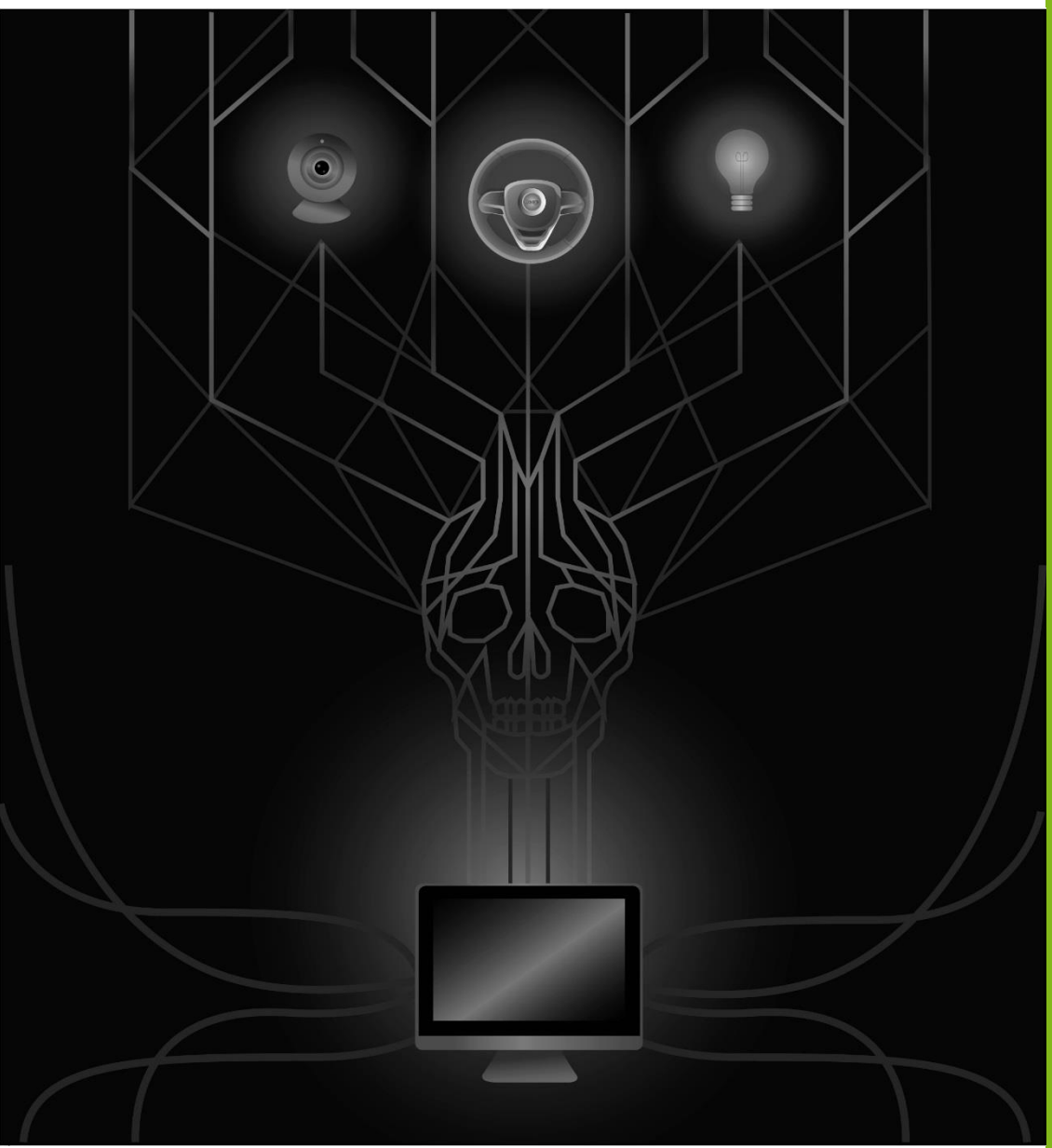
Ari Paasonen

Internet of Things – Haavoittuvuuksien verkko



Tradenomi

Tietojenkäsittely

Syksy 2017

KAJAANIN
AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Tiivistelmä

Tekijä(t): Paasonen Ari

Työn nimi: Internet of Things – Haavoittuvuuksien verkko

Tutkintonimike: tradenomi (AMK), tietotekniikka

Asiasanat: Asioiden internet, tietoturva, kodintekniikka

Tutkimuksessa pyritään selvittämään ja esittelemään IoT:n eli asioiden internetin yleisimmät uhat. Tutkimuksessa käytettyjen esimerkkitapausten IoT-laitteet ovat pääsääntöisesti kohdistettu kuluttajamarkkinoille. Tämän lisäksi tutkimuksessa käsitellään IoT-laitteisiin kohdistuneita verkkohyökkäyksiä.

Tutkimus tapahtuu IoT-teknologioitten lajittelemisella pääryhmiin ja tarkastelemalla näiden pääryhmien yhdistäviä heikkouksia. Sekä IoT-teknologioihin että niiden uhkiin tutustutaan tutkimuksessa esimerkkitapausten avulla.

Tutkimusten perusteella pystytään todistamaan selkeä linja IoT-laitteiden tietoturvassa ja turvallisuudessa kuluttajille. Tulevaisuuden kannalta onkin tärkeää, että IoT-laitteiden ylläpito otetaan tarkemmin huomioon uusia ratkaisuja ja laitteita valmistaessa.

Abstract

Author(s): Paasonen Ari

Title of the Publication: The Internet of Things – A Web of Exploitation

Degree Title: e.g. Bachelor of Engineering, Construction Engineering

Keywords: Internet of Things, security, domestic technology

The aim of this study was to determine and introduce the most common threats to the Internet of Things. The IoT devices used in the example cases of this study were mostly directed towards the consumer market. In addition, this study also covered cyberattacks against IoT devices.

The study was conducted by dividing the IoT technologies into groups and then comparing the weaknesses these groups shared. Both the IoT technologies and their possible weaknesses were introduced through example cases.

Based on this study, a clear connection was made between the information security of the IoT devices and the security and privacy of the consumer. Therefore, it is important for the future that the support and administration of IoT devices are more prominently taken into consideration when new solutions and devices are being manufactured.

Sisällys

1 Johdanto 1

2 Opinnäytetyön rakenne, kysymys ja metodi 5

3 Historia 7

3.1 Internet of Things: lyhyt historia ja tulevaisuus 7

3.2 Internet of Things turvallisuus ja riskit lyhyesti 9

4 Uhat aloittain 10

4.1 Ajoneuvot 10

4.1.1 Esimerkkitapaus: Cherokee Uconnect ja siihen kohdistunut hyökkäys 11

4.2 Kodinkoneet ja elektroniikka 13

4.2.1 Esimerkkitapaus: Philips Hue älyvalo 13

4.2.2 Tulevaisuus 15

4.2.3 Vizio 16

4.2.4 Pohdinta 17

4.3 Verkkohyökkäykset 18

4.3.1 Esimerkkitapaus: Mirai 18

4.3.2 BrickerBot Vigilante Botnet 22

4.3.3 Hajime Vigilante Botnet 23

5 Pohdinta 26

Lähteet 28

1 Johdanto

Internet of Things eli niin sanottu asioiden internet on käsite, joka kattaa kaksi peruspilaria; ”Internet” ja ”asiat”. Kenties epätarkalta ja kaiken kattavalta kuulostavalla ”asiat” termillä tarkoitetaan tässä yhteydessä mitä tahansa esinettä, oli kyseessä sitten älypuhelin, sensori, käyttäjä tai mikä tahansa muu laite tai komponentti mikä on kykenevä kommunikoimaan internetin välityksellä ja olemaan käytettävissä paikasta ja ajasta riippumatta. [1, s. 1.1 Introduction].

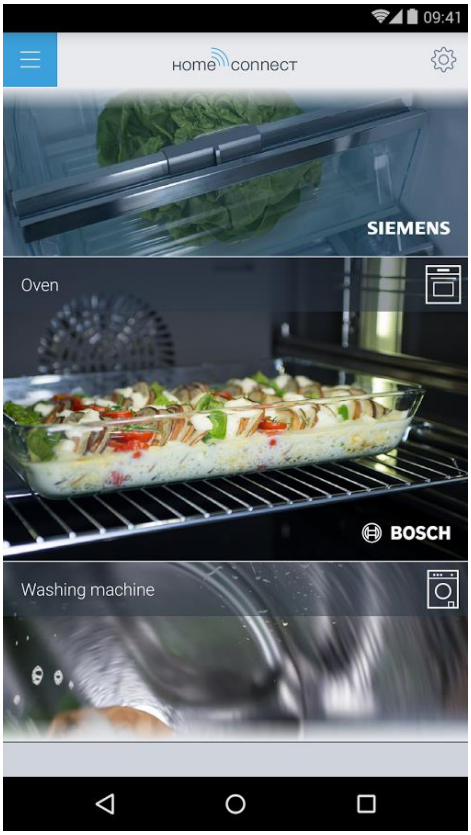
Nykypäivänä yhä useampi laite on tavalla tai toisella yhteydessä internetiin. Näihin laitteisiin voivat lukeutua muun muassa älypuhelimet, pyykinpesukoneet, kahvinkeittimet, erilaiset anturit (mm. lämpö, liike, kamera, ilmanpaine), lamput sekä myös laitteiden yksittäiset komponentit. Täydellistä listaa IoT-laitteista on mahdotonta määritellä, vaan lähestulkoon mikä tahansa laite mikä käyttää olemassa olevaa kommunikointiprotokollaa on potentiaalinen IoT-laite. Internet of Things, lyhennettynä IoT, on teknologian kehittyvässä maailmassa nopeasti nousemassa osaksi tulevaisuuden arkea niin kotitalouksissa kuin myös liiketoiminnassa ja jokapäiväisessä elämässä ja palveluissa. Sitä voidaan soveltaa aina yksinkertaisimmista kodinkoneista monimutkaisimpiin laitteisiin ja jopa terveydenhuoltoon sairaiden potilaiden elintoimintojen tarkkailun muodossa. IoT:n pyrkimyksenä on luoda yhtenäinen verkko, mihin kuuluu sekä älykkäitä objekteja että niitä käyttäviä ihmisiä. Nämä verkon jäsenet ovat universaalisti ja kaikkialla läsnäolevasti kommunikointiyhteydessä toisiinsa. Joissain tilanteissa loppukäyttäjää ei edes tarvita, vaan älylaite toimii itsenäisesti ympäristössä mihin se on asetettu toimimaan. [1, s. 1.3 IoT architectures]. IoT on tuonut lähes rajattomasti mahdollisuuksia parantaa jo olemassa olevia palveluita sekä luoda uusia mahdollisuuksia käyttää älykästä teknologiaa ihmisten hyväksi.

