jamk.fi

Verkkorikollisuus ja verkkoon kytketyt laitteet

Opinnäytetyö

Eeva-Liina Arvola

Opinnäytetyö
Joulukuu 2019
Tekniikan ala
Insinööri (AMK), Tieto- ja viestintätekniikka
Kyberturvallisuus

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Arvola, Eeva-Liina	Opinnäytetyö, AMK	Joulukuu 2019
	Sivumäärä 56	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Verkkorikollisuus ja verkkoon kytketyt laitteet

Tutkinto-ohjelma
Tieto- ja viestintätekniikka

Työn ohjaaja(t)
Jani Immonen, Mieskolainen Matti

Toimeksiantaja(t)
CYBERDI-projekti/JAMK/Kirsi Heiskanen

Tiivistelmä

Opinnäytetyön toimeksiantajana toimi CYBERDI-projekti, joka toteutetaan yhteistyössä JAMK:n sekä Poliisiammattikorkeakoulun kanssa. Projektin osarahoittajana toimii Opetushallitus. Projektin tarkoituksena on lisätä kansalaisten tietoisuutta kyberuhkista ja -rikoksista.

Opinnäytetyön tavoitteena oli tutkia IoT-laitteisiin kohdistuvaa verkkorikollisuutta. Tavoitteena oli löytää vastauksia kysymyksiin, minkälaisia haavoittuvuuksia IoT-laitteista on löydetty, miten hakkerit väärinkäyttävät kuluttajien IoT-laitteita ja miten kuluttajat voisivat suojata omia laitteitaan. Perehdyttiin älykotimääritelmään ja sitä myötä sisäverkkoon ja kuinka suojata sitä. Tavoitteena oli tuoda kuluttajille esille IoT-laitteiden mukana tuomia haasteita ja yksinkertaisia esimerkkejä, miten IoT-laitteita on väärinkäytetty. Aineistona käytettiin alan kirjallisuutta ja verkkojulkaisuja.

Opinnäytetyössä tutkittiin, miten valvontakameroita voidaan skannata verkosta ja sivustoja, jotka jakavat kuluttajien valvontakameroiden lähettämää videokuvaa julkisesti. Esitettiin yksinkertaisia salasanan murtamiskeinoja, jotta voitaisiin osoittaa salasanojen tärkeys ja miksei tunnettuja salasanoja kannata käyttää.

IoT-laitteiden tietoturvassa on parannettavaa laitevalmistajien taholta, mutta yleisimmiksi tietoturvaongelmiksi todettiin kuluttajien jättämät oletussalasanat ja uusien ohjelmistoversioiden päivittämättä jättäminen. Kodinkoneita ei voida suojata yhtä tehokkaasti tietoturvaohjelmilla, kuten tietokoneita, joten nämä laitteet sisältävät suuremman tietoturvariskin. Tietoturvan ylläpitämistä hankaloittaa uusien haittaohjelmien lisääntyminen ja näiden yhä monimutkaisemmat rakenteet.

Avainsanat (asiasanat)
Verkkorikollisuus, kyberrikollisuus, älykoti, IoT-laitteet, sisäverkko

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Arvola, Eeva-Liina	Bachelor's thesis	December 2019
		Language of publication: Finnish
	Number of pages 56	Permission for web publication: x

Title of publication
Cybercrimes in devices connected to network

Degree programme
Information and Communication Technology

Supervisor(s)
Immonen Jani, Mieskolainen Matti

Assigned by
CYBERDI-projekti/JAMK/Heiskanen Kirsi

Abstract

The bachelor's thesis was assigned by CYBERDI project created together with JAMK University of Applied Sciences and the Police University College. The CYBERDI project is partly funded by the Finnish Board of Education. The purpose of the project is to increase citizens' knowledge of cyber threats and crimes.

The aim was to study cybercrimes directed to IoT devices and find answers to questions, what vulnerabilities can be found in IoT devices, how hackers misuse consumers' IoT devices and how consumers could secure their devices. The study discusses the definition of smart home and local area network (LAN) and how to secure it. The aim was to introduce challenges that IoT devices create and to provide examples of misusage of IoT devices. The material was found in literature and online publications.

The thesis also studied how security cameras can be scanned from a network and which websites stream security cameras online publicly. The paper also discusses simple ways to crack passwords to express the importance of passwords and why known password should not be used.

The security of IoT devices needs to be improved from producer side; however, the most common security issues were default passwords that were not changed and the not updated software of devices. Home appliances cannot be secured with security software as well as computers; therefore, these devices present a bigger security risk. New malware with more complex structures complicates the improvement of information security.

Keywords/tags (subjects)
Cybercrime, smart home, IoT devices, Internet of Things, Local Area Network, LAN

Miscellaneous (Confidential information)

Sisältö

Kuviot

Terminologia

BLUETOOTH	Langaton tiedonsiirtotekniikka lyhyellä kantamalla
BOTTIVERKKO	Joukko tietokoneohjelmia, jotka kytkeytyneet tietoverkon välityksellä
CAN	Controller Area Network, automaatioväylä
DDOS	Distributed Denial of Service, hajautettu palvelunesto-hyökkäys
DNS	Domain Name Server, nimipalvelin muuntaa verkkotunnukset IP-osoitteiksi
DOS	Denial of Service, palvelunestohyökkäys
ECU	Engine Control Unit, moottorin kontrollointiyksikkö
FTP	File Transfer Protocol, tiedonsiirtoprotokolla
GATEWAY	Yhdyskäytävä, joka mahdollistaa tiedonsiirron toiseen verkkoon
HONEYPOT	Tietoturvamekanismi, jota käytetään rikollisten huijaamiseen eristetyssä verkossa
HTTP	Hyper Text Transfer Protocol, tiedonsiirtoprotokolla selaimille ja www-palvelimille
IFTTT	If This Then That, ohjelmistoalusta eri valmistajien sovellusten, laitteiden ja palveluiden yhdistämiseen

IOT	Internet of Things
IP-OSOITE	Internet protokollaosoite
MATO	Haittaohjelma, joka leviää tietokoneiden välillä automaattisesti
NAS	Network Attached Storage, verkkoon kytketty tallennustila
NMAP	Avoimen lähdekoodin verkonskannausohjelma
SQL-INJEKTIO	Tietokantainjektio
SSH	Secure Shell, salatun tietoliikenteen protokolla
SSL/TLS	Tietoverkonsalausprotokolla
TCP	Transmission Control Protocol, tietoliikenneprotokolla
TELNET	Tietoliikenneprotokolla
TIETOTURVA-AUKKO	Ohjelmistossa oleva virhe
TROJALAINEN	Naamioitunut haittaohjelma
UDP	User Datagram Protocol, yhteydetön tietoliikenneprotokolla
UPNP	Universal Plug and Play, verkkoprotokollien joukko eri valmistajien laitteiden toimimiseen yhdessä
WIFI	Langaton verkkotekniikka

WLAN	Langaton lähiverkko
XSS	Cross-Site Scripting, web-sovelluksissa esiintyvä tietotur-va-aukko

1 Johdanto

Nykyteknologia ja verkkoon kytketyt laitteet ovat helpottaneet ihmisten arkea. Näiden avulla on pystytty siirtämään viihde, maksuasiat, kommunikointi ja moni muu tehtävä aivan käden ulottuville. Kodin valaistusta voidaan ohjata älypuhelinsovelluksella ja säästytään sängystä nousemiselta, viestit voidaan vastaanottaa älykelloon, eikä puhelinta tarvitse kaivaa esiin lenkillä, etuoven koodin voi vaihtaa suoraan puhelimella eri kaupungista ja näin naapuri pääsee kastelemaan kukat. Moni järjestelmä on tullut tutuksi Internet protokollan (IP) ansiosta ja teknologiaa on pystytty viemään pidemmälle nopeuttamaan ja helpottamaan ihmisten työpäivää ja arkea. Samalla laitteet tuovat myös uhkia päivittäiseen arkeen. Jokainen verkkoon kytketty laita saa IP-osoitteen ja jokainen osoite sallii toisen osoitteen keskustella kanssaan. Moni kuluttaja ei jaksa, viitsi tai osaa huomioida jokaisen uuden yhteydellisen laitteen tarjoavan uuden rajapinnan ulkomaailmaan eikä ajattele näiden laitteiden huonoja puolia. Jokainen uusi IP-osoite antaa väärinkäyttäjille mahdollisuuden tunkeutua kuluttajan tietoihin.

Internet of Things (IoT) tarkoittaa Esineiden Internetiä. Se kattaa sisällään jokaisen laitteen, joka kytketään verkkoon. IoT-laitteiden lisäännyttyä, on verkkorikollisuuden määrä kasvanut. Rikolliset keksivät yhä monimutkaisempia ja haastavampia haittaohjelmia. IoT-laitteiden pienen muistin ja suoritustehon takia, laitteilla ei ole välttämättä tehokasta tietoturvaa tai laitevalmistajat eivät ole ajatelleet tuotetta tehdessä, valmistavansa laitetta, joka sisältää tietokoneen ja näin tietoturvaan ei ole osattu paneutua. Tietoturvaongelmaksi koostuu myös kuluttajien välinpitämättömyys ja osaamattomuus tutustua laitteiden tietoturvaan tarkemmin.

Opinnäytetyön tavoitteena on lisätä tietoisuutta laitteiden tuomista uhkista laitteiden lisääntyessä koteihin huimaa vauhtia. Opinnäytetyössä esitetään IoT-laitteiden haavoittuvuuksia ja esimerkkejä, miten IoT-laitteita on väärinkäytetty ja tuodaan esiin keinoja, joilla parantaa IoT-laitteiden tietoturvallisuutta.

Opinnäytetyön toimeksiantajana toimi Jyväskylän ammattikorkeakoulun sekä Poliisiammattikorkeakoulun kanssa muodostettu yhteystyöprojekti CYBERDI. Projektin ta-

voitteena on, että kansalaiset olisivat aiempaa tietoisempia kyberuhkista ja -rikollisuudesta sekä tavoista, joilla välttyä niiltä. Projektin tarkoituksena on auttaa kansalaisia ymmärtämään älylaitteen yhteys maailmanlaajuiseen verkkoon ja tämän haittapuolet sekä parantamaan ihmisten digitaalista arkea turvallisempaan suuntaan lisäämällä tietoisuutta.

2 Tutkimusasetelma

2.1 Tutkimuskysymys

Tämän tutkimuksen tutkimusongelmana oli verkkorikollisuus IoT-laitteissa. Tutkimuskysymyksenä perehdyttiin aiheeseen, miten IoT-laitteita pystytään hyödyntämään verkkorikollisuudessa? IoT-laitteisiin kuuluvat kaikki laitteet, jotka hyödyntävät verkkoyhteyttä. Tutkimuksessa pääpaino on kuitenkin kodin älylaitteilla, eikä tietokoneiden, tablettien ja älypuhelimien tietoturvallisuuteen paneuduta tarkemmin erikseen. Tutkimuskysymys jaoteltiin seuraaviin alakysymyksiin:

- Minkälaisia haavoittuvuuksia IoT-laitteista on löydetty?
- Minkälaisia keinoja rikolliset käyttävät IoT-laitteisiin tai niiden hyödyntämiseen?
- Miten suojata kodin sisäverkko ja IoT-laitteet?

2.2 Tutkimusmenetelmä

Tutkimuksessa käytettiin menetelmänä laadullista eli kvalitatiivista tutkimusmenetelmää. Laadullisessa tutkimuksessa pyritään tuottamaan tutkittuun ongelmaan ratkaisu tai ymmärrys, muttei ryhdytä käytännön toimenpiteisiin. Kvalitatiivinen tutkimusmenetelmä valittiin, sillä tarkoituksena oli löytää ilmiöön syvällinen näkemys sekä saada ilmiöstä tarkempi kuvaus. (Kananen 2015, 70-71.)

Laadullisessa tutkimuksessa tutkittava ilmiö ei ole ennestään tuttu. Sisältö kerääntyy tutkimuksen myötä ja aineiston määrää ei voida etukäteen määritellä. Tutkimuksessa ei täysin tiedetä, mitä ilmiöstä etsitään, ja näin ollen aineiston määrä määrittyy sen mukaan, milloin tutkimuksen ongelma ratkeaa. Ilmiöstä pyritään löytämään mahdollisimman kattava ja laaja kokonaisuus. Tutkimuksessa käytettiin aineistonkeruumenetelmänä erilaisia dokumentteja. (Mts. 128-129.)

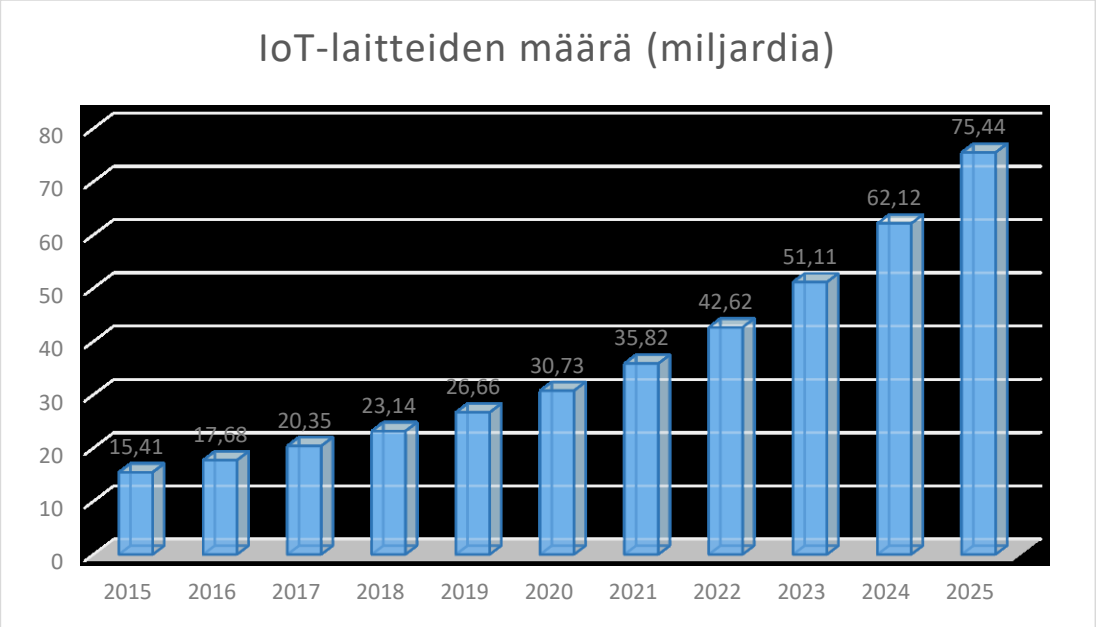
3 Internet of Things

3.1 Esineiden internet

Nykypäivänä edistyksellisinä pidetyt keksinnöt korvataan yhä uudemmalla teknologialla. Paperikartat vaihdettiin GPS-laitteisiin ja sitä myötä puhelinsovelluksiin. Henkilövaa'alla voidaan mitata painon lisäksi kehon koostumusta ja selvittää näin rasvan ja lihasten määrä. Filmikamerat muuttuivat digikameroiksi ja nykyään lähes jokainen kantaa taskussaan hyvänlaatuista kameraa, josta kuvat saa saman tien käyttöön ja ladattua pilveen selattavaksi useammalla eri laitteella. Verkkoon kytkettyjen laitteiden määrä kasvaa huimaa vauhtia. Liikennekamerat, urheiluvälineet, kauppojen hyllyt, lukot, dvd-soittimet, kodinkoneet ja monet muut laitteet kytketään verkkoon keräämään dataa ihmisten toiminnoista ja helpottamaan kuluttajien arkea. Kaikki tämä tieto kerätään analysoitavaksi tietokantoihin erilaisille servereille internetin kautta. Teknologian uudistuttua ennen 60 euroa maksavasta puhelimesta saattaa joutua nykypäivänä maksamaan 700 euroa. (Greengard 2016, 1-12.)

Nyky-yhteiskunnan ihminen on tottunut saamaan tiedon heti, ja jokainen täytyy olla tavoitettavissa koko ajan. Worldometers.info-sivuston mukaan ihmisiä on tällä hetkellä yli 7,7 miljardia maailmassa (Current World Population 2019). Statista.com-sivuston mukaan IoT-laitteita on maailmassa yli 26 miljardia. Kuviosta 1 näkee laitteiden määrän kasvun vuodesta 2015 vuoteen 2019 ja laitteiden kasvun ennusteen vuoteen 2025 asti. Tilastossa laitteisiin luokitellaan myös älypuhelimet, tabletit ja tietokoneet. Kuvion tiedot on kerätty Statista-sivustolta. Tilastollisesti on hyvä huomioida

kehitysmaat ja kuinka suurella osalla maailman ihmisistä on mahdollisuus käyttää IoT-laitteita. (Greengard 2016, 12-14; Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions) 2019.)



