystyä tarjoamaan turvallinen ja yksityisyyttä suojeleva ympäristö, sekä luottamuksellisen tiedon tulee olla hallinnassa. Näiden kolmen tekijän tarjoaminen ei ole kuitenkaan niin yksinkertaista, koska kaikkiin ongelmiin ei ole vielä kehitetty ratkaisua. Siksi tutkijat tekevätkin paljon töitä, löytääkseen oikeat ratkaisut esineiden internetin kyberturvallisuutta ajatellen. Tässä alaluvussa esittelen tarvittavia ratkaisuja esineiden internetin kyberturvallisuuden toteuttamiseksi. Kerron myös ratkaisuista, joita on tähän mennessä suunniteltu tai otettu käyttöön Lisäksi tarkastellaan, mikä tekee näiden ratkaisujen kehittämisestä haasteellista.

Yksityisyyden suojaaminen on erittäin tärkeä osa esineiden internetiä ja sen laajenemista. Yksityisyyden suojaamiseksi on esitetty useita viitekehyksiä, joista yksi lupaavimmista on PRIS. Se tarjoaa hyvin mahdollisen lähtökohdan kunnollisten yksityisyyden suojaamismekanismien määritelmälle esineiden internetissä. Se edustaa tekniikan menetelmää, joka sisällyttää yksityisyysvaatimukset järjestelmän suunnitteluprosessiin. PRIS tarjoaa joukon käsitteitä yksityisyysvaatimusten mallintamiseen ja sääntöjä näiden vaatimusten muuntamiseksi käytännön tekniikoiksi. (Miorandi ym., 2012.) Esineiden internetin yksityisyyteen liittyviä avoimia tutkimusongelmia on useita. Esimerkiksi yleinen yksityisyyden määritelmä esineiden internetissä puuttuu täysin. Yksityisyydelle tärkeää on myös innovatiivisten tekniikoiden kehittäminen, jotka pystyisivät käsittelemään skaalautuvia ja monimuotoisia tapauksia esineiden internetissä, sekä sellaisten ratkaisujen kehittäminen, jotka tasapainottavat anonyymiyden tarvetta joissakin sovelluksissa, jotka sisältävät paikannus- ja seurantaominaisuuksia. On määriteltävä, milloin on mahdollista tunnistaa ja paikantaa älylaite ja milloin on mahdollista päästä käsiksi arkaluontoiseen dataan. (Miorandi ym., 2012.)

Älypuhelin tulee olemaan suuressa roolissa esineiden internetin käytössä. Kun älypuhelimella ohjaillaan muita esineiden internetin laitteita, yhteyden tulee olla hyvin suojattu. Jani Suomalainen (2014) esittelee artikkelissaan älypuhelimen ja esineen parittamiseen palvelimen kautta tarkoitetusta turvallisuusprotokollasta. Parittaminen tapahtuu siten, että ensin älypuhelin suojaa NFC-

pohjaisen (near field communication) OOB-rajapinnan (out-of-band). Tämän jälkeen älypuhelin lähettää julkisen avaimen (public key) OOB-kanavan läpi esineelle, jolloin esine luo tilapäisen avaimen (temporary key). Tämä avain suojataan käyttäen älypuhelimelta saatua julkista avainta. Sitten älypuhelin luo vielä yhden symmetrisen avaimen (symmetric key), jota käytetään esineen ja palvelimen välisessä yhteydessä. Tämä avain suojataan käyttäen OOB-kanavaa, sekä tilapäistä avainta. Seuraavaksi älypuhelin avaa suojatun istunnon palvelimen kanssa käyttäen protokollaan perustuvaa varmennetta ja salasanaa, jonka jälkeen välitetään viimeinen avain käyttäen autenttista ja luottamuksellista kanavaa. (Suomalainen, 2014.) Seuraava kuvio (kuvio 4) havainnollistaa parittamistilanteen.



KUVIO 4 Älypuhelimen ja etäpalvelimen parittaminen (Suomalainen, 2014, 4)

Monet esineiden internetin sovellukset perustuvat monilähetys (multicast) kommunikaatiomalliin, missä yksi lähetin lähettää yleistä dataa monelle vastaanottimelle. Monilähetykseen liittyy turvallisuusriskejä, mutta kommunikaatio on mahdollista suojata käyttämällä yhteistä salattua avainta, joka on jaettu monen käyttäjän kanssa. Tätä avainta kutsutaan ryhmäavaimeksi (group key). Mikäli ryhmän jäsenissä tulee muutoksia, jaettu avain tulisi päivittää uuteen, jotta ryhmästä lähtenyt henkilö ei enää pääse käsiksi tulevaan kommunikaatioon ja uudella jäsenellä ei ole pääsyä menneeseen kommunikaatioon. Ongelmallista tässä on se, että mikäli jäsenet vaihtuvat usein, avainta täytyy vaihtaa jatkuvasti ja se ei ole järkevää resurssien kannalta. (Billure, Tayur & Mahesh, 2015.)

