

Wi-Fi salausprotokollien haavoittuvuudet yksinkertaisessa harjoitusympäristössä

Petri Koskela



Tekijä(t) Petri Koskela	
Koulutusohjelma Tietojenkäsittelyn koulutusohjelma	
Opinnäytetyön otsikko Wi-Fi salausprotokollien haavoittuvuudet yksinkertaisessa harjoitusympäristössä	Sivu- ja liitesivumäärä 33
Opinnäytetyön otsikko englanniksi Wi-Fi vulnerabilities in basic practice setup	
<p>Tässä opinnäytetyössä käytiin läpi langattomien lähiverkkojen salausprotokolliin liittyviä haavoittuvuuksia. Tällä hetkellä laajasti käytössä oleva WPA2-salausprotokolla osoittautui melko turvalliseksi, kunhan sen käyttöön liittyvät uhat tiedostetaan. Hyökkäysten olemassaolon tiedostaminen ja ymmärtäminen auttaa osaltaan myös suojautumaan niitä vastaan.</p> <p>Opinnäytetyössä kuvattiin kolme erilaista skenaariota, kun WPA2-protokollan haavoittuvuuksia vastaan hyökätään yksinkertaisessa harjoitusympäristössä. Vaikka samat haavoittuvuudet ovat olleet olemassa jo vuosikausia, ei niitä ole pystytty jälkikäteen korjaamaan. Tulevaisuus ei myöskään näytä WPA3-protokollan osalta kovin valoisalta, sillä jo nyt tutkijat ovat löytäneet siitä lukuisia haavoittuvuuksia.</p> <p>Työn tuloksissa kävi ilmi, että langattomat verkot ovat alttiita häiriöille ja niiden varaan ei voi suunnitella mitään kriittisiä toimintoja.</p>	
Asiasanat Kyberturvallisuus, tietoturva, Wi-Fi, WLAN	

Sisällys

1	Johdanto	2
2	Langaton verkko.....	3
2.1	IEEE 802.11.....	3
2.2	Wi-Fi Alliance	5
3	Wi-Fi Salausprotokollat	6
3.1	WEP – Wired Equivalent Privacy	6
3.2	WPA – Wi-Fi Protected Access.....	7
3.3	WPA2 – Wi-Fi Protected Access 2	7
3.4	Nelivaiheinen kättely (4-way handshake)	8
3.4.1	PMK - Pairwise Master Key.....	8
3.4.2	PTK – Pairwise Transit Key.....	9
3.4.3	GTK ja GMK.....	9
3.4.4	ANonce ja SNonce.....	9
3.4.5	MIC – Message Integrity Check	9
3.5	WPA3 – Wi-Fi Protected Access 3	10
4	WLAN-verkon haavoittuvuudet.....	12
4.1	Langaton palvelunestohyökkäys	12
4.2	WPA/WPA2-PSK (Pre-Shared Key) hyökkäys	12
4.3	KRACKS – Key Re-installation Attacks	13
4.4	Laitteistovaatimukset hyökkäysten tekemiseksi.....	13
5	Harjoitusympäristön laitteisto.....	14
5.1	Kali Linux	14
5.2	Aircrack-ng ohjelmisto.....	15
5.3	Alfa Networks AC1200	16
5.4	Zyxel VMG3925	16
5.5	OnePlus 5T.....	17
6	Testaussuunnitelma	17
7	Skenaariokuvaukset WLAN-verkkoa vastaan tehdyistä hyökkäyksistä yksinkertaisessa harjoitusympäristössä (kotiverkko).....	19
7.1	Skenaario 1 – Deauth	19
7.1.1	Hyökkäyksen aloitus	19
7.1.2	Päätelaitteen yksilöinti.....	20
7.1.3	Deauth-pakettien lähetys.....	20
7.1.4	Deauth hyökkäyksen tulos	21
7.2	Skenaario 2 – nelivaiheisen kättelyn kaappaus.....	22
7.2.1	Sanakirjahyökkäys	24
7.2.2	Raakalaskenta eli Brute Force	24
7.3	Skenaario 3 – Evil Twin -hyökkäys.....	27

8 Johtopäätökset.....	29
9 Suositellut toimenpiteet lähiverkkoyhteyden turvaamiseksi	31
10 Pohdinta.....	32
Lähteet	34

LYHENTEET

AP	Access point, langattoman lähiverkon yhteyspiste
DoS	Denial of Service, palvelunestohyökkäys
DNS	Domain Name System, Internetin nimipalvelinjärjestelmä
Ethernet	Pakettipohjainen lähiverkkoratkaisu, joka on toteutettu kaapeliyhteydellä
Kali	Linux jakelupaketti, joka on suunniteltu penetraatiotestaukseen
MAC-osoite	Media Access Control, verkkosovittimen ethernet-verkossa yksilöivä osoite.
OSI	Open Systems Interconnection Reference Model kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa
SSID	langattoman lähiverkon verkkotunnus
STA	Station, päätelaite
TKIP	Tietoliikenneyhteyden salausprotokolla (Temporal Key Integrity Protocol)
Wi-Fi	langattoman verkon tuotteista käytetään usein kaupallista nimitystä Wi-Fi
WLAN	langaton lähiverkko
WPA2	langattomien verkkojen tietoturvastandardi

1 Johdanto

Digitalisaatio on tuonut teknologian osaksi yhteiskunnan jokaista osa-aluetta. Ihmiset käsittelevät valtavasti tietoa päivittäin töissä sekä vapaa-ajalla. Monet arkiset asiat, kuten pankkiasiointi pyritään hoitamaan mobiililaitteilla ja yhä useampi kodin laite on yhdistetty Internetiin. Riippuvaisuus digitaalisista palveluista aiheuttaa myös sen, että olemme haavoittuvaisia, kun järjestelmät eivät toimi. Rikolliset hyödyntävät sinnikkäästi kaikkia mahdollisia haavoittuvuuksia digitaalisessa ympäristössä, koska tietoturvaongelmia on valtavasti ja niitä on kaikkialla.