Kuvio 1. IoT-laitteiden määrä ja vuosittaisen kasvun ennuste

Verkkoon kytketyt laitteet tuovat helpotusta ihmisten arkeen monin tavoin. Ne myös auttavat yrityksiä parantamaan kassavirtaa ja tuottamaan palveluitaan tai tuotteitaan kuluttajille mieluisimmiksi sekä helpommin saataviksi. Mikään toimiala ei nykypäivänä toimi ilman internetiä ja verkkoon kytkettyjä laitteita. IoT voidaan määritellä seuraavanlaisesti: Internetin kautta jatkuvasti tavoitettavissa oleva data ja laitteet (Hu 2016, 4). Jokaisella näistä laitteista on uniikki tunnistusnumero UID (*Unique Identification Number)* sekä IP-osoite. Näitä voidaan yhdistää toisiinsa niin langallisten kuin langattomien verkkojen kautta, kuten WiFi sekä Bluetooth. WiFi ja Bluetooth-teknologioiden eroja käsitellään luvussa 3.3.5 *Bluetooth ja WiFi-yhteyksien eroavaisuudet*. Nämä laitteet käyttävät sisäänrakennettua elektronista mikropiiriä sekä radiotaajuista etätunnistusta RFID (*Radio Frequency Identification*) tai RFID-tekniikkaa hyödyntävää tiedonsiirtomenetelmää NFC (*Near Field Communication*). RFID-

tekniikassa hyödynnetään datan seuraamista sekä identifioimista. NFC-tekniikkaa käytetään laitteiden väliseen tiedonsiirtoon lyhyillä matkoilla (Near Field Communication 2017). (Greengard 2016, 15; Hu 2016, 5)

Laitteita löytyy kahden tyyppisiä: fyysisyys-ensin (eng. *physical-first*) sekä digitaalisuus-ensin (eng. *digital-first*). Näiden kahden eron voi todeta sillä, onko laite riippuvainen binäärikoodista vai fyysisestä olemuksesta. Fyysisyys-ensin objektit eivät käsittele digitaalista dataa, ellei niitä ole käsketty tekemään niin. Esimerkiksi vinyylilevy sekä kivijalka-kaupat ovat näitä niin sanottuja fyysisyys-ensin objekteja, kun taas musiikkitiedosto tai e-kirja sekä verkkokaupat ovat digitaalisuus-ensin objekteja. IoT-laitteiden kyky yhdistää nämä objektit toisiinsa tekee Esineiden Internetistä vaikutusvaltaisen. Cisco Systems on yhdistänyt nämä kaksi fyysistä ja digitaalista maailmaa toisiinsa luoden käsityksen Kaikkien Internet (eng. *Internet of Everything*). (Greengard 2016, 16-18.)

Internet of Things -fraasin keksijä Kevin Ashton viittasi tällä fraasilla fyysisessä maailmassa oleviin verkkoon kytkettyihin objekteihin (Gabbai 2015). Ashton viittasi fraasilla ensimmäisen kerran vuonna 1999, mutta IoT juurtaa juurensa jo 15 vuotta taaperin. Rijmenam (2014) toteaa, että jo vuonna 1926 Nikola Tesla kommentoi Colliers Magazines lehden artikkelissa seuraavanlaisesti:

> *When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole... and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket.*

Ennen kuin internet keksittiin vuonna 1969, Alan Turing mainitsi artikkelissaan *Computing Machinery and Intelligence* (1950) ajatuksen, mitä jos laitteet voisivat ajatella (Rijmenam 2014).

3.2 Älykoti

Nykypäivänä ihminen mieltää sanan ”äly” (eng. *smart*) olevan jotain, mikä voi toimia itsenäisesti ja tehdä päätöksiä mahdollisimman vähäisellä manuaalisella toimenpiteellä säästäen näin kustannuksia ja energiaa. Jo vuosina 1915- 1920 kodit täyttyivät erilaisista laitteista, kuten ompelukoneista sekä pölynimureista. Nämä keksinnöt olivat alkua tulevaisuuden keksinnöille ja nykypäivän kodin peruselementeille. Vuonna 1966 ensimmäinen tietokone ECHO IV keksittiin. Tämä ei kuitenkaan lyönyt täysin läpi, mutta oli tärkeä teknologian kehityksen kannalta. (Biswas 2018.)

Moni nykypäivän päivittäin käytetyistä laitteista on saanut alun perin ideansa jo monen vuoden takaisista tieteisfiktioista. Esimerkiksi näytön kautta kommunikointi mainittiin jo alun perin vuonna 1909 elokuvassa The Machine Shop. Vuonna 1975 keksittiin kommunikointiprotokolla X10 kodin automatisointiin. X10 oli yksi suuntainen protokolla, jonka avulla pystyttiin esimerkiksi ohjaamaan sähköverkossa olevia laitteita. Tieto kulki joko sähköverkon välityksellä tai radioteitse. Tämä protokolla ei ole enää käytössä, sillä uudemmat protokollat toimivat tiedonsiirron kannalta nopeammin ja varmemmin. Ensimmäisen internetyhteydellisen jääkaapin kehitti LG Internet Digital DIOS vuonna 2000. Tästä lähti älykotien kehittyminen. (Mt.)

Älykoti määritelmällä tarkoitetaan kotia, joka koostuu erilaisista älylaitteista ja järjestelmistä, joita pystyy monitoroimaan sekä hallitsemaan etänä. Älykoti nimikettä käytetään nykypäivänä paljon uusien kotien suunnittelussa ja erilaiset tietojärjestelmät ovat lisääntymässä koteihin jo rakennusvaiheessa. Älykodin kolme tärkeää elementtiä ovat sisäinen verkko (kaapelikytkentä tai langaton), laitteiden hallintaan käytettävä yhdyskäytävä (eng. *gateway*) sekä kodin automatisointi (laitteet, jotka ovat kytköksissä kodin sisällä sekä hallittavissa kodin ulkopuolella). Yhteydellisiä laitteita on tänä päivänä jo enemmän kuin maailmassa ihmisiä. Tulevaisuudessa voidaan olettaa tuotteiden lisääntyvän huimaa vauhtia, mutta samalla myös tuotteiden hintalaatusuhde sekä turvallisuus paranevat. Yksi keskeisimmistä asioista tulevaisuudessa on laitteiden keskittäminen yhdelle hallintajärjestelmälle. Tällä hetkellä jokainen laite toimii erillisesti ja valoja hallitaan äänen avulla ja lämpötilaa puhelinsovelluksella. Tavoitteena on saada keskitetty hallinta jokaiselle järjestelmälle. (Mt.)

Eri palveluntarjoajat jakavat älykodin erilaisiin kategorioihin. Älykoti voidaan jakaa seuraavasti:

1. Valaistus
2. Turvallisuus
3. Viihde
4. Lämpötila ja ympäristö
5. Puhelinjärjestelmä
6. Kodinkoneet

Erilaisia palveluntarjoajia ja laitevalmistajia löytyy monia. Tuotteet ja niiden ominaisuudet vaihtelevat valmistajien mukaan.

Valaistus

Valaistuksen hallinta on suosituin älykodin järjestelmä. Järjestelmän avulla kuluttaja pystyy hallitsemaan etänä ja automatisoimaan valaistuksen voimakkuutta ja näin valitsemaan tilanteeseen optimaalisimman kirkkauden. (Product categories 2019.)

Valaisimien kirkkautta ja sävyjä pystytään hallitsemaan esimerkiksi älypuhelinsovelluksen avulla. Hallitsemiseen vaaditaan verkkoyhteys ja sovellusta tukeva älypuhelin. Valaisimet täytyy olla kytkettynä verkkoon koko aikaisesti, jotta kaikkia ominaisuuksia voidaan käyttää. Jotkin laitevalmistajat vaativat laitteiden toimintaan erillisen sillan, johon laitteet kytketään verkkoyhteyden lisäksi. Valaisimissa voi olla lisättynä myös ääniohjaus, jonka avulla valaisimia pystytään hallitsemaan äänen avulla sekä ajastin, jonka avulla valaisimet voidaan ajastaa sammumaan sekä syttymään eri aikoihin eri huoneissa. (Aurelle square -paneelivalo 2019; Valoa tunnelmallisiin hetkiin 2018.)

Turvallisuus

Turvallisuus osa-alueella määritellään kodin valvontajärjestelmät sekä lukot. Valvonnalla voidaan tarkoittaa niin sisäistä kuin ulkoista kameravalvontaa, kuin myös harvemmin sattuvia tapahtumia, kuten esimerkiksi tulvan mittaus. Lukkoja pystytään hallitsemaan etänä ja ovikoodia vaihtamaan tarvittaessa internetyhteyden sekä mahdollisen puhelinapplikaation avulla. Kameroista pystytään taltioimaan livekuvaa ja tallentamaan materiaali pilveen. (Product categories 2019.)

Älylukkoja pystytään hallitsemaan Bluetooth tai WiFi-yhteyden avulla. Lukkoa pystytään hallitsemaan älypuhelinsovelluksen avulla. Sovellus lähettää käyttäjälle ilmoituksen aina lukon avautuessa ja lukittuessa. (How the Glue ecosystem works 2019.)

Viihde

Viihde kattaa kodin äänentoisto- sekä videopalvelut. Järjestelmän avulla pystytään hallitsemaan äänentoistolaitteita sekä mahdollisesti jakamaan laitteistoa ympäri taloa, eikä pelkästään yhteen huoneeseen. Laitteet eivät tarvitse erillisiä kaukosäätimiä, vain yhdellä napin painalluksella saadaan aktivoitua kaikki kotiteatterilaitteistot. (Product categories 2019.)

Älykaiuttimia pystytään ohjaamaan äänen avulla ja musiikin kuuntelua pystytään hallitsemaan useammassa huoneessa samanaikaisesti. Älykaiutin saattaa vaatia toimiakseen erillisen saman laitevalmistajan tuottaman järjestelmän. (WK7 2019.)

Lämpötila ja ympäristö

Älylaitteet tarjoavat kuluttajalle mahdollisuuden säästää lämmitys- ja viilennyskustannuksissa. Esimerkiksi lämmitys pystytään automatisoimaan ja ajoittamaan, mikäli lämmitys ei ole tarpeellista kokoaikaisesti. Lämmitystä ja viilennystä pystytään myös hallitsemaan etänä, jolloin kuluttaja voi laittaa esimerkiksi mökin lämmityksen päälle jo etukäteen ja näin tulla valmiiksi lämmitettyyn mökkiin. (Product categories 2019.)

Lämpöpaneeleita pystytään ohjaamaan langattomasti. Ne vaativat toimiakseen WiFi-yhteyden sekä älypuhelinsovelluksen. Näiden avulla kuluttaja pystyy hallitsemaan lämpöpaneelia etänä ja asettamaan lämmityksen päälle, vaikkei olisi paikan päällä. Lämpöpaneeleita voi asentaa useampaan eri kohteeseen, kuten mökki ja koti, ja ohjaamaan kaikkia kohteita sovelluksen avulla. Lämpöpaneelit saattavat sisältää lisäominaisuuksia, kuten toiminnon, jonka avulla lämpöpaneeli tunnistaa, onko kohde tyhjänä ja laskee lämpötilaa, sekä tunnistaa, jos huoneen lämpötila laskee nopeasti (esimerkiksi ikkunan ollessa auki) ja sammuttaa lämmityksen hetkellisesti. Näin säästää kuluttajan lämmityskustannuksissa. (Mill AV600WiFi n.d.)

Puhelinjärjestelmä

Järjestelmään kuuluu esimerkiksi videokuvallinen sekä äänellinen ovikello ja soittajan tunnistus (Product categories 2019). Älyovikellon avulla pystytään tarkastamaan oven takana olevia henkilöitä videokuvasta. Ovikello pitää sisällään myös kaksisuuntaisen puhejärjestelmän ja vaatii toimiakseen WiFi-yhteyden. (Video Doorbell Pro n.d.)

Kodinkoneet

Kodinkoneilla tarkoitetaan jotain konetta, joka suorittaa jotakin kotitaloustyötä liittyen esimerkiksi siivoukseen tai ruuanlaittoon. Näistä kodinkoneista, esimerkiksi uunista, kahvinkeittimestä, jääkaapista, pakastimesta sekä imurista, on kehitetty älyversio. Laitteita pystytään hallitsemaan etänä, ja ne ovat yhdistettynä kodin langattomaan lähiverkkoon. Muitakin älylaitteita löytyy, mm. itkuhälyttimiä sekä leluja.

Kahvinkeittimiä löytyy mm. kalusteisiin upotettavia (ks. kuvio 2). Ne vaativat toimiakseen langattoman verkkoyhteyden ja älypuhelimen tai tablettitietokoneen. Sovelluksen avulla pystytään asettamaan kahvinkeitin keittämään kahvia etänä. (Serie 8 Kalustepeitteinen kahviautomaatti 2018.)

Kuvio 2. Kalusteisiin upotettava kahvinkeitin (Serie 8 Kalustepeitteinen kahviautomaatti)

Höyryuuni sisältää sisäänrakennetun sensorin ja lämpömittarin, joiden avulla varmistetaan paras lopputulos. Uunin päälle laittamista ja lämpötilaa pystytään hallitsemaan etänä älypuhelinsovelluksen ja verkkoyhteyden avulla. (Serie 8 Kompakti höyryuuni 2018.)

Jääkaappi vaatii verkkoyhteyttä, mikäli jääkaapissa huomataan vikaa ja näin valmistajan tuki pystyy etänä tarkastamaan mahdollisen vian syyn ja antamaan korjaus apua. Älyjääkaapit usein sisältävät erilaisia toimintoja kuten jään ennaltaehkäikäisyyn ja kosteuden sekä lämpötilan hallitsemiseen. (Serie 6 Jääkaappipakastin 2018.)

Robotti-imuri toimii WiFi-yhteyden sekä älypuhelinsovelluksen avulla. Imuria pystytään hallitsemaan etänä ja asettamaan imurointi päälle poissa ollessa. Imuria pystytään hallitsemaan myös IFTTT (If This, Then That) -sovelluksen avulla, jolloin voi luoda tapahtumasarjoja, jotka toimivat automaattisesti. Esimerkiksi pysäyttämään imuri, kun puhelin soi tai henkilö poistuu talosta. Kun akku tyhjentyy, imuri palaa automaattisesti latausasemalle ja aloittaa imuroinnin, kun tunnistaa, että akku täysi. (iRobot Roomba 980 käyttöohje 2019.)

3.3 IoT-laitteiden tietoturva

3.3.1 Yleistä

Mikään verkko ei ole täysin varma, eikä mikään verkko ole turvassa heikkouksilta. Jokainen IoT-kerros ja -laite on paljaana erilaisille uhkille. Perinteisissä verkoissa käytettäviä suojaus- ja palautumisjärjestelmiä ei voida hyödyntää IoT-kokonaisuudessa tämän yhdistettävyyden vuoksi. Hyökkäysten sekä uhkien moninkertaistuminen sekä monimutkaisemmat olomuodot ovat aiheuttaneet suuremman tarpeen paneutua tietoturvaan ja suojausmekanismeihin yhä enemmän. IoT-laitteilla on usein hyvin pieni sisäänrakennettu muisti ja prosessori, jolloin datan tallentamisessa hyödynnetään pilvipalveluita. (Hu 2016, 4-8; Rasmussen 2018.)

Jokainen verkkoon kytketty laite antaa uuden rajapinnan ulkopuoliselle hyökkääjälle. Päästyään yhteen laitteeseen ja sitä kautta sisäverkkoon on hyökkääjällä helppo pääsy saastuttaa muita kodin verkkoon kytkettyjä laitteita tai murtautua uhrin tietokoneelle ja anastaa tärkeitä tietoja. Yhden laitteen kautta on myös mahdollista saastuttaa kaikki sisäverkon laitteet. Tästä voi koitua paljon harmia uhrille. Laitteet, joita hallitaan suoraan internetin kautta, ovat suurimmassa vaarassa, esimerkiksi tulostimet tai NAS-palvelimet (*Network-Attached Storage)*. NAS-palvelin on verkkoon kytketty tallennustila, joka sisältää yhden tai useamman kovalevyn, ja sitä voidaan hallita suoraan selaimen kautta (NAS 2019). Riskin aiheuttajana on mm. kuluttajien jättämät oletussalasanat sekä laitevalmistajien viive korjata huomattuja tietoturva-aukkoja. (Hu 2016, 4-8; Rasmussen 2018.)

Vaikka IoT-laitteisiin kohdistuvat hyökkäykset eivät ole käyttäjälle välttämättä yhtä näkyviä kuin kiristysohjelmat, voivat ne kuitenkin viedä laitteen suorituskykyä sekä hidastaa verkkoyhteyksiä. Suurimmilla laitevalmistajilla on usein paremmat suojaukset kuin pienemmillä yrityksillä. Nämä yritykset ovat saaneet apua niin kutsutuilta eettisiltä hakkereilta, jotka yrittävät hakkeroida laitevalmistajien laitteita tunnistaakseen heikkoudet. (Älylaitteiden yleistyminen avaa kodit yllättäville riskeille 2019.)

3.3.2 Haavoittuvuuksia

American Consumer Instituten vuonna 2018 tehdyn tutkimuksen mukaan, jopa yli 80% reitittimistä sisältää tietoturva-aukkoja ja on alttiita haavoittuvuuksille ja hyökkäyksille. Tutkimuksessa tutkittiin 186 WiFi-reititintä 13:lta eri valmistajalta, kuten Linksys, Belkin, D-Link ja Netgear. Hakkerit voivat kaapata reitittimen kuluttajan tietämättä. Tällöin käytetään usein DNS-hijacking nimistä menetelmää, jossa verkkoliikenne ohjataan väärälle sivustolle, jonka kuluttaja luulee oikeaksi ja asettaa luotto- sekä käyttäjätietoja hakkerin kerättäväksi. F-Securen tunnistamista haavoittuvuuksista IoT-laiteille lähes 87 % perustui oletussalasanojen tai heikkojen tunnusten käyttämiseen ja paikkaamattomiin ohjelmistoihin. Samana vuonna F-Securen Honeypot palvelimien havaitsemista hyökkäyksistä 59 % kohdistui Telnet-protokollaan. Tähän vaikuttaa Mirai-haittasovelluksen leviäminen. (Spring 2018; Älylaitteiden yleistyminen avaa kodit yllättäville riskeille 2019.)

