OULUN AMMATTIKORKEAKOULU

Janne Mourujärvi

Langattoman lähiverkon tietoturva kotona

Langattoman lähiverkon tietoturva kotona

Janne Mourujärvi

Opinnäytetyö

Syksy 2020

Tietojenkäsittelyn tutkinto-ohjelma

Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu

Tietojenkäsittelyn tutkinto-ohjelma, järjestelmäasiantuntemus

---

Tekijä(t): Janne Mourujärvi

Opinnäytetyön nimi: Langattoman lähiverkon tietoturva kotona

Työn ohjaaja: Minna Kamula

Työn valmistumislukukausi ja -vuosi: Syksy 2020 Sivumäärä: 42

Opinnäytetyössä käsitellään langatonta lähiverkkoa kotiolosuhteissa, sen tietoturvaa ja konfigurointia. Idea opinnäytetyöhön tuli etätyöntekijöiden ja langattomien lähiverkkoyhteyksien kasvussa yhä enemmän ja enemmän digitalisoituvassa maailmassa. Opinnäytetyössä käydään läpi tällä hetkellä käytössä olevia IEEE 802.11 protokollia ja verkkolaitteita, joiden avulla langaton lähiverkko luodaan. Työssä perehdytään langattoman lähiverkon uhkiin ja sen tietoturvaa uhkaaviin tekijöihin, sekä kuinka niiltä voi suojautua. Aineistona työssä käytettiin julkaisuja, artikkeli- ja kirjalähteitä.

Opinnäytetyön perusteella voi todeta, että turvallinen langaton lähiverkko on helppo konfiguroida, mikäli tietää mitä kaikki eri asetukset tarkoittavat. Hyökkääjiä on silti vaikea estää, jos he haluavat siihen tai siinä liikkuvaan tietoon oikeasti päästä käsiksi. Uusia haavoittuvuuksia löytyy joka päivä lisää ja näitä hyödyntäviä haittaohjelmia ovat alkaneet jopa valtiovallat kehittämään. Julkisia langattomia lähiverkkoja käyttäessä tulisi aina suojautua käyttämällä liikenteen salausprotokollaa, tietoturvaohjelmia ja pitää päivitykset ajan tasalla. Pi-Holen käyttäminen on yksi keino suojata yksityisyyttä ja älylaitteita. Oikeiden lisäosien asentaminen internet selaimeen tuo lisää yksityisyyttä ja turvaa, koska niiden avulla voidaan estää eri asioiden latautumista sivustoilla, jolloin haittaohjelmien pääsy päätelaitteelle on vaikeampaa.

Johtopäätöksenä voidaan pitää sitä, että kotona olevan tietoturvallisuuden suurin tekijä on itse ihminen ja kuinka hän omalla toiminnallaan edesauttaa sen toteutumista. Kyberrikollisuus ja siltä suojautuminen on ikuista kilpajuoksua. Työssä esiintyviä toimenpiteitä voidaan suositella kaikille, jotka käyttävät mitä tahansa äly- tai päätelaitteita.

Asiasanat: Wi-Fi, WLAN, langaton lähiverkko, verkkohyökkäykset, haittaohjelmat, tietoturva

ABSTRACT

Oulu University of Applied Sciences

Business Information Systems, Computer Systems Expertise

Author(s): Janne Mourujärvi

Title of thesis: Home Wireless Network Security

Supervisor(s): Minna Kamula

Term and year when the thesis was submitted: Autumn 2020 Number of pages: 42

This thesis is going to handle wireless network in a home environment, its security and configuration. The idea for the thesis came from the ever-growing number of devices that are using the wireless network and people who are working from home and using them. This thesis introduces the most modern IEEE 802.11 protocols and the types of network devices that are used to create wireless networks in homes. Theses also investigates the different types of attacks and malicious programs every person should be aware of, and how to defend against them. Reference material used consisted of publications, articles and books.

Results that are found in the thesis show that configuring a protected wireless local area network is an easy task if you know what the settings mean. Even with protection, the attacks are hard to prevent, if the attacker really wants to steal your data or get into your systems. New vulnerabilities are found every day and the malicious programs that use them are even developed by countries. Every public Wi-Fi user should be using protection for their communications, security software and keeping their devices up to date. Pi-Hole is one way to keep your privacy and smart devices protected and choosing the proper add-ons for your internet browser helps prevent malicious attackers and drive-by downloads while on the internet.

As a conclusion, the biggest factor in information and device security at home or outside is the human. He or she can, by his own actions, contribute to its realization. Cybercrime and the protection from it, is a never-ending race. The measures presented in this thesis can be recommended to anyone who uses any smart devices or computers.

Keywords: Wi-Fi, WLAN, Wireless Network, Malware, Computer Security, Data Security, Hacking

SISÄLLYS

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on perehtyä langattoman lähiverkon mahdollistavaan tekniikkaan, nykyajan haittaohjelmiin, tietoturvauhkiin, sekä kuinka näiltä voidaan kotiympäristössä suojautua. Työssäni käytin materiaalina verkkolähteitä ja alan kirjallisuutta. Verkkolähteiksi olen valinnut mahdollisimman tuoretta tietoa sisältäviä sivustoja, jotka kuuluvat alan yrityksille ja ammattilaisille.

Wireless Local Area Network (WLAN) eli langaton lähiverkko mahdollistaa erilaisten laitteiden yhdistämisen toisiinsa ilman kaapeleita. Laitteelta vaaditaan vain langattomaan lähiverkkoon yhdistämiseksi laitteelle sopivan WLAN-sovittimen. Langattoman lähiverkon avulla voidaan vaivattomasti yhdistää laitteita lähiverkkoon ja sitä kautta internetiin. Internetiin yhdistettyjen laitteiden määrässä onkin ollut räjähdysmäinen kasvu viime vuosina, jonka vuoksi on järkevää huolehtia, että laitteiden ja lähiverkon tietoturva, sekä konfigurointi ovat ajan tasalla.

Nykyaikana on useita erityyppisiä hyökkäyksiä, haittaohjelmia ja haavoittuvuuksia, joita harrastajat ja ammattirikolliset voivat käyttää tietoturvan murtamiseen ja loukkaamiseen. Mitä enemmän laitteita yhdistetään lähiverkkoon, sitä enemmän on potentiaalisia kohteita hyökkäyksille ja haittaohjelmille. Kaikilta eri hyökkäystavoilta on vaikea suojautua, mutta haittaohjelmien ja hyökkääjien pääsyä laitteille voi vaikeuttaa monin eri tavoin.

1.1 Tavoite

Tutkimusongelmana on halu selvittää, mitkä ovat tällä hetkellä ajankohtaiset uhat langattoman lähiverkon ja sitä käyttävien laitteiden tietoturvalle, sekä kuinka niiltä tavallinen kotikäyttäjä voi suojautua. Tavoitteena on myös selvittää nykyaikaisen langattoman lähiverkon konfiguroinnin vaihtoehdot ja suositukset. Lopullisessa johtopäätöksessä käyn läpi löytyneitä keinoja kodin langattoman lähiverkon suojaukseen.

1.2 Termistö

Access point (AP)	Langattoman lähiverkossa oleva tukiasema, jonka kautta voidaan yhdistää laitteita langattomasti lähiverkkoon.
Aliverkko	Aliverkolla tarkoitetaan tiettyä osaa verkosta, jossa kaikki laitteet jakavat saman aliverkonpeitteen. Samassa aliverkossa olevat laitteet voivat kommunikoida suoraa keskenään ilman reititintä.
Brute-force attack	Väsytyshyökkäyksessä salasanoja tai muita tunnuksia käytetään lukemattomia kertoja siinä toivossa, että jollain kerralla se on oikea.
DDNS	Dynaaminen DNS. Metodi, jolla automaattisesti päivitetään palvelimen nimi DNS:ään.
DNS	Internetin nimipalvelujärjestelmä, jonka tarkoituksena on muuntaa verkkotunnuksia IP-osoitteiksi.
Freeware	Tietokoneohjelma, jota jaetaan ilmaiseksi tai valinnaista maksua vastaan ilman lähdekoodia.
Handshaking	Kättely on protokollaan kuuluva prosessi, jossa kaksi laitetta muodostaa yhteyden ja sopivat sen parametreista.
Internet of things (IoT)	Esineiden internet. Järjestelmä, joka koostuu laitteista, jotka ovat varutettuja yksilöllisillä tunnisteilla. IoT-laitteet voivat siirtää tietoa verkon kautta ilman ihmisen väliintuloa.
IP-Packet	IP-verkossa tietoa siirretään IP-paketeissa. Paketit toimitetaan IP-osoitteen perusteella kohteena olevalle laitteella.
LAN	Local area network. Tietokoneista muodostuva lähiverkko, joka on suhteellisen pienellä alueella. Lähiverkot ovat yhteyksissä toisiin lähiverkkoihin mm. kaapeleiden tai radioaaltojen välityksellä.
OSI-malli	Open Systems Interconnection Reference Model kuvaa kerroksittain seitsemää eri tapaa siirtää tietoa. Jokainen kerros liittyy aikaisempaan ja ylempään kerrokseen.
Payload	Tietosuojassa käytettävä termi, jolla tarkoitetaan tietokoneviruksessa tai madossa olevaa osuutta, joka tekee varsinaiset haitalliset toimet.
PLC	Programmable logic controller on automaatioprosessien ohjauksessa käytetty ohjelmoitava tietokone, joka on suunniteltu luotettavaksi ja kestämään teollisia ympäristöjä.

PUP-ohjelma	Mahdollisesti ei-toivottu ohjelma. Tällainen ohjelma voi vaarantaa yksityisyyden tai heikentää tietokoneen turvallisuutta.
Routing Table	Reititystaulu. Verkkolaitteiden käyttämä taulukko, josta, riippuen laitteesta ilmenee mm. reititysprotokolla, oletusreitti, IP-osoite tai aliverkko, johon pääsee tietystä portista.
SCADA	Supervisory control and data acquisition on teollisuudessa käytetty graafinen käyttöliittymä automaatiojärjestelmiin.
Shareware	Vapaasti jaettava ohjelma, jota voi käyttää maksuttomasti tietyin ehdoin tai rajoituksin.
Spoofing	IP-osoitteen väärentäminen. Lähtevä IP-osoite valehdellaan, jotta voi tekeytyä toiseksi laitteeksi tai piilottaa oman identiteetin.
SQL	Structured Query Language. Relaatiotietokannoissa käytettävä kieli, jota käyttämällä tehdään kyselyitä tietokantoihin, hallitaan tietokantoja ja niiden sisältämää tietoa, sekä yhteyksiä.
TCP	Transmission Control Protocol. Tietokoneiden välinen tietoliikenneprotokolla luotettavan tiedonsiirron toteuttamiseksi.
TLS	Transport Layer Security, aiemmin nimeltään Secure Sockets Layer (SSL), on salausprotokolla, jonka avulla voidaan suojata IP-verkkojen yli tapahtuvaa tietoliikennettä.

2 LANGATON LÄHIVERKKO

Langaton lähiverkko on lähiverkko, joka käyttää datan siirtämisessä radiosignaaleja fyysisen kaapelin sijaan. Näiden radiosignaalien kuljettamisessa kotiympäristössä käytetään pääsääntöisesti taajuusalueita 2,4 GHz ja 5 GHz. Näiden kahden erona on se että, 2,4 GHz taajuudella data eli tieto liikkuu 5 GHz taajuutta hitaammin, mutta se liikkuu kauemmas ja paremmin erilaisten materiaalien läpi kuten seinien (kuva 1). Tämän vuoksi kodin reitittimen paras mahdollinen sijoituskohta on hyvä miettiä tarkkaa, jotta signaalilla olisi mahdollisimman hyvä kuuluvuus päätelaitteille. (Lowe 2016, 137-138.)

Kuva 1. Wi-Fi signaalin kuuluvuus asunnossa. (WiFi-Professionals 2019, viitattu 31.8.2020)

2.1 Langattoman lähiverkon standardi

Langattoman lähiverkon mahdollistava standardi on IEEE 802.11, jonka on kehittänyt Institute of Electrical and Electronics Engineers (IEEE). Tämä tekniikan alan järjestö toimii yli 160 maassa ja siihen kuulu yli 419 000 jäsentä. Järjestö on omistautunut teknillisen huippuosaamisen ja innovaatioiden kehittämiseen ihmiskunnan edun hyväksi. Järjestö on suunniteltu palvelemaan ammattilaisia, jotka työskentelevät elektroniikan, tietotekniikan ja sähköön liittyvillä aloilla.

