Tuomo Lahtinen

Esineiden internet ja sen tietoturva sovelluskerroksella

Tietotekniikan kandidaatintutkielma

20. toukokuuta 2019

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Tuomo Lahtinen

Yhteystiedot: tuomo.t.lahtinen@student.jyu.fi

Ohjaaja: Antti-Juhani Kaijanaho

Työn nimi: Esineiden internet ja sen tietoturva sovelluskerroksella

Title in English: Internet of Things and security of application layer

Työ: Kandidaatintutkielma

Sivumäärä: 25+0

Tiivistelmä: IoT on tulevaisuuden internet, joka on kaikkialla ympärillämme. Se avaa lukuisia mahdollisuuksia, mutta toisaalta sen valtaisa kasvu on myös synnyttänyt riskejä, joita ihmisten tulisi arvioida. IoT sisältää kerroksia ja näihin kerroksiin kohdistuu erilaisia hyökkäyksiä, joiden seuraukset voivat olla ihmiskunnan kannalta vakavia. Hyökkäyksillä voidaan lamauttaa osia kriittisestä infrasta tai kaapata arkaluontoisia tietoja. Meidän tulisikin kiinnittää huomiota jatkossa IoT:n tietoturvaan. Jokaisen ihmisen tulisi ymmärtää perusteet tietoturvasta, jolloin heikoin lenkki vahvistuisi ja hyökkäysten onnistuminen vaikeutuisi.

Avainsanat: Tietoturva, IoT, haittaohjelmat

Abstract: IoT is a future of the Internet. It's everywhere around us and affects us. IoT opens many possibilities for humans but also creates risks which are created by enormous growth of IoT. Humans should evaluate these risks. IoT has different layers and each layer are exposed to different kinds of attacks. These attack can be critical to mankind. Purpose of attacks can be to takedown critical infrastructure or to steal valuable or personal data. In future humans should take care of the security of the Internet. Every people should understand at least the basics of the serurity. That could reinforce us to hold against attacks.

Keywords: Security, IoT, malware

Kuviot

Sisältö

1 Johdanto

Esineiden internet (Internet of Things, IoT) on älykäs, aina saatavilla, aina yhdistettävissä ja se on kaikkien tavoitettavissa, missä ja milloin vain (Vermesan ym. 2009, ss. 10–12). IoT:n voidaan katsoa käsittävän laitteet, jotka ovat kytkettävissä internettiin ja jotka viestivät verkon yli. Näitä laitteita voivat olla Morganin (2014) mukaan muun muassa matkapuhelimet, kuulokkeet, kaiuttimet, kahvinkeittimet, jääkaapit ja älykellot. IoT:n määritteleminen on kuitenkin vaikeaa. Yksiselitteistä ja universaalia määritelmää meillä ei ole IoT:lle (Gremban 2018).

Internet tulee koko ajan laajemmin saatavaksi. Yhdistämisen kustannukset laskevat, jolloin kehitetään uusia laitteita, joita pystytään yhdistämään verkkoon. Lisäksi sensoritekniikka lisääntyy, teknologian kustannukset laskevat ja älypuhelimien myynti on korkealla. Tämä mahdollistaa IoT:n räjähdysmäisen kasvun. (Morgan 2014; Vermesan & Friess 2014, ss. 83.) Ciscon (2014) mukaan IoT:hen on arvioiden mukaan kytkettynä noin 40 miljardia laitetta vuonna 2020, jolloin jokaista maapallolla elävää ihmistä kohden on noin viisi verkkoon kytkettyä laitetta. IoT koskettaa suurinta osaa meistä ja sen tietoturvallisuus on laitteita käyttävien ihmisten hyvinvoinnin kannalta tärkeää (Cisco 2014). IoT avaa lukemattomasti mahdollisuuksia, joita ihmiskunta voi hyödyntää. IoT:n sovelluskohteita ovat terveys, jälleenmyynti ja logistiikka, älykäs liikkuminen ja kuljetukset, älykäs teollisuus ja tuotanto, älykäs energiantuotto ja älyverkot, älykodit, -rakennukset ja infrastruktuuri, älykaupungit, ravinnon ja veden valvonta sekä vapaaehtoinen aistiminen (Kuvio 1).

IoT:stä on kaavailtu uuden sukupolven internettiä. Tämän saavuttaakseen IoT:n on oltava turvallinen ja samaan aikaan hyödyllinen. Turvallisuuteen onkin alettu enemmän kiinnittää huomiota. IoT:n laajetessa, siitä on tullut houkuttelevampi kohde myös hakkereiden silmissä. (Li ym. 2017, ss. 1–5.) IoT-laitteiden määrän kasvaessa on pakko alkaa kiinnittämään huomiota myös laitteiden tietoturvaan ja tietosuojaan. Laitteiden turvallisuusongelmia on paljon ja niiden ratkaiseminen on välttämätöntä (Ristolainen 2018). Suurimmat IoT:n ongelmat ovat käyttäjän todentaminen ja luottamuksellisuus. IoT tarvitsee pelisäännöt sille, miten tietoturva laitteissa

hoidetaan. Kenellä on lopulta vastuu laitteiden tietoturvasta. (Seppänen 2017 .) Tuleeko käyttäjän olla tietoturva-asiantuntija käyttääkseen IoT-laitteita?

Tämä tutkimus toteutetaan kirjallisuuskatsauksena ja se käsittelee IoT:n tietoturvaa sovellusten tasolla. Millaisia hyökkäyksiä tällä tasolla tehdään ja mitä toimia voimme tehdä turvataksemme tietoturvan? Lukijalle tulisi jäädä tekstistä mieleen mikä IoT on ja mihin tarvitsemme sitä. Lisäksi lukijalla tulisi jäädä kuva erilaisista hyökkäystyypeistä ja puolustuskeinoista IoT:n sovelluskerroksella.

Luvussa 2 käydään läpi IoT:n merkitystä ihmisten arkeen. Kuinka käytämme teknologiaa, mitä datan keruu merkitsee meille, sekä millaisia hyötyjä, uhkia ja riskejä IoT synnyttää? Lisäksi käydään läpi IoT:n sisältämät kerrokset. Luvussa 3 käsitellään sovelluskerrosta. Mitä hyökkäyksiä siihen kohdistuu, mitä hyökkäyksillä ajetaan takaa ja minkälaisia haittoja hyökkäykset aiheuttavat? Luvussa 4 tuodaan esille suojautumismahdollisuuksia näitä hyökkäyksiä vastaan ja miten IoT:n tietoturvaa voidaan parantaa, niin laitteen valmistajan kuin käyttäjänkin näkökulmasta. Viimeisessä luvussa 5, joka toimii yhteenvetona, kerrataan tutkimuksen pääkohdat ja pohditaan IoT:n tulevaisuutta.