IoT-teknologiasta on valtavasti hyötyä yritysmaailmassa, missä se tukee muuta yritystoimintaa ja parantaa palvelutasoa, nopeuttaa aiemmin hitaita prosesseja ja toimintamalleja muuttaen niistä dynaamisia ja ketteriä. IoT-teknologiasta hyötyisivät esimerkiksi laitteistojen huoltopalvelut. IoT-laite tarjoaa automaattisesti informaatiota mahdollisista huoltotarpeista laitteistossa, mikä nopeuttaa sekä huoltotoimenpiteitä itsessään, että myös mahdollisia ongelmanratkontatilanteita, joissa huoltoyritys voi tukeutua IoT-laitteen tarjoamaan statistiikkadataan. IoT:lla on siis yhtä paljon käyttömahdollisuuksia kuin laitteitakin. Maailman johtava hissi ja liukuporrasvalmistaja KONE on ottanut käyttöönsä erillisen IoT-palvelun tulevaisuuden hissien ja liukuportaiden monitorointiin ja ylläpitoon. IBM Watson alustaa käyttävä 24/7 Connected Services kerää dataa tuhansilta eri antureilta pilveen.

Tällä tavoin on mahdollista parantaa laitteiden käyttövarmuutta sekä turvallisuutta. Kyseinen teknologia on tuonut hissien huollon täysin uudelle tasolle, missä laiteviat on mahdollista ennakoida ja laitteita on mahdollista monitoroida reaaliajassa ympäri maailmaa. [2.]

Kuluttajien kannalta yksinkertaisena esimerkkinä IoT:sta toimii internettiin kytketty kahvinkeitin. Idea voi kuulostaa absurdilta, mutta IoT-teknologia mahdollistaisi uusia toimintoja ja käyttötapoja olemassa olevalle vanhalle tekniikalle ja tällä tavoin tarjoaisi uusia ominaisuuksia ja käyttötapoja eri laitteille. Tässä esimerkissä kahvinkeitin ja herätyskello kommunikoivat keskenään ja tätä myötä pystyisivät lähettämään käskyjä ja tilannetietoa toisilleen. Kun herätyskello soi, lähettää laite käskyn kahvinkeittimelle aloittaa kahvin keittäminen. Tällä tavoin kaksi IoT-laitetta toimii täydellisessä yhteisvaikutuksessa. [3.] Mikä tekee IoT:stä merkittävän on sen skaalautuvuus, sillä kahvinkeittimen ja herätyskellon lisäksi muita laitteita olisi mahdollista lisätä samaan kommunikaatioverkostoon käyttäjän toiveiden mukaan.

Toisena esimerkkinä kuluttajien IoT-laitteista toimii vuoden 2016 syksyllä monille suomalaisille tutun kodinkone- ja elektroniikkaliike Siemensin lanseeraama Home Connect palvelu. Kyseisen palvelun avulla asiakas pystyy hallitsemaan kaikkia omistamiaan, Wi-Fi-verkkoon yhdistettyjä kodinkoneita etäyhteydellä. Home Connect sovelluksella on mahdollista siis hallinnoida useiden eri laitevalmistajien laitteita yhdellä sovelluksella. [4.]. Vaikka tällä hetkellä Home Connect palvelun tapaiset palvelut eivät vielä tule vakiona mukana kaikissa nykypäivän laitteissa ja kodinkoneissa, on tulevaisuudessa täysin mahdollista, että kaikki taloudessamme olevat kodinkoneet sekä elektroniikka ovat yhdistettynä internettiin ja täysin hallinnoitavissa etänä ja samanaikaisesti. Kuva 1 esittää Siemensin Home Connect Android sovellusta, millä useiden kodinkoneiden hallinta on helppoa ja nopeaa.



Kuva 1. Home Connect sovellus Androidille [5].

Kuten kaikella teknologialla myös IoT:llä on positiivisten ja innovatiivisten puolien lisäksi myös omat vaaransa. F-Securen tutkimusjohtaja Mikko Hyppönen piti vuonna 2014 Helsingissä järjestetyssä DigiExpo tapahtumassa puheen Internetin luomien online palvelujen laajentumisesta arkeemme sekä tämän laajentumisen mukanaan tuomista vaaroista. Sekä tuossa puheessa että toisessa, jo vuonna 2011 TEDx Talks:lle antamassaan esityksessä Hyppönen mainitsi Internetin suurimmiksi uhiksi sen yksityisyyden, internet sensuurin, cyber hyökkäykset sekä verkon kautta tapahtuvat rikokset [6]. Myös IoT on osaltaan avoinna väärinkäytöksille. Koska IoT:n peruspilarina toimii verkkoyhteys ja kommunikaatioprotokollat, niitä uhkaavat vaarat ovat samat kuin muissakin nykypäivän teknologioissa. Kaikkialla läsnä oleva IoT-teknologia antaa rajattomasti mahdollisuuksia väärinkäytöksille, oli kyseessä sitten palvelunestohyökkäys, kiusanteko tai haittaohjelmien levittäminen.

IoT:n haasteena on vuosien ajan ollut kehittää yhtenäinen toimintamalli laitteille ja laitteiden väliselle kommunikoinnille. Sensorit, kommunikaatioverkot ja context-aware processing teknologiat ovat olleet käytössä jo vuosia. IoT:n pyrkimyksenä on tuoda kaikki laitteet yhteen luoden yhtenäisen kommunikaatioverkon. Toiminnan on siis oltava luotettavaa eri

komponenttien välillä. Tämä on tuonut mukanaan omia haasteita siitä, kuinka laitteita tulisi käyttää ja palveluita suunnitella.

IoT on tullut jäädäkseen ja koska sen tulevaisuudessa on odotettavissa vahvaa laajentumista ja käytön yleistymistä, on tärkeää varautua sen mukanaan tuomiin vaaroihin. Tämän tutkimuksen tavoitteena on luoda katsaus IoT:n suurimpiin teknologiaryhmiin sekä esitellä niille tyypillisiä uhkia esimerkkitapausten avulla. Opinnäytetyö ei tule käsittelemään kaikkea IoT-teknologian soveltamisen muotoja sen jatkuvaluonteisen kehittymisen vuoksi, vaan opinnäytetyössä poimitaan esimerkkejä sekä yritysmaailmasta että kuluttajasektorista. Tarkoituksena on tarjota lukijalle perustason tietoa painottuen IoT-laitteiden tietoturvaan ja niihin kohdistuviin uhkiin.

Kokonaisuutena IoT:n arkkitehtuuri on monimutkainen, joten tämän tutkimuksen yhteydessä se on selitetty lyhyesti ja yksinkertaistaen, huomioiden opinnäytetyön luonteen. Tarkoituksena on lähinnä pyrkiä selventämään termi lukijalle siten, että opinnäytetyön esimerkit ja niiden tietoturvauhkat ovat helposti ymmärrettävissä kaiken tasoisille teknologian kuluttajille.

2 Opinnäytetyön rakenne, kysymys ja metodi

Aiemmin täysin fyysisessä maailmassa olleiden toimintojen siirtyessä virtuaaliseen maailmaan syntyy uusien toimintatapojen lisäksi myös täysin uudenlaisia uhkia. Tämän opinnäytetyön tavoitteena on selvittää, mitkä ovat IoT:n huomattavimmat teknologiaryhmät ja antaa käytännön esimerkkejä niille tyypillisistä haavoittuvuuksista. Mahdollisia turvaratkaisuja haavoittuvuuksille käydään läpi ja pohditaan, mutta niiden löytäminen ei ole tutkimuksen pääpainona.

Tämä opinnäytetyö kokonaisuutena sisältää viisi selkeää osiota. Opinnäytetyön alussa olevan johdannon (luku 1) sekä tutkimuskappaleen (luku 2) tehtävä on avata aihetta alustavasti mutta tarpeeksi opinnäytetyön aiheen ymmärtämiseksi. Varsinaisen katsauksen rakenne koostuu johdantoa ja opinnäytetyön rakennetta seuraavasta kahdesta osasta. Näistä ensimmäisessä osassa (luku 3) esitellään lyhyesti mutta kattavasti IoT:n historia, teknologiapohja sekä IoT:n tietoturvallisuus ja sen riskit. Toisessa osiossa (luku 4) perehdytään tarkemmin IoT-teknologioihin ja niiden lajitteluun yleisimpiin pääryhmiin. Pääryhmien yleisen esittelyn lisäksi osiossa keskitytään määrittelemään eri ryhmien suurimmat uhat. Jokaisesta ryhmästä nostetaan esiin ja perehdytään tarkemmin yhteen esimerkkitapaukseen jo tapahtuneesta todellisesta hyökkäyksestä. Opinnäytetyön viimeisessä osassa (luku 5) tutkimuksen tuottamat tulokset käydään läpi ja niiden merkitystä ja mittakaavaa IT- alalla pohditaan.

Teknologiaryhmät ja niiden haavoittuvuudet pyritään löytämään sekä alan teoriaa, että käytäntöä hyödyntäen ja ne esitellään tapausesimerkkien avulla. Lähdekirjallisuuden avulla kartoitetaan ensiksi IoT: iin liitettävät eri laitetyypit. Hypoteesini mukaan näiden laitetyyppien ryhmillä tulee olemaan yhdenmukaisia haavoittuvuuksia ja uhkia niiden samankaltaisuudesta johtuen. Tästä syystä uhkat ovat tehokkainta selventää ryhmäkohtaisten esimerkkitapausten avulla.

Hypoteesini on, että IoT:n huomattavimmat haavoittuvuudet jakautuvat fyysisiin ja tietoteknisiin uhkiin. Fyysisillä uhilla tarkoitetaan Internettiin kytkettyjen laitteiden väärin toimimisesta syntyviä ongelmia ja tietoteknisillä uhilla viitataan Internettiin yhdistettyjen laitteiden puutteellisesta suojauksesta syntyviin tietoturva-aukkoihin, joita esimerkiksi pahantahtoisten tahojen on mahdollista hyväksikäyttää.

Internet of Things laitteita ja ratkaisuja on lukemattomia ja tästä syystä tämä opinnäytetyö ei pyri yksilöimään jokaista IoT-laitetta, vaan tarkoitus on valita tarkasteltavaksi muutamia mielenkiintoisimpia ja ajankohtaisimpia teknologioita.