Järjestöllä on tällä hetkellä yli 1300 eri standardia ja yli 600 standardia kehityksen alla. IEEE tekee myös laajaa julkaisutoimintaa, järjestää konferensseja ja koulutuksia. (IEEE 2020, viitattu 27.8.2020.)

Lukuisten versioiden ja variaatioiden myötä 802.11 standardi on mennyt monimutkaisemmaksi ymmärtää. Tämän vuoksi langattoman lähiverkon standardeille on annettu uudet nimitykset, jotta normaaleilla tietoteknillisten laitteiden käyttäjillä olisi helpompi ymmärtää minkä sukupolven teknologiasta on kyse.

IEEE 802.11n - Wi-Fi 4

Wi-Fi 4 otettiin käyttöön ensimmäistä kertaa vuonna 2009 ja se kehitettiin korvaamaan sitä edeltävät versiot standardista. Wi-Fi 4 versio toimii käyttämällä 2,4 GHz radiotaajuutta ja 5 GHz radiotaajuutta dual-band reitittimissä. Wi-Fi 4 hyödyntää uutta tekniikkaa nimeltä MIMO (multiple-input multiple-output), joka mahdollistaa neljän yhtäaikaisen yhteyden muodostamisen samaan laitteeseen, jolloin tiedonsiirrosta saadaan nopeampaa. Wi-Fi 4 heikkoutena on ollut sen 2,4 GHz taajuusalue, koska sitä taajuutta käyttävät useat eri laitteet kuten itkuhälyttimet, bluetooth-laitteet ja langattomat kaiuttimet. Dual-band reitittimet ovat korjanneet tätä ongelmaa 5 GHz taajuudella. (Jongerius 2020, luku 9, Wi-Fi 4 - 802.11n (HT), viitattu 22.9.2020.)

IEEE 802.11ac - Wi-Fi 5

Tällä hetkellä suosituin langattoman lähiverkon standardi on Wi-Fi 5. Standardi otettiin ensimmäistä kertaa käyttöön vuonna 2014. Wi-Fi 5 toimii 5 GHz radiotaajuudella, mutta on taaksepäin yhteensopiva aikaisempien versioiden kanssa eli se myös pystyy käyttämään 2.4 GHz radiotaajuutta. Standardin MIMO tekniikan kehityksessä tapahtui edistysaskel, jonka avulla saadaan tuplasti enemmän yhtäaikaisia yhteyksiä laitteiseen edeltäjään verrattuna eli jopa kahdeksan yhteyttä samaan laitteeseen. Käytännössä se ei kuitenkaan ole mahdollista, koska ei ole laitteita, jotka kykenisivät hyödyntämään näin montaa yhtäaikaista yhteyttä. (Jongerius 2020, luku 10, Wi-Fi 5 - 802.11ac (VHT), viitattu 22.9.2020.)

IEEE 802.11ax - Wi-Fi 6

Wi-Fi 6 on uusin kehitetty langattoman lähiverkon teknologia. Se on edeltäjiään entistä tehokkaampi sekä kustannuksiltaan, että suorituskyvyltä (kuva 2). Jokainen sukupolvi on tuonut Wi-Fi yhteyteen entistä enemmän ominaisuuksia ja tämä uusin versio vastaa entistä paremmin nykyisen langattoman lähiverkon kasvaviin tarpeisiin eli signaalin kattavuusalueeseen sekä kasvavaan laite- ja tiedonsiirtomääriin. Wi-Fi 6 on kehitetty toimimaan tehokkaammin tiheissä ympäristöissä, ulkoilmassa, ja se on takaisinpäin yhteensopiva 5 GHz ja 2,4 GHz taajuudella toimivien vanhempien Wi-Fi-protokollien kanssa. (Wi-Fi Alliance 2018, viitattu 25.8.2020.)

Feature	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6
Channel bandwidth (MHz)	20, 40	20, 40, 80, 80 + 80, 160	20, 40, 80, 80 + 80, 160
Frequency bands	2.4 and 5 GHz	5 GHz	2.4 and 5 GHz
Maximum data rate	150 Mbps	3.5 Gbps*	9.6 Gbps*
Highest subcarrier modulation	64-QAM	256-QAM	1024-QAM
Spatial streams	1	4	8
Underlying technology	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax

** Depending upon number of spatial streams and channel used*

Kuva 2. Wi-Fi 4, 5 ja 6 vertailutaulukko. (McDowell 2019, viitattu 23.9.2020)

Orthogonal Frequency Division Multiplexin (OFDM) on teknologia, jota Wi-Fi 5, 4 ja niitä vanhemmat standardit käyttävät tiedonsiirrossa. OFDM mahdollistaa useamman laiteen ja AP:n lähettämään ja vastaanottamaan tietoa käyttämällä eri taajuuskanavia. Wi-Fi 6 tuo mukanaan uudemman version tästä teknologiasta, jonka nimeksi on annettu Orthogonal Frequency Division Multiple Access (OFDMA). Iso ero näissä teknologioissa on se, että OFDM siirtää tietoa yhdelle laitteelle kerrallaan, joka on hidasta. OFDMA sen sijaan pystyy lähettämään tietoa usealle laitteet yhtäaikaisesti jakamalla liikenteen pienempiin paketteihin, jolloin pakettien jonotusajat pienenevät. Wi-Fi 6 AP pystyy varaamaan tietyn verran kapasiteettia jokaiselle laitteelle riippuen siitä paljonko laitteet käyttävät kaistaa, jolloin langattoman verkon suorituskyky paranee. OFDMA on kehitetty varsinkin isoja tiloja varten, joissa on paljon yhtäaikaisia käyttäjiä. (Vigliarolo 2020, viitattu 25.8.2020.)

Multi-user multiple input, multiple output (MU-MIMO) toimii halutessaan OFDMA:n kanssa ja se mahdollistaan korkean suoritustehon Wi-Fi 6 verkkolaitteille, kun käytettävänä on rajallinen määrä antenneja. Wi-Fi 5 laitteet tukevat neljää samanaikaista käyttäjää, mutta Wi-Fi 6 laajentaa tämän määrän kahdeksaan samanaikaiseen käyttäjään. Tämä teknologia kehitettiin hyödyntämään kaikkia verkkolaitteen ns. spatial streameja eli yhtä aikaa aktiivisena olevia yhteyksiä, joita

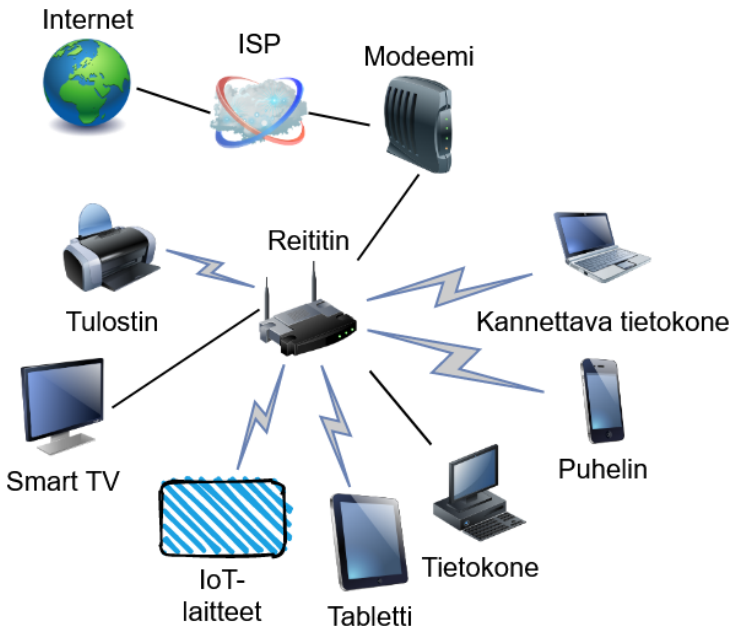
verkkolaitteella voi olla päätelaitteisiin. Wi-Fi 6 tukee korkeimmillaan kahdeksaa yhtäaikaista spatial streamia, mutta nykyaikaiset päätelaitteet tukevat vain yhtä tai kahta spatial streamia. Tämän teknologian hyödyntäminen vaatii, että langaton tukiasema tietää missä suunnassa päätelaite sijaitsee, johon tietoa lähetetään. Tästä syystä MU-MIMO lisää viivettä verrattuna OFDMA-tekniikkaan, mutta sen avulla voidaan siirtää tehokkaasti esimerkiksi tiedostoja, koska se voi varata koko spatial streamin kapasiteetin yhdelle laitteelle. (Ruckus Education 2019, viitattu 28.8.2020.)

Wi-Fi 6:ssa on uusi ominaisuus nimeltä BSS Coloring (Basic Service Set), jonka avulla tehostetaan langattoman lähiverkon käyttöä tiloissa, joissa on useampia langattomia tukiasemia ja lukuisia käyttäjiä. Tavallinen BSS lisää tunnisteen liikenteeseen, josta tunnistaa mistä langattomasta lähiverkosta se on tullut. BSS Coloring lisää tähän vielä numeron 0 ja 63 väliltä, jolloin tukiasema voi tunnistaa ja olla välittämättä tietystä osaa liikennettä. (Coleman 2019, viitattu 27.8.2020.)

TwT (Target Wakeup Time) on myös uusi ominaisuus Wi-Fi 6:ssa. Nimensä mukaisesti sen avulla tukiasema ja päätelaitteet voivat neuvotella ja määritellä, milloin ja kuinka usein molemmat laitteet ovat aktiivisena ja valmiita vastaanottamaan tietoa. Tämä mahdollistaa sen, että päätelaitteet voivat olla lepotilassa, kun sen ei tarvitse lähettää tietoa, jolloin se vähentää päätelaitteiden virrankulutusta. (Ruckus Education 2019, viitattu 28.8.2020.)

2.2 Verkkolaitteet

Verkkolaitteet ovat elektronisia laitteita, jotka ovat tarpeellisia kommunikaation ja yhteyden muodostamiseksi erilaisten päätelaitteiden välille. Näiden verkkolaitteiden ja kaapeleiden avulla muodostetaan lähiverkko, jota pitkin laiteet voivat kommunikoida keskenään (kuva 3). Nykyajan lähiverkoista löytyykin nykyään paljon erilaisia laitteita älytelevisioista kannettaviin tietokoneisiin, jotka hyödyntävät sitä.



Kuva 3. Nykyajan lähiverkko, jossa on sekä langallisia, että langattomia yhteyksiä. Kuva piirretty Draw.io sivuston sovelluksella.

Modeemi

Modeemi (Modulator-Demodulator) muuttaa analogisen signaalin digitaaliseksi tiedoksi eli biteiksi ja bitit takaisin analogiseksi signaaliksi, jotta tietoa voidaan siirtää satelliitin, puhelinlinjan tai kaapelin välityksellä. Modeemi on laite, joka mahdollistaa internet yhteyden tietokoneelle, reitittimelle tai kytkimelle. Nykyaikaiset modeemit ovat pääasiassa DSL tai kaapelimodeemeita, mutta on olemassa myös eri tekniikoihin perustuvia kuten valokuituun. DSL modeemit toimivat tavallista puhelinlinjaa pitkin, mutta käyttävät laajempaa taajuusaluetta, joka mahdollistaa nopeamman tiedonsiirron. Kaapelimodeemit käyttävät kaapelitelevision kaapeleita tiedon lähettämiseen ja vastaanottamiseen. (TechTerms 2019, viitattu 28.8.2020.)

Reititin

Reititin on laite, joka välittää paketteja kahden tai useamman verkon välillä. Reitittimen toimintaperiaatteena on, että se tarkistaa siihen saapuvan paketin IP-osoitteen ja vertaa sitä omaan reititystaulukkoon, jonka perusteella se lähettää paketin eteenpäin seuraavaa laitetta kohti halvinta ja parasta reittiä käyttäen. Reititystaulukkoon on mahdollista määritellä default route eli se reitti, mitä pitkin lähetetään kaikki liikenne, jota ei ole reititystaulukossa. Esimerkiksi kotiympäristössä tyypillisin default route on internet palveluntarjoaja. (Rouse 2019, viitattu 21.6.2020.)