2 Esineiden internet osana arkeamme

Tässä luvussa kerrotaan, kuinka IoT vaikuttaa meidän arkeemme, mitä hyötyjä ja haittoja siitä voi olla, sekä mistä kerroksista IoT koostuu. IoT on vahva osa ihmisten elämää ja kuten Gremban (2018) ilmaisee, on talouden puolella IoT:llä valtava merkitys. Vuonna 2025 IoT:n taloudellinen vaikutus on arvioitu olevan jopa 11,1 biljoonaa dollaria (Gremban 2018). Voidaan sanoa, että M2M (machine-to-machine) ja IoT tulevat luomaan markkinoiden ytimen tulevaisuudessa (Vermesan & Friess 2014, ss. 3).

2.1 Teknologia, data ja hyödyt ihmiskunnalle

Ihminen on riippuvainen teknologiasta. Gilroy-Ware (2016) kirjoittaa tekstissään älypuhelimen käyttäjän käyttävän laitettaan yli kolme tuntia päivässä. Älypuhelimissa ja muissa älylaitteissa on kuitenkin riskejä (Järvinen 2010). Tietokoneissa, puhelimissa ja tableteissa on nykyisin kamera, mikrofoni ja muita integroituja laitteita, joita voidaan hallita ohjelmallisesti. Näiden laitteiden etähallinta on mahdollista erilaisten haitta- ja valvontaohjelmien avulla. Sama pätee kaikkiin laitteisiin, joita voidaan ohjata ohjelmallisesti. Nämä laitteet voidaan kaapata omien etujen tavoitteluun. (Järvinen 2010, ss. 125.) Supon apulaispäällikkö Seppo Ruotsalaisen toteamus blogi-kirjoituksessa kuvaa hyvin mahdollisia uhkia mitä IoT-laitteet tuovat. Hänen mukaansa matkapuhelin voi muuttua salakuunteluvälineeksi kontrolloimalla mikrofonia etänä. Puhelinta ei täten kannattaisi pitää mukana missään, missä keskustellaan luottamuksellisista asioista. (F-Secure Global 2018.) Ihmisten on nähtävä hyödyt haittojen takana. Jos ihmisillä on pelko tietoturvattomuudesta, ei IoT:n hyötyjä pystytä näkemään. IoT sisältää monia positiivisia puolia, vaikka ne eivät olisikaan helposti havaittavissa. (Ploennings ym. 2018 ; Vermesan ym. 2009 .)

IoT tuo arkeemme paljon hyvää, kunhan hallitsemme sen käytön hyvin. Vaikutusalueita ovat muun muassa koulutus, terveydenhuolto, rakentaminen ja yritystoiminta, jossa IoT mahdollistaa asiakkaiden analysoinnin kerätyn datan pohjalta (big da-

ta), tuotekehityksen ja markkinoinnin (Abomhara & Køien 2015). Sensorit keräävät dataa. Datan avulla voimme tehdä analyysejä ja hallita asioita, kuten ennustaa säätä tai sairauksia. Kolikolla on myös kääntöpuolensa. Kerätty data on kyettävä suojaamaan, jotta saamme kaiken hyödyn irti IoT:stä (Ploennings ym. 2018 ; Vermesan ym. 2009 .) Tietosuojan lisäksi on laitevalmistajien ymmärrettävä, miksi dataa kerätään sensoreilla. Ei ole järkevää kerätä massiivisia määriä dataa, jos ei pysty tai tiedä, mihin sitä tulisi käyttää. Jos dataa vain kerätään ilman käyttötarkoitusta, saamme haitat, muttemme hyötyjä (Ploennings ym. 2018).

Yritykset pyrkivät tehostamaan palveluitaan datan avulla. Limnéll ym. (2014) mukaan asiakkaiden tietojen keräämistä perustellaan usein asiakaslähtöisenä palveluna. Asiakkaille pystytään tarjoamaan tuotteita, joita he haluavat ja tarvitsevat. Kyse on ehkä enemmänkin yritysten kilpailusta toisiaan vastaan bittien maailmassa, jossa asiakkaita yritetään palvella mahdollisimman hyvin. Asiakashan hyötyy usein tästä yritysten välisestä kilpailutilanteesta, jossa yritykset kilpailevat juuri yksittäisistä asiakkaista (Limnéll ym. 2014, ss. 186–187,213–218).

Terveydenhuollon tehostaminen IoT:n avulla antaa selviä hyötyjä ihmiskunnalle (Armentano ym. 2018). Leivänpaahtimen tai jääkaapin keräämän datan hyödyllisyys voidaan lähinnä kyseenalaistaan. Armentano ym. (2018) mukaan keinoäly (AI) ja IoT yhdessä mahdollistavat terveydenhuollossa suuria mullistuksia tulevaisuudessa. IoT-laitteilla voidaan seurata tarkasti potilaan terveyden tilaa jatkuvalla sensoriseurannalla, ja tulevaisuudessa voimme jopa käyttää tekniikkaa ennaltaehkäisevästi sairauksia ja tauteja vastaan (Armentano ym. 2018).

2.2 Uhat ja riskit

Tietotekniset laitteet sisältävät uhkia ja riskejä. Uhkat ovat tapahtumia, jotka vaikuttavat negatiivisesti käyttäjään tai yhteiskuntaan ja ne ovat torjuttavissa. Riskejä ei taas pystytä poistamaan kokonaan. Meidän tulee ymmärtää, että riskejä on olemassa ja niitä voidaan hallita ja pienentää, muttei poistaa kokonaan. (Limnéll ym. 2014, ss. 3.) IoT:stä on tulossa suuri uhka ihmiskunnalle globaalien uhkien joukossa.

IoT:n laajeneminen lisää kaapattavien, verkkoon kytkettyjen laitteiden lukumäärää, jolloin uhkien toteutuminen tulee todennäköisemmäksi. IoT tarvitsee sääntelyä ja ohjeistusta käyttöä varten. Tällä hetkellä puutteellinen tietoturva on riski, joka on kasvamassa liian suureksi. Lisäksi markkinat eivät toistaiseksi vaadi tietoturvastandarteja, joilla tietoturvakysymyksiä voitaisiin ratkaista. (Ristolainen 2018 .)