CSO-sivusto (2019) listasi 10 yleisintä haavoittuvuutta IoT-laitteissa:

1. Epäluotettava web-rajapinta
2. Puutteellinen käyttäjän todennus ja valtuutus
3. Epäluotettavat verkkopalvelut
4. Liikenteen salauksen puutteellisuus
5. Yksityisyys
6. Epäluotettava pilvi-rajapinta
7. Epäluotettava sovellus-rajapinta
8. Puutteellinen tietoturvakonfigurointi
9. Epäluotettava ohjelmisto
10. Huono fyysinen turvallisuus (Pal 2019.)

Epäluotettava webrajapinta

Web-rajapinta IoT-laitteissa sallii käyttäjän käyttää laitetta verkon välityksellä. Hyökkääjä saattaa hyödyntää rajapintaa luvattomaan pääsyyn laitteelle. Tietoturva-aukot, jotka mahdollisesti antavat hakkerille pääsyn, ovat heikot oletustunnukset, tunnus-

ten näkyminen verkkoliikenteessä, cros-site scripting (XSS), tietokanta injektio (eng. *SQL-Injection*), account enumeration (väärän kirjautumisyrityksen jälkeen sovellus palauttaa tiedon, onko käyttäjätunnus vai salasana väärä), sessioidenhallinta ja heikot käyttäjätunnuksen lukitsemisasetukset (esimerkiksi vääriä kirjautumisyrityksiä voi olla useita). (Pal 2019.)

Puutteellinen käyttäjän todennus ja valtuutus

Virheellisen käyttäjän valtuutuksen ansiosta, käyttäjä voi saada korkeammat toimintaoikeudet, kuin sallittu. Tietoturva-aukot, jotka vaikuttavat käyttäjän todennukseen ja valtuutukseen tulevat heikosta salasanasta, heikosti suojatusta tunnuksesta, kaksoistodennuksen puutteesta, epäluotettavasta salasanan palauttamisjärjestelmästä, käyttöoikeuksien eskaloinnista sekä roolikohtaisen pääsyhallinan (eng. *access control*) puutteesta. (Mt.)

Epäluotettavat verkkopalvelut

Verkkopalvelut mahdollistavat pääsyn IoT-laitteelle. Verkkopalveluiden heikkoudet saattavat tarjota tunkeutujalle luvattoman pääsyn laitteelle tai siihen liittyviin tietoihin. Tietoturva-aukot, jotka liittyvät verkkopalveluiden heikkouksiin, ovat puskurin ylivuotovirhe (eng. *Buffer overflow*), avoimet portit Universal Plug and Play (UPnP) kautta, jotkin UDP palvelut ja palvelunestohyökkäykset (eng. *Denial of Service*). (Mt.)

Liikenteen salauksen puutteellisuus

Data saattaa liikkua IoT-laitteiden välillä salaamattomana. Tämä voi johtaa luvattomaan datan vakoiluun ja tallentamiseen myöhempää käyttöä varten. Salaamattomat palvelut Internetin tai lähiverkon välityksellä, huonosti toteutettu tai väärin konfiguroitu tietoverkonsalausprotokolla SSL/TLS voivat johtaa tietoturvaongelmiin liikenteen salauksen suhteen. (Mt.)

Yksityisyys

Yksityisyys liittyy datan keräämiseen ja säilyttämiseen; mitä dataa käyttäjistä kerätään ja miten sitä säilytetään. Datan säilyttäminen luo tietoturva-aukkoja, sillä sitä ei välttämättä suojata kunnolla. Käyttäjistä saatetaan kerätä tietoja, mitkä eivät liity laitteen toimintaan ja saattavat sisältää henkilökohtaista tietoa. (Mt.)

Epäluotettavat pilvipalveluiden- ja sovellusrajapinnat

Pilvipalveluiden- ja sovellusrajapintojen liikenne saattaa kulkea salaamattomana ja vahvaa autentikointia ei ole käytetty. Tämä saattaa johtaa hakkerin pääsyyn laitteelle tai siihen kuuluvalle datalle. (Mt.)

Puutteellinen tietoturvakonfigurointi

Puutteellista tietoturvakonfigurointia esiintyy, kun laitteella ei ole tietoturvamonitorointia tai kirjautumista, normaalit käyttäjät eivät ole eristetty ylläpitäjistä tai, kun vahvaa salasanaa ei vaadita. Mahdollisista tietoturvatapahtumista tulisi käyttäjää informoida. (Mt.)

Epäluotettava ohjelmisto

Mikäli laitteen ohjelmistoa ei pystytä päivittämään, luo se tietoturvariskin. Kun ohjelmistosta löydetään tietoturva-aukkoja, tulisi ohjelmisto olla mahdollista päivittää ja päivitysten lataaminen verkosta tulisi olla suojattua. Ohjelmisto voi olla myös epäluotettava, sen sisältäessä kovakoodattua dataa, kuten pääsytietoja. Kovakoodattuja tietoja ei pysty muuttamaan. Näin ollen, mikäli kovakoodattua tietoa pääsee julki, kuten kirjautumistietoja, on hakkereilla tilaisuus hyödyntää niitä. Tietoturva-aukkoja ilmenee, kun päivityksiä ei ole mahdollista asentaa, päivitykset ladataan salaamattomana, päivitystiedosto ei ole salattu tai todennettu ja ohjelmisto sisältää arkaluonteista tietoa. (Mt.)

Huono fyysinen turvallisuus

Fyysisenä heikkoutena voidaan todeta olevan sisäänrakennettu osa muistille. Mikäli hakkeri pääsee fyysisesti käsiksi laitteen muistiin (purkamalla laite), on hänellä pääsy kaikkiin tallennettuihin tiedostoihin. Laitteen ulkoisia portteja (kuten USB) voidaan väärinkäyttää laitteelle pääsyyn hyödyntämällä konfigurointiin ja ylläpitoon tarkoitettuja toimintoja. Tämä voi johtaa luvattomaan pääsyyn laitteelle ja sen tiedostoihin. (Mt.)

3.3.3 Protokollat ja laitteiden avoimet portit

Tieto liikkuu verkkojen ja laitteiden välillä IP-osoitteiden sekä porttien mukaan käyttäen UDP- tai TCP-protokollaa. Jokaisella protokollalla sekä portilla on heikkouksia, ja jokainen portti on potentiaalisessa riskissä hyökkäykselle. Jokaisessa portissa ja niissä toimivissa palveluissa on omat riskinsä. Riskit riippuvat palvelun versiosta, onko konfigurointi tehty oikein sekä onko mahdollinen salasana riittävän vahva. Jokainen avoin portti on mahdollinen kohde. Esimerkiksi portti 21 yhdistää FTP-palvelimet internettiin. FTP-palvelimista on löydetty monia heikkouksia, kuten tunnistamaton kirjautuminen ja XSS (*Cross-site scripting*) sekä Telnet portissa 23 ei salaa tietoa millään tavalla. (Geer 2017.)

Jotkin portit toimivat loistavina sisäänpääsyinä hakkereille ja jotkin portit toimivat taas ulospääsynä, esimerkiksi DNS portti 53. Rikollisten päästyä verkkoon ja saadakseen haluamansa data ulos sieltä, he muuttavat datan DNS-liikenteeksi ja ohjaavat datan omaan DNS-palvelimeen kääntämään se takaisin alkuperäiseen muotoon. DNS on harvoin monitoroitu ja filtteröity ja näin ollen mahdollinen hyödyntää tässä tarkoituksessa. (Mt.)

HTTP-porttia 80 käytetään siirtämään web-liikennettä nettisivuilta. HTTP-liikenteestä on löydettynä mukana mm. SQL-injektioita ja cross-site pyyntöjen väärennöksiä. SQL-injektio on tietokannan saastutustekniikka, jossa syötteitä asetetaan nettisivujen kautta (SQL Injection n.d). Web-liikenne kulkee myös porteissa 8080, 8088 sekä 8888. Trojalaisia ja matoja on ujutettu sisälle käyttäen porttia 1080, joka on suunni-

teltu socketeille. Moni rikollinen valitsee portin, joka on helppo muistaa, kuten samat numerot peräkkäin 666 tai numerot järjestyksessä 6789. Porttia 22 käytetään SSH-yhteyksille, joka tarjoaa etäyhteyden laitteiden välille. Sen turvallisuus nojautuu paljolti riittävään haastavaan salasanaan. Portteja on yhteensä 65 535 TCP:lle sekä toiset 65 535 UDP:lle. Kaikki portit eivät ole kuitenkaan aina käytössä ja turhia portteja ei kannata pitää avoinna. (Mt.)

3.3.4 IoT-laitteiden virheitä

Tietoturvan voidaan kuvata olevan järjestelmän kyky pysyä normitilassaan, vaikka rikollismielistä toimintaa yritetään suorittaa järjestelmään. Usein onnistunut hyökkäys nojaa järjestelmän suunnittelu- tai toteutusvirheeseen (jokin virhe, joka sallii ulkopuolisen päästä sisälle järjestelmään). Nämä virheet monesti toistavat samanlaista kaavaa. Tyypillisiä virheitä löytyy koodista, autentikoinnista ja kryptografiasta ja virhe saattaa muodostua liiasta tekemisestä. (Smith 2017, 71.)

Ohjelmistomaailma on täynnä virheitä ja bugeja koodissa, mitkä auttavat laitteiden saastuttamisessa. Eräässä tilanteessa kuluttajille lähetettiin vartalokameroita, jotka sisälsivät valmiiksi haittaohjelmia, jotka pystyivät saastuttamaan kytketyn järjestelmän. On myös raportoitu tilanne, jossa älylamppu paloi ja lähetti niin monta ilmoitusta asiasta, että kuluttajan koko älykodin langatonverkko kaatui. (Mts. 74.)

On tärkeää, että järjestelmä varmistaa, kuka on aikeissa lähettää päivityksen, muuttaa konfiguraatiota tai muuten toimia kaikilla oikeuksilla. IoT sisältää joitain näkökulmia, joissa autentikointi voi muuttua kriittiseksi. Tehokas autentikointi vaikuttaa hallintaan; mitä isompi ja epäjärjestelmällisempi kokonaisuus, sen vaikeampi sitä on hallita. On huomattu joitain autentikoinnin ongelmakohtia IoT-maailmassa: palvelu ei välttämättä vaadi ollenkaan autentikointia, palvelu käyttää oletuskäyttäjätunnuksia, palvelu käyttää pysyviä salasanoja, joita ei voida muuttaa tai palvelussa on vaikea hallita oikeuksia. (Mts. 75.)

Suurin turvallisuusvirhe on jättää autentikointi kokonaan pois. Tätä ei joko ole osattu ajatella ollenkaan turvallisuuden kannalta, tai suunnittelijalla oli näkemys, jossa teo-

reettisesti väärinkäyttäjiltä estettiin pääsy palveluun. CAN-väylän (*Controller Area Network*) keskus moderneissa autoissa sisältää komponentin, joka odottaa käskyjä, mutta ei missään vaiheessa varmista käskyjen lähettäjää. Esimerkiksi moottorin kontrollointiyksikön (eng. *Engine Control Unit*, ECU) kuuluisi lähettää jarruille toimintoja, mutta mikä vain CAN-väylässä voisi näin tehdä. CAN Bus -järjestelmässä kaikki moduulit yhdistetään keskitetysti, jotta ne voivat toimia yhdessä tehokkaasti (Unterstanding CAN Bus and CAN Loggers 2019). Esimerkkinä on raportoitu tilanne, jossa auton CD-soittimeen on saastutettu haittaohjelma, jonka avulla pysyttiin huijaamaan komentoja CAN-väylälle. (Mts. 75-76.)

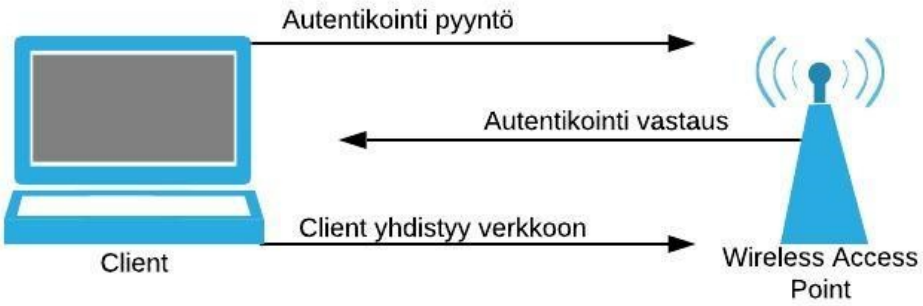
Järjestelmän rajapintaan voidaan asettaa enemmän funktioita, kuin se edes tarvitsisi. Ylimääräiset funktiot voivat tarjota jopa keinon rikolliselle ottaa hallinta järjestelmään. Yleisimpiä keinoja on syöttää rikollismielisesti kehitettyjä syötteitä, jotka eivät vastaa sääntöjä, joita ohjelmoija on tarkoittanut sopivaksi syötteeksi, mutta jotka järjestelmä kuitenkin hyväksyy ja näin huijaa sitä. Tätä käytetään esimerkiksi Buffer Overflow -hyökkäyksessä. Siinä järjestelmä odottaa merkkijonoa käyttäjältä ja kopioi sen puskurin pinoon, mutta ei koskaan tarkista, sopiiko jono itse asiassa puskuriin. Hyökkääjä voi esimerkiksi syöttää pitkän merkkijonon, johon on sisällytetty suoritettavaa koodia, ja ylikirjoittaa palautusosoitteen kohdan pinossa itse asetetulla osoitteella koodissa. Näin järjestelmä rupeaa suorittamaan syötettyä koodia. Tämän kaltaisia hyökkäyksiä on versioitu ja muunneltu moneen otteeseen. Ne ovat lyöneet itsensä läpi myös jo IoT-maailmaan. (Mts. 72.)

3.3.5 Bluetooth ja WiFi-yhteyksien eroavaisuudet

Bluetooth ja WiFi-teknologiat tarjoavat langatonta tiedonsiirtoa laitteiden välillä. Bluetooth on suunniteltu yhdistämään laitteet lyhyen kantaman päässä (noin 10m), kun taas WiFi-yhteydellä kantama on paljon pidempi (noin 100m) ja tiedonsiirto nopeampaa sekä käyttäjämäärä on WiFi-yhteydellä suurempi. Bluetooth käyttää yhteyteen 2.4 GHz ja 2.438 GHz taajuuksia, WiFi käyttää 2.4 GHz ja 5 GHz taajuuksia. (Difference Between Bluetooth and Wifi 2017.)

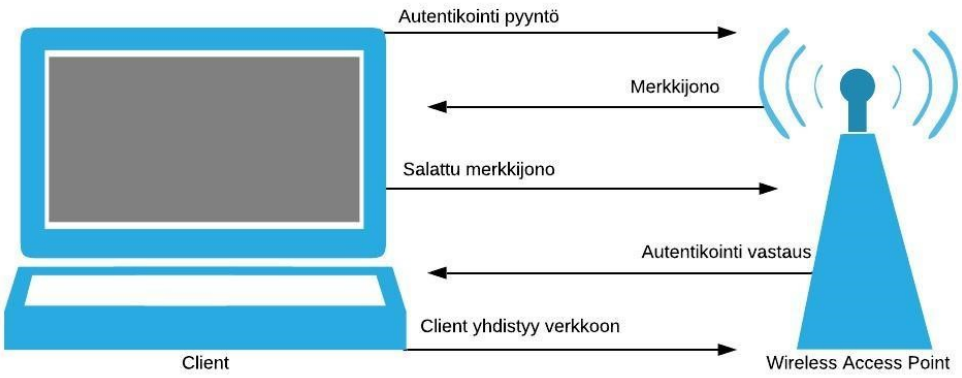
Teknologioiden erot näkyvät myös turvallisuudessa. Bluetooth käyttää 128 bittistä satunnaista numeroa, laitteen 48-bittistä MAC-osoitetta, 128 bittistä kaksoisavain (eng. *two keys*) autentikointia ja 8-128 bittistä salausta datan turvalliseen siirtämiseen. Teknologia sisältää kolme tietoturvakerrosta: ei turvattu (eng. *non-secure*), palvelu (eng. *service* layer) ja yhteys (eng. *link layer*). (Mt.)

WiFi-teknologia perustuu IEEE 802.11 standardiin, joka sisältää ehtoja autentikointiin ja yksityisyyteen. Standardi tukee kahta autentikointi menetelmää: open system (OPA) ja shared key (SKA). Open system autentikoinnissa client (asiakasohjelma) lähettää autentikointi pyynnön langattomalle liityntäpisteelle (eng. *Access point,* AP), joka luo autentikointikoodin (satunnainen koodi, joka tarkoitettu vain kyseiselle sessiolle). Tämän jälkeen client hyväksyy autentikointikoodin ja liittyy verkkoon (ks. kuvio 3). (Difference Between Bluetooth and Wifi 2017; Rouse 2008.)



Kuvio 3. Open System autentikointi

Shared Key autentikoinnissa hyödynnetään salattua avainta. Clientin avain tulee täsmätä AP:n avaimen kanssa. Client lähettää autentikointi pyynnön. AP vastaa lähettämällä luodun merkkijonon. Client salaa vastaanotetun merkkijonon avaimella ja lähettää viestin takaisin AP:lle. AP purkaa salauksen ja vertaa alkuperäistä merkkijonoa purettuun jonoon. Mikäli tulokset täsmäävät toisiinsa, AP lähettää clientille autentikointikoodin liittyäkseen verkkoon. Client hyväksyy koodin ja liittyy verkkoon (ks. kuvio 4). (Rouse 2012.)