Tässä opinnäytetyössä tavoitteenani on oppia ja ymmärtää WLAN-verkkojen suojaamisen kannalta oleelliset asiat, tarjota tietoa lukijalle esimerkein siitä, kuinka WPA2-protokollan haavoittuvuuksia pyritään hyödyntämään erilaisilla hyökkäyksillä yksinkertaisessa harjoitusympäristössä ja saada lukija pohtimaan omien WLAN-verkkojen tietoturvaa.

Työn aihe on myös ajankohtainen, sillä samat ongelmat ovat edelleen olemassa WPA2-protokollan osalta, vaikka se julkaistiin vuonna 2004. Esimerkiksi USA:n sisäministeriö ei läpäissyt vuonna 2020 tietoturva-auditointia pääosin puutteellisten WLAN-verkkojen suojausten vuoksi.

2 Langaton verkko

Langaton lähiverkko eli WLAN (Wireless Local Area Network) on paikallinen tietoverkko, jonka avulla tietokone, TV, matkapuhelin tai muu verkkolaite voidaan yhdistää Internetiin tai toisiin verkkolaitteisiin langattomasti. Langattoman verkon perustamiseksi tarvitaan WLAN-yhteyspiste, johon verkkolaitteet pystyvät yhdistämään oman lähettimensä avulla.

WLAN on nykypäivänä käytössä melkein kaikkialla kuten työpaikoilla, lentokentillä, kouluissa, hotelleissa ja esimerkiksi junissa. Langattomista verkkoyhteyksistä onkin tullut ympäri maailman käytetyimpiä tapoja muodostaa yhteyksiä Internetiin. Suurin syy tähän on mobiililaitteiden valtava määrä sekä niillä käytettävät lukuisat sovellukset, jotka vaativat jatkuvan yhteyden Internetiin tarjotakseen käyttäjilleen ajantasaisia palveluita.

Monessa maassa 4G-liittymien sisältämä data on kallista ja se ei ole rajatonta, joten kahviloiden ja muiden julkisten paikkojen tarjoamat WLAN-yhteydet ovat äärimmäisen suosittuja. Langattomia yhteyksiä on myös huomattavasti helpompi rakentaa kuin perinteisiä langallisia ethernet-yhteyksiä.

WLAN-yhteyspisteen lähetysteho on melko matala ja sen kantama ilman esteitä on pimmillään noin 100-200 metriä. (STUK 2020.)

2.1 IEEE 802.11

802.11 on IEEE:n (Institute of Electrical and Electronics Engineers) vuonna 1997 ratifioima standardi langattomille verkkoyhteyksille. 802.11:n tarjoama nopeus 2,4 Ghz:n taajuudella oli vain 1-2 megabittiä sekunnissa, joka oli yleisesti ottaen liian hidas ja tästä syystä WLAN-ratkaisuja ei vielä otettu laajasti käyttöön esimerkiksi yritysmaailmassa. (Colbah 2019, luku 7.)

802.11:n jälkeen julkaistiin 802.11b, jonka tiedonsiirtonopeus oli 11 megabittiä sekunnissa. 802.11b:n jälkeen tuli 802.11a, joka nosti tiedonsiirtonopeuden 54 megabittiin sekunnissa 5 Ghz:n taajuusalueella. (Colbah 2019, luku 7.)

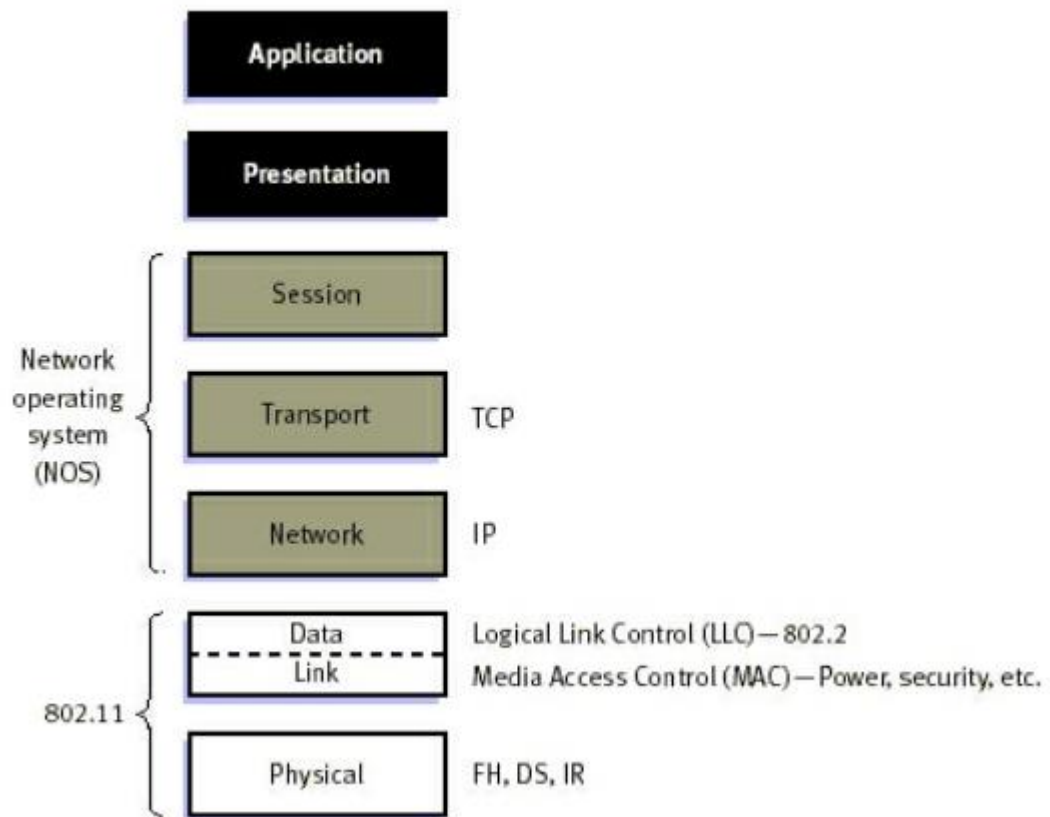
Vuonna 2003 julkaistiin 802.11g, joka käytännössä yhdisti 802.11b:n ja a:n tekniikat. Tämän jälkeen vasta vuonna 2009 julkaistiin 802.11n, joka toi mukanaan tuen MIMO-antenneille. Tämä mahdollisti tiedonsiirron jopa 600 megabittiä sekunnissa. (Colbah 2019, luku 7.)