Esineiden internetissä on erittäin tärkeää pystyä varmistamaan tiedon luottamuksellisuus. Tiedon luottamuksellisuuden turvaamiselle olennaista on tiedon todentaminen (authentication). Esimerkiksi RFID-järjestelmiin on mahdollista hyödyntää muutamia erilaisia todentamismenetelmiä ja kryptausmenetelmiä. Näihin menetelmiin kuuluvat muun muassa tarkistelukko protokolla (hash lock), satunnainen tarkistelukko, tarkisteketju protokolla (hash chain),

sekä interaktiivinen todennusprotokolla. Näissä ratkaisuissa on kuitenkin ongelmia kustannusten suuruuden kanssa. (Billure ym., 2015.) Sensoriverkkojen tiedon turvaamiseen tarvitaan menetelmiä tunkeiluhyökkäyksiä, kuten palvelunestohyökkäyksiä (Denial of Service) vastaan. Verkon turvaamiseen voidaan käyttää erilaisia suodatin sekä havaitsemismekanismeja. Jotta sensoriverkko voisi olla luotettava, sen täytyy pystyä suojaamaan solmukohtiaan hyökkäyksiltä. Todentamisen täytyy kattaa koko sensoriverkko päästä päähän (end-to-end), jotta tiedon siirto olisi suojattua ja pystyttäisiin välttymään esimerkiksi man-in-the-middle-hyökkäyksiltä ja muilta tunkeiluhyökkäyksiltä. (Gou, Yan, Liu & Li, 2013.)

Notran ym. (2014) mukaan ongelmallista esineiden internetin kyberturvallisuuden toteuttamisessa on se, että suuri osa tehdystä tutkimuksesta tuntuu keskittyvän enimmäkseen korkeatasoisiin turvallisuusratkaisuihin. Nämä ratkaisut edellyttäisivät muutoksia siihen, miten esineiden internetin laitteet ovat suunniteltu ja miten ne kommunikoivat. Turvallisuus- sekä yksityisyysuhkia torjuvia, laitteisiin sulautettuja turvallisuusratkaisuja on lähes mahdotonta kehittää, koska laitevalmistajia on niin suuri määrä. Lisäksi esineiden internetin laitteiden pieni koko, rajoittunut laskentateho sekä energiaresurssit estävät laajojen turvallisuusalgoritmien hyödyntämisen. (Notra ym., 2014.)

5 YHTEENVETO

Tutkielmassa käytiin läpi esineiden internetin perustoiminnot, sen tarjoamia toimintoja yksilölle, kyberturvallisuuden ja kyberrikollisuuden merkitys sekä esineiden internetin käytöstä aiheutuvia riskitekijöitä yksilön yksityisyydelle, turvallisuudelle ja palveluiden luottamuksellisuudelle. Lisäksi tarkasteltiin muutamia ratkaisuja näihin riskeihin. Tutkielman tarkoituksena oli lisätä tietoisuutta esineiden internetin käytöstä aiheutuvista riskeistä yksilön yksityisyydelle ja turvallisuudelle sekä tarkastella onko näitä riskejä pyritty tai pystytty ehkäisemään. Sen tarkoituksena oli lisätä ymmärrystä esineiden internetin käyttöön liittyvistä riskeistä ja puutteista yksilön kannalta. Aiheen tutkiminen oli tärkeää, koska sekä esineiden internet, että kyberturvallisuus ovat ajankohtaisia aiheita.

Esineiden internetin palveluista löytyi paljon hyviä toimintoja esimerkiksi vanhuksille tai liikuntarajoitteisille, koska toimintoja voi tehdä etäältä ja vaivattomasti. Esineiden internet tarjoaa paljon ratkaisuja esimerkiksi energian säästöön, etäpalveluihin, kuten terveydenhuolto etäältä, turvallisuusratkaisuja sekä yleistä mukavuutta ja vaivattomuutta edistäviä palveluita. Esineiden internet kasvaa valtavalla vauhdilla ja siihen liitetään koko ajan uusia palveluita. Kyberturvallisuuden merkitystä on myös laajasti korostettu mediassa ja alan tutkimuksissa. Kyberturvallisuuden tarkoitus on suojata yhteiskunnan kriittiset palvelut niin verkossa, kuin myös fyysisessä maailmassa. Esineiden internetin käytössä on tärkeää, että kyberturvallisuus on vahvalla tasolla, jotta palveluiden ja laitteiden käyttö olisi turvallista. Tällä hetkellä esineiden internetin kyberturvallisuuteen liittyy vielä paljon ongelmia ja turvallisuusaukkoja, joiden ratkaisu on välttämätöntä esineiden internetin laajamittaiselle käyttöönotolle. Yksilön kannalta näihin ongelmiin lukeutuvat yksityisyys, turvallisuus sekä palveluiden luottamuksellinen käyttö.