Kuvio 4. Shared Key autentikointi

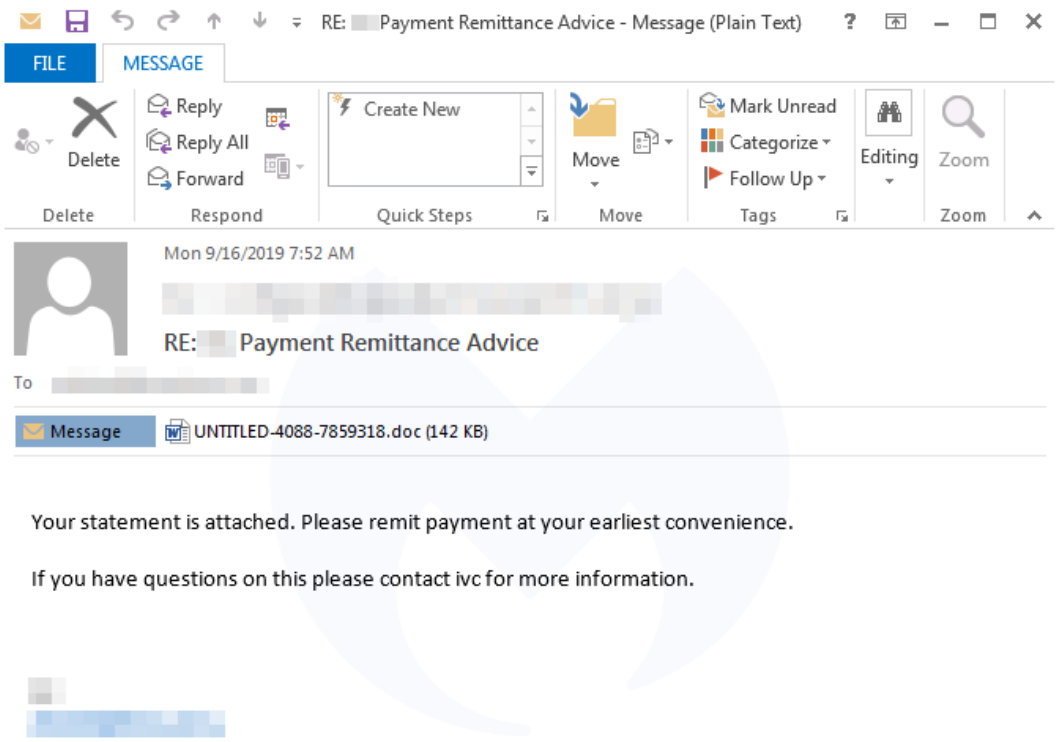
3.3.6 Tunnettuja bottiverkkoja

Vuonna 2016 maailmanlaajuisessa Mirai-bottiverkossa käytettiin tuhansien suomalaisten modeemeja sekä mm. valvontakameroita. Suomessa havaittiin noin 16 000 laitteen saastuneen. Bottiverkon haittaohjelma etsi verkosta laitteen internettiin avoimia palveluja ja murtautui niihin kokeilemalla erilaisia tunnus ja salasana -yhdistelmiä. Ohjelman lähdekoodi julkaistiin aikaisemmin jo netissä ja oli varmaa jo tuolloin, että uusia versioita tullaan näkemään. Vuoden 2016 hyökkäyksessä ohjelma etsi verkosta laitteita, joiden etähallinta oli toteutettu TCP/7547 portissa ja tarkoituksena oli yrittää ottaa laite haltuun. Mirai-bottiverkkoa käytettiin palvelunestohyökkäykseen. Vuonna 2018 F-Securen tunnistamien lukuisten IoT-laitteisiin kohdistuneiden hyökkäysten taustalla oli tavoite tehdä kryptovaluuttaa. Nämä hyökkäykset perustuivat usein Mirai-haittasovelluksen lähdekoodiin. (Mirai-bottiverkko on ottanut haltuunsa tuhansien suomalaisten modeemeja 2016; Älylaitteiden yleistyminen avaa kodit yllättäville riskeille 2019.)

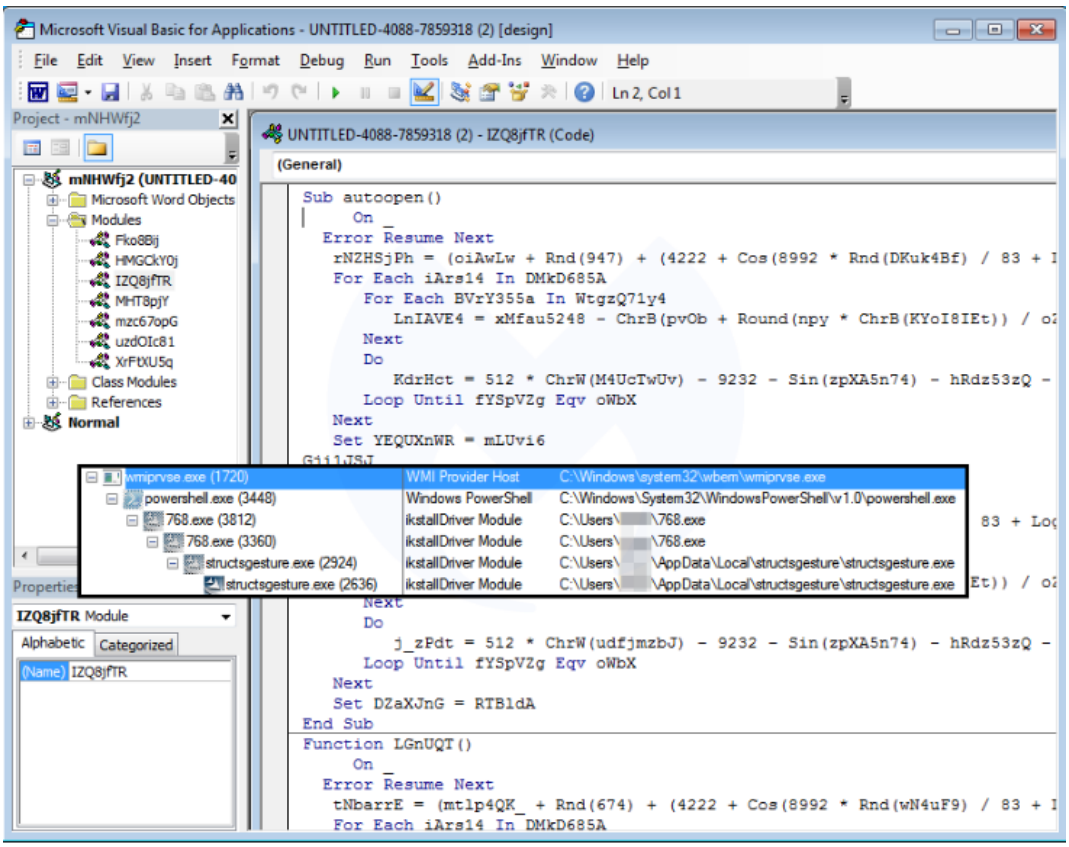
Echobot haittaohjelma havaittiin vuonna 2019 toukokuussa. Sen tarkoituksena on saastuttaa IoT-laitteita ja saada etähallinta erilaisiin laitteisiin ja kokoamaan niistä bottiverkko. Sen on tunnistettu hyödyntävän yli 50 erilaista haavoittuvuutta. Ec-

hobotin on löydetty käyttävän 59 erilaista RCE (*Remote Code Execution*) toteutusta levitäkseen. Echobot-haittaohjelma on muunnelma Mirai-bottiverkosta, jonka koodi on julkisesti saatavilla. (Ilascu 2019; IoT-laitteista kerätään uutta bottiverkkoa – Mirain uusi versio 2019.)

Emotet-bottiverkko hyödyntää levitäkseen roskaposteja, joissa on liitteenä haittaohjelmia sisältäviä dokumentteja. Kuviosta 5 näkee esimerkki sähköpostin. Uhri avaa sähköpostiliitteen, joka sisältää macron, jonka PowerShell komento yrittää aloittaa Emotetin lataamisen, ja näin aloittaa saastuttamisprosessin. Kuviossa 6 on esimerkki dokumentin macron sisällöstä. Toisena vaihtoehtona liitteenä oleva dokumentti sisältää scriptin, joka ladatessa asentaa Emotetin ja alkaa levittämään itseään toisiin laitteisiin samassa verkossa. (Threat Intelligence Team 2019.)



Kuvio 5. Emotet sähköpostiviesti (Threat Intelligence Team 2019)



Kuvio 6. Emotet macro (Threat Intelligence Team 2019)

3.3.7 Haasteita

Mikrobitti.fi -sivuston (2019) artikkelissa haastateltiin Securen johtavaa tutkijaa Jarno Niemelää. Niemelä kommentoi haastattelussa, ettei kotitalouksiin tehtyjä hyökkäyksiä tehdä rahan perässä, kuten yrityksille tehdyt palvelunestohyökkäykset rahankiristys tarkoituksessa. Kotitalouksiin kohdistuvat hyökkäykset ilmenevät usein tapana vallata laitteen resurssit johonkin muuhun käyttötarkoitukseen. Niemelä kommentoi myös kysymystä, miksi nykypäivän IoT-laitteilla on niin huono tietoturva. Hänen mukaansa kysymys on näkemyseroista. Yritykset tarjoavat fyysisiä laitteita, pesukoneita, jääkaappeja ja muita kodinkoneita ja saaden lisämyyntiä uusilla nykyaikaisilla lisäominaisuuksilla, eivätkä ajattele, että ovat valmistamassa tuotetta, joka sisältää tietokoneen. Useat isot yritykset, joilla on paljon mainetta menetettävän, huolehtivat paremmin tietoturvasta älylaitteilla. IoT-laitteiden kohdalla usein tuottajat sekä käyt-

täjät priorisoivat käyttöominaisuudet ja näiden helppouden ylitse tietoturvan ja näin ollen esimerkiksi älykamerat eivät usein sisällä riittävästi muistia ja tehoa suorittaakseen tietoturvatoimintoja (Ahaskar 2019). (Älykkäät kodinkoneet verkkorikollisten tähtäimessä 2019.)

Rikolliset murtavat laitteita, joissa on heikot käyttäjätunnukset, paikkaamattomat ohjelmistot tai muita yleisiä haavoittuvuuksia tai kohdistavat Brute Force -hyökkäyksen laitteelle oletuskäyttäjätunnuksilla. Brute Force -hyökkäyksessä kokeillaan eri salasanoja tai salausavaimia oikean salasanan löytämiseksi. Hakkerit jakavat löydettyjä käyttäjätunnuksia ja salasanoja julkisesti verkossa. Tunnukset ovat kaikkien löydettävissä ja hakkerit pystyvät hyödyntämään samaa käyttäjätunnusta ja sille merkattua salasanaa eri paikoissa, sillä erittäin moni käyttää samoja salasanoja eri kirjautumisalustalle, laitteelle tai nettisivuille. Kirjautumistietoja on saatavilla yli 8,2 miljardille eri käyttäjätunnukselle. Ja lista lisääntyy varmasti koko ajan. (Wroclawski 2019; Älykkäät kodinkoneet verkkorikollisten tähtäimessä 2019)

Laitteiden lähdekoodeja on julkaistu verkossa, joka on aiheuttanut keinon luoda monimutkaisempia hyökkäyksiä. Kodin älylaitteet muodostavat oman systeeminsä ja yhden laitteen tietoturva vaikuttaa myös muihin laitteisiin. Tietoisuuden lisääntyessä ihmisiä on huolettanut laitteiden salakuunteleminen. On kuitenkin hyvä huomioida, että kannamme koko ajan mukanamme älypuhelinta, jota voidaan samalla tavalla salakuunnella. Joissain tietoturvajärjestelmissä on sisäänrakennettu mikrofoni, jonka kautta pystytään kuuntelemaan käyttäjän toimintaa. (Älykkäät kodinkoneet verkkorikollisten tähtäimessä 2019.)

Kodin televisiot, valvontakamerat ja muut älylaitteet sisältävät suuremman tietoturvariskin kuin tietokoneet ja puhelimet, sillä niitä ei voida samalla tavalla suojata tietoturvaohjelmistoilla. Laitteiden tietoturvan ylläpitäminen muodostuu haastavaksi, sillä uusia haittaohjelmia ja viruksia luodaan koko aika lisää ja niistä rakennetaan yhä monimutkaisempia. (Hyttinen 2018.)

3.3.8 Ohjeita älylaitteiden käyttäjille

Laitteiden valinnassa kannattaa suosia tunnettuja laitevalmistajia, joiden tuotteissa ei ole huomattu puutteita tietoturvassa. Ennen laitteen hankintaa, kannattaa tutustua kuluttajien ja testaajien jakamiin arvioihin internetissä. Tunnettujen laitevalmistajien tuotteissa voidaan usein luottaa siihen, että tuotteisiin on saatavilla uusia päivityksiä. Tuntemattomien laitevalmistajien tuotteille ei välttämättä ole saatavilla päivityksiä korjaamaan havaittuja virheitä. (Rasmussen 2018; Älykkäät kodinkoneet verkkorikollisten tähtäimessä 2019)

Laitteisiin kannattaa asettaa automaattinen päivitys päälle, tai ainakin automaattinen päivitysten etsintä, varmistaakseen aina uusimman päivityksen saamisen mahdollisimman pian. Joissain tapauksissa kannattaa selata laitevalmistajan nettisivuja ja etsiä, onko uusia päivityksiä saatavilla. Laitevalmistajat, joille tietoturva on tärkeää, huolehtivat laitteiden uusista päivityksistä säännöllisesti. Jotkin laitteet automaattisesti päivittävät ohjelmiston, mutta jotkin vaativat päivitysten tarkastuksen käsin. (Rasmussen 2018; Wroclawski 2019.)

Oletussalasanojen vaihtaminen on erittäin tärkeää. Laitevalmistajien asettamat salasanat löytyvät internetistä laitteiden käyttöohjeista, jotka ovat kaikkien saatavilla. Salasanaksi kannattaa valita mahdollisimman vahva salasana. Ei ole suositeltavaa käyttää syntymäpäiviä, nimiä tai muita henkilöiden identifiointia. Nämä tiedot usein löytyvät sosiaalisen median kautta. Tunnettuja salasanoja ei myöskään suositella käytettävän, sillä internetistä löytää valmiita tunnettujen salasanojen listoja, jotka kasvat koko ajan. Salasanassa on hyvä käyttää isoja ja pieniä kirjaimia, erikoismerkkejä, numeroita ja erilaisia satunnaisia lausahduksia. Salasanojen valitsemisessa voi hyödyntää erilaisia salasanojen manageri ohjelmia. Ne tuottavat satunnaisia ja tehokkaita salasanoja ja säilövät niitä suojatussa ympäristössä. Eri kirjautumisalustoille on hyvä käyttää eri salasanoja ja vaihtaa salasanat useasti. Kaksivaiheinen autentikointi varmistaa paremman suojauksen. Siinä lähetetään salasanan lisäksi kerran toimiva koodi, usein jokin numeroyhdistelmä, tekstiviestillä, puhelin soitolla, sähköpostilla tai jollain autentikointi applikaatiolla. Tällöin hakkerin saadessaan salasana selville, täytyy hänen asettaa vielä kertakäyttöinen koodi. Kaikki laitteet eivät tätä kuitenkaan

tarjoa, mutta mikäli se on saatavilla, on siitä hyötyä turvallisuuden takaamisessa. (Rasmussen 2018; Wroclawski 2019.)

Laitteet, jotka eivät välttämättä tarvitse verkkoyhteyttä, kannattaa eristää verkosta. IoT-laitteille voi luoda myös oman sisäverkon ja eristää se muista laitteista, kuten tietokoneista. Riskiä voi myös vähentää asettamalla kotiin palomuurin ja älylaitteet toimimaan sen takan. MAC-osoitteiden filtteröinti reitittimellä tai palomuurilla on hyödyksi estämään tuntemattomien pääsyn laitteelle. (Ahaskar 2019; Rasmussen 2018.)

Tietokoneen virusturvasta huolehtiminen on tärkeää. Tietokoneella selataan paljon internetiä ja sieltä voi huomaamatta tulla ladatuksi haittaohjelmia tietokoneelle, jotka leviävät muualle verkkoon. Viestintävirasto ja lehdet ilmoittavat mahdollisista bottiverkko-löydöistä. Ohjeistuksessa saatetaan esimerkiksi kehottaa sulkemaan jokin tietty portti laitteelta. Jotkin kamerat saattavat näyttää tietoja kamerasta, ottaessa kuvan kameran lähettämästä live toistosta. Tämä kannattaa huomioida, mikäli jakaa arvosteluja kamerasta netistä ja miettiä tarkkaan, minkälaisen kuvan jakaa muiden nähtäväksi.

Marraskuussa 2019 Liikenne- ja viestintävirasto Traficom julkaisi Tietoturvamerkin, jonka tarkoituksena on taata kuluttajille, että laitteen tietoturvan perusominaisuudet ovat kunnossa. Laitteen läpäistyä EN 303 645-standardiin perustuvan sertifiointiprosessin, myönnetään sille Tietoturvamerkki. Kuluttajien on jatkossa helpompi seurata tarkastettuja laitteita ja perusominaisuuksilta tietoturvallisia laitteita. (Suomi aloittaa älylaitteiden turvallisuuden varmistamisen ensimmäisenä Euroopassa – uusi Tietoturvamerkki auttaa kuluttajia tekemään turvallisempia kodin älylaitehankintoja 2019.)