Joulukuussa 2013 julkaistiin tällä hetkellä eniten käytössä oleva standardi 802.11ac, jonka myötä teoreettinen tiedonsiirtonopeus kasvoi 7 gigabittiin sekunnissa. Vuonna 2019 markkinoille julkaistiin ensimmäisiä 802.11ax standardin verkkolaitteita, jotka nostavat teoreettisen tiedonsiirtonopeuden 11 gigabittiin sekunnissa. (Cisco 2018, 2.)

Kaikki IEEE:n 802-standardit kohdistuvat OSI-mallin fyysiseen (Physical) sekä siirtokerrokseen (Data Link Layer). OSI-malli on ISO:n kehittämä malli tietoliikennejärjestelmien suunnitteluun. Mallissa kuvataan tiedonsiirtoprotokollien yhdistelmä seitsemässä eri kerroksessa. (Colbah 2019, luku 7.)

Fyysinen kerros määrittelee tiedonsiirron fyysisen median kuten valokuidun tai radiotaajuudet. 802.11 standardi määritettiin alun perin toimimaan 2,4 Ghz:n lisenssivapaalla taajuudella. (Colbah 2019, luku 7.)

Siirtokerros huolehtii ylempien kerrosten tietoliikennepaketin kehystämisestä fyysisen kerroksen siirtoa varten. Siirtokerros 802.11:ssa koostuu kahdesta alikerroksesta: Loogisen linkin hallinta (LLC) ja Media Access Control (MAC-osoite). LLC mahdollistaa yksinkertaisen sillan muodostamisen langattomasta verkosta IEEE-kiinteään verkkoon. 802.11 käyttää MAC-osoitteita yhteyden muodostamiseen yhteyspisteen ja päätelaitteen välillä, kuten kuvassa yksi on nähtävissä. (Colbah 2019.)



Kuva 1. 802.11 ja OSI-malli (Colbah 2019)

2.2 Wi-Fi Alliance

Arkikielessä langattomista verkoista käytetään yleensä termiä WLAN tai Wi-Fi, mutta niillä on terminologian kannalta eroa. WLAN on lyhenne sanoista Wireless Local Area Network eli langaton lähiverkko ja Wi-Fi viittaa Wi-Fi Allianceen. Wi-Fi Alliance on voittoa tavoittelematon organisaatio, joka edistää Wi-Fi-tekniikkaa ja sertifioi Wi-Fi-tuotteiden yhteensopivuuden tiettyjen yhteensopivuusstandardien kanssa. Kaikkia IEEE 802.11 -yhteensopivia verkkolaitteita ei toimiteta varmennettavaksi Wi-Fi Allianceselle, sillä sertifiointiprosessi aiheuttaa kuluja. Wi-Fi-logon puuttuminen tuotteesta ei välttämättä tarkoita, että laite ei ole yhteensopiva muiden Wi-Fi-laitteiden kanssa.

Wi-Fi Alliance omistaa Wi-Fi-tavaramerkin. Valmistajat voivat käyttää tavaramerkkiä sertifioiduihin tuotteisiin, joiden yhteensopivuus on testattu. (Abramowitz 2019.)

3 Wi-Fi Salausprotokollat

Langattomien lähiverkkojen tietoliikenne kulkee radioaaltoina ilmassa toisin kuin perinteisissä kaapeliyhteyksissä, joten sen on oltava salattua. Ilman salausta kuka tahansa voisi passiivisesti kuunnella verkon viestijöiden välistä tiedonvaihtoa. (Puska 2005, 21.)

Langattomien lähiverkkojen käytön yleistymisen on osaltaan vauhdittanut salausprotokollien kehitystä. Koti- sekä yritysverkoissa liikkuu paljon kriittistä tietoa, joka paljastuessaan on tietoturvariski.

Tässä opinnäytetyössä keskityn empirian osalta tällä hetkellä vielä yleisesti käytössä olevaan WPA2-protokollaan, sillä sitä aikaisemmat salausprotokollat ovat haavoittuvaisempia ja niiden käyttäminen nykypäivänä ei ole järkevää. Tätä työtä tehdessä WPA3-protokollaa ei ole otettu merkittävässä määrin käyttöön maailmalla, vaikka kuluttajille on tarjolla kyseistä salausprotokollaa tukevia laitteistoja.

Kaikissa langattoman verkon salausprotokollissa on havaittu haavoittuvuuksia. Mitä vanhempi protokolla, sitä vakavampia haavoittuvuuksia se sisältää. Laittevalmistajat eivät enää esimerkiksi suosittele WEP-protokollan käyttöä, sillä sen ongelma on, että verkkoliikennettä passiivisesti kuuntelemalla on mahdollista havaita WLAN-yhteyden muodostamiseen tarvittava salasana. (Norman 2018, 123.)

Tässä luvussa käydään läpi langattomien verkkojen salausprotokollien historiaa ja ominaisuuksia.