Kytkin

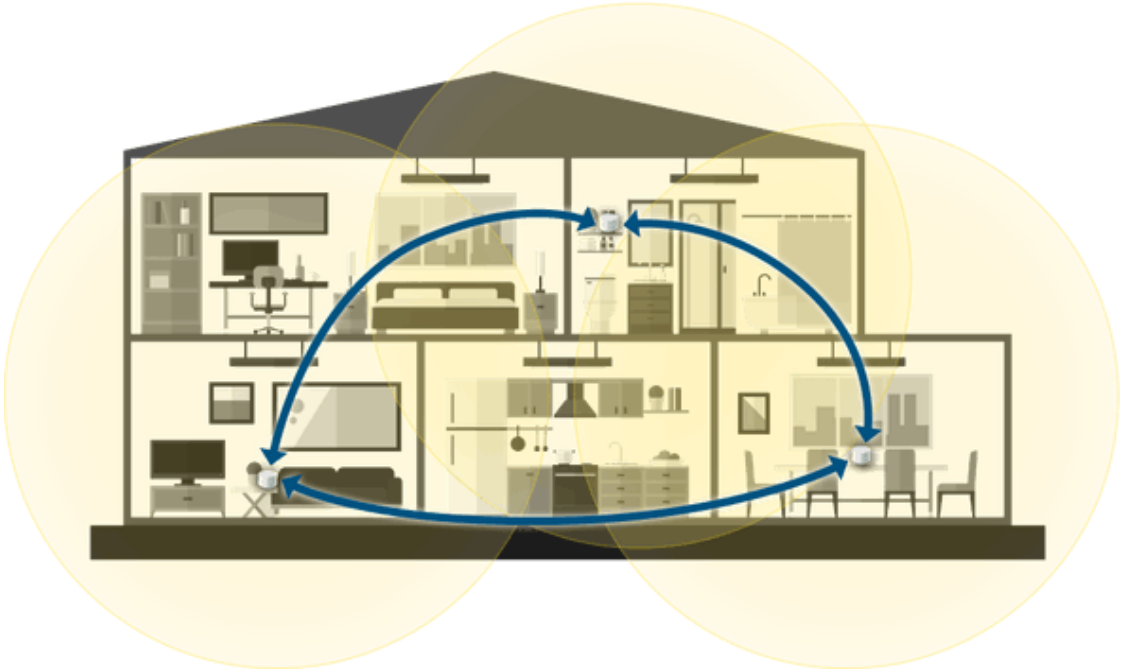
Kytkin on laite, jonka avulla yhdistetään useita eri laitteita samasta verkosta toisiinsa MAC-osoitteiden perusteella. Kotikäytössä olevissa kytkimissä on useita fyysisiä portteja verkkokaapeleiden liittämiseksi ja yrityskäyttöön tarkoitetuissa kytkimissä voi olla jopa useita kymmeniä. Yksinkertaisesti selitettynä kytkin vastaanottaa paketteja joltain laitteelta, joka on yhdistettynä johonkin porttiin ja lähettää sen paketin kohti seuraavaa laitetta, joka on yhdistettynä johonkin toiseen porttiin. Kytkin pitää yllä MAC-osoitteista ja niihin liittyvistä porteista taulukkoa, jonka perusteella se osaa lähettää paketin eteenpäin. Osoitteen puuttuessa taulukosta, paketti lähetetään eteenpäin jokaiseen porttiin paitsi siihen, mistä se on tullut. (MOOC.fi 2020, viitattu 28.8.2020.)

Tukiasema

Tukiasema eli Access point (AP) on laite, kuten WLAN reititin, josta päätelaitteet saavat yhteyden langattomaan lähiverkkoon. Tukiasema on yleensä yhdistettynä verkkokaapelilla toisiin verkkolaitteisiin kuten modeemiin. Esimerkiksi isoissa rakennuksissa voi olla useita WLAN tukiasemia, joiden avulla saadaan riittävän hyvä kuuluvuus ympäri rakennusta. Langatonta tukiasemaa voi käyttää esimerkiksi tilanteessa, jossa halutaan, että vain eri päätelaitteet keskustelevat keskenään ilman, että ne ovat yhteydessä muuhun verkkoon. (MOOC.fi 2020, viitattu 28.8.2020.)

Langaton mesh verkko (WMN)

Langaton mesh verkko on yksi tapa vähentää langattoman lähiverkon radiosignaalien katvealueita, joita esimerkiksi seinät, ovet ja muut esteet aiheuttavat. Langattomaksi mesh-verkoksi kutsutaan lähiverkkoa, jossa on useampia langattomia tukiasemia, jotka ovat liitettynä yhteen samaan verkkoon. Mesh-verkon tukiasemista yksi on yhdistettynä verkkoon kaapelilla ja muut tukiasemat kommunikoivat langattomasti tähän tukiasemaan, joko suoraa tai toisten tukiasemien kautta (kuva 4). Mesh-verkon etuna onkin se, että langattomien päätelaitteiden radiosignaalit pysyvät hyvänä, vaikka laitteen kanssa liikkuisi eri puolella rakennusta, koska ne osaavat automaattisesti yhdistää parhaimman signaalin tarjoavaan tukiasemaan. (Rasmussen 2020, viitattu 24.8.2020.)



Kuva 4. Mesh-verkon toimivuutta havainnollistava kuva, jossa Mesh-laitteet kommunikoivat keskenään ja parantavat WiFi-kuuluvuutta eri puolella asuntoa. (Rasmussen 2020, viitattu 24.8.2020)

3 UHAT JA HAAVOITTUVUUDET

Langattomien lähiverkkojen kätevyys ja matalat kustannukset ovat iso syy niiden suosioon, mutta niitä käyttäessä täytyy muistaa niiden tietoturva. Langaton lähiverkon tietoturvallisuus voi vaarantua tavanomaisten haittaohjelmia kautta, jotka tulevat laitteelle erilaisten reittien kuten sähköpostin, massamuistilaitteiden tai internetin välityksellä. Olemassa on myös erilaisia hyökkäyksiä, jotka kohdistuvat itse radiosignaaleihin, jotka kuljettavat tietoa laitteelta toiselle. Hyökkääjät voivat mm. passiivisesti kuunnella radiosignaaleja ja kerätä lähetettyä tietoa tai aktiivisesti yrittää murtaa salauksia ja ujuttaa haittaohjelmia uhrien laitteille, jotta laitteisiin ja niiden sisältämiin tiedostoihin pääsisi käsiksi. (Vacca 2014, 29–36.)

Europolin IOTCA (Internet organised Crim Threat Assessment) 2019 tutkimuksen mukaan viime aikoina kyberrikollisten suosiossa on ollut mm. DDoS-hyökkäykset, tiedon varastamiseen ja manipulaatioon erikoistuvat haittaohjelmat, maksupetokset anastetuilla pankki- ja luottokortti tiedoilla ja erilaiset kiristyshaittaohjelmat, jotka ovat enimmissä tapauksissa suunnattu yrityksille, mutta ne ovat myös levinneet laajalle alueelle ympäri maailmaa tehden paljon taloudellista vahinkoa. (Europol 2019, 4–9, viitattu 17.9.2020.)

3.1 Haittaohjelmat

Haittaohjelma on yleiskäsite ohjelmalle, jonka tavoitteena on saastuttaa laite haitallisella koodilla. Haittaohjelmien kirjo on laaja, joten niitä jaotellaan sen mukaan, miten ne toimivat ja leviävät. Näille kaikille yhteistä on haitallisten tapahtumien aiheuttaminen tietokonejärjestelmissä. Haittaohjelmat pääsevät laitteille hyökkäyksen yhteydessä tai käyttäjän toimesta. (Firch 2019, viitattu 9.6.2020.)

Exploit

Tietotekniikassa eksploitaatioksi kutsutaan järjestelmien heikkouksien ja haavoittuvuuksien hyödyntämistä vahingollisen tai rikollisen toiminnan toteuttamiseksi. Eksploitaatiot tapahtuu useimmiten vahingollisten koodien avulla, jotka muuttavat kuinka järjestelmät normaalisti toimivat. Näiden heikkouksien ja haavoittuvuuksien hyödyntämisen avulla hyökkääjät ja haittaohjelmat

voivat mm. luoda takaportteja hyökkääjille ja antaa hyökkääjälle täydet oikeudet järjestelmään. (PrivacyCanada 2020, viitattu 9.6.2020.)

Zero-day

Zero-day on haavoittuvuus, joka on ensimmäistä kertaa havaittu laitteessa, komponentissa tai ohjelmassa. Tälle haavoittuvuudelle ei ole valmista korjauspäivitystä tai se ei ole valmistajan tiedossa, jolloin kyberrikollisilla on mahdollisuus hyväksikäyttää tätä aukkoa tietoturvassa. Yleensä nämä zero-day haavoittuvuudet tulevat puhtaasti vahingossa ohjelmoinnin sivutuotoksena. Esimerkiksi zero-day hyökkäyksiin lasketaan sellaiset hyökkäykset, joita vastaan ei ole vielä mitään suojauskeinoja. Ne hyödyntävät ennalta tunnistamattomia tietoturva aukkoja hyökkäysten toteuttamiseksi. (Norton 2020, viitattu 19.6.2020.)

Virus

Virukset kuuluvat yleisimpiin haittaohjelmiin ja niiden leviäminen alkaa usein käyttäjän toimesta. Virukset leviävät kopioimalla itseään ja levittäytymällä automaattisesti. Virukset voivat olla pitkän aikaa uinuvassa tilassa ja hiljalleen saastuttaa laitteita monien eri medioiden kautta, kuten mm. sähköpostin, USB-laitteiden ja lähiverkon laitteiden, jonka jälkeen tiettyjen vaatimuksien täytyttyä se toimittaa lastinsa eli ns. ”payloadin”. (Firch 2019, viitattu 9.6.2020.)

Computer Worm

Mato-haittaohjelma on itsenäisesti toimiva haittaohjelma, joka monistaa itseään levittäytyäkseen toisiin tietokoneisiin. Mato levittäytyy internetin ja muiden medioiden välityksellä ilman ihmisen väliintuloa. Madot voivat muuttaa ja poistaa tiedostoja, sekä lisätä muuta haitallista koodia tietokoneelle. Yksi yleinen versio madosta on sellainen, joka monistaa itseään loputtomasti, jotta tietokoneen resurssit loppuvat kesken. Madot voivat tämän lisäksi viedä tietoa, asentaa takaportteja ja mahdollistaa hyökkääjän saamaan tietokoneen hallinnan itselleen. (Norton 2020, viitattu 11.9.2020.)

Trojan Horse

Troijan hevonen tai ns. troijalainen on haittaohjelma, joka piiloutuu ja tekeytyy joksikin oikeaksi ohjelmaksi. Troijalainen mahdollistaa uhrin laitteen vakoilemisen, tietojen anastamisen, muuttamisen ja itse laitteen suorituskyvyn heikentämisen. Troijalainen voi tulla laitteelle kuten mikä tahansa muukin haittaohjelma, mutta toisin kuin virus, troijalaiset eivät voi itsestään käynnistyä, eikä levittäytyä laitteella tai laitteelta toiselle ilman käyttäjän väliintuloa. (Moes 2019, viitattu 11.6.2020.)

Keylogger

Keylogger on haittaohjelma, joka käyttäjän tietämättä monitoroi ja tallentaa jokaisen käyttäjän tekemän napin painalluksen lokitiedostoihin. Keyloggereiden käyttö on petollista toimintaa, jonka päätarkoituksena on kerätä käyttäjiltä kirjautumistunnuksia, pankkitietoja tai muuta arkaluontoista tietoa. (Panda Security 2017, viitattu 11.6.2020.)

Keyloggerit voidaan jaotella kahteen eri kategoriaan: laitteisto- ja ohjelmapohjaiseen. Näistä harvinaisempia ovat laitteistopohjaiset, koska ne vaativat fyysisen pääsyn uhrin laitteelle. Tästä syystä ohjelmapohjaiset versiot ovat enemmän suosiossa. Ohjelmapohjaiset keyloggerit päätyvät uhrin laitteille useimmiten jonkin toisen haittaohjelman mukana. (Panda Security 2017, viitattu 11.6.2020.)

Ransomware

Ransomware on viime aikoina paljon esillä ollut kiristykseen erikoistuva haittaohjelma, joka salausalgoritmeja käyttämällä salaa laitteen tiedostot sekunneissa tietyllä salausavaimella. Salauksen nopean tapahtumisen takia uhrilla ei ole aikaa reagoida ennen kuin on liian myöhäistä. Tämän jälkeen haittaohjelma alkaa kiristämään uhria ostamaan salausavaimen, jonka avulla hän purkaa tiedostojen salauksen. Useimmissa tapauksissa kiristäjät vaativat maksut kryptovaluuttoina, koska viranomaiset eivät niitä pysty seuraamaan tai paljastamaan näiden valuuttojen omistajia. (Moes 2019, viitattu 11.6.2020.)