3.4 Sisäverkko

3.4.1 Yleistä

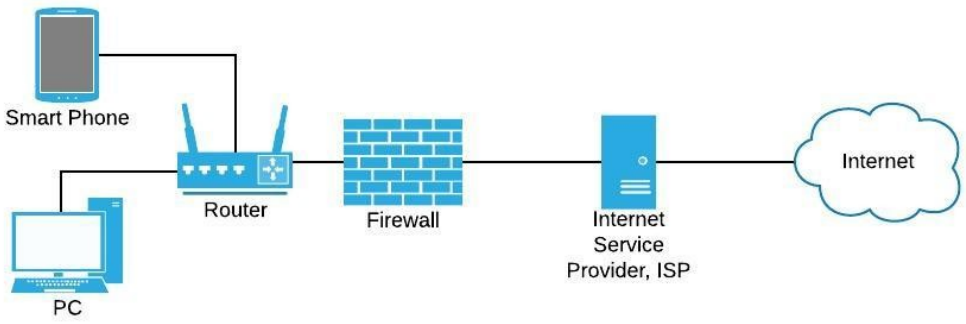
Sisäverkko eli lähiverkko (eng. *Local Area Network*, LAN) on tietoverkko rajatun alueen sisällä. Tällä tarkoitetaan esimerkiksi omakotitalon omaa sisäistä verkkoa, kerrostalohuoneiston verkkoa tai yrityksen sisäistä verkkoa. Sisäverkko yrityksen ja kodin välillä voi erota huomattavasti. Yrityksen verkkoon voi kuulua kymmeniä laitteita, kun taas kodin sisäverkko voi koostua vain muutamasta laitteesta. Lähiverkoksi laskettaisiin organisaation toimipisteiden verkot, sillä verkkoarkkitehtuurisesti nämä ovat yhtä ja samaa lähiverkkoa. Sisäverkolla kuitenkin tarkoitetaan sisäistä tietoverkkoa ja kotitalouksissa puhutaan kodin seinien sisäisestä verkkoalueesta. Tämä alue koostuu modeemista/reitittimestä, sisäverkon kaapeloinnista, langattomasta verkosta sekä laitteista. (Elektronikkari 2017; Koivunen 2010.)

3.4.2 Sisäverkon turvallisuus ja suojaus

Kotiverkkoon yhdistetyt laitteet ovat mahdollista suojata hyödyntämällä tietoturvareitititintä ja asettamalla kodin laitteet reitittimen taakse (Älylaitteiden yleistyminen avaa kodit yllättäville riskeille 2019). Tietoturvareititin suojaa kuluttajaa haitalliselta liikenteeltä. Ne toimivat normaalin reitittimen tavoin, mutta pitävät sisällään erilaisia suojia. Ne sisältävät osoitteenmuunnoksen (eng. *Network Address Translation,* NAT), mikä torjuu internetistä sisäverkkoon otettuja yhteyksiä. Mikäli yhteys on alun perin avattu sisäverkosta, esimerkiksi kun käyttäjä klikkaa haitallista linkkiä, ei NAT:lla ole enää turvallisuuden kannalta hyötyä. Laitevalmistajat pitävät usein yllä listaa haitallisista nettisivuista, jonka reititin säännöllisesti lataa pilvestä. Kuluttajan yrittäessä siirtyä listasta löytyvälle nettisivulle, sivun lataaminen estetään. Laitteet tarkkailevat kuluttajien verkkoliikennettä ja etsivät tunnettuja haittaohjelmia. Reitittimen tietoturvapalvelu saattaa olla kuitenkin erikseen maksullista. (Riikonen 2018.)

Palomuurin tarkoituksena on ehkäistä sisäverkkoon ja sisäverkon laitteisiin haitallista pääsyä ja luoda keskitetty turvallisuudenhallinta. Palomuureja on fyysisinä laitteina, mutta se voi toimia myös ohjelmistona. Palomuurilla rajoitetaan sisäverkosta lähtevää tai sisäverkkoon pääsevää liikennettä erilaisilla säännöillä. Sillä saadaan rajoitet-

tua myös ohjelmia, joilla on lupa käyttää verkkoyhteyttä. Ohjelmistopalomuureja löytyy ilmaisina sekä maksullisina. Ne usein sisältävät jo valmiiksi virustorjuntaohjelman. Ohjelmistopalomuurin pystyy lataamaan tietokoneelle. Modeemit sisältävät usein palomuurin oletuksena, mutta nämä ovat heikosti konfiguroitu. Laitepalomuuri asetetaan verkkotopologiassa reitittimen tai modeemin eteen suojaamaan sisäverkkoa (ks. kuvio 7). Palomuurin konfigurointiin olisi hyvä panostaa ja perehtyä ja sallia vain tarvittava liikenne. (Mikä on palomuuri?. 2019.)



Kuvio 7.Verkkotopologia palomuuri

VPN (*Virtual Private Network*) on virtuaalinen erillisverkko. Se salaa kuluttajan yhteyden internetiin. VPN avulla tietoliikenne kryptataan ja varmistetaan, ettei liikennettä pystytä tutkimaan luvatta. Käyttäjän lähettämän salatun datan pystyy ainoastaan vastaanottaja purkamaan. VPN avulla luodaan virtuaalinen tunneli kahden laitteen välillä. Kuviosta 8 näkee verkkotopologia kuvan VPN kanssa. Se salaa käyttäjän IP-osoitteen ja käyttäjän sijaintia ei pystytä paikantamaan. Yleisimpiä protokollia, joita käytetään VPN tunnelin muodostamiseen ovat IPSec (*IP Security Architecture*), PPTP (*Point-To-Point Tunneling Protocol*) tai L2TP (*Layer 2 Tunneling Protocol*). (Beal 2019.)

Kuvio 8. Verkkotopologia VPN

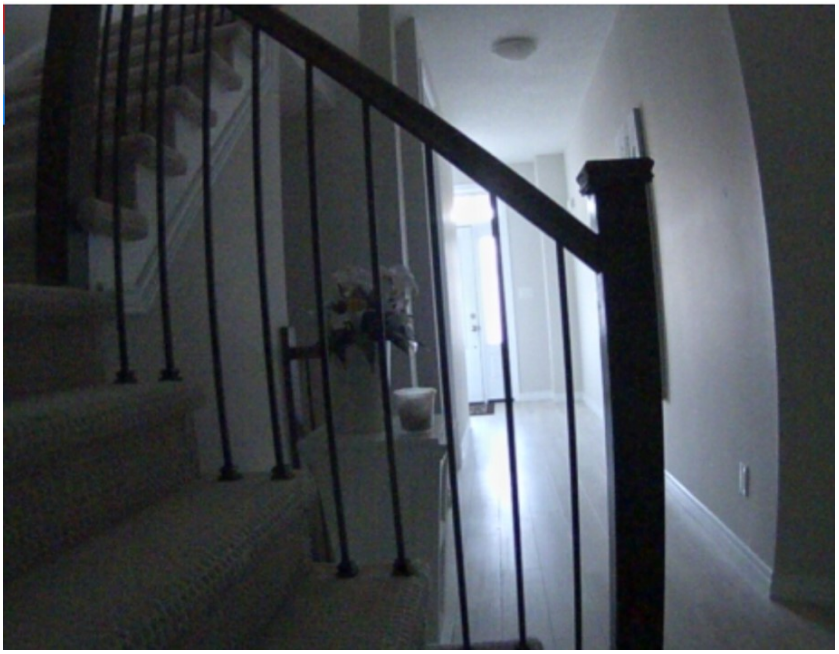
4 IoT-laitteiden väärinkäytöksiä

4.1 Valvontakameroiden suoratoistosivusto

Insecam.org sivusto on kerännyt IP kameroita ympäri maailmaa, jotka eivät vaadi salasanoja. Sivusto näyttää livekuvaa yli sadasta eri maasta ja yli 20 000 kamerasta. Suomesta löytyy tällä hetkellä 62 kameraa ja Jyväskylästä 2. Sivusto ilmoittaa etusivullaan, että kamerat ovat filtteröity, eikä kenenkään yksityisyyttä loukata. Kameran pystyy poistamaan sivustolta sähköpostia laittamalla tai yksinkertaisesti asettamalla kameraan salasanan sekä kameroita pystyy lisäämään sivustolle lähettämällä sähköpostiviestiä ylläpitäjille. Kuviosta 9 näkee kuvakaappauksen kamerasta, joka löytyy Rovaniemeltä 6.11.2019 kello 12:34. Sivusto ei anna yksityisyyden takia tarkkaa osoitetta, mistä kamera löytyy, vaan kartta osoittaa pelkästään kaupunkiin. (Network live IP video cameras directory Insecam.com n.d.)

Kuvio 9. Valvontakamerakuva Rovaniemeltä

Gizmodo-sivuston artikkelin mukaan sivustolta löytyi vuonna 2014 yli 73 000 kameraa ja pelkästään Yhdysvalloista 11 000 (Zhang 2014). Vuonna 2019 sivustolta löytyy Yhdysvalloista 4467 kameraa. Artikkelissa kerrotaan Insecomin käyttäneen oletussalasanoja kameroihin ja sivusto on perustettu näyttämään turvallisuusasetusten tärkeyden kuluttajille (mt). Sivustolla näytetään kuitenkin myös mainoksia, eli sivusto kerää myös mainospalkkioita. Kameran saa helposti pois sivustolta, mutta se kuitenkin vaatii, että kuluttaja tietää kyseisestä sivustosta. Vaikka sivuston mukaan kamerat ovat filtteröityjä, eikä yksityisyyttä loukata, löytyy kameroista myös kotien sisältä livekuvaa. Suurin osa kameroista näyttää olevan kaduilta, parkkipaikoilta ja muilta julkisilta paikoilta, mutta esimerkiksi kuviosta 10 näkee kuvakaappauksen kanadalaisen asunnon sisältä 6.11.2019. Kuluttajat ovat asettaneet kamerat omaa turvallisuutta varten. Kamerat ovat takaamassa, ettei asuntoihin tunkeuduttaisi. Vaikka sivustolta löytyvä kamera ei osoittaisi kodin sisälle vaan pihaan, tämä on oiva keino rikollisille hyödyntää videokuvaa. Kuvasta näkee selkeästi, milloin asukas poistuu talosta ja näin ollen pystyy ajoittamaan murtautumisen tähän hetkeen.



Kuvio 10. Valvontakamerakuva asunnosta

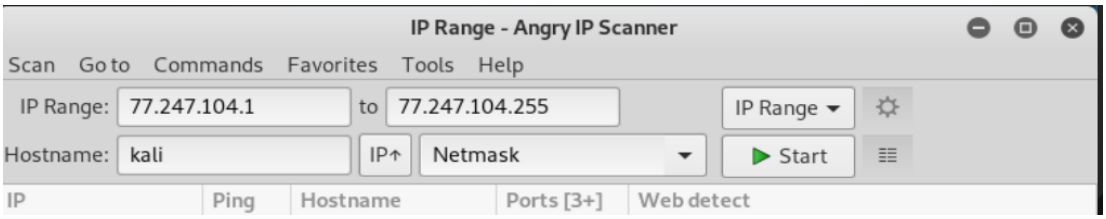
Toinen samantyylinen sivusto löytyy osoitteesta opentopia.com. Sivusto kertoo nettikameroiden löytyneen automaattisesti ja kamerat ovat jollain tavalla saatavilla julkisesti verkosta. Sivustolla on saatavilla yhteensä 642 kameraa, joista osa löytyy myös Suomesta. (Opentopia 2011.)

4.2 Valvontakameroiden skannaaminen verkosta

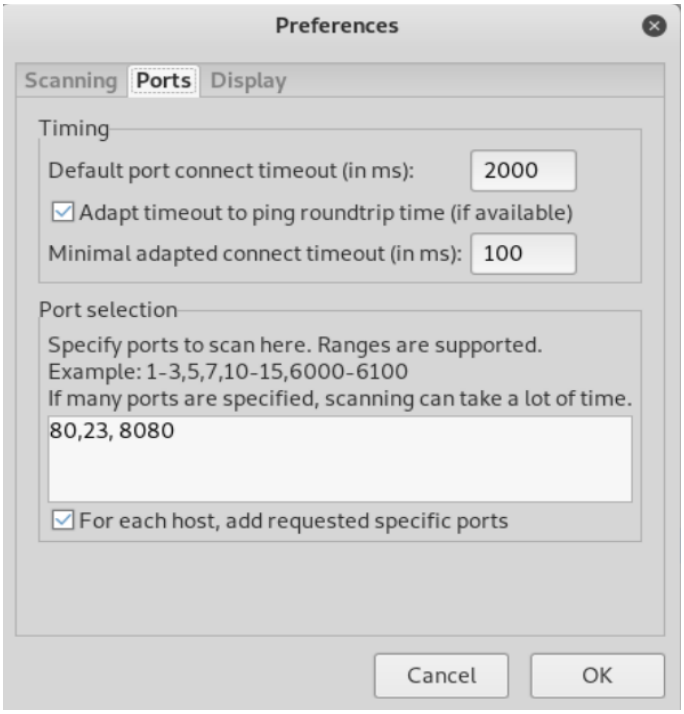
4.2.1 Angry IP Scanner

Angry IP Scanner on graafisen käyttöliittymän omaava porttiskanneri. Sillä pystyy skannaamaan verkkojen IP-osoitteita sekä portteja. On tärkeää huomioida oletussalasanojen vaihtamisen tärkeys. Valvontakameroita pystyy löytämään helposti skannaamalla verkosta, ja mikäli oletustunnuksia ei ole vaihdettu, on hakkereilla helppo pääsy valvontakameran sisältöön.

Angry IP Scanner on ilmainen ohjelma, jonka pystyy lataamaan verkosta monelle eri käyttöjärjestelmälle. Ohjelman asennuksen jälkeen valitaan IP-osoitteiden joukko. Oman julkisen IP-osoitteen pystyy löytämään helposti Googlesta hakemalla ”my ip”, jolloin Google tarjoaa useampaa eri vaihtoehtosivustoa. Jos julkinen IP-osoite on esimerkiksi 77.247.104.57, voi joukoksi valita 77.247.104.1-77.247.104.255 (ks. kuvio 11). Seuraavaksi valitaan portit, mitkä ohjelma skannaa (ks. kuvio 12). Portit 80 ja 8080 ovat HTTP portteja ja portti 23 on Telnetille varattu portti. Portit pystyy lisäämään valitsemalla **Tools** > **Preferences** > **Ports**.

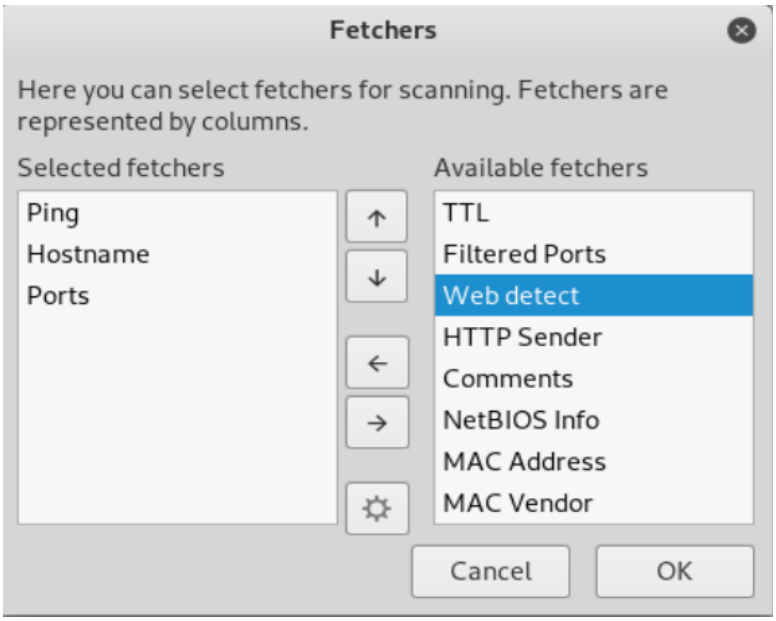


Kuvio 11. IP-osoitejoukko



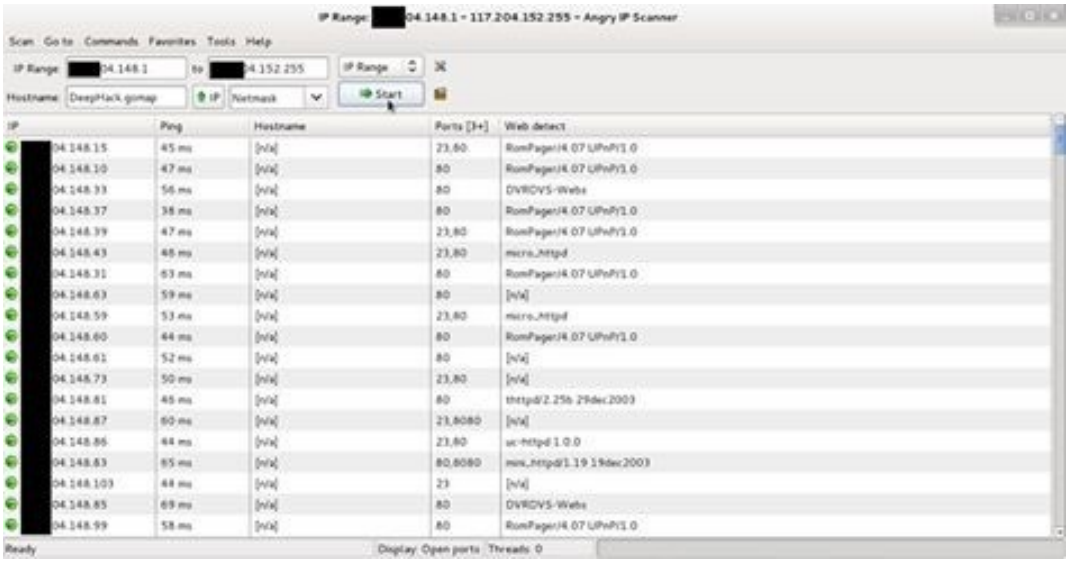
Kuvio 12. Valitut portit

Tämän jälkeen lisätään hakuvalinta, jossa skanneri etsii lisätietoja IP-osoitteesta löytyvästä laitteesta, kuten reitittimen nimen ja mallin sekä valvontakameran nimen ja mallin. Valinnat löytyvät **Tools** > **Fetchers**. Siirrettään kuviosta 13 sinisellä valittu Web detect nuolesta vasemmalle puolelle. Tämän jälkeen valitaan **OK** ja **Start**, jolloin valitut tiedot tallentuvat ja skannaaminen aloitetaan.