Kirjallisuuskatsauksen perusteella voidaan siis todeta, että esineiden internet tarjoaa ihmiselle monia hyviä palveluita, jotka tekevät parhaimmillaan elämästämme mukavampaa ja helpompaa. Sen käyttöön kuitenkin liittyy vielä paljon riskejä ja selvittämättömiä ongelmia koskien ihmisten yksityisyyttä ja tiedon luottamuksellisuutta, koska kaikkiin kyberturvallisuusaukkoihin ei ole

vielä kehitetty ratkaisuja. Tutkijoiden mielestä esineiden internet uhkaa yksityisyyttä, koska sen kautta on helppoa salakuunnella tai varastaa arkaluontoista tietoa. Toiminnot ja palvelut ovat pääosin langattoman verkon varassa ja siksi niihin on helppo tehdä huomaamattomia hyökkäyksiä. Esineiden internetissä on myös suoria turvallisuusriskejä, koska sen kautta voidaan tehdä myös fyysistä vahinkoa käyttämällä palveluita väärin. Lisäksi palveluiden luottamuksellisuuden takaaminen on iso ongelma, koska tiedon turvallista kulkua ei ole pystytty täysin takaamaan, minkä takia arkaluontoinen tieto, kuten potilastiedot, voivat olla vaarassa. Lisäksi kyberrikollisuuden lisääntyessä ja rikollisten keksiessä koko ajan uusia keinoja kyberhyökkäyksiin mielestäni on jopa pelottava ajatus liittää suurin osa käyttämistämme laitteista verkkoon. Monet tutkijat väittävät, että esineiden internetin avulla voidaan lisätä ihmisten turvallisuutta, mutta mielestäni nykytilassa tilanne on lähes päinvastainen, eikä ihmisten pitäisi sokeasti omaksua uutta teknologiaa ilman, että se on varmasti turvallinen. Vielä silloinkin, kun palveluiden vakuutettaisiin olevan täysin turvallisia, saattaisin itse miettiä muutamaan kertaan haluanko antaa kaikkia tietojani ja elämääni verkkoon, kuten laajamittaisen esineiden internetin tapauksessa kävisi.

Esittelin tutkielmassa myös muutamia ratkaisuja esineiden internetin yksityisyyden, turvallisuuden ja luottamuksellisuuden toteuttamiseksi. Yksityisyyden suojaamiseksi tarkoitetuista viitekehyksistä valitsin PRIS-viitekehyksen, jonka tavoitteena on tarjota määritelmä yksityisyyden suojaamismekanismeille internetissä. Lisäksi se asettaa vaatimuksia yksityisyydelle. Käsittelin myös Jani Suomalaisen (2014) esittämää turvallisuusprotokollaa älypuhelimen ja esineen parittamiseen. Älypuhelimet ovat suuressa roolissa esineiden internetissä, joten niiden käyttö tulee olla hyvin suojattua. Protokolla perustuu älypuhelimen, esineen ja palvelimen väliseen salausavainten lähettämiseen, jolla pystytään varmentamaan yhteyden muodostamisen turvallisuus. Palveluiden luottamuksellisuus on myös erittäin tärkeää esineiden internetissä, joten luottamuksellisuuden turvaamiselle esitin ratkaisuja tiedon todentamisesta ja kryptaamisesta erilaisten tarkistelukkojen avulla. Tarkistelukkojen ja todentamismenetelmien avulla pystytään estämään muun muassa palvelunestohyökkäyksiä. Lisäksi kerroin sensoriverkkojen turvaamiseen tarkoitetuista suodatin ja havaitsemismekanismeista, joilla voidaan estää hyökkäyksiä sensoriverkon solmukohtiin.

Esineiden internet vaatii vielä paljon tutkimustyötä turvallisuuden kannalta, ennen kuin sitä voidaan alkaa edes suunnittelemaan otettavaksi laajamittaisesti käyttöön yhteiskunnan palveluissa. Palveluiden tulee pystyä vakuuttamaan tiedon luottamuksellisuus, jotta ihmiset olisivat valmiita hyväksymään niiden käytön. Tutkimusta tulisi tehdä vielä kaikilla tässä tutkielmassa esitetyillä kolmella pääalueella, eli esineiden internetin yksityisyys, turvallisuus sekä palveluiden luottamuksellisuus. Alan artikkeleista löytyi lukuisia konkreettisia esimerkkejä mahdollisista riskeistä ja ongelmatilanteista, mutta ratkaisuja näihin olikin huomattavasti hankalampi löytää. Suurin osa tutkijoista listasi vaatimuksia turvallisuudelle, mutta ei niinkään ratkaisuja.