Yleisimmät tavat Ransomwaren leviämiseen on kuten muillakin haittaohjelmilla, mutta sitä levitetään varsinkin sähköpostien liitetiedostoina tai linkkeinä sivustoille, joiden kautta tämä

haittaohjelma pääsee laitteelle. Viime aikoina haittaohjelmaa on levitetty sosiaalisen median ja pikaviestintä sovelluksien kautta. (Moes 2019, viitattu 11.6.2020.)

Adware

Adware on PUP-ohjelma (suom. mahdollisesti ei-toivottu ohjelma), joka tekee rahaa sen kehittäjälle mainostuloilla, joita se saa mainosten näyttämisestä laitteella. Ohjelma voi muuttaa laitteen selainasetuksia ja kerätä laitteelta erilaisia tietoja, kuten internet selaushistoria ja sijaintitiedot. Näitä tietoja hyväksikäyttäen ohjelma näyttää profiloituja mainoksia käyttäjälle, mutta myös geneerisiä huijausmainoksia eli esimerkiksi: kuinka rikastua nopeasti, valheelliset haittaohjelma-varoitukset ja ihme laihdutuskuurit. Ohjelman kehittäjä voi myös myydä keräämänsä tiedon eteenpäin kolmannelle osapuolelle, joka voi entistä tarkemmin kohdentaa mainoksia käyttäjälle. (Malwarebytes 2020, viitattu 17.6.2020.)

Adwarella on kaksi eri pääkeinoa päästä laitteelle, joista yleisempi on asentuminen jonkin ilmaisohjelman kylkiäisenä käyttäjän siitä tietämättä. Tämä mahdollistaa ohjelman tarjoamisen ilmaisversiona, koska sen tekijä saa mainostuloja adwaren kautta. Toisena keinona päästä laitteelle on vierailla saastuneella sivustolla, jossa adware latautuu laitteelle selainhaavoittuvuuksia hyväksikäyttäen. Latautumisen jälkeen se alkaa keräämään tietoja laitteelta, ohjaamaan sivupyyntöjä muualle ja näyttämään käyttäjälle mainoksia. (Malwarebytes 2020, viitattu 17.6.2020.)

Rootkit

Rootkit on haittaohjelma, jolla on etuoikeutettu pääsy laitteella, joka mahdollistaa laitteen tai ohjelman täyden hallinnan. Rootkit voi piilottaa tiettyjen ohjelmien ja prosessien olemassaolon normaaleilta tavoilta havaita haittaohjelman, jolloin sitä on vaikea löytämistä laitteelta. Rootkit voi olla asennettuna kernel tasolla, joka tarkoittaa sitä, että sen löytäminen ja poistaminen voi olla lähes mahdotonta. (Technibble 2011, viitattu 18.6.2020.)

Hyökkääjä voi asentaa rootkitin laitteelle, mikäli hänellä on järjestelmänvalvojan tai ns. root oikeudet. Oikeuksien saaminen tapahtuu suorana hyökkäyksenä järjestelmää vastaan haavoittuvuuksia hyväksikäyttäen, varastetuilla käyttäjätunnuksilla tai käyttäjän itse asentamana. Asentumisen jälkeen rootkit säilyttää korkeimmat oikeudet tehdä muutoksia ja piilottaa itsensä. (Vacca 2014, 11.)

3.2 Hyökkäykset

SQL-injektio

SQL-injektio on hyökkäys, jossa haitallisia SQL-kyselyitä lähetetään tietokantaan esimerkiksi nettisivulla olevan syöttökentän kautta. SQL-injektion avulla hyökkääjä voi varastaa tietoja kuten käyttäjätietoja ja muutella taulukoissa olemassa olevaa dataa. Pahimmassa tapauksessa heikosti suojattuun tietokantaan kohdistuvassa hyökkäyksessä voidaan varastaa, muuttaa ja poistaa kaiken sen sisältämän tiedon. SQL-injektioiden vaarallisuus riippuu hyökkääjän taidoista ja kyvystä kuvitella tietokannan rakenne, sekä itse tietokannan tietoturvamekanismit. (Owasp 2020, viitattu 17.6.2020.)

Bottiverkko

Bottiverkko (engl. Botnet) koostuu yhdestä tai useammasta laitteesta, jotka ovat toisiinsa yhteyksissä internetin välityksellä. Kyberrikolliset käyttävät näitä erikoistuneita troijalaisia hevosia murtamaan laitteiden suojaukset, jolloin he saavat laitteet omaan haltuunsa. Murretut ja saastuneet laitteet ovat tämän jälkeen osana bottiverkkoa, jota voidaan etähallita ja käyttää rikolliseen toimintaan. Mitä useampaan laitteeseen troijalainen leviää, sitä isompi ja tehokkaampi tästä bottiverkosta tulee. Bottiverkkoja käytetään useimmiten isoissa palvelinestohyökkäyksissä tai roskapostikampanjoissa. (Kaspersky 2020, viitattu 18.6.2020.)

Palvelunestohyökkäys

Distributed Denial of Service (DDoS) on hyökkäys, jonka tarkoituksena on hidastaa tai pysäyttää hyökkäyksen kohteena oleva verkko, palvelu, palvelimen tai infrastruktuuri massiivisella internet liikenteen määrällä. Palvelunestohyökkäys saavuttaa niiden tehokkuuden useiden laitteiden avulla, mitä enemmän, sitä tehokkaampi. Useimmiten palvelunestohyökkäyksessä käytetyt laitteet ovat tietokoneita tai IoT-laitteita. (Cloudflare 2020, viitattu 18.6.2020.)

Palvelunestohyökkäykset voidaan jaotella muutamaan pääkategoriaan. Näistä ensimmäinen tunnetaan nimellä ”layer 7 DDoS attack”, jolla tarkoitetaan, että hyökkäys tapahtuu OSI-mallin ylintä kerrosta eli sovelluskerrosta hyödyntäen. Hyökkäyksen tehtävänä on ylikuormittaa kohteen resurssien käyttö luomalla useita HTTP-pyyntöjä. Hyökkäys on hyökkääjän näkökulmasta kustannustehokasta, koska HTTP-pyyntö ei vaadi paljoa resursseja hyökkääjältä. Kohteena oleva palvelin joutuu verkkosivuston monimutkaisuuden mukaan, lataamaan useita tiedostoja ja tietokantapyyntöjä, jotta se voi luoda verkkosivunäkymän. (Cloudflare 2020, viitattu 18.6.2020.)

Toisena pääkategoriana on protokolla hyökkäykset, jotka tunnetaan myös nimellä ”state-exhaust attacks”, joiden tarkoituksena on kuluttaa loppuun kaikki mahdolliset resurssit palvelimilta, palomuureilta ja kuormitusten tasapainottajilta. Protokollahyökkäykset hyväksikäyttävät heikkouksia OSI-mallin verkko- ja kuljetuskerroksissa, joiden avulla kohde saadaan ison rasituksen alle. Tämä aiheuttaa sen, ettei palvelimeen saada enää yhteyttä. Esimerkkinä SYN floodiksi nimetty hyökkäys hukuttaa kohteen tekaistuista IP-osoitteista tulevilla TCP-kättelypyynnöillä TCP-yhteyden aloittamiseksi. Palvelin vastaa pyyntöön ja jää odottamaan vastausta, jota ei ikinä tule. (Cloudflare 2020, viitattu 18.6.2020.)

Kolmantena kategoriana on volumetriset hyökkäykset, joissa on tarkoituksena ylikuormittaa kohteena oleva palvelin ja verkko massiivisella määrällä liikennettä. Tästä hyvä esimerkki on ns. DNS Amplification, jossa bottiverkko hyödyntää avoimia DNS nimipalvelimia ja käyttää tekaistua kohdepalvelimen IP-osoitetta, jolloin bottiverkon tekemät DNS-pyyntöjen vastaukset menevät hyökkäyksen kohteena olevalle palvelimelle eivätkä takaisin boteille. (Cloudflare 2020, viitattu 18.6.2020.)

Man-in-the-middle (MITM)

MITM hyökkäyksessä on nimensä mukaisesti kahden osapuolen keskustelu, jonka välissä on hyökkääjä. Hyökkäyksen tarkoituksena on välittää tietoa keskustelijoiden kesken ilman, että he tietävät hyökkääjän olevan heidän välissä. Hyökkääjän ujuttautumisen jälkeen hän jatkaa viestien välittämistä osapuolten kesken, jolloin osapuolilla ei ole tietoa, että heidän välissä on ylimääräinen henkilö. Hyökkääjä voi muuttaa keskustelun sisältöä haluamallansa tavalla tai jäädä väliin salakuuntelemaan ja keräämään tietoa. (Norton 2020, viitattu 20.9.2020.)

Tavanomaisessa MITM hyökkäyksessä hyökkääjä saa haltuunsa heikosti suojatun reitittimen. Tämänlaisia reitittimiä voi löytyä mm. yleisiltä alueilta, joissa on tarjolla ilmainen Wi-Fi tai mahdollisesti kodeista, joissa niitä ei ole konfiguroitu tarpeeksi hyvin. Hyökkääjä tekeytyy reitittimeksi, jos hän löytää ja pääsee käsiksi haavoittuvaan reitittimeen. Tämän jälkeen hyökkääjä voi ottaa talteen kaiken liikenteen mitä käyttäjät tekevät, sekä mahdollisesti ujuttamaan haittaohjelmia kuten keyloggereita käyttäjien laitteille, jolloin hyökkääjä saa kaikki kirjoitetut tiedot itselleen eli esimerkiksi henkilö-, kirjautumis- ja pankkitiedot. (Norton 2020, viitattu 20.9.2020.)

Esimerkiksi henkilö A haluaa tehdä tilisiirron ystävälle. Henkilö A luulee asioivansa nettiselaimella suoraa pankin kanssa. Heidän välissä on kuitenkin heidän tietämättään kolmas osapuoli eli hyökkääjä. Henkilön A kirjautuu verkkopankkiin, mutta yhteydenotto tapahtuukin hyökkääjän tietokoneelle eikä pankin palvelimelle. Hyökkääjä näyttää henkilölle A verkkopankin sivun, jonka jälkeen henkilö A yrittää kirjautua verkkopankkiin omilla tunnuksillaan. Hyökkääjä saa henkilön A kirjautumistunnukset, joilla hyökkääjä kirjautuu verkkopankkiin ja näyttää henkilölle A verkkopankin. Henkilö A alkaa tekemään tilisiirtoa ystävälleen, mutta hänen tietämättään hyökkääjä muuttaa tilisiirron tietoja. Tilisiirron varmennusvaiheessa verkkopankki pyytää tunnuslukua varmennukseksi, jolloin hyökkääjä välittää tämän kyselyn henkilölle A. Tämän jälkeen henkilö A kertoo tunnusluvun tilisiirron varmistamiseksi, mutta vastaus menee edelleenkin hyökkääjälle. Hyökkääjä antaa tämän tunnusluvun verkkopankille ja tilisiirto toteutuu sellaisena kuin hyökkääjä sen halusi.

Wardriving

Wardriving hyökkäykseksi kutsutaan sellaista hyökkäystä, jossa hyökkääjä esimerkiksi ajaa autolla ympäriinsä etsien langattomia lähiverkkoja. Hyökkääjän löytää kohteen kannettavan tietokoneen avulla, joka on konfiguroitu vastaanottamaan ja kaappaamaan langattomasti tapahtuvaa tiedonsiirtoa. Hyökkääjä voi käyttää tällaista hyökkäystä anastamaan uhrilta pankki- ja henkilötietoja, mikäli langattomassa lähiverkossa ei käytetä minkäänlaista suojausta. (Siciliano 2014, viitattu 14.9.2020.)

Rogue Access Point

Rogue AP on langaton tukiasema, joka on asennettu jo ennestään turvalliseen lähiverkkoon ilman lähiverkon ylläpitäjän tietämystä tai lupaa. Tällaiset tukiasemat eivät ole kalliita ja riittää, että ne

ovat kiinni verkkokaapelilla johonkin verkkolaitteeseen, josta ne toimivat avoimena reittinä suojattuun lähiverkkoon ja sitä kautta hyökkäysalustana muille lähiverkossa sijaitseville laitteille. Ainoa helppo tapa löytää ylimääräinen tukiasema on käyttää hyväksi langatonta lähiverkkoa käyttävää kannettavaa laitetta, jonka avulla voi paikantaa missä on voimakkain signaali, sekä laite, joka sitä lähettää. (Messer 2018, viitattu 19.9.2020.)