3.1 WEP – Wired Equivalent Privacy

Edellisessä luvussa käsiteltiin 802.11 -standardia, joka kuvaa liikennettä langattomissa verkoissa. WEP oli ensimmäinen salausprotokolla, joka luotiin salaamaan langattonta verkkoliikennettä ja estämään sen salakuuntelua. WEP:n toissijainen tehtävä on estää luvaton pääsy langattomaan verkkoon. Tämä toiminto ei ole kuitenkaan tavoite 802.11-standardissa, mutta sitä pidetään usein WEP:n ominaisuutena. (Berkeley, Borisov & Goldberg 2011.)

WEP hyödyntää RC4 salausalgoritmia. Algoritmi perustuu vaihtelevan pituiseen salausavaimen. Alussa RC4 oli rajoitettu 40 bittiin USA:n vientirajoitusten takia. Tällä hetkellä sitä voidaan käyttää myös 64- ja 128 bittisinä. (Puska 2005, 79.)

3.2 WPA – Wi-Fi Protected Access

Vuonna 2001 IEEE perusti 802.11i -työryhmän suunnittelemaan uutta salausprotokollaa langattomille lähiverkoille. Työryhmä suunnitteli lopulta kaksi protokollaa; yhden, joka mahdollistaisi vanhentuneiden WEP-laitteistojen päivittämisen sekä toisen, joka perustui moderniin AES-lohkosalausmenetelmään. AES käyttää RC4:tä vahvempaa Rijndael-algoritmia ja 128, 192 ja 156 bitin salausavainta. Protokollat saivat nimet TKIP (Temporal Key Integrity Protocol) ja CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). (Halvorsen & Haugen 2011, 37.)

TKIP:llä oli suunnitteluvaiheessa yksi tärkeä tavoite; sen pitäisi olla toteutettavissa vanhalta WEP-laitteistolla päivityksen kautta. Tästä syystä TKIP:lle oli olemassa tietyt rajoitukset, miten se voitiin suunnitella. Näistä rajoituksista johtuen TKIP käyttää osittain samoja WEP-standardeja, mutta se tuo lisäturvaa kaikkia tunnettuja WEP-hyökkäyksiä vastaan. (Halvorsen & Haugen 2011, 37.)

CCMP suunniteltiin alusta asti tietoturva edellä. Sitä ei suunniteltu yhteensopivaksi vanhojen laitteistojen kanssa. (Halvorsen & Haugen 2011, 47.)

Wi-Fi Alliance ei ollut tyytyväinen IEEE:n työryhmän nopeuteen 802.11i -standardin parissa ja se halusi tarjota kuluttajille nopeammin parempaa tietoturvaa laitteistojen osalta. Tämä johti lopulta siihen, että Wi-Fi Alliance kehitti oman salausprotokollan IEEE 802.11i -työryhmän tulosten pohjalta. Wi-Fi Alliance antoi salausprotokollalleen nimen WPA (Wi-Fi Protected Access). (Halvorsen & Haugen 2011, 17.)

WPA- ja WPA2-protokollat vaativat niiden murtamiseen muutakin kuin passiivista verkko liikenteen kuuntelua. (Norman 2018.)

WPA-protokolla korjasi useimpia WEP-protokollan haavoittuvuuksia, koska se perustuu suurelta osin IEEE 802.11i-standardiin. Sen tietoturvaa parannettiin ottamalla käyttöön Temporal Key Integrity Protocol (TKIP). Kun WEP:n käyttämät salausavaimet ovat muuttumattomia ja ne pitää syöttää manuaalisesti yhteyspisteeseen sekä päätelaitteisiin, käyttää TKIP pakettikohtaisia avaimia, joilla taataan viestin eheys ja avaimen jakelutoiminto. (Puska 2005, 82.)

3.3 WPA2 – Wi-Fi Protected Access 2

IEEE:n 802.11i -työryhmä sai vuonna 2004 valmiiksi 802.11i -standardin ja IEEE antoi sille nimeksi Robust Security Network (RSN). RSN sisälsi kaksi tilaa: TKIP:n sekä

CCMP:n. RSN:n julkaisun hetkellä Wi-Fi Alliancen WPA-tavaramerkki oli kuitenkin saanut jo laajasti jalansijaa reititinvalmistajien keskuudessa ja Wi-Fi Alliance nimesi RSN standardin WPA2:ksi. (Halvorsen & Haugen 2011, 37.)

WPA2 tarjoaa parempaa suojaa kuin WPA luomalla jokaiselle verkkoon liittyvälle päätelaitteelle oman istuntoavaimen. Tämän seurauksena jokainen tietoliikennepaketti salataan päätelaittekohtaisella, yksilöllisellä salausavaimella. (Halvorsen & Haugen 2011, 37.)

3.4 Nelivaiheinen kättely (4-way handshake)

Nelivaiheinen kättely on prosessi, jossa yhteyspiste ja päätelaite sopivat yhteyden muodostamisesta. Kättelyssä yhteyspiste sekä päätelaite vaihtavat neljä viestiä keskenään, joiden tarkoitus on todistaa, että molemmat osapuolet tietävät langattoman verkon salasanan. Käydään aluksi läpi kättelyssä käytettävät salausavaimia koskevat termit:

PMK (Pairwise Master Key)

PTK (Pairwise Transient Key)

GTK (Group Transient Key)

GMK (Group Master Key)

ANonce

SNonce

MIC

3.4.1 PMK - Pairwise Master Key

PMK:n ymmärtämiseksi tarkastellaan lisäksi termejä PSK (Pre-Shared Key) sekä passphrase. Passphrase on langattomalle verkolle määritetty salasana. PSK muuntaa passphrasen 256-bittiseksi merkkijonoksi. WPA/WPA2-personal -protokollissa PMK on yhtä kuin PSK. Kättely on suunniteltu siten, että päätelaite sekä yhteyspiste voivat todistaa toisilleen tietävänsä PMK:n/PSK:n paljastamatta langattoman verkon salasanaa. (Ronder 2020.)

PMK on suunniteltu pysymään voimassa koko session ajan ilman, että se paljastuu. Tästä syystä on johdettava salausavaimet salaamaan liikenne päätelaitteen ja yhteyspisteen välillä. (Ronder 2020.)