3 Historia

3.1 Internet of Things: lyhyt historia ja tulevaisuus

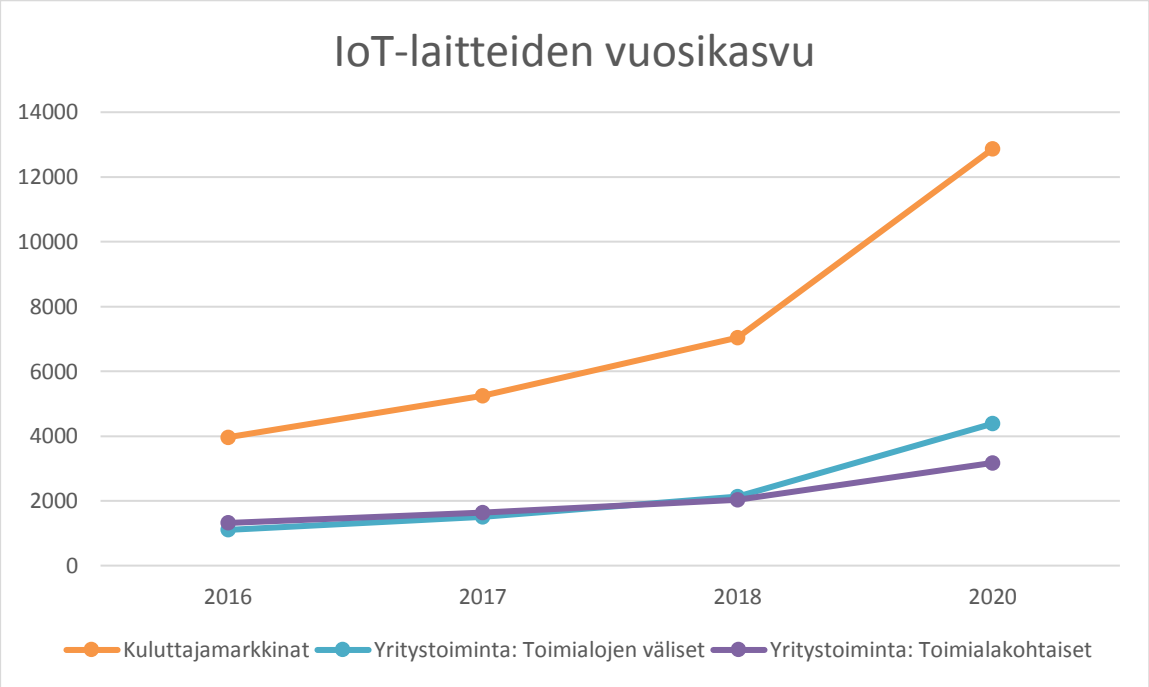
Internet of Things on muuttunut tunnetuksi teknologian termiksi vasta viime vuosien aikana, johtuen teknologian käyttöönoton räjähdysmäisestä kasvusta jokapäiväisissä laitteissa. Internet of Things- termiä käytti ensimmäisenä Kevin Ashton vuonna 1999 järjestämässään esitelmässä Procter & Gamblen toimitusketjun hallinnasta RFID teknologian avulla. RFID (Radio Frequency IDentification) on nimitys teknologialle, joilla voidaan yksilöidä kohteita radiotaajuuksien avulla. Tekniikkaa käytettäessä kohteen tuotesisältö tallentuu RFID tunnisteelle, josta se voidaan noutaa radioaaltojen avulla erillisellä lukijalla. Prosessiin liittyy yleensä myös jokin taustajärjestelmä, jolle tunnisteen tiedot siirtyvät. [7.]. Kyseistä teknologiaa pidetäänkin yleisesti asioiden internetin perustana.

RFID-teknologia on rinnastettavissa viivakoodeihin käyttökohteidensa puolesta. Näiden kahden tekniikan ero piilee lukukontaktissa. Viivakoodissa lukupään on havaittava luettava viivakoodi visuaalisesti, kun taas RFID-tunnistetta käytettäessä sitä ei vaadita, vaan tunniste luetaan ilmateitse. Toisin kuin viivakoodeissa, RFID-tunnisteen muokkaus on myös mahdollista jälkikäteen ja ne kestävät paremmin haastavammissa olosuhteissa. [7.]

RFID-termin alle kuuluu monta erilaista teknologiaa. Esimerkiksi tunnisteen lukuetäisyys ja tunnistamisnopeus vaihtelevat standardeittain. RFID-tekniikka on ollut teknisesti mahdollista jo vuosikymmeniä, ja sitä on hyödynnetty jo pitkään esimerkiksi kulkuavaimissa, matkakorteissa ja eläinten merkitsemisessä. Teknologiaa käytetään kasvavassa määrin teollisuudessa osana tuotannon tehostamista ja laadunvalvontaa sekä logistiikassa tavaravirtojen seuraamiseen. [8.]

IoT:n syntyyn vaikuttivat myös merkittävästi langattomat tiedonsiirtoteknologiat esimerkiksi Bluetooth ja Wireless Sensor Networks (WSN). Kyseisten teknologioiden yleistyminen johti niiden käyttöönottoon yhä laajemmassa skaalassa laitteita. Kyseisten teknologioiden kehitys toimi kehityspolkuna IoT-teknologialle. [1. s. 1.2.1., IoT emergence, 1.1.Introduction). IoT:n nykyinen kehitystaso on hyvin pitkälti juuri langattoman tiedonsiirtoteknologian aikaansaamaa.

Gartnerin teettämän tutkimuksen mukaan vuonna 2017 internetiin kytkettyjä laitteita tulee olemaan noin 8.4 miljardia kappaletta. Kyseinen luku tulee kasvamaan noin 30% vuositasoa ja vuoteen 2020 mennessä IoT-laitteita arvioidaan olevan yhteensä yli 20 miljardia. Kuva 2 esittää Gartnerin vuoden 2017 alussa laatiman arvion IoT-laitteiden käyttöönotosta maailmassa. Kuluttajamarkkinoihin lukeutuvat kaikki kuluttajille kohdistetut laitteet, kuten televisiot, älypuhelimet ja lähetinvastaanottimet. Kuluttajille kohdistetut IoT-laitteet kattavat noin 63% kokonaismäärästä IoT-laitteita vuonna 2017 ja määrä tulee kasvamaan tulevaisuudessa entisestään. Yritystoimintaan kohdistettuja IoT-laitteita, jotka ovat toimialoista riippumattomia ovat muun muassa valvontajärjestelmät, älyvalaistus ja LVI-tekniikat. Yritystoiminnan toimialakohtaiset IoT-laitteet kattavat muun muassa tehdasjärjestelmät ja terveydenhoitoon kohdistuneet teknologiat ja kaikki muu mikä on kohdistettua vain tietylle toimialalle. Kaaviosta on havaittavissa, että yritysmaailma ei tule olemaan IoT:n keskittynyt toimialue, vaan kaikista suurin osuus on kuluttajamarkkinoilla. Tästä syystä tämä opinnäytetyö tulee painottumaan tarkastelemaan kuluttajamarkkinoille kohdistettuja IoT-laitteita ja niiden tietoturvaa. [9.]



Kuva 2. IoT-laitteiden arvioitu vuosikasvu.

3.2 Internet of Things turvallisuus ja riskit lyhyesti

Koska IoT käyttää toimiakseen verkkoyhteyden vaativaa tiedonsiirtoteknologiaa, sitä ja siirrettävää tietoa uhkaavat matkalla monet vaarat. Mahdollisia uhkia siirrettävää tietoa koskien ovat esimerkiksi sen varastaminen, haavoittuminen tai tuhoutuminen. Varsinkin salaista, arkaluontoista tai arvokasta tietoa siirrettäessä on pystyttävä huolehtimaan siitä, ettei ulkopuoliset pääse käsiksi siirrettävään dataan. Tähän on ratkaisuksi tarjolla ainoastaan datan salaus olemassa olevilla salausalgoritmeilla ja tekniikoilla. Tämä ei kuitenkaan välttämättä tarjoa täyttä suojaa ulkopuolisilta, jos IoT-laitteessa on haavoittuvia komponentteja, joiden kautta haittaohjelma pystyy tunkeutumaan järjestelmään ja kaappaamaan siirrettävän datan ennen salausta.

4 Uhat aloittain

Vaikka IoT on teoriassa sovellettavissa lähes mihin tahansa teknologiaan, on sille kuitenkin käytännössä syntynyt muutamia suurempia käyttöaloja ja -tarkoituksia. Nämä ryhmät nousevat selvästi esiin alaan tutustuttaessa ja tässä tutkimuksessa esiteltävät pääryhmät ovatkin juuri nuo tärkeimmät alat.

IoT:n vaikutuksiin sen monilla käyttöaloilla pystytään parhaiten syventymään tapauskohtaisten esimerkkien avulla. Koska IoT on soveltuvuutensa ansiosta levinnyt laajalle, tässä tutkimuksessa tarkasteltavaksi on valittu esimerkkitapauksia sen yleisimmiltä ja tätä kautta eniten uhkia kohtaavilta käyttöaloilta. Alalukuihin järjestetyissä kappaleissa esitellään esimerkkitapaukset ja käydään läpi niihin kohdistuneet huomattavimmat uhkat. Esimerkit on valittu niin, että ne kuvastavat parhaiten ryhmälleen tyypillisiä asioiden internettiin kohdistuvia uhkia.

4.1 Ajoneuvot

Autoteollisuus on ottanut IoT:n ja uusimmat teknologiat vastaan erittäin nopeasti. Nykypäivänä lähes jokainen uusi auto on tavalla tai toisella kytkettynä internetiin. Autonvalmistajalla on mahdollisuus päivittää auton järjestelmiä sekä kerätä mahdollista järjestelmädataa auton toiminnasta. Uusilla IoT:n avaamilla mahdollisuuksilla ajoneuvoista pystytään esimerkiksi tekemään kauko-ohjattavia tai itsestään ajavia. Lisäämällä ajoneuvoihin uusia kommunikointiväyliä sekä teknologioita tuodaan myös mukaan riskejä, joiden kanssa IT-teollisuus on kamppaillut vuosikymmenten ajan.

Ajoneuvon järjestelmille suunnitellulla haittaohjelmalla voisi olla katastrofaalinen vaikutus ihmisten turvallisuuteen liikenteessä. Tästä syystä ennen kuin IoT-teknologiaa otetaan laajemmin käyttöön ajoneuvoissa, on varmistuttava siitä, että teollisuuden parhaat käytännöt otetaan huomioon jo järjestelmien ja ominaisuuksien suunnitteluvaiheessa. Jälkikäteen tehdyt järjestelmämuutokset voivat osoittautua haasteellisiksi, kalliiksi ja joissain tilanteissa mahdottomiksi. Teknologian näkökannalta olisi hyvin epätodennäköistä, ettei autoteollisuus omaksuisi IoT-teknologiaa osaksi vakiovarustuksia tulevaisuuden ajoneuvoissaan.

4.1.1 Esimerkkitapaus: Cherokee Uconnect ja siihen kohdistunut hyökkäys

Täydellisenä esimerkkinä IoT:n käytöstä ajoneuvoissa toimii Jeep-autovalmistajan Cherokee maastoauto ja sen internetiin kytketty Uconnect käyttöjärjestelmä. Uconnect käyttöjärjestelmän kautta on mahdollista hallita ajoneuvon viihde-elektroniikkaa, ajoneuvoon liitettyä älypuhelinta, navigointia, äänikomentoja sekä kojelaudan toimintoja. Tämän lisäksi järjestelmään on mahdollista ladata erillisiä applikaatioita ja toimintoja. [10.]