Kuvio 13. Lisävalinnat

Kuviosta 14 näkee Aryan Gupta (2017) blogipostauksessa näytetyn skannauksen tulokset. Valvontakameroita löytyi nimellä uc-httpd 1.0.0, DVRDVS-Webs, Webs, Hikvision-Webs sekä iBall-Baton. Reitittimiä löytyi mm. Microhttpd sekä omPager/4.07 UPnP/1.0. Kopioimalla laitteen IP-osoitteen ja hakemalla osoite verkkoselaimella, löytää laitteen hallintasivun. (Gupta 2017.)

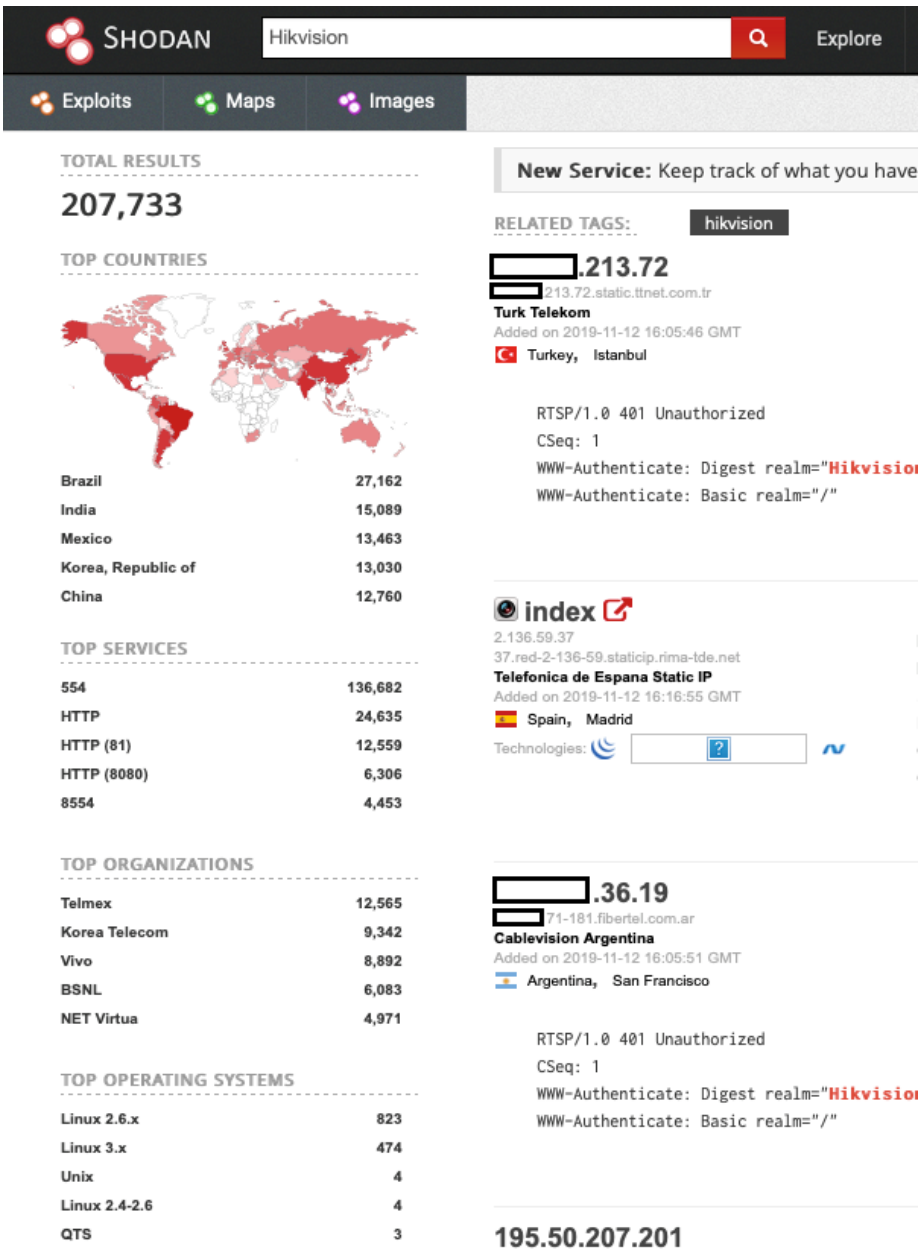


Kuvio 14. Skannauksen tulokset (Gupta 2017.)

Hallintasivun kirjautumiskohtaan päästyään, voi kokeilla erilaisia oletuskäyttäjätunnuksia ja salasanoja, ellei tiedä kyseisen laitteen käyttäjätunnusta. Yleisimpiä oletuskäyttäjätunnuksia ovat admin, root, administrator sekä user (Bauer n.d). Salasanoista löytyy monia erilaisia, esimerkkeinä admin, password, 1234 sekä 9999 (mt). Oletussalasanalistoja löytyy internetistä helposti sekä laitevalmistajat jakavat internetissä laitteiden käyttöohjeita, joissa on ilmaistu oletuskäyttäjätunnus ja salasana. Mikäli oletustunnukset eivät toimi, voi tilanteessa yrittää hakkeroida salasanan erilaisilla keinoilla, kuten brute force- tai sanakirjahyökkäys.

4.2.2 Shodan

Shodan on verkkosivusto, joka näyttää IoT-laitteita (kuten valvontakameroita) ympäri maailmaa. Sen käyttöön ei tarvitse erillistä ohjelmaa, vaan laitteiden skannaus on tehty jo valmiiksi. Sivustolta pystyy hakemaan laitteen tai valmistajan nimellä ja sivusto kertoo tietoa laitteista kuten, montako laitteita löytyy maailmasta, IP-osoitteita, avoimia portteja sekä sijainnin. Hikvision valmistaa valvontakameroita ja kuviosta 15 näkee tällä hetkellä olevien skannattujen kameroiden määrän.

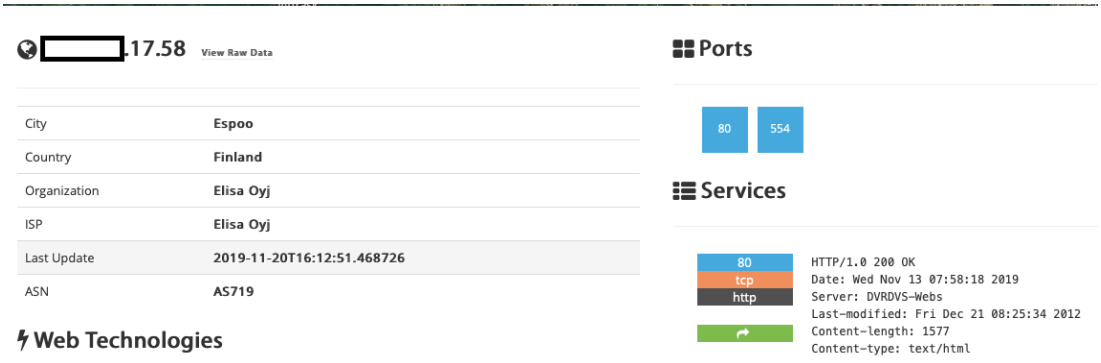


Kuvio 15. Shodan Hikvision haku

Kirjautuessa sisään pystyy hakukriteereinä valita maan. Kuviosta 16 näkee Suomesta haetut kamerat ja kuinka monta kameraa löytyy mistäkin kaupungista.

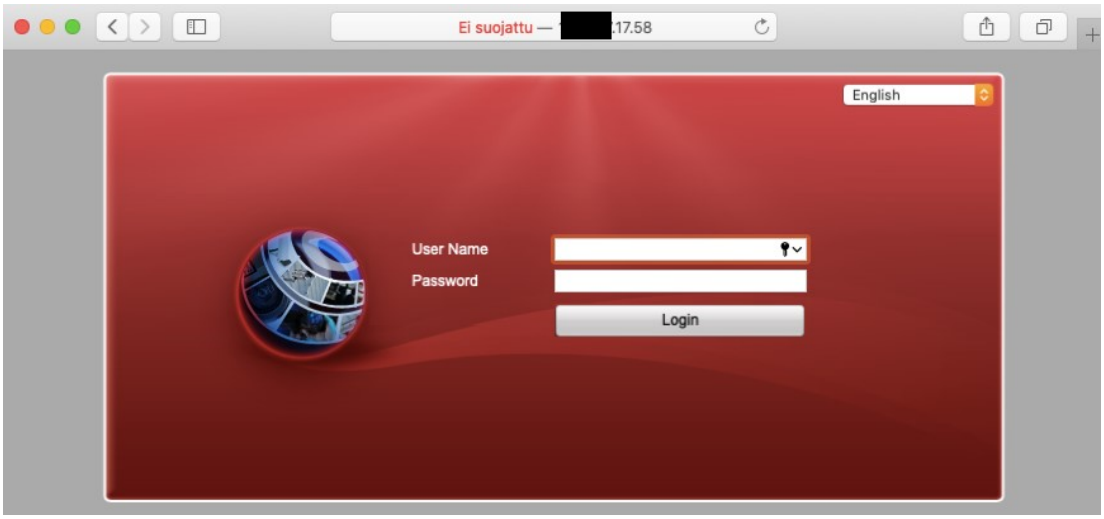
Kuvio 16. Hikvision kamerat Suomessa

Valitessa yksi kameroista löytää lisätietoja kamerasta, kuten käytetty portti (ks. kuvio 17).



Kuvio 17. Hikvision kamera lisätietoja

Mentäessä selaimella kameran IP-osoitteeseen, päästään kameran kirjautumissivulle. Kameran hallintasivun näkee kuviosta 18. Tämän jälkeen hakkeri pystyy kokeilemaan oletuskäyttäjätunnuksia ja salasanoja tai suorittamaan salasanan murtamishyökkäyksen.



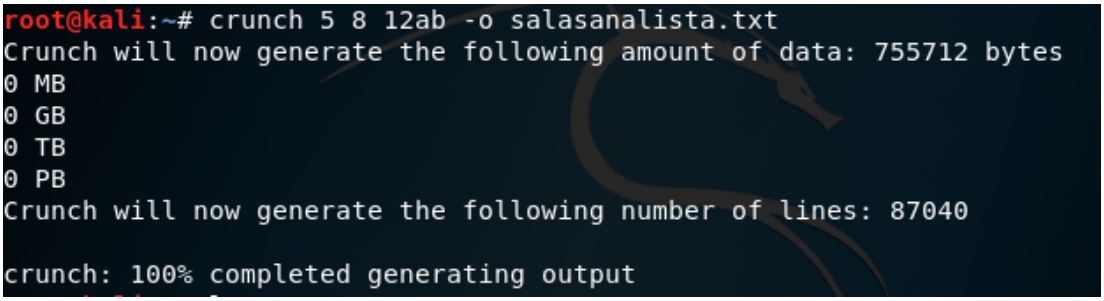
Kuvio 18. Kameran hallintasivu

4.3 Salasanan murtaminen

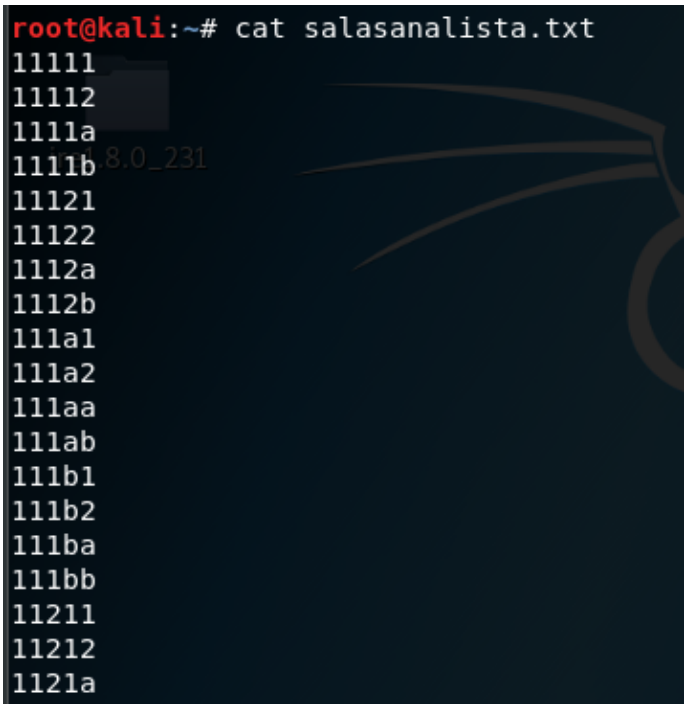
4.3.1 Sanakirjahyökkäys

Sanakirjahyökkäyksessä (eng. *dictionary attack*) luodaan salasanalista tekstitiedostoon ja kokeillaan listasta löytyviä salasanoja. Internetistä löytyy valmiita listoja tunnetuista salasanoista. Listat sisältävät sadasta salasanasta moneen kymmeneen miljoonaan salasanaan. Listoja voi myös tehdä itse listaamalla sanoja tai käyttää työkalua, joka luo satunnaisia merkkijonoja käskyjen mukaan. Esimerkiksi Kali Linux käyttöjärjestelmä sisältää ohjelman Crunch, joka luo salasanalistoja asetettujen käskyjen mukaisesti. Kuviosta 19 näkee komennon listan luomiseen. **5** määrittää minimi merkkimäärän, **8** määrittää maksimi merkkimäärän sanassa, **12ab** määrittää, mitä merkkejä sanoissa käytetään sekä **-o** määrittää tiedostolle nimen sekä mihin se tallennetaan.

Kuviosta 20 näkee otteen listasta. Listaan luotiin yhteensä 87 040 sanaa, joten kuvissa näkyy vain pieni ote koko listasta.



Kuvio 19. Salasanalistan luominen



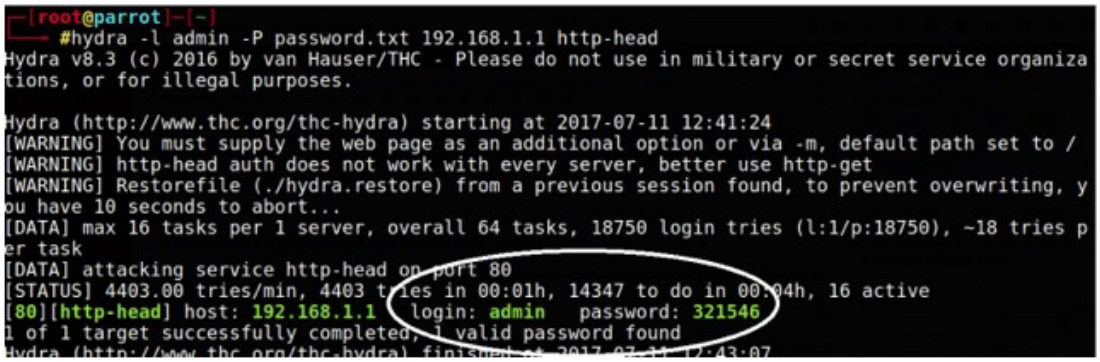
Kuvio 20. Salasanalista

Hydra on käyttäjätunnuksien murtamiseen käytetty ohjelma, joka tukee monia eri protokollia. Hydra on tehokas työkalu brute force- sekä sanakirjahyökkäyksiin. Kuviossa 21 on esimerkki komento, miten Hydraa pystytään käyttämään. Hydra kertoo, mitä ohjelmaa käytetään, **-l** määrittää käyttäjätunnuksen (*admin*), **-P** määrittää salasanalistan (*salasanalista.txt*) tiedostona, mikäli kirjoitettaisiin **-p** määrittäisi tämän pelkän yhden salasanan. Käyttäjätunnuksia voidaan myös syöttää listasta, jolloin käytetään määritettä **-L**. **192.168.1.1** on kohteen IP-osoite sekä **http-head** on käytettävä protokolla. Protokolla voi olla mikä vaan Hydran tukemista protokollista, kuitenkaan kohteella ei välttämättä ole kaikki portit auki jokaiselle protokollalle.

```
root@kali:~# hydra -l admin -P salasanalista.txt 192.168.1.1 http-head
```

Kuvio 21. Hydra komento

Komennon jälkeen Hydra lähtee suorittamaan komentoa. Mikäli kyseinen portti (tässä HTTP) ei ole avoinna kohteella, antaa Hydra error-viestin, ettei kohde ole saavutettavissa. Portin ollessa avoinna, Hydra kokeilee jokaista käyttäjätunnus ja salasana yhdistelmää oikean vaihtoehdon löytämiseksi. Mikäli käyttäjätunnus sekä salasana ovat määritetty listana, kokeilee se jokaista yhdistelmää. Mitä pidemmät listat, sitä enemmän aikaa kuluu. Kuviosta 22 näkee löydetyn salasanan käyttäjätunnukselle admin. Yhteensä yrityksiä on ollut 18750, joista 4403 suoritetaan minuutin aikana. Salasanan löydettyä voi ne syöttää IoT-laitteen, kuten reitittimen tai valvontakameran, verkkoselaimella toimivalle hallintasivulle.