Sovelluksen ala	Mihin käytetään
E-terveys	Terveyden huollon ja potilaan välisen toimimisen tehostamiseen. Potilaat, joita tulee jatkuvasti sensoroida, saavat valtavasti hyötyä IoT-laitteiden lisääntyessä. Potilaan ei enää tarvitse olla läsnä hoitopaikassa vaan potilaan tilaa voidaan tarkkailla etänä. Erilaiset terveyden seuranta sovellukset tai sensorit, jotka lähettävät dataa eteenpäin.
Jälleenmyynti ja logistiikka	Myynnissä tunnistetaan asiakas, kirjataan tapahtuma ja tehdään tarjouksia asiakkaille näiden tapahtumien mukaan tai muutetaan jopa liiketoimintamallia asiakkaiden käytöksen mukaan. Logistiikassa hallintaan kokonaisuutta. Milloin, mitä, kuinka paljon kuljetetaan ja seurataan tarkasti logististen prosessien etenemistä.
Älykäs liikkuminen ja kuljetukset	IoV eli Internet of Vehicles, jossa kulkuvälineet ja niihin liittyvät järjestelmät viestivät keskenään. Esim. Tietullien toiminta, liikennemerkkien tunnistaminen, julkisen liikenteen aikataulut sekä navigointi.
Älykäs teollisuus ja tuotanto	Voidaan yhdistää älyverkkoon ja muihin IoT-sovelluksiin, joilla esimerkiksi tuotantoa voidaan ohjailla tarkasti sekä valvoa sitä sensoreilla. Näistä voidaan muodostaa/parannella liiketoimintamallia.
Älykäs energiantuotto ja älyverkko	Kokonaisuudesta yksittäisen talouden sähköjärjestelmään. Älykäs energia tarvitsee sensoreita ja tavan hallita ja reakoida nopeasti sähköntarpeen muutoksiin.
Älykodit, -rakennukset ja infrastruktuuri	Muodostaa fyysistä maailmaa missä elämme (älykaupungit). Voidaan hallita laitteita verkon yli mm. valot, sähkö ja vesi, turvallisuus, pysäköinti, jätteiden käsittely, erilaisten toimintojen hallinta sekä henkilökohtaiset profiilit.
Älykaupungit	Koostuu lähinnä muiden sovellus alojen sovelluksista, jotka muodostavat suuren älykaupunki kokonaisuuden.
Ravinnon ja veden valvonta	Tarkkaillaan ruuan alkuperää, määrää, tarvetta, laatua sekä logistiikkaa erilaisilla sensoreilla ja sovelluksilla.
Vapaaehtoinen aistiminen	Tämä käsittää erilaisten palautteiden, arvostelujen ja kuvien jakamisen muiden kanssa. Näistä voidaan tekoälyn avulla muodostaa parempaa kuvaa ympäristöstä.

Kuvio 1. IoT-sovelluskohteita (Vermesan & Friess 2014, luku 3.3).

IoT-laitteet ovat oivallinen kohde hyökkäykselle, koska usein laitteet toimivat M2M-periaatteella, jolloin ihminen ei valvo laitteiden toimintaa. Tällöin mahdolliset hyökkäykset havaitaan selvästi hitaammin kuin järjestelmissä ja laitteissa, joita kontrolloi ihminen. Isoja uhkakuvia yksityiselle ihmiselle ovat muun muassa henkilötietojen kaappaus, kodin lämmityksen tai sähkönjakelun katkaiseminen sekä kodin turvajärjestelmän sammuttaminen, joka mahdollistaisi murron asuntoon. Julkisella puolella uhkat ovat suuremmat, koska uhka koskettaa isompaa määrää ihmisiä. Hyökkäykset infrastruktuuria kohtaan voisivat aiheuttaa kaaosta, jos hyökkääjä esimerkiksi pääsee käsiksi sähkötuotantoon tai vedenjakeluun. (Abomhara & Køien 2015 ;

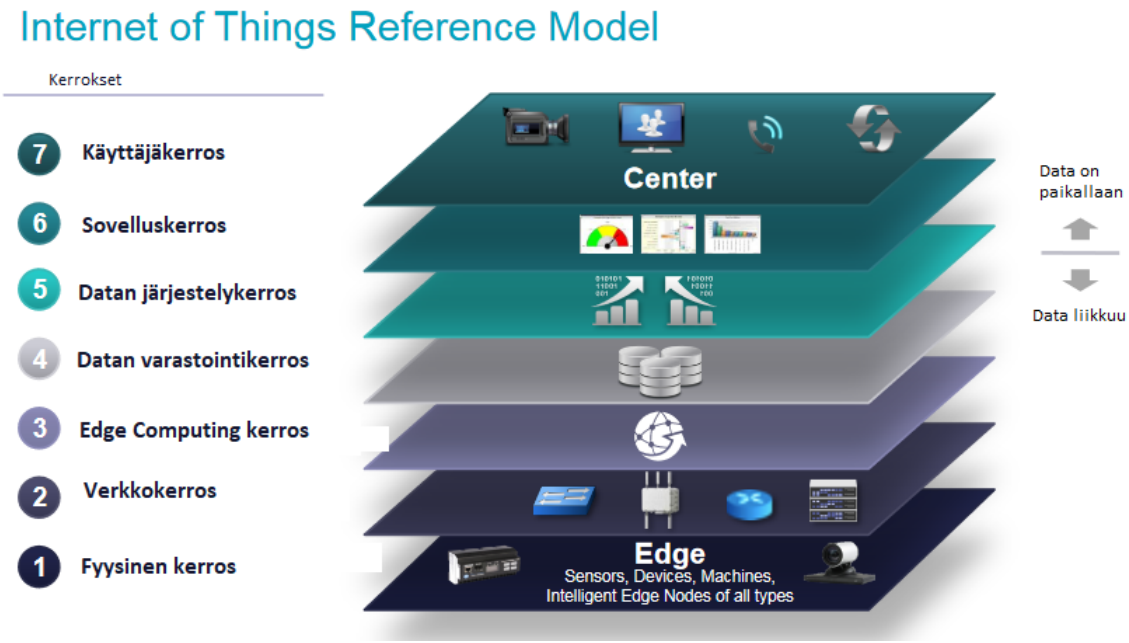
Radoglou Grammatikis ym. 2019 .) Kuviossa 1 esitellyt sovellukset voivat helpottaa elämäämme, mutta ne tuovat myös lisää riskejä ja uhkia ihmiskunnalle, joista juuri edellämainitut hyökkäykset kriittistä infraa kohtaan ovat vakava uhka (Vermesan & Friess 2014, ss. 90–91).

2.3 IoT:n kerrokset

IoT:n voidaan sanoa käsittävän seitsemän eri kerrosta Ciscon (2014) ”IoT Reference Modelin” mukaan. Kerrokset ovat esitetty kuviossa 2 ja ne ovat fyysinen kerros, verkkokerros, edge computing kerros, datan varastointikerros, datan järjestelykerros, sovelluskerros ja käyttäjäkerros.