IoT laitteet ja ratkaisut ovat erittäin kiinnostava kohde hakkereille laitteiden lukumäärän ja mahdollisten tietoturvahaavoittuvuuksien vuoksi. Charlie Miller ja Chris Valasek onnistuivat murtautumaan Jeep Cherokeen CAN väylään (Controller Area Network) auton viihdejärjestelmän Uconnectin kautta. Hyökkäyksen aikana Charlie ja Chris kykenivät hallinnoimaan ajoneuvon eri toimintoja etänä kilometrien etäisyydeltä. Hallintaan ei vaadittu suoraa näköyhteyttä kohdeajoneuvoon. Järjestelmään murtautuneilla oli mahdollisuus hallita muun muassa ajoneuvon ilmastointia, radiota, pyyhkijöitä, polkimia, jarruja ja ratin toimintaa. [11.]

CAN väylää käytetään ajoneuvoissa tiedon välittämisestä eri moduuleille, kuten esimerkiksi vakionopeudensäätimelle tai nopeusmittarille. CAN-väylässä komennot ja käskyt välittyvät kaikille ajoneuvon moduuleilla ja moduuli toteuttaa itsenäisesti päätöksen siitä onko kyseinen data kohdistettu moduulille itselleen kohdistettua vai ei. CAN-väylän toimintaa voidaankin kuvailla vastaavan vanhaa HUB:ia verkkoteknologiassa, jossa tieto replikoidaan kaikkiin HUB:in portteihin ja päätelaite reagoi vain sille kohdistettuihin Ethernet-kehyksiin. [11.]. CAN väylän hyväksikäyttö hyökkäyksessä kuvastaa hyvin sellaisen teknologian haasteellisuutta, jossa yhden uuden komponentin (tässä tapauksessa uconnect) yhdistäminen olemassa olevaan teknologiaan ei suoraan ole turvallista. Järjestelmä olisi syytä toteuttaa modulaarisesti, jolloin jokainen oma moduulinsa toimii itsenäisesti vaarantamatta muiden moduulien toimintaa.

Historiassa ajoneuvojen CAN väylän murtaminen on onnistunut vain suoralla kaapeliyhteydellä tai bluetooth yhteyden välityksellä, eli toisin sanoen hyökkääjän on oltava auton välittömässä läheisyydessä. Bluetooth pystyy toimimaan kymmenien metrien etäisyydeltä, mutta jatkuvaluonteinen yhteys liikkuvaan ajoneuvoon olisi erittäin haastavaa kyseisen protokollan avulla. Internet of Things on kuitenkin tuonut merkittävän edun hyökkääjälle: hyökkäys voidaan toteuttaa täysin etänä. Tämä tekee hyökkäyksestä entistäkin vaarallisemman sekä antaa hyökkääjälle mahdollisuuden suojata selustansa viranomaisilta. Etänä toteutettu hyökkäys helpottaa myös hyökkääjän kykyä peittää omat jälkensä hyökkäyksen jälkeen, mikä tekee jälkiselvityksestä entistäkin vaikeampaa.

Charlie Millerin ja Chris Valasekin kohdistama etähyökkäys kohdistui järjestelmän nollapäivähaavoittuvuuteen (A Zero-Day vulnerability), mikä käytännössä tarkoittaa sitä, että hyökkäys toteutettiin välittömästi haavoittuvuuden löydyttyä. Nollapäivähaavoittuvuudet ovat tietoturvan kannalta merkittäviä siitä syystä, ettei kyseiseen haavoittuvuuteen ole tarjolla päivitystä tai suojakeinoa. [12]. Useat nollapäivähaavoittuvuudet kohdistuvat käyttöjärjestelmien tai ohjelmistojen haavoittuvuuksiin, joilla ei ole suoranaista vaikutusta ihmishenkiin ja näiden hyökkäysten pyrkimyksenä on usein levittää haittaohjelmia muihin ympäristön palvelimiin/työasemiin. Charlie Millerin ja Chris Valasekin havaitsema haavoittuvuus kuitenkin mahdollistaisi laajamittaisen liikenneonnettomuuden, milloin tahansa ja missä tahansa osassa maailmaa. [11].

Nollapäivähaavoittuvuudet IoT-laitteissa on valtava uhka, sillä hyökkäys on voinut tehdä valtavan määrän tuhoa ennen kuin haavoittuvuudet on saatu paikattua. Joissain heikommin suunnitelluissa IoT-laitteissa ei ole tarjolla OTA firmware (Over-The-Air) päivitystä, jolla haavoittuvuus on mahdollista paikata. Tämä johtuu usein IoT-laitteiden erittäin lyhyestä elinkaaresta.

Charlie Millerin ja Chris Valasekin hyökkäys toimii täydellisenä esimerkkinä siitä, miksi IoT-järjestelmien käyttöönotossa on otettava erityisesti huomioon järjestelmän tietoturva ja hyökkäyksiltä suojautuminen. Järjestelmät eivät saisi olla suorassa yhteydessä toisiinsa, mikä mahdollistaisi koko järjestelmän saastuttamisen yhden haavoittuvan moduulin kautta. Mahdollinen moduulien välinen kommunikaatio olisi syytä myös rajoittaa niin, ettei saastunut komponentti pysty komentamaan toista moduulia. Turvautumista vastaavilta hyökkäyksiltä hankaloittaa CAN-väylän rajoitteet, sillä kyseinen teknologia on ollut käytössä jo useiden vuosien ajan.

Mikä tekee Jeepin Cherokee- auton murtamisesta merkittävän on se, että kyseinen auto on myynnissä ja vastaava hyökkäys olisi voinut tapahtua suuremmalle käyttäjäryhmälle. Hyökkäyksellä olisi ollut katastrofaalinen vaikutus eikä kuolemilta olisi mitä todennäköisimmin voitu välttyä. Vaikka Jeep on paikannut haavoittuvuuden ei se siltikään tarkoita sitä, ettei järjestelmässä olisi jäljellä haavoittuvuutta mitä voitaisiin käyttää vastaaviin hyökkäyksiin tulevaisuudessa.

4.2 Kodinkoneet ja elektroniikka

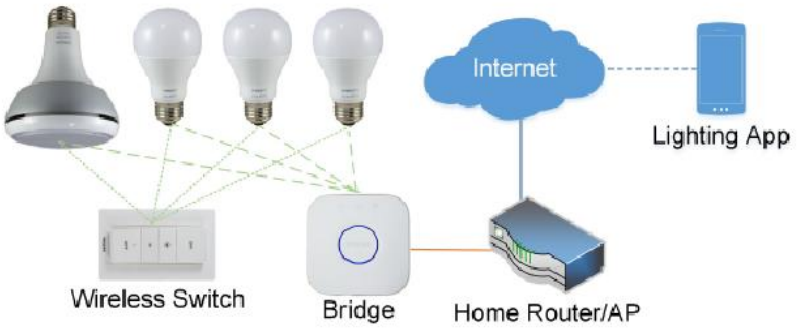
Yksi suurimmista IoT:n tuomista mahdollisuuksista hyötynyt ryhmä on kodinkoneet. Kodin automatiikka on nostanut IoT-laitteiden käyttömahdollisuuksia, eivätkä hyökkäykset tästä johtuen enää keskity ainoastaan valvontakameroihin tai reitittimiin, vaan mikä tahansa internetiin tai laajempaan verkkoon kytketty laite on nyt potentiaalinen uhri hyökkäykselle.

4.2.1 Esimerkkitapaus: Philips Hue älyvalo

Yhtenä hieman poikkeuksellisena IoT-laitteena voidaan pitää Philipsin lanseeraamaa Hue-älyvaloa. Uuden valon ideana on tarjota käyttäjälle mahdollisuus hallita laitteella muun muassa sen väriä, kirkkautta sekä tarjota mahdollisuuden asettaa erilaisia valoprofiileja. Valojen hallinta onnistuu etänä laitteelle suunnitellun älypuhelinsovelluksen avulla. Kaikki tämä voi kuulostaa kuluttajalle houkuttelevalta, mutta todellisuudessa Hue-älyvalo lukeutuu IoT-laitteeksi, mihin kohdistuvat samat tietoturvauhat kuin muihinkin vastaaviin internetiin kytkettyihin laitteisiin. Tavallinen kuluttaja ei välttämättä kiinnitä huomiota hankkimansa laitteen mahdollisiin riskeihin, vaan keskittyy pääsääntöisesti vain uusien ominaisuuksien tarkasteluun.

Philipsin Hue-älyvalon avulla kuluttajalla on mahdollisuus hallinnoida koko asuntonsa valaistusta yhdestä paikasta käsin. Älyvaloilla pystyy tuottamaan 16 miljoonaa eri sävyistä valoa, synkronoimaan valot reagoimaan musiikin tahtiin sekä ajastaa valaistusta haluamalleen ajankohdalle. Valoja hallitaan keskitetyn sillan (eng. Bridge) kautta minkä kapasiteetti on 50 älyvalolle ja 10 lisävarusteelle. Silta toimii 2400-2483,5 MHz taajuuskaistalla, eli se toimii tavallisessa 2,4GHz langattomassa verkossa aivan kuten muutkin WLAN verkot. [13.]

Useat IoT-laitteet ovat valinneet Zigbee protokollan laitteiden väliseen kommunikaatioon sen yksinkertaisuuden, yhteensopivuuden, alhaisen hinnan, alhaisen virrankulutuksen ja hallintaetäisyyden takia. Philipsin Hue älyvalo ei ole tähän poikkeus. Yksi suurimmista elektroniikan alan yrityksistä on ottanut käyttöönsä Zigbeen teknologian omissa IoT-laitteissaan, mukaanlukien Hue-älyvalossa. [14. s. 1]



Kuva 3. Hue älyvalo [14, s. 4]

Philipsin Hue-älyvaloon kohdistunut haavoittuvuus ja hyökkäys poikkeavat muista IoT-laitteisiin kohdistuneista tietomurroista. Tietoturva-asiantuntijat Kanadassa ja Isrealissa ovat kyenneet hakkeroimaan Philipsin älyvalot etänä käyttäen lennokkia. Hyökkäys pohjautui ZigBee Light Link Touchlink järjestelmässä löytyvään haavoittuvuuteen, jonka avulla hyökkääjät kykenivät morsettamaan älyvaloilla S-O-S hätämerkkiä.