Evil Twin

Evil Twin on osittain samankaltainen kuin Rogue AP, mutta niiden käyttö edellyttää, että hyökkääjä tietää, mitkä ovat tämän olemassa olevan langattoman lähiverkon konfiguroinnit eli SSID, salausprotokolla ja mahdollisesti salasana. Evil Twinin avulla hyökkäyksen onnistuminen edellyttää, että langaton tukiasema on tarpeeksi lähellä hyökkäyksen kohteita tai siinä on erityisen tehokas antenni. Tällöin sen lähettämä radiosignaali on voimakkaampi kuin oikean tukiaseman, jolloin laitteet yhdistävät Evil Twiniin. Yhdistämisen jälkeen kaikki langaton verkkoliikenne menee tämän Evil Twinin kautta ja se voidaan tallentaa. Julkisissa paikoissa kuten kahviloissa, Evil Twin on helppo toteuttaa, koska monet paikat tarjoavat ilmaista langatonta lähiverkkoyhteyttä. Tämän vuoksi julkisilla paikoilla on suositeltavaa käyttää jotain kommunikaation salausta kuten HTTPS- tai VPN-yhteyttä, jotta Evil Twin ei näe keskustelun sisältöä. (Messer 2018, viitattu 19.9.2020.)

3.3 Esimerkkitapaukset

Stuxnet

Stuxnet on vuonna 2010 löydetty mato, jonka kohteena oli Iranin ydinlaitoksen käyttämä SCADA-järjestelmä. Stuxnetin uskotaan vahingoittaneen ja hidastaneen Iranin ydinohjelman etenemistä. Stuxnetin paljastuminen nosti mediamylläkän, koska se kohdisti nimenomaan tietyn mallista PLC:tä tietynlaisessa konfiguraatiossa, jota käytettiin Iranin ydinlaitoksen automaatiossa. Tämän lisäksi se sisälsi viitteitä, jonka mukaan Stuxnetin olisi yhdessä kehittäneet Israelin tiedustelu, U.S. National Security Agency (NSA) ja Central Intelligence Agency (CIA). (McAfee 2020, viitattu 8.9.2020.)

Stuxnet käytti leviämisväylänä neljää zero-day haavoittuvuutta, Windows käyttöjärjestelmiä ja USB muistitikkuja. Se etsi saastuneesta tietokoneesta "Siemens Step 7" -ohjelmaa, jota teollisuuden tietokoneet käyttivät PLC:eiden automaatioon ja sähkömekaanisten laitteiden monitorointiin. PLC

laitteen löytämisen jälkeen Stuxnet aloitti lähettämään vahingollisia käskyjä PLC:lle ja valheellista palautetta pääohjaimelle, jolloin laitteita monitoroivat henkilöt eivät tienneet ongelmista ennen kuin oli jo liian myöhäistä. Stuxnet tuhosi useita sentrifugeja Iranin Natanzissa sijaitsevassa uraanin rikastamislaitoksessa muuttamalla sentrifugien pyörintää turvallisten toimintarajojen ulkopuolelle, joka aiheutti niiden hajoamisen. (McAfee 2020, viitattu 8.9.2020.)

WannaCry

WannaCry (WannaCrypt) on kiristyshaittaohjelman, joka salaa laitteen tiedostot ja pyytää maksamaan Bitcoineja salausavaimen saamiseen, jolla tiedostojen salaukset voidaan purkaa. WannaCryn ensimmäinen maailmanlaajuinen hyökkäysaalto alkoi toukokuussa 2017 ja kohteena oli tietokoneet, jotka käyttivät Microsoftin Windows-käyttöjärjestelmää. Haittaohjelma levisi ensimmäisinä päivinä yli 200 000 tietokoneen yli 150 eri maassa. Microsoft julkaisi suojauspäivitykset käyttöjärjestelmilleen haavoittuvuuden paikkaamiseksi aikaisemmin saman vuonna, mutta kaikki eivät olleet niitä asentaneet, joka johti suureen määrään saastumisia. (Kaspersky 2020, viitattu 14.9.2020.)

WannaCry käyttää leviämiseen NSA:n löytämää SMB (server message block) haavoittuvuutta nimeltä "EternalBlue", joka löytyi vanhemmista Windows käyttöjärjestelmistä. Windows käyttää tätä SMB:tä mm. tiedostojen ja tulostimien jakamiseen. WannaCry hyödyntää tätä haavoittuvuutta Windows-käyttöjärjestelmää käyttävän laitteen vaarantamiseen, haittaohjelman asentamiseen ja levittämiseen toisiin laitteisiin lähiverkossa. WannaCry käyttää TCP porttia 445 ja SMB versiota 1 levittymiseen. (Thomas, Oppenheim, Islam 2017, viitattu 14.9.2020.)

KRACK

Key Reinstallation Attack (KRACK) on Mathy Vanhoefin vuonna 2017 löytämä vakava tietoturvahaavoittuvuus WPA2-salausprotokollassa, jota käytetään langattoman lähiverkon liikenteen salaamisessa. Hyökkäys ajoittuu langattoman lähiverkkoyhteyden muodostamisen kättelyvaiheeseen. Tavanomaisessa Wi-Fi yhteyden luomisessa käytetään 4-suuntaista kättelyä, jossa päätelaite sopii tukiaseman kanssa salausavaimen, jota käytetään heidän välillä tapahtuvan liikenteen salaamisessa. KRACK hyökkäys tapahtuu kättelyn kolmannen ja neljännen vaiheen välissä. Hyökkääjä voi hyödyntää tätä haavoittuvuutta päästäkseen MITM-asemaan, jolloin hän pääsee käsiksi kaikkeen suojaamattomaan liikenteeseen, joka uhri lähettää langattoman

lähiverkon yli. Hyökkäys toimii laitteisiin, joissa on Linux tai Android -käyttöjärjestelmä, sekä heikommin tai ei ollenkaan muita käyttöjärjestelmiä vastaan. (Vanhoef 2017, viitattu 21.9.2020.)

Hyökkäyksen ensimmäisessä vaiheessa uhri on päätelaitteellansa aikomassa yhdistää luotettavaan langattomaan lähiverkkoon, joka on salattu WPA2:lla sekä vierailla sivustolla, jossa on käytössä HTTPS. Hyökkääjä skannaa langattoman yhteyden ja tukiaseman tiedot, jonka jälkeen hän monistaa tämän ja luo itsestään valetukiaseman samalla nimellä eri kanavalle. Seuraavassa vaiheessa varmistetaan, että uhri pystyy pääsemään internettiin, käytetään liikenteen analysointityökalua ja SSL-salauksen purkamistyökalua. Tämän jälkeen esityöt ovat valmiita, ja seuraavalla kertaa, kun uhri yrittää yhdistää oikeaan langattomaan lähiverkkoon – lähettää valetukiasema uhrin laitteelle viestin, että sen pitää vaihtaa oikealta kanavalta valetukiaseman kanavalle, jolloin hyökkääjä on valmiina pääsemään MITM-asemaan. (Vanhoef 2017, viitattu 21.9.2020.)

Toisessa vaiheessa alkaa itse hyökkäys, jossa oikea tukiasema ja päätelaite toteuttaa kättelyn kolmanteen vaiheeseen asti, mutta neljäs vaihe ei ikinä toteudu loppuun asti, koska valetukiasema kaappaa viestin välistä. Tämä johtaa siihen, että oikea tukiasema lähettää uudelleen ja uudelleen kolmannen kättelyviestin, koska se uskoo viestin katoavan matkalla. Päätelaite vastaanottaa kolmannen kättelyviestin useita kertoja ja jokainen kerta se tallentaa saman salausavaimen ja nollaa inkrementaalisen lähetettyjen pakettien arvon, jonka avulla normaalisti varmistetaan, että viesti on lähetetty vain kerran. Tämä johtaa siihen, että hyökkääjä voi alkaa vertailemaan lähetettyjä paketteja toisiinsa ja tulkitsemaan käytetyn salausavaimen, jonka selvitettyä hyökkääjä pääsee MITM-asemaan ja voi aloittaa liikenteen seurannan, tallentamisen, ohjaamisen ja haittaohjelmien asentamisen. (Vanhoef 2017, viitattu 21.9.2020.)

4 TIETOTURVA

Tietoteknillisten laitteiden suojaaminen on koko ajan entistä tärkeämpään, koska kyberrikokset kehittyvät ympäri maailmaa entistä tehokkaammiksi. Langattomat lähiverkkojen suojaukset eivät ole täysi este niille ulkopuolisille, jotka haluavat niihin päästä käsiksi. Lähiverkon oikeaoppisella suojauksella kuitenkin saadaan riskiä pienennettyä huomattavasti. Päätelaitteille on myös tarjolla useita eri vaihtoehtoja itse laitteiden, niiden lähettämän ja säilyttämän tiedon turvaamiseksi.

4.1 Reitittimen konfigurointi

SSID

SSID (eng. Set-Service-Identifier) on nimi, jolla Wi-Fi verkkoa mainostetaan. Nimen valitsemisessa on hyvä käyttää nimeä, jolla on sinulle merkitystä, mutta ulkopuoliset ihmiset eivät osaa yhdistää sitä nimeä sinuun. Yksi vaihtoehto tässä on myös valita, ettei SSID:tä mainosteta ollenkaan, mutta tämä ei yksinään riitä suojausmekanismiksi. (Lowe 2016, 149.)

Salasana

Vahvan salasanan valitseminen on tärkeimpiä asioita Wi-Fi verkon luonnissa. Wi-Fi-yhteyden salasana on järkevää olla nykysuositusten mukainen, eli sellainen, jossa on: pieniä ja isoja kirjaimia, erikoismerkkejä ja numeroita. Riittävä pituus ja monimutkaisuus on avainasia salasanan valitsemisessa. Salasanan valitsemisessa kannattaa valita helposti muistettava eli yhdistää useampia sanoja yhteen, laittaa numeroita ja erikoismerkkejä. Itse reitittimessä tulee olla vahva salasana, jottei ulkopuoliset pääse muuttamaan sen asetuksia, joka voisi mitätöidä reitittimen kautta tulevat tietoturvaratkaisut. (Lowe 2016, 149.)

Tämänhetkisen suosituksen mukaan salasanan pituus tulisi olla vähintään 12 merkkiä pitkä ja turvalliseksi salasanaksi voidaan luokitella 16 merkkiä pitkä yhdistelmä. Salasanan kannattaa olla sellainen, jota ei käytä missään muualla, jottei tietovuodoista saaduissa salasanalistoissa ole salasanoja, jotka kelpaisivat omiin järjestelmiin. (Mattila 2020, viitattu 23.9.2020.)

Luotetut laitteet

Luotetut laitteet eli MAC-osoitteiden suodatus (eng. Mac address filtering) päästää verkkoon ainoastaan luotetut laitteet, eli laitteet, joiden MAC-osoite on hyväksytty reitittimen suodatuslistassa. Tällä suodatuksella on hyvät puolet ja huonot puolensa. Tämä suodatus aiheuttaa lisätyötä, koska jokainen laite täytyy erikseen lisätä reitittimen suodatuslistaan. Hyvä puoli tässä on, että verkkoon pystyy ainoastaan yhdistämään tietyt valitut laitteet, mutta tämä ei kuitenkaan takaa, ettei verkkoon pääse ulkopuolisia. Ulkopuolinen henkilö voi saada selville kohdelaitteen MAC-osoitteen ja käyttää sitä tekeytyäkseen luotetuksi laitteeksi. (Lowe 2016, 149.)

DHCP

Dynamic Host Configuration Protocol palvelin on lähiverkossa sijaitseva palvelin, joka vastaa automaattisesti verkon laitteiden IP-osoitepyyntöihin ja jakaa niille IP osoitteen altaan mukaan. Tämä IP-osoitteiden allas on ryhmä osoitteita tietystä aliverkosta, jotka verkon ylläpitäjä on valinnut jaettavaksi. Ilman DHCP palvelinta lähiverkon kaikkien laitteiden verkkoasetukset pitäisi asettaa manuaalisesti, jotta ne löytävät toisensa. Isommissa lähiverkoissa DHCP palvelin on omana palvelimena, mutta kotiympäristöissä se on useimmiten sisäänrakennettuna reitittimessä. (Infoblox 2017, viitattu 21.6.2020.)