Ensimmäinen kerros (fyysinen kerros) sisältää fyysiset laitteet, kuten kamerat ja sensorit (Ahmed ym. 2017 ; Cisco 2014). Toinen kerros (verkkokerros) vastaa ensimmäisen kerroksen viestien välityksestä. Kolmannella kerroksella (Edge computing) käsitellään dataa, jotta ylemmät kerrokset pystyvät hyödyntämään sitä jatkossa. Edge computing tarkoitus on tuoda prosessointi mahdollisimman lähelle päätelaitetta ja käyttötilannetta. Neljäs kerros muuttaa datan liikkuvasta paikallaan olevaksi toisin sanoen tällä kerroksella hoidetaan datan varastoiminen. Viidennellä kerroksella dataa haetaan, valitaan ja muokataan palvelemaan sovelluksen tarpeita. (Cisco 2014 .) Kuudes kerros on sovelluskerros, johon tässä tutkimuksessa keskitytään. Sovelluskerroksella sovellukset hallitsevat IoT-laitteita, raportoivat tai analysoivat dataa (Ahmed ym. (2017); Cisco (2014)). Viimeinen kerros koostuu ihmisistä, toisin sanoen laitteiden käyttäjistä, joita varten IoT on olemassa (Cisco 2014).

Kuten yllä jo kerrottiin, on jokaisella kerroksella omat tehtävänsä. Lisäksi kerrokset tuovat suojaa kyberhyökkäyksiä vastaan. Kaikkien kerrosten suojaus on oltava kunnossa, jotta kerrokset suojaisivat laitetta tehokkaimmin (Cobb & Myers 2014). Kun suojaus on kunnossa kaikilla kerroksilla, on hyökkääjän vaikea tunkeutua läpi. Jokaisen kerroksen suojaus on täysin itsenäinen, eivätkä kerrokset pysty viestimään keskenään mahdollisista hyökkäyksistä. (Limnéll ym. 2014, ss. 194–195.)



Kuvio 2. IoT:n kerrokset. Mukailtu (Cisco 2014).

3 Sovelluskerrokseen kohdistuvat hyökkäykset

Tässä luvussa kuvataan hyökkäystyyppejä IoT:n sovelluskerrosta vastaan. IoT-laitteet ovat haavoittuvaisia hyökkäyksiä kohtaan alhaisen laskentakapasiteetin takia (Abomhara & Køien 2015 ; Kessler 2014 ; Radoglou Grammatikis ym. 2019). Rajoittunut laskentateho ja muisti estävät kunnollisen suojauksen käytön laitteissa. Muun muassa erilaiset haittaohjelmien torjumiseen käytettävät ohjelmistot eivät välttämättä jaksa toimia IoT-laitteissa, ja salauksiakaan emme voi aina käyttää tästä samasta syystä. (Radoglou Grammatikis ym. 2019.) M2M-laitteet automatisoivat toimia, mutta vaikeuttavat hyökkäysten havainnointia, kuten kävi ilmi alaluvussa 2.2.

3.1 Palvelunestohyökkäykset

Palvelunestohyökkäys (denial-of-service, DoS) ja hajautettu palvelunestohyökkäys (distributed denial-of-service, DDoS) ovat hyökkäyksiä, joissa resurssista tai palvelusta yritetään tehdä saavuttamaton käyttäjille. DoS hyökkäykset ovat vanhoja, mutta DDoS hyökkäys on verrattaen melko uusi hyökkäyksen muoto. Kesslerin 2014 mukaan DDoS hyökkäyksiä alkoi ilmaantua vasta 2000-luvun paikkeilla. (Kessler 2014 .) DDoS hyökkäyksessä käytetään apuna botteja, jotka muodostavat bottiverkon. Bottiverkko muodostuu yhteen kytketyistä ja etähallittavista kaapatuista tietokoneista tai laitteista, joita voi olla jopa tuhansia. (Limnéll ym. 2014, ss. 112 ; Radoglou Grammatikis ym. 2019 .) DDos hyökkäyksessä kuormitetaan serveriä HTTP pyynnöillä, jotka haittaavat serverin toimintaa tai jopa kaatavat sen, jolloin palvelunestohyökkäys on onnistunut (Yi & Shun-Zheng 2009). IoT-laitteet ovat haavoittuvia palvelunestohyökkäyksiä kohtaan niiden alhaisen laskentakapasiteetin takia, jolloin laitteet ovat helposti ylikuormitettavissa, mikä aiheuttaa laitteen toiminnan lamaantumisen (Abomhara & Køien 2015 ; Kessler 2014).

DDoS hyökkäys kohdistuu yleensä yritykseen ja sen palveluihin. Kesslerin 2014 mukaan hyökkäyksellä on kuitenkin kaksi kohdetta: yritys ja yrityksen asiakkaat. Asiakkaathan kärsivät jopa enemmän kuin itse yritys hyökkäyksestä. Pahimmillaan

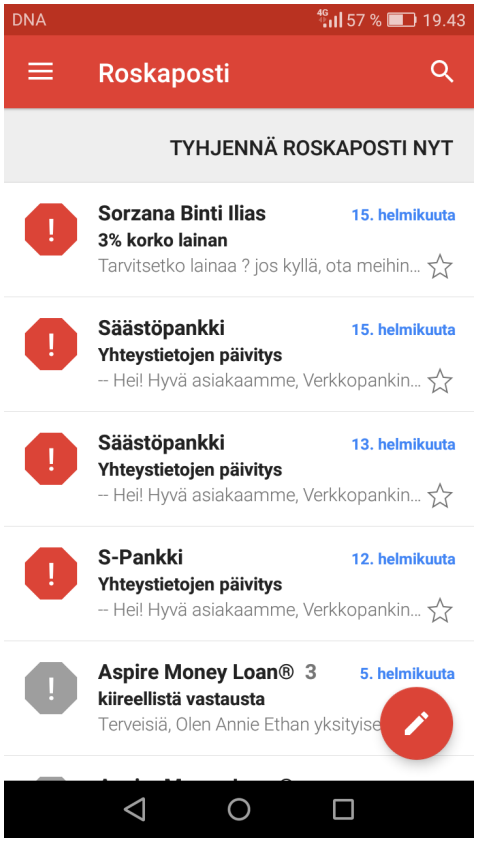
hyökkäykset voivat aiheuttaa merkittäviä rahallisia menetyksiä yrityksille kuten kävi Amazonille. Amazon on suuri nettikauppa, jonka myynti tapahtuu verkon välityksellä. Vuonna 2000 Amazonin sivusto oli kaatuneena noin kymmenen tuntia, mikä aiheutti yritykselle 600 000 dollarin menetyksen. (Kessler 2014 .) Toinen esimerkki laajasta palvelunestohyökkäyksestä on Mirai-bottiverkko. Mirai-bottiverkon hyökkäyksessä käytettiin jopa puoltamiljoonaa kaapattua IoT-laitetta (Kambourakis ym. 2017). Laitteet kaapattiin yksinkertaisesti hyödyntämällä tietoturva-aukkoja, jotka muodostuivat heikoista salasanoista (Ristolainen 2018). Onkin tärkeää vaihtaa laitteiden oletussalasanat uuteen salasanaan. Computer Weeklyn julkaisussa Cobb (2012) kertoo, että järjestelmänvalvoja on vastuussa oletussalasanan vaihtamisesta välittömästi asennuksen jälkeen vahvaan salasanaan.