Hyökkäys oli mahdollista toteuttaa yli 300m etäisyydeltä asentaen muokatun firmwaren laitteille ja estäen järjestelmän päivitysmahdollisuuden tulevaisuudessa. Tämä tarkoittaa myös sitä, ettei haitallista firmwarea ole mahdollista poistaa kyseisiltä laitteilta tulevaisuudessa. Saastuneiden laitteiden korjaus olisi mahdollista vain laitteiden takaisinvetämisellä ja korvaamisella päivitetyllä laitteella.

Vaikka yllä oleva hyökkäys älyvaloihin voi kuulostaa lähinnä vain kiusanteolta, voi sillä olla henkeä vaarantava vaikutus epileptikoille. Saastuneen älyvalon avulla tunkeutuja kykenisi myös saastuttamaan verkon muita laitteita. Yritysmaailmassa tämä voisi tarkoittaa sitä, että tunkeutuja pääsee käsiksi suojattuihin palvelimiin ja päätelaitteisiin käyttäen älyvaloja terminointipisteenä hyökkäykselle. Mikä tekee hyökkäyksestä normaalia vaarallisemman on se, että hyökkäys olisi mahdollista toteuttaa etänä käyttäen lennokkia. [15.]

Hyökkäys pohjautuu kahteen erilliseen hyökkäysmalliin. Näistä ensimmäinen A Correlation Power Analysis (CPA), jonka avulla hyökkääjä kykenee salaamaan, allekirjoittamaan ja lähettämään haitallisia firmware-päivityksiä laitteille OTA-päivitysten (Over-the-Air) avulla. CPA:n yhdistäminen A Takeover Attack:iin mahdollistaisi keinon hyökkääjälle hallinnoida älyvaloja pitkien välimatkojen päästä ilman kustomoitua laitteistoa.

Kyseisiä hyökkäysmalleja kohdistettiin ZigBee Light Link Touchlinkissä löytyvään haavoittuvuuteen, minkä avulla mato pystyy replikoitumaan IoT-laitteiden välillä langattomasti

käyttäen ZigBee:n kommunikointiprotokollaa. ZigBee:n laitteistossa olevan laitebugin takia on mahdollista nollata kohdelaite tehdasasetuksille jopa 400 metrin etäisyydeltä käyttäen standardin mukaista ZigBeen lähetintä. Tehdasasetusten jälkeen kohteelle on mahdollista lähettää lisää komentoja, mitkä mahdollistavat laitteen täydellisen hallinnan. [14. s. 2]

Hue-älyvalolle suunniteltu mato kykenee leviämään viereisiin laitteisiin, mikä tarkoittaa eksponentiaalista, räjähdysmäistä kasvua saastuneissa laitteissa hyvin lyhyessä ajassa. Hyökkäykseen riittää vain yksi saastunut lamppu, johon mato on saatu istutettua. Mato aloittaa itsensä replikoimisen viereisiin valoihin, joista se leviää yhä laajemmalle alueelle. Asiantuntijoiden mukaan hyvin suunnitellulla hyökkäyksellä on mahdollista hallita kauppakeskuksen suuruisen alueen älyvaloja minuuteissa. [15.]

Philipsin älyvalo on kuitenkin mahdollista palauttaa entiseen tilaansa viemällä valo hallintapaneelin (silta) läheisyyteen, jolloin hallinta laitteelle palautuu ennalleen. [14. s. 2] Tämä olisi kuitenkin mahdollista ohittaa estämällä laitteistopäivitykset saastuneessa koodissa, jolloin laitetta ei ole mahdollista palauttaa entiseen tilaan ja se on pahimmassa tapauksessa vaihdettava uuteen laitteeseen.

Tästä syystä älyvalojen hallinnalla ei ole välttämättä suurta hyötyä itse hyökkääjälle, mutta mahdollisuus käyttää älyvaloa DDoS hyökkäyksissä voi osoittautua suureksi vaaraksi eri verkkopalveluille. Saastuneita älyvaloja olisi myös mahdollista käyttää muiden Zigbee protokollaa käyttävien IoT-laitteiden hallintaan.

4.2.2 Tulevaisuus

Philips Hue-älyvalo on täydellinen esimerkki siitä, kuinka harmittomalta vaikuttava kuluttajatuote voi osoittautua suureksi vaaraksi kuluttajan terveydelle ja turvallisuudelle. Epileptikolle onnistunut hyökkäys voi osoittautua kohtalokkaaksi. Räjähdysmäinen leviäminen älylaitteiden välillä viestittää myös siitä, kuinka haastavaa on suojautua kohdistettuilta IoT-hyökkäyksiltä.

Philipsin Hue älyvalon käyttäessä laajasti käytettyä Zigbee protokollaa, mahdollistaisi se myös muiden IoT-laitteiden saastuttamisen samalla alueella, mikä tekisi hyökkäyksen estämisestä ja lieventämisestä lähes mahdotonta.

4.2.3 Vizio

IoT:n monikäyttöisyys tulee esiin kodin elektroniikassa. Nykypäivänä lähes kaikki kodinkoneet on mahdollista liittää internetiin ja tällä tavoin lisätä niiden käyttömahdollisuuksia ja ominaisuuksia. Kuten koko tämän opinnäytetyön aikana on todettu, ei IoT ole ongelmaton tietoturvan näkökannalta. Laitteisiin on mahdollista asentaa haittaohjelmia, joilla on mahdollista estää laitteen toiminta tai häiritä muiden laitteiden toimintaa. Älytelevisioissa on kuitenkin mahdollista, että haittaohjelma tai epäilyttävä toiminta on lähtöisin laitevalmistajan asentamasta toiminnosta, mikä käyttää hyväksi IoT-teknologiaa.

Televisiovalmistaja Vizio ei ehkä ole Suomen markkinoilla tunnettu televisiomerkki, mutta esimerkiksi USA:ssa valmistajalla on selvä jalansija kuluttajamarkkinoilla. Vuodesta 2010 lähtien Vizio on myynyt yli 11 miljoonaa älytelevisiota. Saatuaan merkittävän markkinaosuuden älytelevisioiden myynnistä, on Vizio tehnyt muutoksia älytelevisioihin vuodesta 2014 lähtien. Muutosten myötä laitevalmistaja on asennuttanut älytelevisioihin erillisen toiminnon, minkä avulla Vizio voi seurata kuluttajien television katsomistottumuksia. Koska älytelevisiot lukeutuvat IoT:n piiriin on älytelevisioilla mahdollisuus kommunikoida internetin avulla. Kyseisen keinon avulla Vizio onnistui keräämään kuluttajien dataa omille palvelimilleen. Vizio myös onnistui asentamaan kyseisen toiminnallisuuden myös vanhempiin älytelevisioihin jälkiasennuksena järjestelmäpäivitysten muodossa. [16.]

Data kerättiin analysoimalla valikoituja pikselialueita ruudulta ja vertailemalla kerättyä dataa omista tietokannoista löytyvään dataan. Tällä tavoin Vizio pystyi kartoittamaan kuluttajien katsomistottumuksia erittäin tarkasti. Datan määrä oli valtava, ja tiettyjen lähteiden mukaan kerättyjä pikselialueita eli ns. datapisteitä olisi kerätty miljardeja kertoja vuorokaudessa myydyiltä älytelevisioilta. Mikä tekee datan keräämiseen suunnittelun toiminnallisuudesta monin kerroin vaarallisemman on se, että dataa pystyttiin keräämään myös DVD/Bluray-soittimista, suoratoistolaitteista, laajakaistapalveluista sekä kaapeliboxeista (eng. Set-top box, STU) mitkä olivat kytkettyinä Vizion älytelevisioon. Kaikki tämä oli toteutettu kertomatta siitä kuluttajalle riittävällä tasolla. [16.]

Myöhemmin Vizio myi kaiken keräämän kuluttajadatan kolmansille osapuolille, pääsääntöisesti mainostajille. Kyseessä ollut data ei kuitenkaan ollut vain yleisdataa katsojaluvuista, vaan Vizio myi kolmansille osapuolille käyttäjien IP-osoitteen (Internet Protocol Address). Kolmannet osapuolet kykenivät löytämään IP-osoitteiden avulla yksityisen kuluttajan tai talouden, mutta kuluttajien ja talouden nimeä ei ollut luvallista selvittää kerätystä datasta. Kuluttajasta saatiin kuitenkin paljon muuta tietoa selville, kuten esimerkiksi

sukupuoli, ikä, siviilisääty, kotitalouden koko ja omistajuus sekä kuluttajan koulutustaso. [16.]

Kaikki tämä eskaloitui alkuvuodesta 2017 kun Vizio määrättiin maksamaan 2.2 miljoonaa dollaria Federal Trade Commissionille (FTC) ja poistamaan kaikki kerätty data ennen 1.3.2017.

4.2.4 Pohdinta

Älytelevisiot ovat muuttaneet perinteisen television toiminnan ja lisänneet lisäominaisuuksia normaalin television katselun rinnalle. Nykypäivän televisioissa on erillinen käyttöjärjestelmä, mistä löytyy eri sovelluksia esimerkiksi suoratoistopalveluihin kuten Youtube, HBO, Netflix ja Cmore. Tämän lisäksi joissain televisioissa on verkkoselain sekä muita käytännöllisiä sovelluksia, mitkä entisestään laajentavat käyttökokemusta.

Kuluttajat eivät kuitenkaan pysty suojautumaan vakoilulta, jos se tapahtuu laitevalmistajan taholta. Kuluttajien on luotettava laitevalmistajaan siinä, ettei heidän television käyttämistään seurata tai yksityisyyttä muulla tavoin loukata. Jos laitevalmistaja päättää kerätä asiakkaiden dataa on siitä mainittava selkeästi käyttöehdoissa. Mikä tekee Vizion tapauksesta merkittävän on se, että kyseessä on tunnettu laitevalmistaja jolla on vuosikymmenien kokemus alalla. Kuluttajan ostaessa tuotteen tunnetulta laitevalmistajalta yksityisyyden kunnioittamista voidaan pitää ominaisarvona.

4.3 Verkkohyökkäykset

IoT-laitteille on kehitetty lukuisia haittaohjelmia, mutta eräästä haittaohjelmasta tuli maailmankuulu yhden vuorokauden sisällä. 21 lokakuuta 2016 Mirai-bottiverkon hyökkäys aiheutti palvelukatkoksen valtavalle määrälle verkkosivuja, joita käyttivät miljoonat ihmiset ympäri maailmaa. Asiantuntijat kuitenkin spekuloivat, että vaikka kyseessä oli laajamittaisin hyökkäys IoT:n ja jopa Internetin historiassa on tämä vasta alkusoittoa tulevalle. Osa asiantuntijoista myös arvelee, että kyseessä oli vain testi Mirain potentiaalista ja todellinen hyökkäys on vasta tulossa.