WPS - Wi-Fi Protected Setup

WPS on käyttäjäystävällinen tapa, mutta tietoturvamielessä turvaton yhdistää uusia laitteita Wi-Fi verkkoon, koska kuka tahansa voi liittää oma laitteensa lähiverkkoon. Tämä tapa vaatii käyttäjältä vain PIN-koodin tai ei mitään muuta kuin napin painalluksen reitittimestä tai reitittimen asetuksista. PIN-koodin käyttäminen oikean salasanan sijaan on väsytyshyökkäyksen kohteena erittäin helppo murtaa. WPS-napin painaminen vaatii pääsyn reitittimelle fyysisesti tai reitittimen asetuksiin, jolloin siihen käsiin pääsemiseksi tarvitsee itse reitittimen hallinta salasanan ja käyttäjätunnuksen. (Hoffman 2017, viitattu 14.5.2020.)

Etähallinta

Reitittimen etähallinta on kätevä tapa saada etäyhteys reitittimeen, mikäli on tarve päästä muutamaan asetuksia tai käynnistämään reitittimen uudelleen lähiverkon ulkopuolelta.

Yhdistäminen tapahtuu esimerkiksi internet-selainta käyttämällä laittamalla reitittimen julkisen IP-osoitteen ja porttinumeron selaimen osoiteriville. Tämä kätevyys tuo kuitenkin mukanaan omat tietoturvariskinsä ja tästä syystä etähallinta on oletusarvoisesti poissa päältä, joten sen hyödyntäminen vaatii etähallinnan aktivoinnin reitittimen asetuksista. (Saha 2018, viitattu 17.8.2020.)

Mikäli haluaa laittaa etähallinnan päälle, on syytä varmistaa muutama asia. Ensimmäisenä asiana kannattaa varmistaa, että reitittimen oletuksena olevat järjestelmänvalvojan tunnukset ovat muutettu vaikeasti murrettaviksi. Toisena asiana on se, että internet-palveluntarjoajan antama IP-osoite reitittimelle on yleensä ns. dynaaminen osoite eli reitittimen IP-osoite muuttuu tietyn ajan välein. Tähän asiaan tuo helpotusta palvelut kuten ”noip.com”, joka mahdollistaa tietyn nimen yhdistämisen reitittimen dynaamiseen IP-osoitteeseen, jolloin reitittimeen voi yhdistää valitsemansa nimen ja portin avulla, esim. ”perunapelto.ddns.net:1024”. Kolmantena muistettavana asiana määrittele tietyt protokollat ja IP-osoitteet, jotka ovat ainoita, joista on pääsy reitittimelle etäyhteyden kautta. Tässäkin on hyvä huomioida etäyhteyttä ottavan laitteen IP-osoitteen muuttuminen dynaamisen osoitteen takia. (Saha 2018, viitattu 17.8.2020.)

Guest Wi-Fi network

Reitittimessä voi olla tarjolla ominaisuus langaton ”vieraiden verkko” eli guest Wi-Fi network, jonka tarkoituksena on erottaa kodin lähiverkossa olevat omat laitteet vieraiden laitteista. Guest networkin avulla luodaan erillinen lähiverkko, johon vieraat voivat yhdistää, laitteensa mikäli heidän tarvitsee käyttää Wi-Fi yhteyttä. Tämänlaisen verkon etuna on se, että vieraiden tai omista laitteista ei ole yhteyttä toisen verkon laitteisiin, jolloin voisi esimerkiksi tietämättään levittää haittaohjelmia. Toisena etuna voit laittaa kaikki langatonta lähiverkkoa tarvitsevat IoT-laitteet tähän verkkoon, jolloin lievennetään IoT-laitteiden tuomaa tietoturvariskiä. (Aver 2018, viitattu 18.8.2020.)

Itse guest networkin luominen on lähes samanlainen prosessi kuin normaalin lähiverkon. Verkolle annetaan SSID, salausprotokolla, salasana ja mahdolliset rajoitteet. Verkon luomisvaiheessa on hyvä varmistaa, että valintaruutu, jossa puhutaan lähiverkon resursseihin pääsystä, ei ole valittuna. Tämä valinta erottaa lähiverkot toisistaan. (Aver 2018, viitattu 18.8.2020.)

Salausprotokolla

WEP (Wired Equivalent Privacy) on alkuperäinen langattoman lähiverkon salausprotokolla, joka virallisesti hylättiin vuonna 2004. Tätä protokollaa ei suositella käytettäväksi, koska se on murrettu jo 2000-luvun alussa. WEP:ssä kaikilla langattomaan lähiverkkoon liitetyillä laitteilla on sama staattinen verkon avain, joka ei muutu missään vaiheessa. WEP:n tietoturvaa parantamaan kehitettiin WPA (Wi-Fi Protected Access), jossa verkon avain luodaan dynaamisesti jokaista lähetettävää pakettia varten. WPA 2 toi mukanaan uuden standardin salausta varten, nimeltään AES (Advanced Encryption Standard), jota pidetään tällä hetkellä vahvimpana salausprotokollana. (Johnson 2020, viitattu 18.8.2020.)

WPA 3 on uusin versio, joka on vasta julkaistu ja sitä tukevia laitteita alkaa hiljalleen tulemaan markkinoille. WPA 3 tuo mukanaan entistä pidemmät salausavaimet liikenteelle, viimeisimpiä suojaus mekaniikoita, parannetun autentikoinnin, poistaa käytöstä vanhat protokollat tietoturvasyistä ja pakottaa Protected Management Frames (PMF) käytön. PMF on WPA 2:ssa ja WPA 3:ssa käytettävä suojausmenetelmä, jolla parannetaan pakettien suojausta. Lisäsuojaa autentikaatio vaiheeseen tuo uusi Simultaneous Authentication of Equals (SAE), joka myös tekee vaikeammaksi kaapattujen tietojen suojauksen purkamisen offline-tilassa ja korvaa edeltäjänsä Pre-shared Keys (PSK). Tämän lisäksi avoimissa langattomissa WPA 3 verkoissa hyödynnetään Opportunistic Wireless Encryptionia (OWE), joka salaa liikenteen. Hyökkääjien on nyt entistä haastavampi salakuunnella ja tulkita kaapattua tietoa, koska se on salattua. (Wi-Fi Alliance 2020, viitattu 18.8.2020.)

4.2 Hyödylliset ohjelmat

Päivitykset

Ohjelmistojen tuoreimmat päivitykset ovat tärkeä osa tietoturvallisuutta, koska niiden avulla ennalta ehkäistään tai paikataan kriittisiä reikiä suojauksessa eli haavoittuvuuksia. Päivitysten mukana voi tulla parannuksia ohjelman toimivuuteen, lisää uusia ominaisuuksia tai vanhoja karsitaan pois. Päivitysten tuomat uudet ominaisuudet voivat lisätä väyliä hyökkäyksen toteuttamiseksi, mutta useimmiten hyökkääjät ja haittaohjelmat käyttävät ohjelmistoissa jo olemassa olevia haavoittuvuuksia hyväkseen hyökkäyksen toteuttamiseksi. Tämän vuoksi mm.

käyttöjärjestelmissä, palomuureissa, virusturvissa ja internet selaimissa on erittäin tärkeä pitää päivitykset ajan tasalla, koska näiden avulla saa käytettävän laitteen tietoturvan hyvälle mallille. (Davis 2017, viitattu 17.8.2020.)

Palomuuri

Palomuuri on ohjelma, joka tarkkailee, sekä hallitsee saapuvaa ja lähtevää verkkoliikennettä. Palomuurin tarkoituksena on luoda suojaava seinä sisäisen verkon ja ulkoverkon välille, jonka avulla pystytään estämään haitallista tai vahingollista liikennettä. Verkkoliikenteen salliminen ja estäminen perustuu asetettuihin suojaussääntöihin. Nämä suojaussäännöt kertovat mistä osoitteesta yhteys sallitaan mihinkin osoitteeseen ja porttiin. (Forcepoint 2020, viitattu 20.6.2020.)

Palomuureja on sekä software, että hardware versioita. Software versio palomuurista on ohjelma, joka on asennettuna laitteelle ja säännöstelee liikennettä eri ohjelmien ja niille sallittujen porttinumeroiden perusteella. Hardware versio on fyysinen laite, joka sijaitsee oman ja ulkoverkon välissä. (Forcepoint 2020, viitattu 20.6.2020.)

Next-generation firewall (NGFW) on uusin palomuuriteknologia, joka toimii usealla OSI-mallin kerroksella ja yhdistää tavanomaisen palomuurin sekä lähiverkon laitteiden liikenteen pakettien syvätutkimuksen ja tunkeilijoiden havaitsemisen. NGFW käyttävät tarkempaa ja syvempää liikenteen tarkkailua edeltäjiinsä verrattuna tarkkailemalla pakettien sisällön ja digitaalisia allekirjoituksia hyökkäysten ja haittaohjelmien estämiseksi. NGFW toiminta perustuu liikenteen analysointiin, salausten purkamiseen ja tulkintaan. Palomuuri tekee päätöksiä sen mukaan, mitä säännöksiä siihen on konfiguroitu tai, jos se löytää poikkeuksia tavanomaisen liikenteen tallennettuun otokseen verrattuna. (Miller 2014, 36–37.)

Anti-malware ohjelmat

Haittaohjelmien koodit jättävät jälkiä laitteelle, vaikka käyttäjä ei itse vielä huomannut mitään poikkeavaa laitteen toiminnassa. Haittaohjelmia ei välttämättä huomaa ennen kuin on jo liian myöhäistä ja ne ovat jo tehneet tuhojaan. Haittaohjelmien pääsyn laitteelle voi käyttäjäkin tunnistaa, jos mm. tiedostojen koko on kasvanut ilman mitään erityistä syytä, käyttöjärjestelmän toiminta on hidastanut, laite käynnistää itseään uudestaan tai käytettävissä oleva muisti on huomattavasti vähentynyt. (West, Dean, Andrews 2016, 417–418.)

Yksinkertaisimmillaan anti-malware ohjelma suojaa laitetta kyberrikollisia ja haittaohjelmia vastaan. Näissä ohjelmassa on oma tietokanta, jonka perusteella se etsii ja poistaa haittaohjelmia sekä monitoroi kaikkia käynnissä olevia ohjelmia. (Kleut 2020, viitattu 20.6.2020.)

Tarkemmin tarkastellessa eri anti-malware ohjelmia, ne sisältävät erilaisia keinoja haittaohjelmien kitkemiseksi ja estämiseksi. Yhtenä ominaisuutena on ns. "signature scanning" eli tiedoston sisältöä verrattaan tietokantaan, joka sisältää tunnistettujen haittaohjelmien uniikkeja koodeja. Toinen keino tunnistaa haittaohjelmia on tarkastella tiedostojen aikaisempien tiedostoversioiden tarkistussummaa (engl. checksum) ja vertailla niitä nykyisiin. Kolmas tapa on käyttää koneoppimista hyödyksi eli tarkastellaan tavallista laitteiden ja verkon toimintaa, jonka perusteella voidaan tehokkaammin löytää haittaohjelmia. Hyvä esimerkki tästä on Windows 10 -käyttöjärjestelmän mukana tuleva antivirus ohjelma, joka kerää tietoa kaikilta laitteilta, joilta tiedonkeruuta ei ole erikseen kielletty. Tämänlaisella toiminnalla saadaan valtava määrä tietoa laitteiden ja ohjelmien normaalista toiminnasta erilaisissa konfiguraatioissa. (West, Dean, Andrews 2016, 417–418 & Kleut 2020, viitattu 20.6.2020.)

VPN - Virtual Private Network

VPN mahdollistaa turvallisen yhteyden muodostamisen laitteelta toiseen verkkoon. Tätä tekniikkaa käytetään varsinkin organisaatioiden verkkoihin yhdistämiseen, jolloin pystyy käyttämään organisaation sisäverkon resursseja. VPN-yhteyttä voidaan käyttää aluesuojattujen sivustojen selaamiseen ja suojaamaan viestien tiedot varsinkin julkisissa Wi-Fi verkoissa. VPN yhdistää laitteet Internetin kautta palvelimelle, jonka kautta oletuksena kaikki liikenne muihin verkkoihin tapahtuu. Tämä liikenne on suojattua laitteelta VPN-palvelimelle, joten sillä välillä olevat laitteet eivät voi lukea tätä liikennettä. (Hoffman 2019, viitattu 14.5.2020.)