3.2 Tietojenkalastelu

Tietojenkalastelu on eräs vanhimmista hyökkäysmuodoista, joka ulottuu myös tietotekniikan ulkopuolelle muun muassa yritys- ja sotilastiedustelu. Tässä kappaleessa käsitellään tietojenkalastelua sähköpostikalasteluna. Tietojenkalastelu sähköpostilla on Cobbin 2014 mukaan melko uusi vitsaus ja ennen vuotta 2002 ei oikeastaan ole rekisteröity tämän kategorian hyökkäyksiä. Tänä päivänä tietojenkalastelu on päivittäistä ja sitä toteutetaan lähinnä sähköpostin kautta "kalastellen". Sähköpostilla pyritään vaikuttamaan lukijaan niin, että lukija vastaa tietojenkalasteluviestiin antaen pyydetyt tiedot. (Cobb 2014 .) Yleensä tietojenkalastelulla pyritään saamaan kohteeksi valikoidun henkilön pankkitunnukset, pankkikortin numero, PIN-koodi tai salasanat ja käyttäjätunnukset johonkin palveluun (Ahmed ym. 2017 ; Cobb 2014).

Tietojenkalasteluviestit ovat aidon näköisiä ja niissä on pyritty käyttämään samanlaista ulkoasua kuin ison organisaation aidossa viestissä. Pikaisella katsauksella viesti voi näyttää aidolta, mutta huolellisempi tarkastelu osoittaa yleensä, että kysessä on tietojenkalasteluyritys. Tietojenkalasteluun tehdyt sähköpostit ovatkin tehty hämäämään lukijaa. (Cobb 2014.) Cobb (2014) kertoo tekstissään muutaman vinkin, josta tietojenkalasteluviestin voi tunnistaa. *Linkit* ovat yleensä pitkiä ja monimut-

kaisia tai sitten linkin osoite on asetettu HTML:ää käyttäen näkymättömäksi, joilloin linkin päämäärää ei voi tietää. *Salasanan tai PIN-koodin vaihto* on yleinen tietojenkalasteluviestin teema. Täytyy muistaa, että mikään luottamuksellinen taho, kuten pankki, ei kysele asiakkaansa salasanoja tai tunnuksia sähköpostitse, eikä pyydä päivittämään niitä (Limnéll ym. 2014, ss. 51). Viimeinen vinkki on *kömmähtelevä kieli*, joka on usein selvä merkki huijausviestistä. Jos viesti on kirjoitettu selvästi havaittavissa olevilla kirjoitusvirheillä, ei viestiin kannata reakoida mitenkään.



Kuvio 3. Roskaposti. Kuvio Tuomo Lahtinen.

Kuviossa 3 näkyy sähköpostipalvelun roskapostikansio, jonne on tullut kahdelta pankilta viestiä ja kahdelta lainantarjoajalta. Ehkä ilmeisin syy, miksi näitä viestejä ei ole avattu on se, että sähkopostilaatikon omistaja ei ole kummankaan pankin asiakas ja silti otsikkona on ”Yhteistietojen päivitys”, joka voisi vedota kyseisten pankkien asiakkaisiin. Limnéll ym. (2014, ss. 50–52) ovat listanneet kyberturvallisuuden perusperiaatteita ja ohje ”Varovaisuus kannattaa ja terveen järjen käyttä-

misellä parannat omaa ja yhteisösi turvallisuutta," toimii todella usein tietoturva-asioissa. Roskapostin kohdalla terveen järjenkäyttäminen on avainasia. Koska sähköpostikansion omistaja ei ole pankin asiakas, hän ei avaa sähköpostiin tullutta yhteystietojen päivityskehoitusta, joka näkyy kuviossa 3.

3.3 Virukset, madot, troijalaiset

Näissä hyökkäyksissä hyökkääjä vaikuttaa IoT-järjestelmään istuttamalla haitallisen ohjelman järjestelmään. Haittaohjelma voi estää järjestelmää toimimasta normaalisti, muuttaa/varastaa dataa ja ohjelman avulla hyökkääjä pääsee käsiksi luottamukselliseen dataan tai avaa takaportin järjestelmään. (Ahmed ym. 2017 .)

Virukset ovat itseään kopioivia koodeja, jotka tarvitsevat isäntäkoodin tai dokumentin sekä ihmisen apua levitäkseen. Ensimmäiset virukset luotiin 80-luvulla. (Guess & Salveggio 2014 .) Nykyisin virukset ovat yleisiä haittaohjelmia ja ne toimivat useilla eri tavoilla. Guess & Salveggio (2014) listaavat tekstissään erilaisia virustyyppejä. Niitä ovat muun muassa tiedoston saastuttaja, makro- ja kryptovirus ja boot sector virukset. Tosin viruksia ei ole nykyisin enää helppo kategorioida, vaan virusten toiminnot voivat sekoittua usean kategorian kesken. Virukset voivat avata takaportteja, hidastaa konetta tai lukita sen. Virukset voivat myös muuttaa tietokoneen käyttöoikeuksia. (Guess & Salveggio 2014 .)

Madot ovat haittaohjelmia, joilla on kyky monistautua, kuten viruksillakin (Limnéll ym. 2014, ss. 111). Viruksista poiketen, matojen ei tarvitse integroitua suoritettavaan koodiin, vaan ne toimivat itsenäisesti (Guess & Salveggio 2014). Madot käyttävät kohdejärjestelmän haavoittuvaisuuksia hyväkseen levitäkseen eteenpäin (Limnéll ym. 2014, ss. 111). Tyypillisiä tartunnan leviämistapoja ovat haavoittuvaiset palvelut, sähköposti, välitön viestintä kuten WhatsApp ja avoimet tiedostonjakelut. Usein mato käyttää useita eri tapoja levitä ja niitä käytetään yleensä muiden haittaohjelmien levitykseen. (Guess & Salveggio 2014 .)

Troijalaisten toiminta on erilainen kuin matojen tai virusten. Ne ovat sovelluksia, jotka huomaamattomasti pääsevät järjestelmiin sisään ja avaavat takaportin järjes-

telmään tai varastavat dataa (Limnéll ym. 2014, ss. 111). Niiden avulla muutetaan usein tietokoneita zombi-koneiksi toisin sanoen liitetään kone osaksi bottiverkkoa, jota myöhemmin hyödynnetään palvelunestohyökkäyksessä. Muita troijalaisen toimintatapoja ovat muun muassa datan poistaminen tai muuntaminen, näppäimistön lyöntien tallennus, eri ohjelmistojen poiskytkentä tai tiedostojen lataus ilman käyttäjän lupaa. Yleisimpiä leviämistapoja ovat liitteiden tai näytönsäästäjien mukana tulevat troijalaiset. Paras keino suojautua troijalaisilta on tietämys tietoturvasta. Laitteeseen päässyttä troijalaista vastaan on vaikea taistella ja ennaltaehkäisy on selvästi helpoin tapa torjua troijalaista. (Cobb 2014 .)