4.3.1 Esimerkkitapaus: Mirai

Mirai-haittaohjelman toimintaperiaate jakautuu kahteen osaan: haittaohjelman levitykseen ja verkkohyökkäyksiin. Mirain toimintamalli ei eroa perinteisistä bottiverkoista vaan haittaohjelman toiminta keskittyy uhrikoneisiin ja uhrikoneita hallinnoiviin noodeihin. Uhrikoneita kutsutaan usein myös nimellä ”zombi” ja hallintanoodeja ”bottipaimeniksi” tai ”bottimastereiksi” [17.].

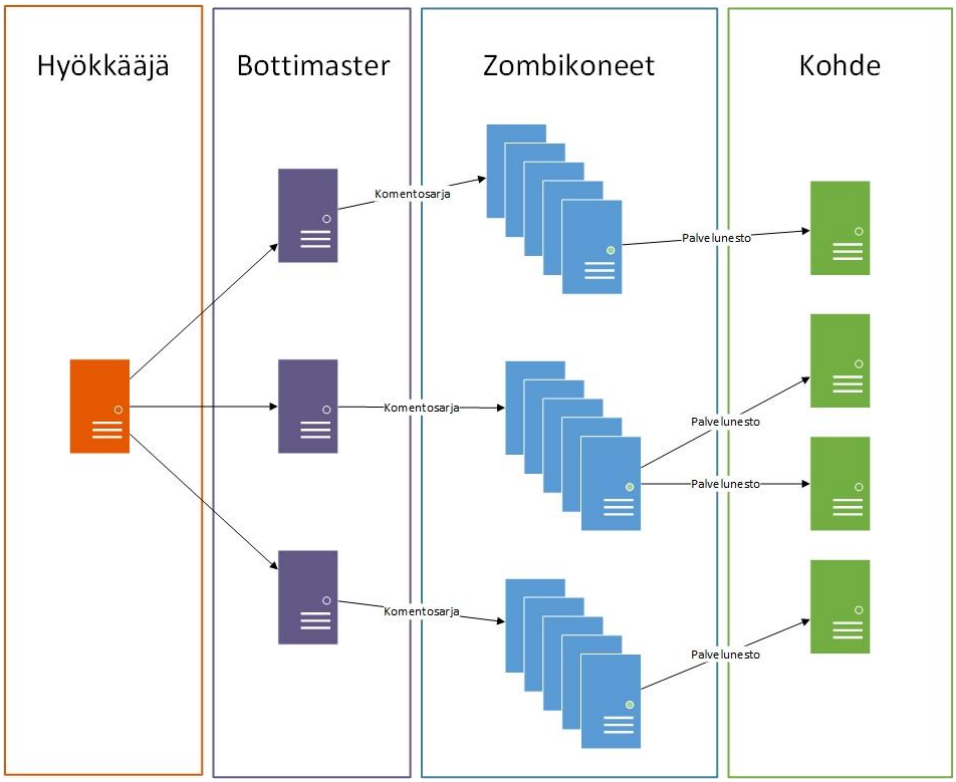
Mirai-haittaohjelman kohteena toimivat Internet of Things-laitteet, jotka ovat suorassa yhteydessä internetiin. Näitä laitteita ovat muun muassa web-kamerat, CCTV (Closed-circuit television) kamerat, DVR:t (Digital Video Recorder) sekä reitittimet. Saastuttaakseen kyseiset IoT-laitteet Mirai-haittaohjelma pyrkii kirjautumaan laitteille heikon käyttäjätunnus ja salasana- yhdistelmän turvin. Hyvin useat laitevalmistajat käyttävät verkkoon kytketyissä laitteissa vakiosalasanaa ja tunnusta. Vakiosalasanan asettaminen verkkolaitteeseen ei ole itsessään ongelma, mutta silloin, kun käyttäjää ei vaadita vaihtamaan salasanaa ennen laitteen käyttöönottoa tekee IoT-laitteesta täydellisen kohteen niin Mirai-haittaohjelmalle kuin myös muille vastaaville haittaohjelmille. Laitteelle murtautuminen tapahtuu perinteisen sanakirjahyökkäyksen (eng. Dictionary attack) avulla, jossa hyökkääjä käy läpi listan potentiaalisista salasana/tunnus yhdistelmistä. Hyökkäyksen tekniikkana käytettiin väsytyshyökkäystä tai raakahyökkäystä (Brute Forcea). Väsytyshyökkäyksessä hyökkäystä ei pysäytetä epäonnistuneeseen yritykseen vaan toimintaa jatketaan niin kauan, kunnes järjestelmään päästään käsiksi tai salasana/käyttäjätunnus yhdistelmät loppuvat sanakirjatiedostosta. Jos mikään tunnus ei toimi kyseiselle laitteelle aloitetaan sama hyökkäys toisella kohteella. [18.] Mikä tekee Mirai-haittaohjelmasta mielenkiintoisen, on sen käyttämä sanakirjatiedoston pituus. Usein sanakirjahyökkäyksessä käytetään

tuhansia, ellei jopa miljoonia rivejä tunnuksia sisältäviä tiedostoja, mutta Imperva Capsulan tutkijoiden mukaan Mirai käytti ainoastaan 44 salasana/tunnusriviä. Tämä myös viittaa siihen, että Mirain kehittäjällä/kehittäjillä on ollut tarkka kuva siitä, minkä luokan laitteet halutaan tartuttaa.

Suurin osa internetiin kytketyistä työasemista on suojattu jollain tasolla haittaohjelmia vastaan, oli kyseessä sitten käyttöjärjestelmän oma tietoturvaohjelmisto tai kolmannen osapuolen ratkaisu. Tästä syystä useat bottitartunnat havaitaan työasemilta nopeasti, mikä tekee työasemien käyttämisestä uhrikoneena haastavampaa. Tämän lisäksi on mahdollista, että käyttäjä sammuttaa työasemansa työpäivän päätteeksi, mikä laskee potentiaalisen hyökkäyksen hyökkäysikkunaa.

Mirain kaltaiseen DDoS hyökkäykseen päätelaitteelta ei vaadita valtavaa laskentatehoa tai kapasiteettia. IoT-laitteet ovat täydellinen kohde DDoS-hyökkäyksen aiheuttajiksi, sillä kyseisten laitteiden perustana on aina ollut niiden huomaamattomuus, helppous ja ympärivuorokautinen toiminta. Erittäin harva käyttäjä sammuttaa IoT-laitettaan esimerkiksi työpäivän päätteeksi tai nukkumaan mennessään, mikä antaa entistä enemmän aikaa ja vapautta haittaohjelmalle toimia. Kaikkialla läsnä oleva (eng. Ubiquitous) teknologia mahdollistaa maailmanlaajuisten verkkohyökkäysten toteuttamisen vaivattomasti. Mirai-haittaohjelmaa on tämän lisäksi hankalaa havaita, sillä se ei vaikuta laitteen normaaliin toimintaan.

Mirain toiminta keskittyy hajautettuun palvelunestohyökkäykseen (lyh. DDoS) minkä päämääränä on nimensä mukaisesti estää kohdepalvelun toiminta. Palvelun toiminta saadaan pysäytettyä pommittamalla palvelinta niin valtavalla määrällä kyselyitä, ettei palvelin tai kuormantasaajat kykene suoriutumaan niistä aiheuttaen palvelun hitautta ja palvelukatkoja. Pilvipalveluiden elastisuus ei myöskään pysty reagoimaan lyhyen aikajakson sisällä tuleviin kyselyihin, vaikka palvelinten määrää kasvatettaisiin hyökkäyksen aikana. Sillä välin, kun palvelin lähettää vastauksia sekä Mirain bottiverkon kyselyihin, että normaalien käyttäjien kyselyihin palvelun toiminta on hidastunut normaaliin verrattuna huomattavasti. Riittävä rasitus palvelimeen voi aiheuttaa sen kaatumisen ja palvelun totaalisen pysähtymisen. Kuva 4 esittää DDoS hyökkäyksen perustoimintaa ja sen vaikutusta palveluun. Bottiverkossa hyökkääjä hallinnoi bottimastereita, joiden alaisuudessa toimivat kaikki bottiverkon orjakoneet (zombi). Orjakoneet toteuttavat lopullisen hyökkäyksen lopulliselle kohteelle.



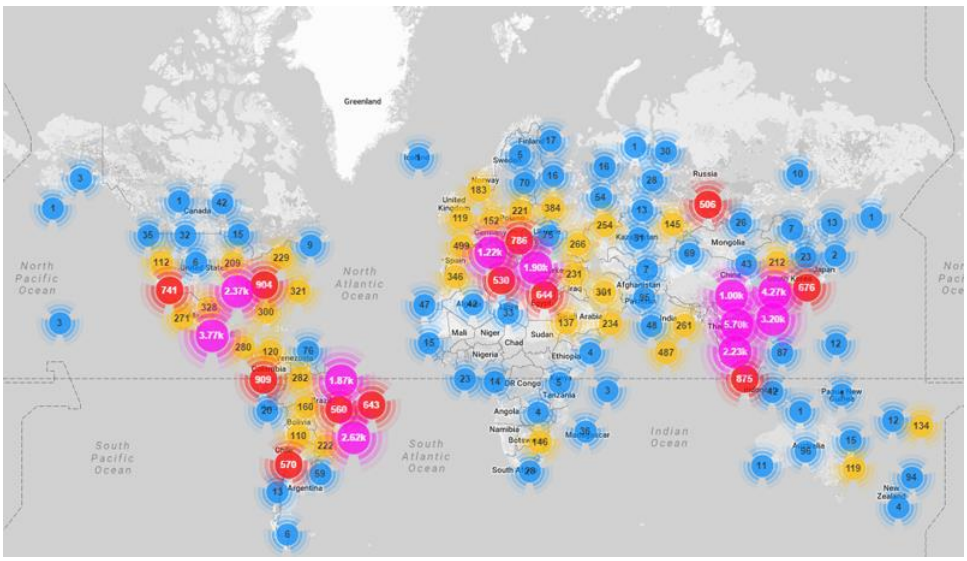
Kuva 4. Bottiverkon kautta tapahtuva DDoS hyökkäys.

Mikä tekee hajautetusta palvelunestohyökkäyksestä haastavan on se, ettei hyökkääjän pyyntöjä ole helppo erottaa normaalin käyttäjän lähettämistä pyynnöistä. Tästä syystä pyyntöjä on haastavaa erotella toisistaan ja hyödyntää filteröintiä. [19.]