3.4.2 PTK – Pairwise Transit Key

Parittaisen tilapäisavaimen (PTK) muodostamiseen tarvitaan PMK (Pairwise Master Key), yhteyspisteen muodostama AP Nonce (ANonce) eli satunnaisluku, päätelaitteen muodostama STA Nonce (SNonce) sekä molempien laitteiden MAC-osoitteet. (Puska 2005, 84.)

3.4.3 GTK ja GMK

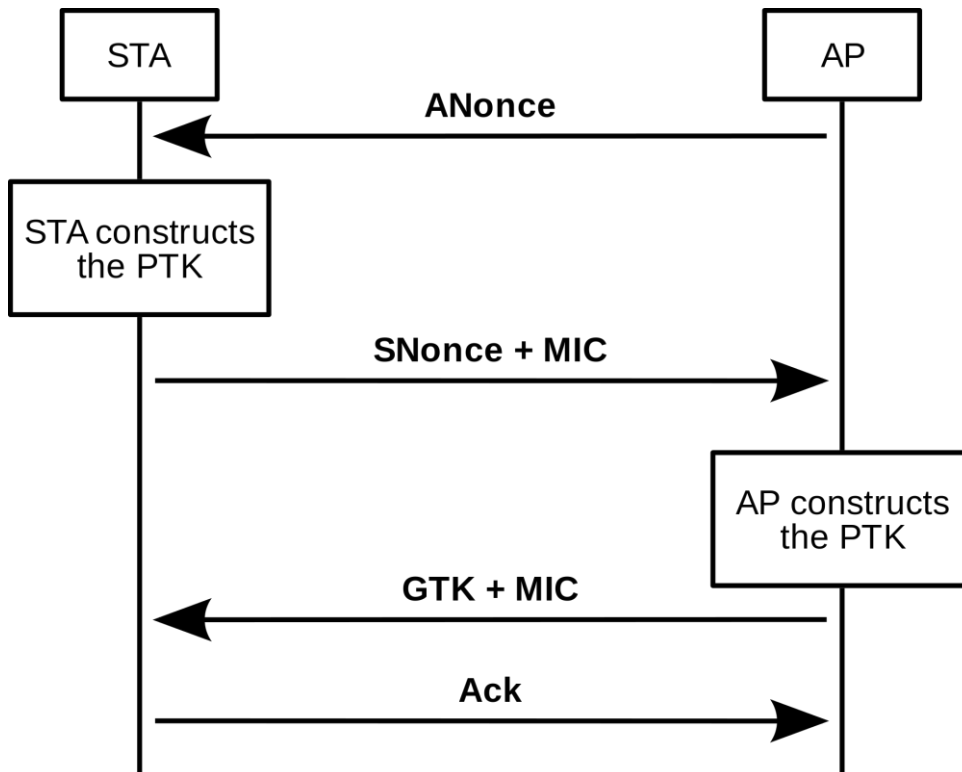
GTK (Groupwise Transient Key) johdetaan GMK:sta (Groupwise Master Key). GTK on avain, joka jaetaan kaikkien yhteyspisteeseen liittyvien päätelaitteiden välillä. Jokaiselle yhteyspisteellä on oma GTK, joka jaetaan siihen liittyvien päätelaitteiden välillä, jotta ne voivat purkaa ryhmälähetyksiä. (Puska 2005, 84.)

3.4.4 ANonce ja SNonce

Nonce tarkoittaa satunnaislukua, jonka yhteyspiste ja päätelaite generoivat muiden avainten muodostusta varten. (Puska 2005, 84.)

3.4.5 MIC – Message Integrity Check

MIC (Message Integrity Check) on pakettien eheyttä valvova toiminto, joka tarkistaa jokaisen paketin, jolloin mahdollinen hyökkääjä ei pysty kaappaamaan paketteja ja muuttamaan niiden tietoja. (Puska 2005, 84.)



Kuva 2. The four-way handshake in 802.11i. Kuvassa STA (Station) eli päätelaite ja AP (Access point) eli yhteyspiste (Wikimedia Commons 2005)

Viesti 1: Yhteyspiste lähettää satunnaisluvun (ANonce) päätelaitteelle, joka generoi tästä ja omasta satunnaisluvustaan (SNonce) parittaisen tilapäisavaimen (PTK). (Puska 2005, 84.)

Viesti 2: Päätelaite lähettää oman satunnaislukunsa (SNonce) yhdessä MIC-otsikon kanssa, joka varmistaa viestin eheyden. (Puska 2005, 84.)

Viesti 3: PTK-avaimesta lasketaan avaintenvaihdon vahvistusavain, avaintenvaihdon salausavain (Key Exchange Key) ja tilapäisavain (TK, Temporary Key). Ryhmä- ja yhteislähetystyksiä varten yhteyspiste generoi satunnaisen ryhmälähetysavaimen (GTK, Group Transient Key), salaa sen avaintenvaihdon salausavaimella ja lähettää päätelaitteelle, jotta päätelaite pystyy purkamaan ryhmälähetystyksiä- ja yhteislähetystyksiä. (Puska 2005, 84.)

Viesti 4: Päätelaite tarkastaa kolmannen viestin eheyden MIC-otsikon avulla ja ilmoittaa sitten yhteyspisteelle varmistuksen. (Puska 2005, 84.)

3.5 WPA3 – Wi-Fi Protected Access 3

Wi-Fi Alliance julkaisi huhtikuussa 2019 uuden WPA3-protokollansa, koska WPA2-protokolla on jo yli 14 vuotta vanha. WPA3 sisältää uuden Dragonfly-handshake nimellä

tunnetun kättelyn, jonka pitäisi estää langattoman verkon salasanan murtaminen. Tutkijat Vanhoef ja Ronen ovat kuitenkin löytäneet jo uusia haavoittuvuuksia myös WPA3-protokollan osalta. (Vanhoef & Ronen 2019.)