4 Suojautuminen hyökkäyksiä vastaan

Tässä luvussa käsitellään suojautumista yllä esitettyjä hyökkäyksiä vastaan. Onnistunut sovelluskerroksen suojaus käsittää toimivan tunnistautumisen hallinnan ja tehokkaan tietosuojan kuten Vermesan ym. (2009, ss. 31–32) kuvailevat IoT Road Map:ssä. Limnéllin 2014 mukaan on tärkeää ymmärtää, että hyökkäyksiä voidaan toteuttaa melko helposti. Lisäksi tietotekniset laitteet sisältävät aina riskejä, joita meidän tulee arvioida (Limnéll ym. 2014, ss. 105–111,122–124).

4.1 Salasanat

Monet hyökkäykset ovat torjuttavissa hyvällä salasanalla (Ahmed ym. 2017). Alaluvussa 3.1 käytiin jo Mirai-bottiverkon avulla tehty palvelunestohyökkäys läpi, jossa algoritmi etsi heikkoja salasanoja, jonka kautta pääsisi laitteeseen sisään. Käytetyimpien heikkojen salasanojen joukkoon kuuluvat muun muassa SplashDatan (2019) listauksen mukaan *password*, eripituiset järjestykselliset numerojonot kuten *123456* sekä näppäimistöllä rivissä olevat aakkoset kuten *qwerty*. Jo Mel Brooksin elokuvassa Space Balls (1987) vitsailtiin salasanalle 12345 ja harmillisen vähän on noista vuosista opittu tähän päivään mennessä.

Salasanan vahvuus määräytyy pitkälti sen pituudesta ja erikoismerkit vaikeuttavat salasanan arvausta. Raa'an voiman hyökkäyksissä (brute-force attack) pituus on tärkein tekijä estemään salasanan murron. (Cobb 2012.) Cobbin 2012 mukaan salasana *Zq!5$7e* murtuu nopeammin kuin *Password1*, koska siinä on vähemmän merkkejä. Toki tässä tapauksessa hyökkäyksessä käytettäisiin oletusta, että erikoismerkit ovat mukana. Jos hyökkäyksen toteuttaisi vain aakkosilla ja numeroilla murtuisi *Password1* nopeammin eikä *Zq!5$7é* murtuisi ollenkaan. Limnéll ym. (2014) kirjoittaa, että vahvan salasanan lisäksi samaa salasanaa ei kannata käyttää useissa palveluissa. Jos käytät yhtä salasanaa useassa palvelussa ja salasana murretaan, on hyökkääjällä pääsy useille käyttäjätileille ja suurempaan määrään arkaluontoista tietoa (Limnéll ym. 2014, ss. 50–51).

4.2 Virustentorjunta

Haittaohjelmat ovat vaikuttaneet meihin yli kolmen vuosikymmenen ajan ja näitä vastaan on kehitetty virustentorjunta ohjelmia (Cobb & Myers 2014). Virustentorjuntaohjelmat ovat tärkeitä luottamuksellisuuden, luotettavuuden ja eheyden kannalta IoT verkoissa (Ahmed ym. 2017). Nämä ohjelmat tarkkailevat tietokoneessa tapahtuvaa toimintaa ja yrittävät havaita kaikki poikkeavuudet normaaliin tilanteeseen, mutta kuten Cobb & Myers (2014) tekstissään kirjoittavat, aina mahdollisten poikkeavuuksien havaitseminen ei ole helppoa. Joka päivä syntyy jopa miljoonia uusia haittaohjelmia, jotka hyödyntävät tietoturva-aukkoja (Cobb & Myers 2014).

Virustentorjuntaohjelmat voidaan asettaa skannaamaan tietokonetta käynnistyksen yhteydessä tai tarpeen mukaan. Ohjelmisto voi myös tehdä jatkuvaa seurantaa ja se onkin tehokkain tapa suojautua hyökkäyksiä vastaan. Toinen tehokas tapa on skannata aina, kun liikennettä tapahtuu sisään tai ulos tietokoneesta. Torjuntaohjelmat voivat hidastaa tietokoneen toimintaa merkittävästi, jos ohjelmaa ei ole optimoitu kunnolla. Ohjelmat kuluttavat reilusti muistia, jonka takia virustorjuntaohjelmistojen asentaminen IoT-laitteisiin on haastavaa. (Cobb & Myers 2014.)

Virustentorjuntaohjelmat käyttävät erilaisia skannausmetodeja. Yksikään skannausmetodi ei ole yksinään riittävä varmistaakseen aukottoman virusten havaitsemisen. Jokainen haittaohjelma käyttää erilaista koodia suorittaakseen toimintonsa ja näiden toimintojen havaitsemiseen tarvitaan useampia metodeja, jotta virukset pystytään tunnistamaan, estämään tai lopettamaan niiden toimet ja palauttamaan tämän jälkeen järjestelmä normaalitilaan (Cobb & Myers 2014.).

4.3 Access Control List

IoT tarvitsee useita erilaisia tapoja hallita sitä, kenellä on oikeus käyttää laitteita tai päästä käsiksi dataan (Vermesan & Friess 2014, ss. 91). Access Control List (pääsylista, ACL) suojaa IoT-laitteita määrittämällä, mitä liikennettä päästetään ulos ja mitä sisään (Cisco 2014). Ahmedin ym. (2017) mukaan ACL:llä voidaan tarkastella myös IoT-laitteeseen sisään pyrkivien käyttäjien pyyntöjä. ACL on suojaustekniikkana te-

hokas, kun puhutaan järjestelmän luotettavuudesta ja datan tietosuojasta (Ahmed ym. 2017). ACL on lista, joka voidaan asettaa esimerkiksi reitittimeen. ACL on siis apuväline, joka kertoo reitittimille, mikä liikenne sallitaan ja mikä liikenne tulee estää (Cisco 2014).

Ciscon (2014) ohjeesta käy ilmi, että ACL:ää voidaan käyttää useammalla tavalla. Voidaan muun muassa määrittää IP-osoitteet, joista liikenne sallitaan tai voidaan sallia sähköpostit, mutta estää Telnet-liikenne. Joissakin tapauksissa ACL:än käytöllä pyritään rajoittamaan liikennettä ja näin resurssien vapauttaminen muihin tarkoituksiin on mahdollista. (Cisco 2014 .)