Vuoden 2016 todennäköisesti merkittävimpänä tapahtumana tietoturvan saralla on Mirai-haittaohjelman keskitetty verkkohyökkäys amerikkalaiseen Dyn-verkkopalveluun. Dyn tarjoaa nimipalveluita (DNS) merkittäville verkkopalveluille kuten esimerkiksi Amazon, BBC, Box, GitHub, PayPal, Spotify ja Twitter. Ilman toimivaa DNS-palvelua normaalin internetin toiminnassa on havaittavissa selviä katkoksia. DNS (Domain Name System) huolehtii verkkopalvelinten IP-osoitteiden muuntamisesta verkko-osoitteeksi (www.google.com). Ilman nimipalvelua verkkosivulle on mahdollista päästä ainoastaan IP-osoitteen avulla. Tämä tosin aiheuttaa ongelmia SSL-varmenteiden tunnistamisessa ja verkkosivu ei välttämättä toimi oikein. Tästä syystä DNS-palvelut ovat internetin tärkeimpiä palveluita, ja tämän takia myös hyökkäysten pääsääntöisenä kohteena.

Kuten aiemmassa kappaleessa totesimme, IoT-laitteet mahdollistavat verkkohyökkäyksen toteuttamisen aikavyöhykkeestä välittämättä. Tämä on nähtävissä Mirai-bottiverkon hyökkäyksessä käytettyjen zombi-koneiden kartasta (kuva 5). Jos kyseessä olisivat olleet

normaalit työasemat, olisi hyökkäys todennäköisesti keskittynyt vain niihin alueisiin, joissa saastuneita laitteita on kytkettynä verkkoon.



Kuva 5. Mirai-verkkohyökkäyksessä käytettyjä bottiverkon zombi-koneita [18].

Mirai-haittaohjelman tulevaisuus jää nähtäväksi. Haittaohjelman lähdekoodi löytyy vapaasti ladattavissa internetistä mikä varmasti aiheuttaa Mirain haarautumisen yhä monipuolisimpiin ja kehittyneempiin haittaohjelmiin. Jos spekulaatiot laajamittaisemmasta hyökkäyksestä pitävät paikkansa, tulee tietoturva olemaan yhä merkittävämmässä roolissa nykyisiä IT-alan yrityksiä ja palveluita.

Tulevaisuuden kannalta IoT-laitteiden valmistajien olisi otettava erityisesti huomioon laitteen tietoturva ja huolehtia laitteiden firmware-päivityksistä. Valitettavasti useissa IoT-laitteissa ei ole otettu tietoturvaa lainkaan huomioon eikä firmware-päivityksiä ole mahdollista asentaa kyseiselle laitteelle verkon yli. Kyseiset laitteet tulevatkin olemaan todennäköisesti mukana tulevaisuuden verkkohyökkäyksissä niin pitkään, kunnes kuluttaja lopettaa laitteen käytön.

4.3.2 BrickerBot Vigilante Botnet

Mirai-bottiverkko on täydellinen esimerkki siitä, miten vaarallisia hallitsemattomat IoT-laitteet pystyvät olemaan. IoT-laitteiden päämääränä on usein kuluttajaystävällinen käyttöönotto ja käytön helppous. Tämä yhdistettynä heikkoon suojaukseen voi johtaa katastrofiin.

Tarkoin keskitetyt ja suunnitellut hyökkäykset voivat aiheuttaa pitkäaikaisia katkoksia palveluissa joita miljoonat ihmiset käyttävät päivittäin. Osa bottiverkoista ei kuitenkaan pyri tekemään haittaa suurille palveluntarjoajille tai yksittäisille palvelimille. Tästä hyvänä esimerkkinä on Mirai-bottiverkon innoittamana kehitetty BrickerBot. Kyseisen bottiverkon pyrkimyksenä on muuttaa internetin käyttö hieman turvallisemmaksi heikosti suojatuista IoT-laitteista. Toimintatapa ei tosin vastaa kuluttajien kannalta ideaalia ratkaisua, sillä pyrkimyksenä on tuhota laitteet etänä ja aiheuttaa niiden toiminnalle pysyvää vahinkoa [20].

BrickerBot:in päämääränä on nimensä mukaisesti etsiä ja tuhota heikosti suojattuja IoT-laitteita. BrickerBot tarttuu kohdelaitteeseen avoimen telnet portin ja tehdasasetettujen käyttäjätunnusten ja salasanojen turvin. BrickerBotin toimintatapa on äärimmäisen yksinkertainen, sillä sen pyrkimyksenä on vain tehdä haavoittuvista IoT-laitteista käyttökelvottomia tuhoamalla laitteen tallennusmedian. Kyseistä hyökkäystä kutsutaan PDoS hyökkäykseksi (eng. Permanent Denial of Service), eli pysyväksi palvelunestohyökkäykseksi. BrickerBot ajaa listan erittäin tehokkaita komentoja, millä on pysyvät vaikutukset laitteen toimintaan. BrickerBotin aiheuttaman tuhon jälkeen osaa laitteista ei voi palauttaa toimintakelpoiseksi edes tehdasasetusten palauttamisella. [20.] Tuhoamalla IoT-laitteen järjestelmätiedostot ja palautusmahdollisuuden pakottaa BrickerBot kuluttajan palauttamaan laitteen takaisin valmistajalle tai hankkimaan uuden, toivomuksen mukaan paremmin suojatun IoT-laitteen.

BrickerBotin kehittäjä, Hackerforum-verkkosivuilla nimellä Janit0r esiintynyt henkilö on seurannut IoT-aikakauden kehitystä ja Mirai-bottiverkon aiheuttamat tuhot ja haitat vuoden 2016 loppupuolella saivat kehittäjän luomaan omanlaisensa haittaohjelman, minkä pyrkimyksenä on kitkeä haavoittuvaiset ja tehdasasetetuilla salasanoilla varustetut IoT-laitteet pois käytöstä. Tavoitteena on vähentää tulevaisuuden Mirai-bottiverkkohyökkäyksiä samalla pienentäen haittaohjelmien hyökkäyspinta-alaa [21].

```
1  busybox cat /dev/urandom >/dev/mtdblock0 &
2  busybox cat /dev/urandom >/dev/sda &
3  busybox cat /dev/urandom >/dev/mtdblock10 &
4  busybox cat /dev/urandom >/dev/mmc0 &
5  busybox cat /dev/urandom >/dev/sdb &
6  busybox cat /dev/urandom >/dev/ram0 &
7  busybox cat /dev/urandom >/dev/mtd0 &
8  busybox cat /dev/urandom >/dev/mtd1 &
9  busybox cat /dev/urandom >/dev/mtdblock1 &
10 busybox cat /dev/urandom >/dev/mtdblock2 &
11 busybox cat /dev/urandom >/dev/mtdblock3 &
12 fdisk -C 1 -H 1 -S 1 /dev/mtd0
13 w
14 fdisk -C 1 -H 1 -S 1 /dev/mtd1
15 w
16 fdisk -C 1 -H 1 -S 1 /dev/sda
17 w
18 fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
19 w
20 route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
21 sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
22 halt -n -f
23 reboot
```

Kuva 6. Bricker Botin kolmannen version suorittamat komennot [20].

On selvää, että Mirain kaltaiset bottiverkot ovat äärimmäisen vaarallisia ja niitä vastaan on kehitettävä pysyviä ratkaisuja. BrickerBotin toimintatapa ei kuitenkaan tarjoa pysyvää ratkaisua ongelmaan, sillä jos vaadittuja muutoksia laitteelle valmistajan toimesta ei tehdä, tulee internet olemaan täynnä haavoittuvia IoT-laitteita myös tulevaisuudessa. Suuret laitevalmistajat tulevat varmasti huomioimaan vahvistetut tietoturvavaatimukset tulevissa firmware- ja laitepäivityksissä, mutta pienemmät laitevalmistajat saattavat jättää päivitykset huomioimatta. Suurin osa halvoista IoT-laitteista ei tue OTA-päivitysmekanismia, mikä mahdollistaisi päivitysten ajamisen suoraan laitteelle. Tähän syynä voi olla vaatimattomat kehitysympäristöt ja liian niukat testimahdollisuudet sen varmistamiseen, että laitteet toimivat päivitysten jälkeen samalla tavalla kuin ennenkin. Pysyvä muutos IoT-laitteiden turvallisuuteen on tultava valmistajalta ja niiden kehittäjiltä. Suurin osa kuluttajista eivät ole tietoisia laitteisiin kohdistustuvista tietoturvariskeistä.

4.3.3 Hajime Vigilante Botnet

Mirai-bottiverkon aiheuttamat häiriöt ovat herättäneet kuluttajien ja laitevalmistajien huomion. Kaikki eivät kuitenkaan ole pahantahtoisia ja pyri aiheuttamaan palvelunestohyökkäyksillä haittaa muille ihmisille. Hajime-bottiverkon pyrkimyksenä ei ole tuhota laitetta

BrickerBotin tavoin tai käyttää sitä DDoS hyökkäyksiin myöhemmin kuten Mirai bottiverkko. Kyseessä on tietomurtoja tutkivan valkohatun (eng. Whitehat) kehittämä haittaohjelma, minkä pyrkimyksenä on luoda IoT-laitteista hieman turvatumpia suojaamalla hyökkäyksiin käytettyjä yleisiä portteja (23, 7547, 5555, and 5358). Kyseisiä portteja on käytetty eniten Mirai-bottiverkon hyökkäyksissä. [22.]

Hajime-bottiverkko ei käytä keskitettyä komentopalvelinta, joita usein käytetään bottiverkoissa (eng. command and control server). Tällä Hajime pyrkii pysyttelemään paremmin piilossa internetin palveluntarjoajilta (eng. Internet Service Provider) ja käyttääkin perinteistä peer-to-peer teknologiaa päivittääkseen ja komentaakseen bottiverkkoon liitettyjä IoT-laitteita. [22.]. Hajime myös salaa kaiken komentoliikenteen yksityisillä ja julkisilla avaimilla. Käyttämällä julkisia ja yleisesti tunnettua BitTorrent protokollaa kykenee Hajime pysyttelemään piilossa ja vikasietoisena suojautumiskeinoista huolimatta [23.].

Mikä tekee Hajimesta vaarallisen on sen perimmäisen toimintatavan epämääräisyys. Asiantuntijat eivät pysty varmuudella kertomaan mikä Hajimen perimmäinen tarkoitus on, eikä kukaan pysty varmuudella sanomaan, ettei Hajimea tulevaisuudessa käytetä verkkohyökkäyksiin tai muuhun haitalliseen toimintaan. Haittaohjelma ei kuitenkaan ole pureutunut järjestelmään syvälle, vaan IoT-laite palautuu entiselleen pelkällä uudelleenkäynnistämisellä. Laite on kuitenkin uudelleenkäynnistämisen jälkeen edelleen haavoittuvainen muille verkkohyökkäyksille kuin myös Hajimelle. Tästä syystä Hajimea ei voida pitää kuin kevyenä yrityksenä suojata IoT-laitteita Mirain kaltaisilta bottiverkoilta, mutta sen vaarallisuus on vielä avoin. [22.]