Kuvio 22. Löydetty salasana (Singh 2017)

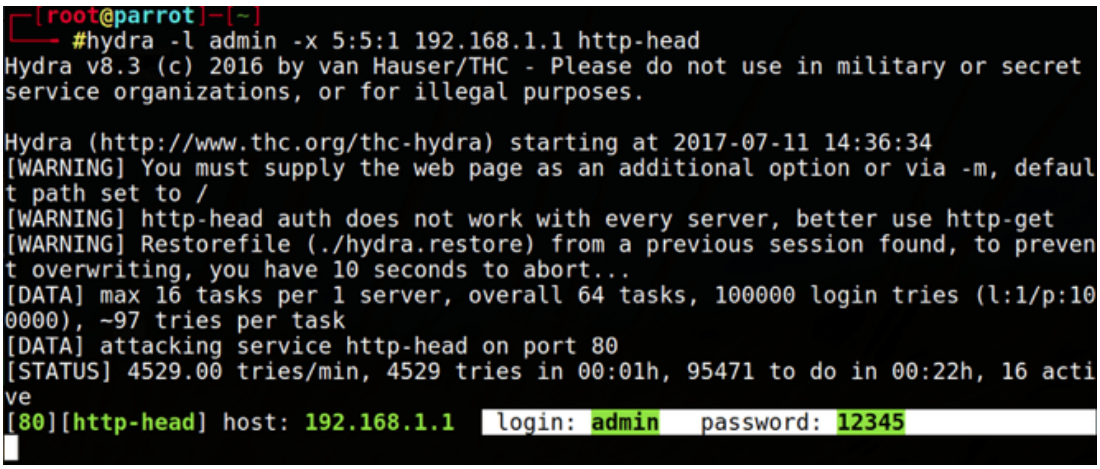
4.3.2 Brute Force -hyökkäys

Brute Force -hyökkäys (suom. *väsytyshyökkäys*) toimii lähes samalla tavalla kuin sanakirjahyökkäys, mutta siinä ei käytetä valmista sanalistaa, vaan komennossa määritellään merkkikriteerit ja testataan mahdollisia yhdistelmiä merkeistä. Kuvion 23 komennossa **-l** määrittää käyttäjätunnuksen, **4** salasanan minimi pituuden, **9** maksimi pituuden sekä **a1** määrittää, että käytetään pieniä kirjaimia sekä numeroita **0-9** välillä. Isoja kirjaimia halutessa lisätään **A**. **-F** määrittää, että toiminta lopetetaan, kun oikea salasana löytyy. Lisäksi kohteen IP-osoite sekä kohdeportti.

```
root@kali:~# hydra -l admin 4:9:a1 -F 192.168.1.1 http-head
```

Kuvio 23. Brute Force komento

Kuviossa 24 on suoritetun komennon tulokset. Siinä kriteereinä käytettiin minimi sekä maksimi merkkejä **5** ja pelkästään numeroita. Komennon suorittaja on esimerkkitarkoituksessa, käyttänyt helppo ja yksinkertaista salasanaa.

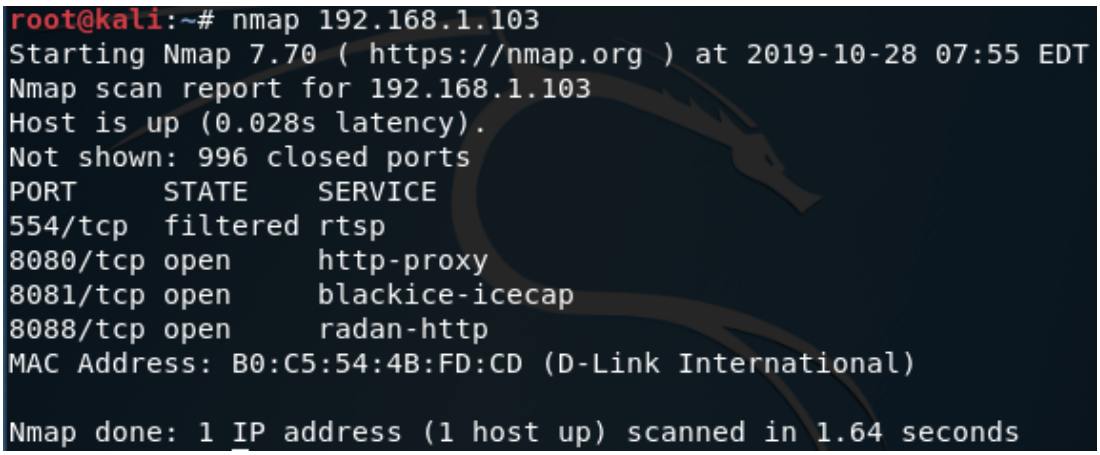


Kuvio 24. Brute Force tulos (Singh 2017.)

4.4 D-Link valvontakamera

Tutkimuksessa tutkittiin tarkemmin D-Link DCS-P6000LH Mini HD WiFi kameraa. Se on pieni kokoinen sisäkamera yö- sekä päiväkuvaukseen. Siinä on sisäänrakennettu mikrofoni, joka tallentaa videokuvan ohella myös äänet. Kamera lähettää live-kuvaa langattoman verkkoyhteyden avulla. Tutkimuksessa tarkoituksena oli löytää haavoittuvuuksia edellä mainitusta kamerasta sekä esittää keinoja, miten IoT-laitteita voidaan väärinkäyttää ulkoverkosta. Kyseinen kamera vaatii kuitenkin WLAN-yhteyden ja toimii reitittimen takana, eikä näin ollen näy ulkoverkkoon.

Komennolla **nmap -sn 192.168.1.0/24**, nmap skannaa kaikki kyseisessä verkossa olevat laitteet, näiden IP-osoitteet sekä MAC-osoitteet. D-Link kamera on osoitteessa 192.168.1.103. Skannaamalla nmap avulla kyseinen IP-osoite, nähdään laitteen avoimet portit. Kuviosta 25 näkee D-Link kameran avoimet portit sekä protokollat, joita se käyttää. Protokollalla voi olla tunnettuja heikkouksia sekä tiettyihin portteihin voi olla tehtynä tiettyjä hyökkäyksiä. Esimerkiksi portteja hyödyntäen käyttämällä troijan hevosia tai backdooreja.



Kuvio 25. Kameran avoimet portit

TCP portissa 554 toimii palvelu RTSP (*Real Time Streaming Protocol*). Sitä käytetään IP-verkossa multimedian suoratoistoon. Eli tämän portin kautta kulkee livekuva puhelinapplikaatioon D-Link kamerassa. Esimerkiksi Vivotek IP kameroista on löydetty heikkous, jonka avulla hakkeri on pystynyt lähettämään muokattuja RTSP paketteja kyseiseen porttiin ja näin pystynyt ohittamaan autentikoinnin ja päässyt käsiksi videokuvaan (Port 554 Detail 2019).

ICECap Manager kuuntelee porttia 8081 ja siirtää hälytys viestejä serverille porttiin 8082. Sillä on ylläpitäjän (eng. *Adminstrator*) käyttäjätunnuksena iceman sekä tyhjä salasana. Etäkäyttäjä voi kirjautua ICECap manageriin portista 8081 käyttäen oletustunnuksia ja lähettää virheellisiä viestejä. (HTTP ICECap Default Admin Password 2017.)

D-Link kamera toimii puhelinsovelluksen avulla, eikä kameran videokuvaa pysty katsomaan verkkoselaimella. Kamera yhdistetään puhelinsovellukseen uniikin QR-koodin avulla. Varmistaakseen, ettei kameraa voi lisätä toiselle käyttäjätunnukselle samanaikaisesti, tutkimuksessa luotiin toinen käyttäjätunnus ja yritettiin lisätä sama kamera uudelle tunnukselle. Applikaatio kuitenkin antoi virheviestin, ettei kameraa pysty lisäämään, sillä se on yhdistettynä toiseen käyttäjätunnukseen. Näin pystyttiin

varmistamaan, ettei kukaan henkilö pysty vieraillessa ottamaan kuvaa QR-koodista ja lisäämään kameraa omaan tunnukseen ja näin katsoa livekuvaa samanaikaisesti kuluttajan tietämättä.

5 Johtopäätökset

Verkkorikollisuus IoT-laitteissa on noussut isoksi puheenaiheeksi nykypäivänä. Laitteisiin kohdistuvat väärinkäytökset eivät välttämättä näy käyttäjälle millään tavalla ja IoT-laitteista koostettuja bottiverkkoja muodostetaan tuhansien kuluttajien tietämättä. Päästyään yhteen laitteeseen, on rikollisella pääsy myös muihin sisäverkon laitteisiin. Mikäli yhdessä sisäverkkoon kytketyssä laitteessa on huono tietoturvan hallinta, vaikuttaa se siis myös muihin laitteisiin.

Opinnäytetyön tulokseksi saatiin kattava määrä tietoa IoT-laitteiden haavoittuvuuksista. IoT-laitteiden heikkouksina pystyttiin listaamaan epäluotettavat web-, pilvi- ja sovellusrajapinnat, epäluotettavat verkkopalvelut ja ohjelmistot, puutteellinen käyttäjän todennus ja valtuutus, puutteellinen tietoturvakonfigurointi ja liikenteen salaus, yksityisyyden puute sekä huono fyysinen turvallisuus. Rikolliset ovat käyttäneet IoT-laitteiden väärinkäyttöksiin muun muassa DNS-hijacking menetelmää, jossa verkkoliikenne ohjataan väärälle sivustolle, SQL-injektioita, joissa tietokanta saastutetaan, XSS tietoturva-aukkoa, Buffer Overflow -virhettä, palvelunestohyökkäyksiä ja kuluttajien jättämiä oletuskäyttäjätunnuksia ja –salasanoja.

Usein onnistunut hyökkäys nojaa järjestelmän suunnittelu- ja toteutusvirheeseen. Virheitä löytyy koodista, autentikoinnista, kryptografiasta tai ylimääräisistä funktioista. Jokaisella portilla ja protokollalla on haavoittuvuuksia ja jokaisen portin palvelu on alttiina väärinkäytöksille. Näitä haavoittuvuuksia jaetaan internetissä kaikkien tietoisuuteen ja rikolliset hyödyntävät näitä tietoja hyökkäyksissään. Esimerkiksi Telnet protokolla ei suojaa liikennettä millään tavalla. Laitteiden avoimia portteja ja palveluita pystytään skannaamaan ulkoa päin, joten ylimääräisiä portteja ei suositella pidettävän auki laitteilla.

Verkkojen ja laitteiden skannaamiseen löytyy ohjelmia, jotka tarjoavat paljon tietoa verkosta ja laitteista muutamalla klikkauksella. Skannauksella pystytään tunnistamaan muun muassa laitteiden ja verkkojen IP-osoitteita, laitteiden nimiä, malleja, avoimia portteja ja käyttöjärjestelmiä. Aina ei edes tarvitse ladata ohjelmaa, vaan esimerkiksi valvontakameroita löytää netistä jo valmiiksi skannattuina. Sivustojen suunnittelijat väittävät, ettei kenenkään yksityisyyttä loukata, vaikka kuluttajan valvontakameran videokuva lähetetään jokaiselle nähtäväksi, joka vain osaa löytää tiensä sivustolle. Tämä luo ristiriitaisia kysymyksiä yksityisyydestä, kuten missä menee yksityisyyden raja? Sivusto on saatettu luoda, jotta kuluttajat ymmärtäisivät salasanojen asettamisen ja muuttamisen tärkeyden, mutta turvallisuuden takia ostettu kamera, saattaa aiheuttaa myös vaaraa. Rikolliset voivat hyödyntää videokuvaa tunnistamaan, milloin asukkaat eivät ole kotona, ja näin ajastaman fyysisen taloon murtautumisen tiettyyn aikaan.

Salasanan vaihtaminen IoT-laitteelle tulisi olla ensimmäinen toimenpide laitteen käyttöönottamisessa. Internet on täynnä jo valmiiksi luotuja salasanalistoja, jotka helpottavat rikollisten toimia. Listoihin on valmiiksi kirjoitettu miljoonia yleisimpiä salasanoja. Listojen pituudet kasvat samalla, kun löydettyjä salasana- ja käyttäjätunnusyhdistelmiä lisätään koko ajan. Tästä syystä kuluttajien ei tulisi käyttää samoja salasanoja eri kirjautumisalustoille. On myös tärkeää käyttää riittävän haastavaa salasanaa. Sosiaalisen median kautta pystyy löytämään paljon tietoa kuluttajasta. Salasanoissa ei suositella käytettävän syntymäpäiviä, nimiä tai muita julkisesti ilmoitettuja tietoja, sillä näitä tietoja käytetään yleisesti salasanoissa ja rikolliset kokeilevat erilaisia salasanayhdistelmiä löytääkseen oikean salasanan. Salasanojen testaamiseen on saatavilla erilaisia ohjelmia ja internetistä löytyy paljon yksinkertaisia ohjeita. Rikollisella ei tarvitse olla edes alan ammattitaitoa hyödyntääkseen näitä ohjelmia.

Kodin sisäverkon suojaamiseen voi käyttää tietoturvareititintä, joka toimii normaalin reitittimen tapaan, mutta sisältää myös tietoturvaominaisuuksia ja suojaavat kuluttajaa haitalliselta liikenteeltä. Vaihtoehtona kuluttaja voi myös käyttää palomuuria, jolla rajoitetaan sisäverkosta lähtevää ja sisäverkkoon pääsevää liikennettä. Molemmat laitteet asetetaan sisäverkkoon internetin ja muiden kodin laitteiden väliin. VPN avulla pystytään salaamaan kuluttajan liikenne ja estämään ulkopuolisten pääsy tark-

kailemaan liikkuvaa dataa. VPN piilottaa kuluttajan IP-osoitteen ja näin sijaintia ei pystytä paikantamaan.

IoT-laitteiden turvallisuuden parantamiseksi pystyttiin tunnistamaan seuraavia toimenpiteitä:

- Oletussalasanojen vaihtaminen
- Turvallisten salasanojen käyttäminen
- Laitteella olevien ylimääräisten porttien sulkeminen
- Ohjelmistoversioiden päivittäminen
- Tunnetuiden laitevalmistajien tuotteiden käyttäminen
- Tarpeettomien laitteiden eristäminen verkosta
- Palomuurin käyttäminen sisäverkossa

IoT-laitteiden tietoturvaa tulisi parantaa laitevalmistajien taholta ja siihen tulisi paneutua enemmän. Kuitenkin erittäin iso ja yllättävä osa laitteiden väärinkäytöksistä johtuu kuluttajien tietämättömyydestä tai piittaamattomuudesta. Kuluttajien suurin virhe on jättää oletuskäyttäjätunnukset ja -salasanat laitteille. Nämä tiedot ovat jokaisen löydettävissä internetistä laitteiden käyttöohjeista. Kuluttajat luottavat liikaa laitevalmistajiin, eikä laitteiden tietoturvaan tutustuta tarkemmin. Tähän voi vaikuttaa myös ihmisten tietämättömyys ja välinpitämättömyys aiheesta. Tietoturva asioista puhutaan paljon, mutta niitä saisi tuoda kuluttajille vielä enemmän esiin ja painottaa pohtimaan, onko kyseinen laite tarpeen kytkeä verkkoon.

6 Pohdinta

Opinnäytetyön tavoitteena oli lisätä kuluttajien tietoisuutta verkkorikollisuudesta verkkoon kytketyistä laitteista ja löytää keinoja, miten rikolliset väärinkäyttävät IoT-laitteita ja kuinka kuluttajat voisivat suojata omia laitteitaan ja sisäverkkoaan paremmin. Opinnäytetyössä käytettiin kvalitatiivista tutkimusmenetelmää. Tarkoituk-

sena oli tuoda tutkittuun ongelmaan ymmärrystä, muttei tehdä käytännön toimenpiteitä. Tutkimuksen kysymyksiin etsittiin vastauksia erilaisista verkkojulkaisuista ja alan kirjallisuudesta. Teoriaan käytettävät lähteet rajattiin mahdollisimman uusiin julkaisuihin. Julkaisuiden luotettavuus arvioitiin asiantuntijoiden kommenttien perusteella ja asioiden toistettavuudesta eri lähteillä. Tutkimuksessa käytettiin kirjallisia lähteitä, mutta ajankohtaisuuden ja uusien tutkimusten takia, oli verkkojulkaisuja paremmin saatavilla.

Mielipiteet älylaitteiden ja älykodin suhteen ovat jakautuvia. Toiset ajattelevat uuden teknologian tuovan paljon hyötyjä arkipäiväiseen elämään ja toiset eivät halua kotinsa olevan valvonnan alla. Usein vanhemmalla väestöllä on negatiivisempi ajatusmaailma liittyen uusiin teknologisiin keksintöihin. Tähän voi vaikuttaa haluttomuus oppia uutta tai tämän vaikeus. Joitain laitteita voi olla vaikea käyttää, mikäli ei ole tutustunut jo aikaisemmin erilaisiin teknologioihin. Älylaitteet tuovat kuitenkin paljon myös hyötyjä. Esimerkiksi lomaillessa pystyy kuluttaja valvomaan etänä kotiaan ja tarkkailemaan matkalla ollessaankin, ettei ulkopuolisia ilmesty talolle. Älylaitteilla voidaan myös parantaa yksin asuvien vanhusten turvallisuutta monitoroimalla heidän terveyttään ja tarpeen tullen hälyttämään ensihoitaja paikalle automaattisesti. Sekä liiketunnistimet pystyvät valvomaan lamppuja ja tiputtamaan talon lämmitystä, kun eivät tunnista liikettä ja näin ollen säästää sähkö- sekä lämmityskustannuksissa.