4.3 Lisävaihtoehdot

Wireless intrusion prevention system (WIPS)

WIPS on verkkolaitteessa oleva moduuli tai erillinen laite, joka monitoroi radioaaltoja luvattomien langattomien tukiasemien löytämiseksi. WIPS etsii luvattomia tukiasemia MAC-osoitteiden ja

signaalien yksilöllisten sormenjälkien avulla. Tällaisen laitteen löydettyä WIPS aloittaa automaattisesti vastatoimet tunkeilijan estämiseksi ja ilmoittaa järjestelmänvalvojalle ylimääräisestä tukiasemasta, joka voi mahdollisesti olla Rogue AP tai Evil Twin. WIPS koostuu kolmesta eri komponentista, joita ovat: sensorit, palvelin ja konsoli. Sensorit asennetaan ympäri rakennusta, jotta ne voivat tarkkailla radioaaltoja antenneillaan ja lähettää tiedot palvelimelle. Palvelin analysoi sensorien lähettämät tiedot ja ilmoittaa järjestelmänvalvojan konsolille luvattomasta liikenteestä. (Kuan 2011, viitattu 30.9.2020.)

Pi-Hole

Pi-hole on Jacob Salmelan aloittama avoimeen lähdekoodiin perustuva lähiverkossa toimiva mainoksia ja seurantaevästeitä estävä DNS-palvelin. Pi-hole on Linux-pohjainen, kevyt ja vähän resursseja vaativa ohjelma, jonka voi asentaa mille tahansa laitteelle. Ohjelma on suunniteltu helposti asennettavaksi ja ylläpidettäväksi. Pi-holen avulla mainosten ja seurantaevästeiden eston pystyy toteuttamaan mille tahansa päätelaitteelle. Mainosten ja seurantaevästeiden estämisen lisäksi Pi-hole voi toimia omana DHCP-palvelimena. (Bate 2018, viitattu 7.6.2020.)

Pi-holeen saa ladattua listan verkkotunnuksista, jotka ovat tunnettuja mainos- tai seurantaeväste osoitteita. Päätelaitteiden lähettämät osoitepyynnöt ohjantuvat Pi-holeen ja se tarkistaa onko tämä osoite verkkotunnus listassa. Osoitteen ollessa listalla avautuu verkkosivu normaalisti, mutta ilman mainoksia, koska niiden osoitteet ovat estetty. (Anand 2019, viitattu 7.6.2020.)

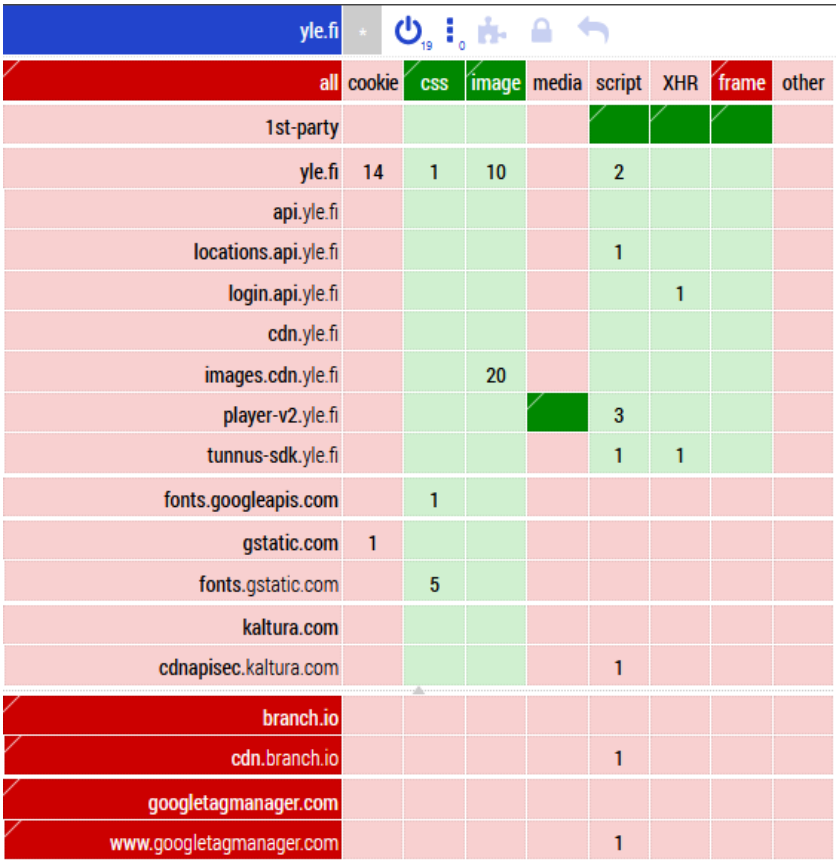
Sipulireititys (onion routing)

Sipulireititys on tekniikka, jota käytetään sipuliverkossa, joka koostuu vapaaehtoisten ylläpitämistä salattuja paketteja reitittävistä laitteista. Sipulireititys on tapa keskustella anonyymisti tietokoneverkossa. Tekniikka saa nimensä siitä, että lähetettävät ja vastaanotetut viestit on kapseloitu kerroksittain. Nämä salatut viestit lähetetään eteenpäin sipulireitittimiä pitkin päämääräänsä. Jokainen sipulireitin ottaa kerroksen pois salauksesta ja lähettää sen seuraavalle, joka tekee samat asiat, kunnes näkyvissä on vain viimeinen kerros ja viesti on toimitettu päämääräänsä. Viesti takaisinpäin kulkee samalla tyylillä, mutta salataan käänteisessä järjestyksessä. Viestin alkuperäinen lähettäjä ja sisältö pysyy anonyyminä salakuuntelijoille ja viestejä välittäville tahoille, koska he tietävät ainoastaan lähimmän "naapurinsa" sipuliverkossa. Sipulireitityksessä on kuitenkin yksi pieni heikkous, jonka kautta viestin lähettäjä voi selvitä.

Lähettäjä on mahdollista saada selvillä lähettäjän ja lopullisen päämäärän kuuntelulla, vertailemalla viestien kokoa ja lähetystiheyttä toisiinsa. Tämän hetken tunnetuin ohjelma, joka käyttää sipulireititystä on Torprojectin Tor Browser. (Nigam 2018, viitattu 23.9.2020.)

Nettiselainten lisäosat

Jokaisella on oma mielipide mieluisimmasta nettiselaimesta, mutta nettiselainta valittaessa on hyvä katsoa lisäosia, joita niihin on tarjolla. Lisäosat tuovat lisää suojaa yksityisyydelle ja päätelaitteille, koska internet sivustoilla voi olla mm. erilaisia itsestään latautuvia haittaohjelmia, haitallisia skriptejä, evästeitä ja selaimen uudelleenohjauksia, jotka kannattaa estää (kuva 6). Suojaavilla lisäosilla voidaan myös estää, ponnahdusikkunat ja häiritsevät mainokset, joiden kautta voi myös tulla haittaohjelmia. Tällä hetkellä hyviä suojaa lisääviä lisäosia ovat mm. uBlock Origin, jolla voi estää haitallisia mainoksia, seurantaa ja sivustolla olevia elementtejä, HTTPS Everywhere, joka pyytää nettisivulta SSL yhteyttä, sekä Self-Destructing Cookies, joka automaattisesti poistaa evästeet välilehtien sulkemisen jälkeen. (Viljanen 2018, viitattu 23.9.2020.)



Kuva 6. Kuvakaappaus uMatrix-lisäosan sivukohtaisesta konfiguraatioikkunasta vierailessa yle.fi-sivustolla.

5 JOHTOPÄÄTÖS

Langattomien yhteyksien määrä kasvaa koko ajan laitteiden määrän ja digitalisaation myötä. Nykyään ei enää tarvitse vetää verkkokaapeleita joka paikkaan yhteyden saamiseksi. Langatonta verkkoa hyödyntäviä laitteita on nykyään lähes joka paikassa, koska langattomuus on halpa ja kätevä tapa yhdistää laitteita toisiinsa ja internettiin. Kasvava määrä laitteita kuitenkin tarkoittaa myös kasvavaa määrää potentiaalisia hyökkäyksen kohteita kyberrikollisille.

Kyberrikollisten joka päivä kasvavan kohteiden määrän ja repertuaarin takia niiltä kokonaan suojautuminen ei ole täysin varmaa. Niiden uhriksi joutumista voi pienentää huomattavasti erilaisilla tavoilla kuten laitteiden päivityksillä, viestinnänsalauksella, virusturvalla ja palomuurilla. Näiden lisäksi on tärkeää ajatella kriittisesti mitä kannattaa tehdä ja mihin luottaa. Erityisesti kannattaa miettiä julkisien ja avoimien verkkojen käyttöä, koska hyökkääjä voi lymytä yllättävän lähellä. Tämän vuoksi olisi suositeltavaa käyttää jotain salausmekaniikkaa kuten VPN tai TOR, ettei liikennettä kuuntelevat tahot ainakaan saa mitään tietoa käsiinsä.

Internetissä tai sähköpostien liitetiedostoja ladattaessa ja avatessa kannattaa varmistaa, että ne ovat oikeasti sellaisia kuten pitääkin. Ne voivat olla helposti haittaohjelmia, vaikka päällepäin näyttäisivätkin luotettavilta. Ohjelman tai tiedoston avaamisen jälkeen voi olla jo liian myöhäistä ja haittaohjelma leviää päätelaitteelle, sekä mahdollisesti muihin laitteisiin, jotka ovat yhdistettynä lähiverkkoon.

Epäluotettavalta verkkosivuilta voi vierailun aikana tarttua haittaohjelmia ilman, että käyttäjä sitä edes huomaa. Virusturvat ja selainlisäosat ovat ehdottoman tärkeitä pienentämään riskin mahdollisuutta. Selainlisäosilla saadaan myös häiritsevät ja jopa aggressiiviset mainostajat, sekä muut tiedonkerääjät hallintaan. Internettiä käyttäessä erilaisilla älylaitteilla on mietittävä niidenkin tietoturvallisuutta, jota voidaan parantaa esimerkiksi Pi-Holen avulla, jonka avulla voi mm. estää haitallisia mainoksia ja seurantaevästeitä.

Langattoman lähiverkon ja sen sisältämien laitteiden tietoturva koostuu useasta eri tekijästä. Haittaohjelmien kirjo on hyvin laaja ja niiden pääsy päätelaitteelle voi vaarantaa koko lähiverkon turvallisuuden. Haittaohjelmille altistuneet päätelaitteet voivat levittää haittaohjelmia, toimia porttina

hyökkääjille ja joutua osaksi bottiverkkoa. Haittaohjelmia eivät kehitä enää pelkästään kyberrikolliset, vaan myös valtiovallat kehittävät niitä eri tarkoituksiin kuten Stuxnet.

Hyökkäykset, joiden tarkoituksena on varastaa tiedot langattomasta liikenteestä tapahtuvat oman lähiverkon radiosignaalin kuuluvuuden alueelta. Monesti näissä hyökkäyksissä hyödynnetään radiosignaaleja kaappaavia laitteita, jotka tekeytyvät samaksi lähiverkoksi, mutta paremmalla signaalilla, jolloin päätelaite yhdistäisi siihen. Tällöin kaikki liikenne menisi hyökkääjän laitteen kautta ja hän pystyy kuuntelemaan, tallentamaan ja manipuloimaan liikennettä. Ainoat tavat suojautua tällaiselta on joko itse etsiä liikennettä kaappaava laite tai hankkia tunkeilijoiden tunnistamiseen erikoistuva järjestelmä.

Kodin turvallisen lähiverkon toteuttaminen langattomasti on loppujen lopuksi helppo toteuttaa, mikäli tietää mitä kaikkia laitteita on olemassa, mitä eri ominaisuudet ja asetukset käytännössä tarkoittavat. Tässä on lyhyesti kiteytettynä huomioitavat ominaisuudet ja asetukset:

Ensimmäiseksi kannattaa valita verkkolaite, joka tukee vähintään Wi-Fi versiota 5. Wi-Fi 6 on uusinta tekniikkaa, mutta sitä tukevat verkkolaitteet ovat vielä melko hintavia. Wi-Fi 6 etuna on parempi kantama signaalille, toimintakyky usean yhtä aikaa yhdistetyn laitteen kanssa ja tuki WPA3-salaukselle, johon on suositeltavaa siirtyä heti kun on mahdollista parhaimman suojauksen saamiseksi.

Toiseksi kannattaa käyttää 5 GHz taajuutta, jonka avulla saadaan mahdollisimman nopea yhteys, jota muut laitteet eivät häiritse yhtä paljon ja heikennetään signaalin kuuluvuutta kodin ulkopuolelle, koska signaalin kantama ei ole yhtä hyvä kuin 2,4 GHz taajuudella. Halutessaan langattoman lähiverkon kuuluvuutta voi parantaa mm. Mesh-verkon avulla, mikäli kodin koko sitä vaatii.