LÄHTEET

Abomhara, M., & Koien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. Teoksessa *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*, 1-8.

Abomhara, M., & Koien, G. M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security*, 4, 65-88.

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.

Billure, R., Tayur, V. M., & Mahesh, V. (2015). Internet of Things-a study on the security challenges. Teoksessa *Advance Computing Conference (IACC), 2015 IEEE International*, 247-252.

Chan, H., & Perrig, A. (2003). Security and privacy in sensor networks. *Computer*, *36*(10), 103-105.

Chou, L. D., Sheu, C. C., & Chen, H. W., (2006). Design and prototype implementation of a novel automatic vehicle parking system. Teoksessa *Hybrid Information Technology, 2006. ICHIT'06. International Conference on* Vol. 2, 292-297.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719-731.

Covington, M. J., & Carskadden, R. (2013). Threat implications of the internet of things. Teoksessa *Cyber Conflict (CyCon), 2013 5th International Conference on,* 1-12.

Dlamini, M. T., Eloff, M. M., & Eloff, J. H. P. (2009). Internet of things: emerging and future scenarios from an information security perspective. Southern Africa Telecommunication Networks and Applications Conference.

Dohr, A., Modre-Opsrian, R., Drobics, M., Hayn, D., & Schreier, G., (2010). The internet of things for ambient assisted living. Teoksessa *2010 Seventh International Conference on Information Technology*, 804-809.

Fink, G. A., Zarzhitsky, D. V., Carroll, T. E., & Farquhar, E. D. (2015). Security and privacy grand challenges for the Internet of Things. In*Collaboration Technologies and Systems (CTS), 2015 International Conference on,* 27-34.

Ghose, A., Biswas, P., Bhaumik, C., Sharma, M., Pal, A., & Jha, A. (2012). Road condition monitoring and alert application: Using in-vehicle Smartphone as Internet-connected sensor. Teoksessa *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, 489-491.

Giusto, D., Iera, A., Morabito, G., & Atzori, L. (Eds.). (2010). *The internet of things: 20th Tyrrhenian workshop on digital communications*. Springer Science & Business Media.

Gomez, C., & Paradells, J. (2010). Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine*, 48(6), 92-101.

Gou, Q., Yan, L., Liu, Y., & Li, Y. (2013). Construction and strategies in IoT security system. Teoksessa *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*, 1129-1132.

Greenberg, A. (2015, 21. heinäkuuta). Hackers remotely kill a jeep on a highway – with me in it. *Wired*. Haettu 18.2.2016 osoitteesta http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

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.

Huang, Y., & Li, G. (2010). Descriptive models for Internet of Things. In *Intelligent Control and Information Processing (ICICIP), 2010 International Conference on,* 483-486.

International strategy for cyberspace (2011). Haettu 3.2.2016 osoitteesta https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Lehto, M., & Kähkönen, A. (2015). Kyberturvallisuuden kansallinen osaaminen. Haettu 31.12.2015 osoitteesta **http://urn.fi/URN:ISBN:978-951-39-6105-3**

Libicki, M. C. (2007). *Conquest in cyberspace: national security and information warfare*. Cambridge University Press.

Kumar, S. (2014). Ubiquitous smart home system using android application, *International Journal of Computer Networks & Communications* Vol.6, No.1, January 2014, 33-43.

Kopetz, H. (2011). Internet of things, *Real-time systems,* 307-323.

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.

Notra, S., Siddiqi, M., Gharakheili, H. H., Sivaraman, V., & Boreli, R. (2014). An experimental study of security and privacy risks with emerging household appliances. Teoksessa *Communications and Network Security (CNS), 2014 IEEE Conference*, 79-84.

Richardson, R., & Director, C. S. I. (2008). CSI computer crime and security survey. *Computer Security Institute*, *1*, 1-30.

Smith, R., Grabosky, P., & Urbas, G. (2004). Cyber criminals on trial. *Criminal Justice Matters*, *58*(1), 22-23.

Suomalainen, J. (2014). Smartphone assisted security pairings for the internet of things. Teoksessa *Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2014 4th International Conference on,* 1-5.

Suomen kyberturvallisuusstrategia (2013), Haettu 3.2.2016 osoitteesta http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit

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

Weber, R. H., & Weber, R. (2010). *Internet of Things*. New York: Springer.

Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. *International Journal of Communication Systems*, 25(9), 1101.

Zhu, Q., Wang, R., Chen, Q., Liu, Y., & Qin, W. (2010). Iot gateway: Bridgingwireless sensor networks into internet of things. Teoksessa *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, 347-352.