Vaikka Hajime häviää laitteelta sen uudelleenkäynnistämisen jälkeen, on se kuitenkin hyvin suunniteltu ja on erittäin joustava muutoksille. Kehittäjä kykenee tekemään Hajimesta Mirain kaltaisen haittaohjelman hyvin pienellä aikavälillä. Hajime on saastuttanut pääsääntöisesti IoT-laitteita Brasiliassa, Vietnamissa ja Iranissa, mutta hyökkäyksiä on tapahtunut kaikilla mantereilla. [23.]

```
root@raspberrypi:/home/pi/analysis/sample001# strace -f -tt -s 65535 -o sample001.04.strace.txt ./hajime.bin
iptables v1.4.21: Couldn't load target `CWMP_CR':No such file or directory

Try `iptables -h' or 'iptables --help' for more information.
iptables: No chain/target/match by that name.
Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!

Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!

Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!
```

Kuva 7. Hajimen tulostama viesti terminaalipäätteeseen aina kymmenen minuutin välein [23].

5 Pohdinta

Asioiden internet on tullut pysyäkseen. Teknologia tuo valtavan määrän helpotusta ja hyötyä niin kuluttajille kuin myös yrityksille. Yksi syy asioiden internetin valtavaan kasvuun on sen modulaarisuus, mikä mahdollistaa sen käyttämistä lähes missä tarkoituksessa tahansa. Tämä tarkoittaa sitä, että IoT:n käyttökohteen rajoituksena on kehittäjien mielikuvitus. Tämä tuo mukanaan omia riskejä, jotka laite- ja sovelluskehittäjien on otettava huomioon. Tämän opinnäytetyön läpikäymät esimerkit eivät ole täydellinen lista kaikista asioiden internetiin kohdistuvista vaaroista, mutta se käy läpi perusperiaatteen kyseiseen teknologiaan kohdistuvista vaaroista. Käyttökohteiden rajattomuus tuo myös mukanaan valtavan määrän potentiaalisia hyökkäystapoja. Räjähdysmäinen kasvu IoT:n saralla on valtava riski tietoturvan näkökannalta, jos IoT-laitteiden tietoturvaa ei huomioida riittävällä tasolla suunnittelusta lähtien. Tietoturva ja suojautuminen verkkohyökkäyksiltä on kasvattanut merkitystään yrityksissä niin tiukentuneiden määräysten sekä auditointien takia. Tähän on myös vaikuttanut kehittyneet haittaohjelmat, kuten viime vuosina laajasti levinneet kiristysohjelmat (eng. ransomware), mitkä kykenevät pysäyttämään liiketoiminnan kokonaan. IoT tulee olemaan ratkaisevassa roolissa, sillä haavoittuva tai saastunut IoT-laite voi pahimmassa tapauksessa häiritä yrityksen tai kuluttajan omaan verkkoon liitettyjä muita laitteita.

Kuluttajat usein eivät huomioi hankkimiinsa laitteisiin kohdistuvia vaaroja, vaan luottavat laitevalmistajien ammattitaitoon valmistaa turvallisia ja helppokäyttöisiä laitteita. Nykypäivänä kuitenkin osa vastuusta on siirretty loppukäyttäjälle, sillä osa laitteista vaatii edelleen manuaalista firmware päivitystä tai sovelluspäivitystä. Internet on tämän lisäksi täynnä IoT-laitteita, joiden myyntihinta kertoo osan totuudesta. Laitteiden hintaa saadaan mahdollisimman alhaiseksi karsimalla kustannuksista, jotka eivät ole heti havaittavissa lopputuotteessa, kuten esimerkiksi tietoturvaan käytetyt resurssit ja tarkka suunnittelu.

Suurin osa kuluttajista ei ole tietoisia IoT-laitteisiin kohdistuvista tietoturvauhkista. Osasyynä tähän johtuu varmasti siitä, että asioiden internetin käsite on niin valtava ja normaalin kuluttajan näkökannalta epämääräinen. Todennäköistä onkin, ettei suurin osa internetiin liitettyjen web-kameroiden omistaja ole edes tietoinen kyseessä olevan IoT-laite. Kuluttajilla on kuitenkin useita keinoja, joilla on mahdollista vähentää omiin IoT-laitteisiin kohdistuvat uhkat. Järjestelmähaavoittuvuuksia on haastavaa korjata ilman laitevalmistajan tekemiä päivityksiä, mutta ennaltaehkäisevä toiminta auttaa vähentämään niihin kohdistuvia vaaroja.

Kuluttajien onkin syytä seurata omien IoT-laitteidensa versiopäivityksiä ja varmistaa aika-ajoin onko uusia päivityksiä tullut saataville. Päivityksiä on kuitenkin turha odottaa laitteisiin, jotka ovat olleet käytössä useita vuosia, sillä laite on saattanut päätyä elinkaarensa loppuun (EoL, End of Life) eikä uusia järjestelmäpäivityksiä tule tarjolle.

Useat kodin modeemit ja reitittimet tarjoavat mahdollisuuden käyttää UPnP (Universal Plug and Play) protokollaa, mikä mahdollistaa verkkoon liitetyn laitteen automaattisesti konfiguroida modeemia/reititintä avaamaan kyseisen laitteen käyttämiä portteja. Tällä tavoin kuluttajien ei tarvitse itse tehdä mitään verkon näkökannalta ja IoT-laite silti toimii odotetulla tavalla ja on saavutettavissa internetin yli. UPnP:n kohdistuu paljon vaaroja, sillä saastunut laite pystyisi avaamaan myös listan muita portteja, joita käytettäisiin haittaohjelman levittämiseen ja muuhun haitalliseen työhön. Useat tietoturva-asiantuntijat suosittelevatkin, että kuluttajat poistavat UPnP:n käytöstään omista verkkolaitteistaan.

Jos modeemi/reititin tukee erillisiä VLAN:eja (Virtual Local Area Network) on kuluttajien mahdollista luoda IoT-laitteilleen oman verkkosegmentin, mistä verkkoliikenne on rajoitettua. Tällä tavoin on mahdollista suojata oman kodin verkon muut laitteet mahdollisesti saastuneelta IoT-laitteelta. Useimmat kuluttajille suunnitellut verkkolaitteet eivät kuitenkaan tue VLAN:ien luomista. Modeemeille ja reitittimille on tarjolla kustomoituja firmwareja, mitkä lisäävät normaalien toiminnallisuuksien lisäksi muun muassa VLAN-ominaisuuden (mm. OpenWRT). Suuri osa kuluttajille suunnatuista WLAN-tukiasemista tarjoaa mahdollisuuden luoda kaksi erillistä langatonta verkkosegmenttiä kodin omille laitteille sekä vierailijoille. Tämä on myös yksi mahdollinen keino eristää IoT-laitteet kodin muista verkkoon kytketyistä laitteista.

Lähteet

[1] Buyya R, Dastjerdi A. Internet of Things Principles and Paradigms. Cambridge, MA, USA: Elsevier; 2016.

[2] Kone tuo älypalvelut hisseihin – Watson IoT apuna Saatavilla:

https://www.uusiteknologia.fi/2017/02/09/kone-to-alypalvelut-hisseihin-watson-iot-apuna/ Haettu 8/10/2017, 2017.

[3] A Simple Explanation Of 'The Internet Of Things' Saatavilla:

https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#391ad7761d09 Haettu 3/2/2017, 2014

[4] Samsung Connect Home Saatavilla:

http://www.samsung.com/us/explore/connect-home/. Haettu 9/17/2017, 2017.

[5] Home Connect Saatavilla:

https://play.google.com/store/apps/details?id=com.bshg.homeconnect.android.release

Haettu 10/10/2017.

[6] Three Types of Online Attacks Saatavilla:

https://www.ted.com/talks/mikko_hypponen_three_types_of_online_attack

Haettu 8/2/2017, 2011.

[7] That 'Internet of Things' Thing Saatavilla:

http://www.rfidjournal.com/articles/view?4986. Haettu 6/7/2017, 2009.

[8] Mitä on RFID? Saatavilla

http://www.rfidlab.fi/rfid-teknologia/mita-on-rfid/. Haettu: 6/6/2017.

[9] Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016

Saatavilla:

http://www.gartner.com/newsroom/id/3598917. Haettu 8/8/2017, 2017.

[10] Jeep Uconnect Saatavilla:

http://www.driveuconnect.com/

Haettu 6/6/2017, 2017.

[11] Hackers Remotely Kill a Jeep on the Highway—With Me in It Saatavilla:

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ Haettu 15/5/2017, 2015.

[12] Definition zero-day exploit Saatavilla:

http://searchsecurity.techtarget.com/definition/zero-day-exploit. Haettu 4/5/2017, 2010.

[13] Philips Hue Saatavilla:

https://www.down-load.p4c.philips.com/files/8/8718696461532/8718696461532_pss_finfi.pdf

Haettu 4/5/2017, 2017.

[14] O'Flynn, C, Shamir, A, Weingarten, A. IoT Goes Nuclear: Creating a ZigBee Chain Reaction Saatavilla:

http://iotworm.eyalro.net/iotworm.pdf. Haettu 4/5/2017, 2017.

[15] Researchers hack Philips Hue smart bulbs from the sky Saatavilla:

https://www.techhive.com/article/3138872/internet-of-things/researchers-hack-philips-hue-smart-bulbs-from-the-sky.html. Haettu 4/5/2017, 2016.

[16] What Vizio was doing behind the TV screen Saatavilla:

https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-be-hind-tv-screen. Haettu 5/5/2017, 2017.

[17] Botit ja bottiverkot—kasvava uhka Saatavilla:

https://fi.norton.com/botnet. Haettu 7/6/2017.

[18] Breaking Down Mirai: An IoT DDoS Botnet Analysis Saatavilla:

https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Haettu 8/6/2017.

[19] Security Tip (ST04-015) Understanding Denial-of-Service Attacks Saatavilla:

https://www.us-cert.gov/ncas/tips/ST04-015. Haettu 5/4/2017.

[20] BrickerBot PDoS Attack: Back With A Vengeance Saatavilla:

https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/

Haettu 10/6/2017. 2017.

[21] BrickerBot is a vigilante worm that destroys insecure IoT devices Saatavilla:

https://techcrunch.com/2017/04/25/brickerbot-is-a-vigilante-worm-that-destroys-insecure-iot-devices/. Haettu 10/6/2017, 2017.

[22] Hajime 'Vigilante Botnet' Growing Rapidly; HIjacks 300,000 IoT Devices Worldwide Saatavilla:

http://thehackernews.com/2017/04/vigilante-hacker-iot-botnet_26.html.

Haettu 10/6/2017, 2017.

[23] Hajime – Sophisticated, Flexible, Thoughtfully Designed and Future-Proof Saatavilla:

https://blog.radware.com/security/2017/04/hajime-futureproof-botnet/

Haettu 10/6/2017, 2017.