ACL:n käytöllä on hyötyjä, vaikka sen käyttö ei olekaan ihan yleistä yksityisillä ihmisillä. Yrityksille voi olla suurtakin hyötyä rajata esimerkiksi liikennettä, jota päästetään yrityksen sisäiseen verkkoon. Jos verkon liikennettä ei rajata, on liikenteellä pääsy kaikkiin verkon osiin. (Cisco 2014 .) Ajatellaan tilannetta, että verkossa vain tietyn tietokoneen täytyy olla yhteydessä tiettyyn IoT-laitteeseen. Miksi haluaisimme että IoT-laitteeseen voisi yhdistää myös toisen koneen? Tässä tilanteessahan voidaan sallia vain tämän yhden tietokoneen pääsy IoT-laitteeseen.

4.4 Palomuuri

Ihmisiltä kysyttäessä tietokoneen suojauksesta, usein mainitaan palomuuri. Palomuuri on välttämätön, muttei riittävä suoja kaikkia hyökkäyksiä vastaan. Joskus murtautumiset eivät ole epäilyttäviä, vaan murtautuminen voidaan toteuttaa ”valeasussa”. Tämänkaltaista murtautumista käyttävät muun muassa troijalaiset, jotka esiteltiin luvussa 3.3. Tässä tapauksessa palomuuri ei tunnista hyökkäystä ja tarvitaan palomuurin rinnalle myös muuta suojausta. (Bace 2014 .)

Palomuurin tehtävä on estää luvattomat murtautumiset koneeseen/laitteeseen (Bace 2014). Se valvoo taukoamatta verkon liikennettä useilla IoT-kerroksilla (Radoglou Grammatikis ym. 2019) ja käy läpi vastaanotettavat paketit, joista epäilyttävät tai ei halutut paketit estetään ja muut päästetään verkossa eteenpäin. Palomuuria tarvitaan, jos salaus, tunnistautuminen ja ACL eivät pysty estämään luvatonta käyttäjää.

(Ahmed ym. 2017 .) Kuten jo alaluvussa 4.1 kerrottiin, on salasanoilla iso rooli tietoturvassa. Jos laitteeseen on valittu heikko salasana, voi salaus ja tunnistautuminen epäonnistua välittömästi, jolloin luvattomalle käyttäjälle tarjoutuu avointa polkua eteenpäin.

4.5 Riskikartoitus

Riskikartoitus on hyvä tapa parantaa tietoturvaa tarkastelemalla olemassa olevia arkkitehtuureja, nykyistä tietoturvaa ja mahdollisia riskejä, joita tietoteknisiin laitteisiin ja järjestelmiin liittyy. Riskit tulee tunnistaa ja ehkäistä, jos se on mahdollista. Riskejä pystytään vähintään pienentämään, jollei kokonaan poistamaan. Riskikartoituksella voidaan löytää tietoturvasta puutteita ja aukkoja, joita sitten korjaillaan muilla tässä luvussa esitetyillä menetelmillä. (Limnéll ym. 2014, ss. 105–111.)

Radoglou Grammatikis ym. (2019) esittelevät tekstissään riskimallin, joka helpottaa riskien todennäköisyyden ja mahdollisten seurausten suuruuden tunnistamista. Mallissa (kuvio 4) annetaan arvoja neljään eri kohtaan, jotka ovat riskin todennäköisyys, toteutuneen riskin vaikutusten suuruus, vastatoimet ja riskin taso. Nämä neljä kohtaa täytettynä antavat hyvän kuvan siitä onko uhka todellinen ja tarvitaanko toimia riskin pienentämiseen. Riskimalleja on olemassa useita ja tärkeintä on ehkä löytää se itselle käyvä malli.

Riskianalyysi				
Turvallisuus uhka	Todennäköisyys	Vaikutus	Vastatoimet	Riskin taso
DDoS hyökkäys sähköverkkoa kohtaan	Harvinainen	Katastrofaalinen	x	Pieni
Henkilötietojen kaappaus tietojenkalastelulla	Todennäköinen	Vakava		Suuri

Kuvio 4. Riskimalli. Mukailtu (Radoglou Grammatikis ym. 2019).

5 Yhteenveto

IoT luo meille paljon mahdollisuuksia, mutta sen tietoturvaan tulee kiinnittää tulevaisuudessa enemmän huomiota. IoT leviää kaikkialle ja voimmekin kohta alkaa käyttämään lyhennettä IoE eli Internet of Everything. Laajeneminen kriittiseen infrastruktuuriin, terveydenhuoltoon ja robottiautoihin luo esimerkiksi suuria tietoturvahaasteita. Infran lamauttaminen on todella suuri riski. Radoglou Grammatikis ym. (2019) mainitsevat tekstissään Ukrainan (2015) joulukuussa tapahtuneen hyökkäyksen, jossa sähköverkkoa vastaan hyökättiin ja 225 000 ihmistä jäi sähköttä. Hyökkäykset terveydenhuoltoa tai robottiautoja vastaan voivat välittömästi uhata jopa ihmishenkiä. Meillä on keinoja suojata IoT-laitteita, mutta tarvitsemme myös markkinoiden halun mukaan tähän. Jos kuluttajat vaativat tietoturvaa, saamme laitevalmistajatkin tekemään toimia tietoturvan parantamiseksi. Standardit IoT-laitteille ovat askel, joka meidän tulee ottaa.

Sovelluskerrokseen kohdistuu erilaisia hyökkäyksiä, joista DDoS-hyökkäykset ovat ihmiskunnan kannalta kaikkein vakavimpia. Hyökkäysten tekeminen on nykyisin todella helppoa ja hyökkäyksiä voi ostaa palveluina muun muassa pimeästä verkosta (Tor-verkosta). Niin kauan kuin hyökkäysten kohteeksi löytyy helppoja kohteita ja hyökkäysten tekeminen on helppoa, tulevat erilaiset hyökkäykset vaikuttamaan vahvasti keskuudessamme. Monet hyökkäykset, jotka esiteltiin tässä työssä, ovat torjuttavissa tietoturvallisuuden ymmärtämisellä. Järki ja varovaisuus torjuu tietojenkalastelu yrityksiä. Laitteisiin tunkeutumista vastaan voidaan vaikeuttaa vahvoilla salasanoilla, palomuurilla sekä toimivalla virustentorjuntaohjelmistolla. Riskikartoituksella saamme selville, mitä toimia ja millä suuruudella toimia tulee suorittaa.

Turvallisuus on keskeisessä osassa myös tulevaisuudessa puhuttaessa IoT:stä. Luotettavuus ja turvallisuus ovat avainasioita. Kun tunnemme hyökkäysmuodot, voimme keskittyä tehokkaasti niiden torjuntaan. Tulevaisuudessa tutkimuksien kysymys voisi olla, miten saamme alhaisen laskentakapasiteetin laitteet suojattua? Tutkimuksissa voisikin tarkastella käytännön tasolla menetelmiä, joilla voisimme suojata näi-

tä alhaisen laskentakapasiteetin laitteita.