Wi-Fi Alliance julkaisi sivuillaan tiedotteen edellä mainittujen haavoittuvuuksien löytymisen jälkeen:

“Recently published research identified vulnerabilities in a limited number of early implementations of WPA3™-Personal, where those devices allow collection of side channel information on a device running an attacker’s software, do not properly implement certain cryptographic operations, or use unsuitable cryptographic elements. WPA3-Personal is in the early stages of deployment, and the small number of device manufacturers that are affected have already started deploying patches to resolve the issues. These issues can all be mitigated through software updates without any impact on devices’ ability to work well together. There is no evidence that these vulnerabilities have been exploited.” (Wi-Fi Alliance 2019.)

WPA3-protokolla tulee todennäköisesti yleistymään hiljalleen, kun uusia WPA3-sertifioituja verkkolaitteita julkaistaan markkinoille.

4 WLAN-verkon haavoittuvuudet

WLAN helpottaa verkkojen rakentamista, mutta se tuo mukanaan erilaisia tietoturvaongelmia langattomuuden vuoksi. Hyökkääjän ei esimerkiksi enää tarvitse päästä fyysisesti tilaan, jossa yhteys sijaitsee, koska langaton yhteyspiste toimii radiotaajuuksilla. Yhteyspisteeseen kohdistetun hyökkäyksen toteuttamiseen on vain oltava radiotaajuuksien kantaman sisällä. Tämän vuoksi hyökkäys on mahdollista toteuttaa melko kaukaa yhteyspisteen sijainti ja hyökkääjän laitteen antennien voimakkuus huomioon ottaen. Esimerkiksi lentokentillä hyökkääjän on helppo sulautua massaan ja luoda oma yhteyspiste kuvitteellisella nimellä kuten ”Free Airport Wi-Fi”, johon ihmiset mielellään yhdistävät omat laitteensa olettaen, että yhteyspiste on lentokentän tarjoama, vaikka se todellisuudessa on tietoja kalastelevan hyökkääjän hallussa.

4.1 Langaton palvelunestohyökkäys

Palvelunestohyökkäyksillä (DoS – Denial of Service) pyritään estämään käyttäjien pääsy johonkin tiettyyn palveluun tai resurssiin. Yleisimmät syyt palvelunestohyökkäysten toteuttamiseen ovat kiusanteko, aktivismi, kiristys ja valtiolähtöinen elektroninen sodankäynti. Tällöin puhutaan yleensä hajautetusta palvelunestohyökkäyksestä (DDoS – Distributed Denial of Service), jonka tarkoituksena on kohdistaa esimerkiksi verkkosivulle niin paljon samanaikaista tietoliikennettä, että sen toiminta häiriintyy. Tällaisilta hyökkäyksiltä on lähes mahdoton suojautua ja se on erittäin kallista. (Norman 2018, 145-146.)

Langattoman palvelunestohyökkäyksen tekeminen WLAN-yhteyspistettä vastaan on erittäin helppoa. Hyökkääjän tarvitsee olla käytännössä vain yhteyspisteen radiotaajuuksien kantaman sisällä. Tällaisesta hyökkäyksestä käytetään yleisesti termiä Wi-Fi deauthentication attack. Hyökkäyksellä vaikutetaan yhteyspisteen ja käyttäjän väliseen kommunikointiin. (Norman 2018, 144.)

Deauth-hyökkäystä voidaan käyttää katkaisemaan toistuvasti käyttäjien muodostamia yhteyksiä tukiasemiin tai sitä voidaan käyttää ensiaskeleena muissa hyökkäyksissä, joiden tarkoitus on tunkeutua yhteyspisteeseen. Deauth ei siis yksinään anna vielä pääsyä mihinkään resurssiin. (Norman 2018, 145.)

4.2 WPA/WPA2-PSK (Pre-Shared Key) hyökkäys

Toisin kuin hyökätessä WEP-protokollaa vastaan, WPA/WPA2-protokollia vastaan voidaan käyttää vain raakalaskentaa (Brute Force, Luku 7.2.2). Hyökkäys alkaa, kun yhteyspisteen ja päätelaitteen suorittama nelivaiheinen kättely saadaan kaapattua. Tämän jäl-

keen kaapatun kättelyn sisältämistä salausavaimista voidaan yrittää murtaa langattoman verkon esijaettua salasanaa (Pre-Shared Key) sanakirjahyökkäyksen avulla. Salasanan murtaminen on lähes mahdotonta, koska PSK voi olla 8-63 merkkiä pitkä. Salasana murtaa yleensä vain silloin, kun se on jokin yleinen pääteltävissä oleva sana. Langattoman verkon salasanaa kannattaakin valita mahdollisimman pitkä salasana, joka sisältää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä. (Aircrack-ng.org 2010.)

4.3 KRACKS – Key Re-installation Attacks

Belgialainen tutkija Mathy Vanhoef julkaisi tutkimustuloksiaan uudesta vakavasta WPA2-protokollan haavoittuvuudesta lokakuussa vuonna 2017. Haavoittuvuus sai nimen KRACKS, joka tulee sanoista Key Re-installation Attacks. KRACKS -hyökkäys iskee WPA2-protokollan nelivaiheiseen kättelyyn (4-way handshake). (Vanhoef 2017.)

KRACKS -hyökkäyksessä luodaan kopio (Evil twin) kohdetukiasemasta, jolle asetetaan sama nimi (SSID) sekä MAC-osoite. Tämän jälkeen kohteena olevaan päätelaitteeseen kohdistetaan deauth -hyökkäys, jolla saadaan päätelaite siirtymään hyökkääjän verkkoon, jossa kättelyä voidaan manipuloida vapaasti. Kättelyn kolmas viesti voidaan lähettää käyttäjälle uudelleen väittäen, että yhteyspiste ei saanut siitä vastausta. Näin ollen päätelaite asentaa saman, jo aikaisemmin neuvotellun salausavaimen, mutta nyt hyökkääjä on päässyt manipuloimaan avainta, joka ei salaakaan päätelaitteen ja yhteyspisteen välistä liikennettä. Tämän jälkeen hyökkääjä voi purkaa lisäksi HTTPS-salauksen päätelaitteen käyttäjän www-selainistunnosta ja nähdä verkkoliikennettä seuraamalla selkokielisenä esimerkiksi sen, mitä tietoja käyttäjä syöttää verkkosivujen kirjautumiskenttiin. (Vanhoef 2017.)