Ihmiset ovat kuitenkin edelleen hyvin välinpitämättömiä tietoturvan suhteen. Asioista on kirjoiteltu paljon uutisissa ja tieto kiertää esimerkiksi verkkolehtien, Facebookin ja Twitterin kautta monelle ihmiselle. Silti ihmiset eivät ole niin kiinnostuneita asiasta. Tai saattavat olla, mutta eivät ole riittävän kiinnostuneita tekemään asialle mitään. Tähän myös vaikuttaa paljon osaaminen ja asioista pitäisi ottaa itse selvää. Jos ei ole minkäänlaista mielenkiintoa tietoteknisiin välineisiin, luotetaan sokeasti laitevalmistajiin ja eikä välttämättä edes ajatella mahdollisia ongelmia ja tietoturvaan liittyviä asioita älylaitteissa.

Laitevalmistajien tulisi paneutua enemmän laitteiden tietoturvallisiin ominaisuuksiin. Laitevalmistajat pyrkivät kuitenkin panostamaan laitteiden käyttöominaisuuksiin ja lisäämään myyntiä. Internetistä löytää tietoturva-asiantuntijoiden kirjoittamia artik-

keleita aiheista ja erilaisia keinoja hakkeroitua IoT-laitteisiin. Kysymykseksi herää, miksei IoT-laitteiden suunnittelijat ja valmistajat paneudu laitteiden tietoturvaan paremmin, kun tietoturva-asiantuntijoita kuitenkin löytyy? Tähän vaikuttaa varmasti raha. Tuotteet halutaan markkinoille nopeasti ja kuluttajien ostettavaksi, jotta yritykset tuottaisivat enemmän rahaa.

IoT-laitteet tuovat helpotusta kuluttajien arkeen, mutta on hyvä miettiä, onko tiettyjen laitteiden tarpeellista olla kytkettynä verkkoon. Kuluttajat saattavat haluta uusia moderneja keksintöjä koteihin, muttei tuotteen käyttöä ajatella kokonaisvaltaisesti. Esimerkiksi uuni, jonka pystyy kytkeä verkkoon ja hallita uunin lämpötilaa ja päälle laittamista etänä, voi tuottaa myös fyysistä vaaraa. Mikään laite ja verkko ei ole täysin turvallinen. Mitä jos rikollinen pääsee hallitsemaan verkkoon kytkettyä uunia ja asettamaan uunin päälle korkealle lämpötilalle, kun kuluttaja ei ole kotona, ja näin luoden tulipaloriskin. Kuluttajien tulisi miettiä IoT-laitteita ostaessa, onko tuote tarpeellinen kytkeä verkkoon ja miettiä myös laitteen haittapuolia.

Tutkimuksessa tarkoituksena oli valita yksi IoT-laite ja etsiä heikkouksia kyseisestä laitteesta ja näyttää esimerkkejä, miten hakkerit voivat väärinkäyttää laitteita yksinkertaisestikin. Valittu kamera ei kuitenkaan näkynyt ulkoverkkoon ja kameraan ei onnistuttu suorittamaan toimenpiteitä, mitä olisi toivottu. Tutkimuksessa kuitenkin löydettiin paljon tietoa, miten hakkerit väärinkäyttävät IoT-laitteita ja kuinka kuluttajien yksityisyyttä voidaan loukata helposti heidän tietämättä. Tutkimuksessa tuli yllätyksenä Suomessakin toimineiden bottiverkkojen laajuus ja kuinka moni laite oli saastutettu. Verkkorikollisuus tapahtuu usein kuluttajan tietämättä ja asian julkituomiseen saataisiin panostaa Suomessa enemmän. Kirjallisia lähteitä etsiessä, löytyi suomenkielisiä lähteitä vain muutamia verkkouutisia. Näissä uutisissa puhuttiin paljon, kuinka suomalaisten laitteita on väärinkäytetty, mutta ei tuotu kunnolla esiin, miten. Tämä saattaa vaikutta lukijaan etäiseltä eikä lukija pysty saamaan kattavaa kuvaa IoT-laitteiden riskeistä, kun niitä ei konkretisoida. Varmasti monelle kuluttajalle vaikuttaa yhtenä syynä välinpitämättömyyteen tietoverkkoliikennettä ja tietoturvaa kohtaan, ettei asioita pystytä näkemään ja kokemaan konkreettisesti ja hahmottamaan, mistä oikein kyse.

Opinnäytetyön yhtenä tarkoituksena oli herättää lukijassa ajatuksia laitteiden haitta-puolista ja tuomaan yksinkertaisia keinoja, joilla lukija voisi tehdä omasta digitaalises-ta arjesta turvallisemman. Tietoturva-asioista saataisiin Suomessa puhua vielä enemmän ja pyrkiä lisäämään kuluttajien tietoisuutta. Tietoturvallisuudesta olisi hyvä yrittää tehdä mahdollisimman yksinkertaisia julkaisuja, jotta jokainen kansalainen pystyisi ymmärtämään ja hahmottamaan, mistä ja kuinka tärkeästä asiasta on kyse.

Lähteet

Ahaskar, A. 2019. How hackers can snoop on you via your smart cameras. Artikkeli Livemint-sivustolla. Viitattu 8.11.2019. https://www.livemint.com/technology/tech-news/how-hackers-can-snoop-on-you-via-your-smart-cameras-1567709174895.html

Aurelle Square -paneelivalo. 2019. Philips Hue Aurelle Square -paneelivalo esittely. Viitattu 7.8.2019. https://www2.meethue.com/fi-fi/p/hue-white--tunnelmavalo-aurelle-square--paneelivalo/3216231P5

Bauer, J. N.d. Common Router Passwords. Listaus yleisimmistä oletuskäyttätunnuksista ja -salasanoista Setup Router -sivustolla. Viitattu 12.11.2019. https://setuprouter.com/common-passwords/#Default-Router-Passwords

Beal v. 2019. VPN – virtual private network. Artikkeli Webopedia sivustolla. Viitattu 25.11.2019. https://www.webopedia.com/TERM/V/VPN.html

Biswas, I. 2018. Smart homes: past, present, and future. Artikkeli Colocation America sivustolla. Viitattu 11.7.2019. https://www.colocationamerica.com/blog/smart-homes-past-present-future

Current World Population. 2019. Reaaliaikainen maailman ihmisten lukumäärä mittari. Viitattu 1.7.2019. https://www.worldometers.info/world-population/

Elektronikkari. 2017. Blogikirjoitus Vuodatus sivustolla. Viitattu 10.10.2019. https://elektronikkari.vuodatus.net/lue/2017/07/kodin-sisaverkko

Gabbai, A. 2015. Kevin Ashton Describes “the Internet of Things”. Artikkeli Smithsonian sivustolla. Viitattu 11.7.2019. https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/

Geer. 2017. Securing risky network ports. Artikkeli Network World sivustolla. Viitattu 27.10.2019. https://www.networkworld.com/article/3191513/securing-risky-network-ports.html

Greengard, S. 2015. The Internet of Things. Yhdysvallat: Massachusetts Institute of Technology.

Gupta, A. 2017. How to Hack any CCTV camera using Kali Linux. Blogikirjoitus. Viitattu 12.11.2019. https://hackkersadda.blogspot.com/2017/06/how-to-hack-any-cctv-cameras-using-kali.html

How the Glue ecosystem works. 2019. Glue tuotteen esittely sivustolla. Viitattu

2.12.2019. https://www.gluehome.com/

HTTP ICECap Default Admin Password. 2017. Symantec sivusto. Viitattu 6.11.2019. https://www.symantec.com/security_response/attacksignatures/detail.jsp%3Fasid%3D20899

Hu, F. 2016. Security and Privacy in Internet of Things (IoTs). Florida: CRC Press Taylor & Francis Group.

Hyttinen, T. 2018. Ilmalämpöpumppu toimii tunketujan reittinä kodin sisäverkkoon – Asiantuntija: Tähtäimessä ovat niin verkkopankkitunnukset, luottokortti tietodot kuin muutkin laitteet. Artikkeli Talouselämä-sivustolla. Viitattu 8.11.2019. https://www.talouselama.fi/uutiset/ilmalampopumppu-toimii-tunkeutujan-reittina-kodin-sisaverkkoon-asiantuntija-tahtaimessa-ovat-niin-verkkopankkitunnukset-luottokortin-tiedot-kuin-muutkin-laitteet/91279419-7e11-3738-8b5f-45852ec7552b

Ilascu, I. 2019. New Echobot Botnet Variant Uses Over 50 Exploits to Propagate. Artikkeli Bleeping Computer -sivustolla. Viitattu 8.11.2019. https://www.bleepingcomputer.com/news/security/new-echobot-botnet-variant-uses-over-50-exploits-to-propagate/

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). 2019. Artikkeli Statistic sivustolla. Viitattu 29.11.2019. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

IoT-laitteista kerätään uutta bottiverkkoa – Mirain uusi versio. 2019. Artikkeli Uusi Teknologia -sivustolla. Viitattu 8.11.2019. https://www.uusiteknologia.fi/2019/09/13/iot-laitteista-kerataan-uutta-bottiverkkoa-mirain-uusi-versio/

iRobot Roomba 980 käyttöohje. 2019. Laitteen käyttöohje. Viitattu 2.12.2019. https://www.kayttooh.je/irobot/roomba-980/k%C3%A4ytt%C3%B6ohje

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas : Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylä: Jyväskylän ammatikorkeakoulu.

Knud, L. 2018. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. Artikkeli Iot Analytics sivustolla. Viitattu 1.7.2019. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

Koivunen, E. 2010. Sisäverkko-ohje valtiovaranministeriön sivustolla. Viitattu 10.10.2019. https://www.vahtiohje.fi/web/guest/johdanto26;jsessionid=138C0703ECDD3D47176C1117E28A8F665855F880B57261BEB24168E3E5AB942E0003CA09539E68ACEE37A4

Mikä on palomuuri?. 2019. Blogikirjoitus Digivinkit-sivustolla. Viitattu 13.11.2019. https://www.digivinkit.fi/palomuuri/

Mill AV600WiFi. N.d. Mill-tuotteen esittely sivustolla. Viitattu 7.7.2019. https://www.millheat.com/mill-wifi/av600wifi

Mirai-bottiverkko on ottanut haltuunsa tuhansien suomalaisten modeemeja. 2016. Viestintäviraston kyberturvallisuuskeskuksen ilmoitus. Viitattu 12.9.2019. https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/11/ttn20161129174l.html

NAS. 2019. Dustinhome verkkokauppa. Viitattu 12.9.2019. https://www.dustinhome.fi/group/laitteistot/tallennus-muistikortit/nas/?ssel=false&_ga=2.8080178.1603320946.1568362290-1145482767.1568362290

Near Field Communication. 2017. Near Field Communcation -sivusto. Viitattu 1.11.2019. http://nearfieldcommunication.org

Network live IP video cameras directory Insecam.com. N.d. Etusivu Insecam-sivustolla. Viitattu 6.11.2019. http://www.insecam.org/en/

Opentopia. 2011. Sivuston etusivu. Viitattu 6.11.2019. http://www.opentopia.com/hiddencam.php

Pal A. 2019. The Internet of Things (IoT) - Threats and Countermeasures. Viitattu 15.11.2019. https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/

Port 554 Detail. 2019. Portin tiedot Speedguide-sivustolla. Viitattu 6.11.2019. http://www.insecam.org/en/bycountry/FI/?page=1

Product categories. 2019. Smarthome tuotteiden jaottelu. Viitattu 11.7.2019. https://www.smarthome.com/productcategories.html

Rasmussen, H. 2018. Älykoti voi kutsua hakkerit kylään. Artikkeli Kotimikro-sivustolla. Viitattu 12.9.2019. https://kotimikro.fi/yhteiskunta/alykoti/alykoti-voi-kutsua-hakkerit-kylaan

Riikonen P. 2018. Kannattaako ostaa uusi tietoturvareititin? Testissä F-Secure Sense ja kaksi muuta laitetta. Artikkeli Mikrobitti-sivustolla. Viitattu 13.11.2019. https://www.mikrobitti.fi/testit/kannattaako-ostaa-uusi-tietoturvareititin-testissa-f-secure-sense-ja-kaksi-muuta-laitetta/96f255e3-9174-3bc6-ad5c-c02876c03df4

Rijmenam, M. 2014. Where Does The Internet of Things Come From?. Artikkeli Datafloq-sivustolla. Viitattu 11.7.2019. https://datafloq.com/read/where-does-the-internet-of-things-come-from/524

Rouse M. 2008. Open System Authentication (OSA). Artikkeli SearchSecurity sivustolla. Viitattu 2.12.2019. https://searchsecurity.techtarget.com/definition/Open-System-Authentication-OSA

Rouse M. 2012. Shared Key Authentication (SKA). Artikkeli SearchSecurity sivustolla. Viitattu 2.12.2019. https://searchsecurity.techtarget.com/definition/Shared-Key-Authentication-SKA

Serie 6 Jääkaappipakastin. 2018. Bosch tuotteen esittely sivustolla. Viitattu 9.9.2019. https://www.bosch-home.fi/tuotelista/kylmalaitteet/jaakaappipakastimet/vapaasti-sijoitettavat/KGN36HI32?breadcrumb=null

Serie 8 Kalustepeitteinen kahviautomaatti. 2018. Bosch tuotteen esittely sivustolla. Viitattu 9.9.2019. https://www.bosch-home.fi/tuotelista/espresso-ja-kahvinkeittimet/kalusteisiin-sijoitettavat-kahviautomaatit/CTL636EB6?breadcrumb=builtinfullyautomaticcoffeemachines

Serie 8 Kompakti höyryuuni. 2018. Bosch tuotteen esittely sivustolla. Viitattu 9.9.2019. https://www.bosch-home.fi/tuotelista/liedet-uunit-keittotasot-ja-liesituulettimet/uunit/kalusteisiin-sijoitettavat-kompaktiuunit/CSG856RC6?breadcrumb=steamovens

Signh, H. 2017. How to Hack router usernamer & password 2018. Artikkeli Opentechinfo-sivustolla. Viitattu 12.11.2019. https://www.opentechinfo.com/hack-router/

Smith, S. 2017. The Internet of Risky Things.

Spring, T. 2018. ThreatList: 83% of Routers Contain Vulnerable Code. Artikkeli Threatpost-sivustolla. Viitattu 7.10.2019. https://threatpost.com/threatlist-83-of-routers-contain-vulnerable-code/137966/

SQL Injection. N.d. W3 School oppimateriaali. Viitattu 1.11.2019. https://www.w3schools.com/sql/sql_injection.asp

Suomi aloittaa älylaitteiden turvallisuuden varmistamisen ensimmäisenä Euroopassa – uusi Tietoturvamerkki auttaa kuluttajia tekemään turvallisempia kodin älylaitehankintoja. 2019. Artikkeli Traficom sivustolla. Viitattu 2.12.2019. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suomi-aloittaa-alylaitteiden-turvallisuuden-varmistamisen-ensimmaisena-euroopassa

Threat Intelligence Team. 2019. Emotet is back: botnet springs back to life with new spam campaing. Artikkeli Malwarebytes Labs -sivustolla. Viitattu 8.11.2019. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

Understanding CAN Bus and CAN Loggers. 2019. Sewell-sivusto. Viitattu 29.10.2019. https://sewelldirect.com/blogs/learning-center/understanding-can-bus-and-can-loggers

Valoa tunnelmallisiin hetkiin. 2018. Philips Hue White ambiance Aurelle Square -paneelivalo esittely .Viitattu 7.8.2019. http://download.p4c.philips.com/files/3/3216231p5/3216231p5_pss_finfi.pdf.

Video Doorbell Pro. N.d. Ring verkkokauppa. Viitattu 9.9.2019. https://shop.ring.com/products/video-doorbell-pro

WK7. 2019. LG tuotteen esittely sivustolla. Viitattu 2.12.2019.

https://www.lg.com/au/smart-speaker/lg-WK7

Wroclawski, D. 2019. How to Keep Your Home Security Cameras From Being Hacked. Artikkeli Consumer Reports -sivustolla. Viitattu 8.11.2019. https://www.consumerreports.org/home-security-cameras/keep-home-security-cameras-from-being-hacked/

Zhang, S. 2014. A Creepy Website Is Streaming From 73 000 Private Security Cameras. Artikkeli Gizmodo-sivustolla. https://gizmodo.com/a-creepy-website-is-streaming-from-73-000-private-secur-1655653510

Älykkäät kodinkoneet verkkorikollisten tähtäimessä. 2019. Uutinen Mikrobitti-sivustolla. Viitattu 9.9.2019. https://www.mikrobitti.fi/uutiset/alykkaat-kodinkoneet-verkkorikollisten-tahtaimessa/0c07c604-28b6-4c9f-83dc-10513b5146f4

Älylaitteiden yleistyminen avaa kodit yllättäville riskeille. 2019. Blogikirjoitus F-Secure sivustolla. Viitattu 7.10.2019. https://blog.f-secure.com/fi/alylaitteiden-yleistyminen-avaa-kodit-yllattaville-riskeille/