Kolmanneksi alkaa itse langattoman lähiverkon konfiguraatio, jossa aluksi valitset itselle tutun SSID:n, jota muut eivät osaa yhdistää sinuun. Salasanaksi suositellaan nykyään ainakin 12-merkkiä sisältävän merkkijonon, joka sisältää pieniä-, suuria- ja erikoismerkkejä. Tämän jälkeen valitse joko WPA2-AES tai WPA3 tavaksi autentikoida ja salata liikenne, koska aikaisemmat ovat jo murrettu aikoja sitten.

Neljännessä vaiheessa voi miettiä lisäominaisuuksia. Etähallintaa ei kannata laittaa päälle, koska on aika harvinaista, että ulkoverkosta käsin tarvitsee hallita verkkolaitetta. WPS on kätevä tapa

liittää päätelaitteita langattomaan lähiverkkoon ja sitä varten se on myös kehitetty, mutta WPS PIN-koodi on liian helppo murtaa. Guest Wi-Fi on hyvä ratkaisu, mikäli kylässä käy vieraita, jotka tarvitsevat yhteyden internettiin, koska he eivät pääse sitä kautta muuhun lähiverkkoon käsiksi. Laitteita voi suodattaa niiden MAC-osoitteiden avulla, mutta senkin osoitteen voi huijata, joten se ei estä hyökkääjiä.

Tietotekniikka kehittyy koko ajan ja erilaisten uhkien kirjo kasvaa. Jokaisen henkilön kannattaa tarkastaa omien laitteiden ominaisuudet, mitä ne tekevät ja onko niissä päällä turhia toimintoja, joita ei tarvitse. Vaikka langaton lähiverkko ja päätelaitteet olisivat suojattuja parhaimman mukaan, voi niihin silti kohdistua hyökkäyksiä tai uusia haittaohjelmia, joita ei ole vielä tunnistettu. Ihmisen oma käytös voi vaikuttaa paljon siihen pääseekö haittaohjelmia päätelaitteelle, jotka vaarantavat koko lähiverkon turvallisuuden.

6 POHDINTA

Opinnäytetyön tutkimusongelmana oli selvittää nykyajan ajankohtaisia uhkien kirjoa ja mitä tärkeimpiä keinoja niiltä suojautumiseen on kotiympäristössä olemassa. Työn taustalla oli halu tuoda tavallisten käyttäjien tietoisuuteen keinoja suojata heidän laitteita ja internetin välityksellä lähetettävää tietoa. Opinnäytetyön aihevalinnan taustalla oli myös kasvu langattomien lähiverkkoyhteyksien ja etätyöntekijöiden määrässä.

Opinnäytetyön aihe oli mielenkiintoinen ja hyvin monipuolinen. Aiheesta kirjoittaessa joutui useasti miettimään, kuinka kirjoitettava asia liittyi aiheeseen ja miten asian esittäisi tavalliselle ihmiselle, jolla ei ole IT-alan tutkintoa. Opinnäytetyössä käytettyjen lähteiden määrä oli suuri, joista valtaosa oli ammattilaisten tai alan yritysten kirjoittamia kirjoja, artikkeleita ja julkaisuja. Työn luotettavuutta olisi voinut lisätä esittelemällä käytännössä hyökkäyksiä, sekä demonstroida suojausten vaikutus hyökkäysten onnistumiseen.

Alkuperäisessä aikataulun mukaisesti työn oli tarkoitus olla valmiina kesän 2020 aikana, mutta se oli työmäärään nähden liian optimistinen tavoite. Työn valmistuminen venyi saman vuoden syys- ja lokakuun taitteeseen asti. Opinnäytetyön alkuperäiseen ajatuskarttaan olisi voinut tehdä aiheeseen syventyessä tarkennuksia ja rajauksia, jolloin olisi ollut tarkempi kokonaiskuva kirjoitettavista ja puuttuvista asioista. Tämän avulla olisi voinut kirjoittamisen aikatauluttaa huolellisemmin, jolloin kirjoittaminen ei olisi viivästynyt yhtä paljon.

Tämän opinnäytetyön sisältöä voidaan käyttää ymmärtämään langattomaan lähiverkkoon ja päätelaitteisiin kohdistuvia uhkia. Tietoturvan toteutumiseksi jokaisen käyttäjän tulisi tietää minkälaisia uhkia on olemassa, jotta niiltä edes tajuaa suojautua. Opinnäytetyö antaakin hyvän katsauksen tapoihin suojatautua haittaohjelmilta ja hyökkäyksiltä, mutta sen ulkopuolelle jää esimerkiksi social engineering (suom. sosiaalinen manipulointi), jonka avulla voidaan päihittää parhaimmatkin suojaukset. Uhkilta suojautuminen on ikuista kilpajuoksua, koska tekniikat ja hyökkääjät kehittyvät koko ajan.

LÄHTEET

Anand 2019. Complete Pi Hole setup guide. Viitattu 7.6.2020, https://www.smarthomebeginner.com/pi-hole-setup-guide/

Aver H., 2018. What's a guest Wi-Fi network, and why do you need one? Viitattu 18.8.2020, https://www.kaspersky.com/blog/guest-wifi/23843/

Bate A. 2018. Block ads at home using Pi-hole. Viitattu 7.6.2020, https://www.raspberrypi.org/blog/pi-hole-raspberry-pi/

Cloudflare 2020. What is a DDoS Attack? Viitattu 18.6.2020, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Coleman D. 2019. What is bss color in 802 11ax? Viitattu 27.8.2020, https://www.extremenetworks.com/extreme-networks-blog/what-is-bss-color-in-802-11ax/

Davis G. 2017. Why Software Updates Are So Important. Viitattu 17.8.2020, https://www.mcafee.com/blogs/consumer/consumer-threat-notices/software-updates-important/

Europol 2019. IOCTA - Internet organised crime threat assessment. Viitattu 17.9.2020, https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

Firch J. 2019. What are the most common types of network vulnerabilities? Viitattu 9.6.2020, https://purplesec.us/common-network-vulnerabilities/

Forcepoint 2020. How does firewall work. Viitattu 20.6.2020. https://www.forcepoint.com/cyber-edu/firewall

Hoffman C. 2019. What is a VPN, and why would I need one? Viitattu 14.5.2020, https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/

Hoffman C. 2017. Wi-Fi Protected Setup (WPS) is Insecure. Viitattu 14.5.2020, https://www.howtogeek.com/176124/wi-fi-protected-setup-wps-is-insecure-heres-why-you-should-disable-it/

IEEE 2020. About IEEE. Viitattu 27.8.2020, https://www.ieee.org/about/

Infoblox 2017. What is a DHCP Server. Viitattu 21.6.2020, https://www.infoblox.com/glossary/dhcp-server/

Johnson A. 2020. Wireless Concepts. Viitattu 18.8.2020, https://www.ciscopress.com/articles/article.asp?p=2999384&seqNum=6

Jongerius J. 2020. Wi-Fi 4/5/6/6E (802.11 n/ac/ax). Viitattu 22.9.2020, https://www.duckware.com/tech/wifi-in-the-us.html

Kaspersky 2020. What is a Botnet? Viitattu 18.6.2020, https://www.kaspersky.com/resource-center/threats/botnet-attacks

Kaspersky 2020. What is WannaCry ransomware? Viitattu 14.9.2020, https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

Kleut J. 2020. What is antivirus software? Viitattu 20.6.2020, https://us.norton.com/internetsecurity-malware-what-is-antivirus.html

Kuan C. C. 2011. Understanding Wireless Intrusion Prevention Systems. Viitattu 30.9.2020, https://www.networkworld.com/article/2199876/understanding-wireless-intrusion-prevention-systems.html

Lowe D. 2016. Networking for dummies 11th Edition. John Wiley & Sons, Inc. USA.

Malwarebytes 2020. All about adware. Viitattu 17.6.2020, https://www.malwarebytes.com/adware/

Mattila A-L. 2020. Millainen salasanan tulee olla. Viitattu 23.9.2020, https://it.oamk.fi/1594

McAfee 2020. What is Stuxnet. Viitattu 8.9.2020, https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html

McDowell G. 2019. Kuva. Viitattu 23.9.2020, https://www.online-tech-tips.com/computer-tips/what-is-wifi-6-and-is-it-worth-waiting-for/

Messer 2018. Rogue Access Points and Evil Ewins - CompTIA Security+. Viitattu 19.9.2020, https://www.professormesser.com/security-plus/sy0-501/rogue-access-points/

Miller L. 2014. Cybersecurity for dummies. John Wiley & Sons, Inc., USA.

MOOC.fi 2020. Kotiverkko. Viitattu 28.8.2020, https://tietoliikenteen-perusteet-1-20.mooc.fi/osa-2/1-kotiverkko

MOOC.fi 2020. Kytkin. Viitattu 28.8.2020, https://tietoliikenteen-perusteet-2-20.mooc.fi/osa-5/4-kytkin

Moes T. 2019. What is a Trojan Horse Virus? Viitattu 11.6.2020, https://softwarelab.org/what-is-a-trojan-horse/

Moes T. 2019. What is Ransomware? Viitattu 11.6.2020, https://softwarelab.org/what-is-ransomware/

Nigam P. 2018. Onion Routing. Viitattu 23.9.2020, https://www.geeksforgeeks.org/onion-routing/

Norton 2020. What is a computer worm, and how does it work? Viitattu 11.9.2020, https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html

Norton 2020. What is a man-in-the-middle attack? Viitattu 20.9.2020, https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

Norton 2020. Zero-day vulnerability. Viitattu 19.6.2020, https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html

Owasp 2020. SQL Injection. Viitattu 17.6.2020, https://owasp.org/www-community/attacks/SQL_Injection

Panda Security 2017. Keyloggers: Be careful what you type. Viitattu 11.6.2020, https://www.pandasecurity.com/mediacenter/security/keyloggers-be-careful-what-you-type/

PrivacyCanada. 2020. Network Vulnerabilities. Viitattu 9.6.2020, https://privacycanada.net/network-vulnerabilities/

Rasmussen H. 2020. Mikä on mesh-verkko? Viitattu 24.8.2020, https://kotimikro.fi/internet/verkko/mika-on-mesh-verkko

Rouse M. 2019. Definition Router. Viitattu 21.6.2020, https://searchnetworking.techtarget.com/definition/router

Ruckus Education 2019. WiFi 6 (802.11ax) High Level Overview. Viitattu 28.8.2020, https://www.youtube.com/watch?v=9PcRwuto_1Q

Saha M. 2018. How to Access Router Remotely. Viitattu 17.8.2020, https://techwiser.com/access-your-router/

Siciliano R., 2014. What is Wardriving? Viitattu 14.9.2020, https://www.mcafee.com/blogs/consumer/identity-protection/wardriving/

Technibble 2011. What is a Rootkit? Viitattu 18.6.2020, https://www.technibble.com/how-to-remove-a-rootkit-from-a-windows-system/

TechTerms 2019. Modem. Viitattu 28.8.2020, https://techterms.com/definition/modem

Thomas W., Oppenheim N., Islam A. 2017. SMB Exploited: WannaCry Use of "EternalBlue". Viitattu 14.9.2020, https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html

Vacca, J. 2014. Network and System Security Second Edition. Sygress, USA.

Vanhoef M. 2017. Key Reinstallation Attacks – Breaking WPA2 by forcing nonce reuse. Viitattu 21.9.2020, https://www.krackattacks.com

Vigliarolo B. 2020. Wi-Fi 6 (802.11ax): A cheat sheet. Viitattu 25.8.2020, https://www.techrepublic.com/article/wi-fi-6-802-11ax-a-cheat-sheet/

Viljanen V. 2018. Suojattu selain. Viitattu 23.9.2020, https://www.yksityisyydensuoja.fi/suojattu-selain

West J., Dean T., Andrews J. 2016. Network+ Guide to Networks, Seventh Edition. Boston, USA.

Wi-Fi Alliance. 2020. Discover Wi-Fi. Viitattu 18.8.2020, https://www.wi-fi.org/discover-wi-fi/security

Wi-Fi Alliance. 2018. Wi-Fi 6: High performance, next generation Wi-Fi. Viitattu 25.8.2020, https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_6_White_Paper_20181003.pdf

Wi-Fi Professionals 2019. Kuva. Viitattu 31.8.2020, https://www.wifi-professionals.com/2019/04/home-routers-location