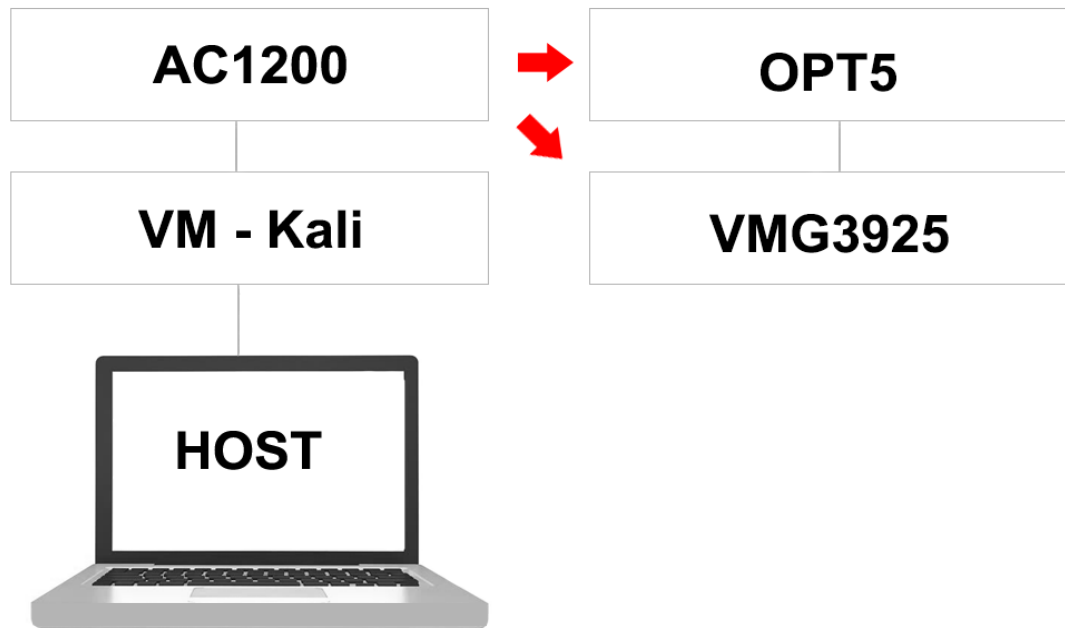
Vanhoefin löydökset olivat siinä mielessä merkittäviä, että haavoittuvuuden julkaisuhetkellä miljoonat laitteet olivat alttiita sille. Arvioiden mukaan jopa 50% Android -pohjaisista laitteista. (Vanhoef 2017.)

4.4 Laitteistovaatimukset hyökkäysten tekemiseksi

Vaadittavat laitteet hyökkäysten toteuttamiseksi ovat tietokone, sopiva käyttöjärjestelmä, esimerkiksi jokin Linux-jakelupaketti, kuten Kali ja verkkokortti, jonka saa monitor-tilaan. Monitor-tilassa voidaan kaapata lähellä olevien langattomien laitteiden ja verkkojen lähettämää ja vastaanottamaa dataa, josta nähdään helposti yhteyspisteet ja niissä yhdistettyinä olevat laitteet. Seuraavassa luvussa on kuvattu tarkemmin harjoitusympäristön laitteisto. (Norman 2018, 55.)

5 Harjoitusympäristön laitteisto

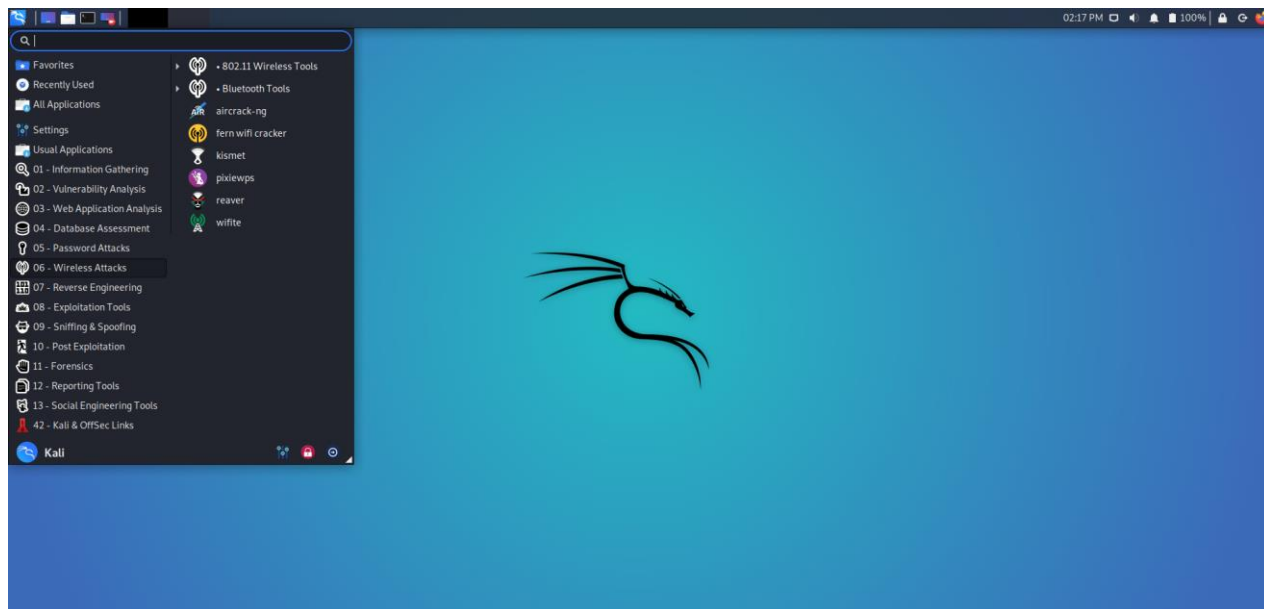
Tässä luvussa on kuvattu yksinkertainen harjoitusympäristö, joka rakennettiin tätä opinnäytetyötä varten. Kaikki työssä tehdyt hyökkäykset on kohdistettu tähän harjoitusympäristöön. Harjoitusympäristö koostuu seuraavanlaisesta kokoonpanosta: isäntäkone (host), virtuaalikone (Kali Linux), Alfa Networks AC1200 -verkkokortti, Oneplus 5T-puhelin ja Zyxel VMG3925 WLAN-reititin.