Kirjallisuutta

Abomhara, M. & Køien, G. 2015. *"Cyber Security and the Internet of Things:Vulnerabilities,Threats, Intrudersand Attacks"*. Journal of Cyber Security, Vol. 4, s. 65–88. Saatavilla WWW-muodossa <URL: https://www.researchgate.net/profile/Geir_Koien/publication/277718176_Cyber_Security_and_the_Internet_of_Things_Vulnerabilities_Threats_Intruders_and_Attacks/links/55e3f79508ae6abe6e8e853b/Cyber-Security-and-the-Internet-of-Things-Vulnerabilities-Threats-I pdf>. Viitattu 20.5.2019.

Ahmed, A., Ahmed, M., Khan, O. & Shah, M. 2017. *"A Comprehensive Analysis on the Security Threatsand their Countermeasures of IoT"*. International Journal of Advanced Computer Science and Applications, Vol. 8, nro. 7, s. 489–498. Saatavilla WWW-muodossa <URL: http://thesai.org/Downloads/Volume8No7/Paper_68-A_Comprehensive_Analysis_on_the_Security_Threats.pdf>. Viitattu 20.5.2019.

Armentano, R., Bhadoria, S., Chatterjee, P. & Deka, C. 2018. *"The Internet of Things : Foundation for Smart Cities, EHealth, and Ubiquitous Computing"*. E-kirja. CRC Press, Taylor & Francis Group [2018]. s. 371–386.

Bace, R. 2014. *"INTRUSION DETECTION AND INTRUSION PREVENTION DEVICES"*. Teoksessa Bosworth, S., Kabay, M. & Whyne, E. 2014. Computer security handbook. E-kirja. Luku 27.

Cisco. 2014. *"The Internet of Things Reference Model"*. Saatavilla WWW-muodossa <URL: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf>. Viitattu 20.5.2019.

Cisco. 2014. *"Cisco IOS Security Configuration Guide, Release 12.2"*. Saatavilla WWW-muodossa <URL: https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c.html>. Viitattu 20.5.2019.

Cobb, C & Myers, A. 2014. *"ANTIVIRUS TECHNOLOGY"*. Teoksessa Bosworth, S., Kabay, M. & Whyne, E. 2014. Computer security handbook. E-kirja. Luku 41.

Cobb, M. 2012. *"Password security best practices: Change passwords to passphrases"*. Computer Weekly. Saatavilla WWW-muodossa <URL: https://www.computerweekly.com/tip/Password-security-best-practices-Change-passwords-to-passphrases>. Viitattu 20.5.2019.

Cobb, S. 2014. *"SPAM, PHISHING, AND TROJANS: ATTACKS MEANT TO FOOL"*. Teoksessa Bosworth, S., Kabay, M. & Whyne, E. 2014. Computer security handbook. E-kirja. Luku 20.

F-Secure Global. 2018. *"Suomen ylin johto F-Securen Tietoturvallinen Suomi -seminaarissa"*. Saatavilla WWW-muodossa <URL: https://blog.f-secure.com/fi/suomen-ylin-johto-f-securen-tietoturvallinen-suomi-seminaarissa/>. Viitattu 20.5.2019.

Gilroy-Ware, M. 2016. *"Smartphones are stealing our time. This new year, I want to claim it back"*. The Guardian. Saatavilla WWW-muodossa <URL: https://www.theguardian.com/commentisfree/2016/dec/29/smartphones-time-new-year-apps-resolution-facebook>. Viitattu 20.5.2019.

Gremban, K. 2018. *"Editorial and introduction to the issue: risk and rewards of the internet of things"*. IEEE Internet of Things Magazine. Vol 1. s. 2–3.

Guess, R. & Salveggio, E. 2014. *"MALICIOUS CODE"*. Teoksessa Bosworth, S., Kabay, M. & Whyne, E. 2014. Computer security handbook. E-kirja. Luku 16.

Hall, J. 2019. TeamsID. *"SplashData's Top 100 Worst Passwords of 2018"*. Saatavilla WWW-muodossa <URL: https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/>. Viitattu 20.5.2019.

Järvinen, P. 2010. *"Yksityisyys Turvaa digitaalinen kotirauhasi"*.

Kambourakis, G., Kolias, C. & Stavrou, A.2017. *"The Mirai Botnet and the IoT Zombie Armies"*. IEEE Military Communications Conferencee.

Kessler, G. 2014. *"DENIAL-OF-SERVICE ATTACKS"*. Teoksessa Bosworth, S., Kabay, M. & Whyne, E. 2014. Computer security handbook. E-kirja. Luku 18.

Li, S., Xu, L. & Romdhani, I. 2017. *"Securing the Internet of Things"*. E-kirja. Cambrid-

ge, MA.

Limnéll, J., Majewski, K. & Salminen, M. 2014. *"Kyberturvallisuus"*. Docendo.

Jacob Morgan. 2014. *"A Simple Explanation Of 'The Internet Of Things'"*. Forbes. Saatavilla WWW-muodossa <URL: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#69760df91d09>. Viitattu 20.5.2019.

Ploennings, J., Cohn, J. & Stanford-Clark, A. 2018. *"The Future of IoT"*. IEEE Internet of Things Magazine. Vol 1. s. 28–33.

Radoglou Grammatikis, P., Sarigiannidis, G. & Moscholios, D. 2019. *"Securing the Internet of Things: Challenges, threats and solutions"*. Internet of Things. Vol 5. s. 41–70.

Ristolainen, S. 2018. *"Herätys! IoT on turvattava juuri nyt"*. F-Secure Blog. Saatavilla WWW-muodossa <URL: https://blog.f-secure.com/fi/heratys-iot-on-turvattava-juuri-nyt/>. Viitattu 20.5.2019.

Saana Seppänen. 2017. *"Omakynä: Meidän täytyy keksiä säännöt IoT:lle"*. Viestintävirasto [teema]. Saatavilla WWW-muodossa <URL: https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/11/ttn201711301336.html>. Viitattu 20.5.2019.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I., Mazura, M., Harrison, M., Eisenhauer, M. & Dooby, P. 2009. *"Internet of Things Strategic Research Roadmap"*. Saatavilla WWW-muodossa <URL: https://www.researchgate.net/publication/267566519_Internet_of_Things_Strategic_Research_Roadmap>. Viitattu 20.5.2019.

Vermesan, O. & Friess, P. 2014. *"Internet of Things – From Research and Innovation to Market Deployment"*. River Publishers.

Yi, X., & Shun-Zheng, Y. 2009. *"Monitoring the Application-Layer DDoS Attacks for Popular Websites"*. IEEE/ACM TRANSACTIONS ON NETWORKING, Vol. 17, Nro. 1.