Kuva 3. Harjoitusympäristön laitteisto

5.1 Kali Linux

Kali Linux on Offensive Securityn kehittämä Debian-pohjainen käyttöjärjestelmä, joka on suunniteltu digitaaliforensiikkaan sekä penetraatiotestaukseen. Kali Linux sisältää yli 600 esiasennettua työkalua. Tässä työssä ei käydä läpi työkalujen asentamista eikä niillä suoritettavia komentoja. (Kuva 4.)



Kuva 4. Kali Linux

5.2 Aircrack-ng ohjelmisto

Kali Linuxissa on valmiiksi asennettuna Aircrack-ng niminen ohjelmisto, jota käytetään tässä työssä. Aircrack-ng on 802.11 -standardiin tehty ohjelmisto, joka soveltuu erityisesti tietoturva-auditointiin ja penetraatiotestaukseen. Aircrack-ng perustuu avoimeen lähdekoodiin. Aircrack-ng sisältää useita komentorivipohjaisia työkaluja, joita voidaan käyttää langattomien verkkojen auditointiin. Ohjelmisto tarjoaa työkalut langattoman verkon tietoliikenteen kuunteluun ja murtamiseen. Työkaluilla voidaan auditoida WEP, WPA- ja WPA2-protokollaa käyttäviä langattomia verkkoja. Aircrack-ng käyttää raakalaskentaa (Brute Force) sekä sanakirjahyökkäystä WPA- ja WPA2-protokollia vastaan, joista kerron lisää luvussa 7. (Aircrack-ng.org 2010.)

Aircrack-ng -ohjelmisto perustuu verkkoliikenteeseen, joka on kaapattu mukana toimitetulla airodump-ng-työkalulla tai millä tahansa muulla verkkoliikenteen sieppaustyökalulla. Aircrack-ng tarjoaa myös airmon-ng -työkalun, joka mahdollistaa monitor-tilan käyttämisen WLAN-verkkokortilla. Monitor-tilan avulla voidaan kaapata ja injektoida raakaa 802.11 -standardin mukaista verkkoliikennettä. Monitor-tila on edellytys useimmille hyökkäyksille, jotka kohdistuvat langattomiin verkkoihin. Aireplay-ng -työkalua käytetään verkkoliikenteen injektointiin, esimerkiksi langattomaan palvelunestohyökkäykseen. (Aircrack-ng.org 2010.)

5.3 Alfa Networks AC1200

AC1200 on Alfa Networksin valmistama verkkokortti, joka soveltuu penetraatiotestaukseen, sillä se tukee langattoman verkkoliikenteen kuunteluun käytettävää monitor-tilaa. AC1200 tukee 802.11ac/n -standardia. (Kuva 5.)

Vastaavia laitteita oli tarjolla kuluttajille jo vuonna 2001, vaikka 2,4 Ghz:n signaalin purkaminen oli hankalaa. (Berkeley, ym. 2001.)



Kuva 5. AC1200-verkkokortti (Alfa networks 2020)

5.4 Zyxel VMG3925

VMG3925 on Zyxelin valmistama reititin, joka soveltuu erityisesti kotikäyttöön. (Kuva 6.) VMG3925-reititin tukee 2,4- ja 5 Ghz:n taajuuksia seuraavilla standardeilla:

802.11b/g/n	2.4 GHz
802.11a/n/ac	5 GHz



Kuva 6. Zyxel VMG3925 (Zyxel 2016)

5.5 OnePlus 5T

OnePlus 5T on vuonna 2017 julkaistu Android-pohjainen puhelin. (Kuva 7.)



Kuva 7. OnePlus 5T (GSMArena.com 2017)

6 Testaussuunnitelma

Hyökkäykset testiympäristössä kohdistuvat WPA2-protokollalla suojattuun langattomaan lähiverkkoon. Hyökkäykset on jaettu kolmeen osaan:

1. Deauth eli langaton palvelunestohyökkäys
2. Nelivaiheisen kättelyn (handshake) kaappaus
3. Evil Twin -valeyhteyspiste

Ensimmäisessä vaiheessa kartoitetaan lähiverkko ja siihen yhteyden muodostanut päätelaite. Tämän jälkeen päätelaitteelle lähetetään deauth-käskey, jonka pitäisi katkaista päätelaitteen yhteys yhteyspisteeseen. Ensimmäisen vaiheen tutkimuskysymys on:

Onnistuuko deauth-hyökkäys ja mitkä ovat sen vaikutukset?

Toisessa vaiheessa yritetään murtaa WLAN-verkon kohtuullisen helppo salasana kaappaamalla verkkoliikenteestä päätelaitteen ja yhteyspisteen välinen nelivaiheinen kättely (handshake). Jos handshake saadaan kaapattua, tehdään sanakirjahyökkäys sen sisältämiin salausavaimiin salasanan murtamiseksi. Toisen vaiheen tutkimuskysymys on:

Onnistuuko nelivaiheisen kättelyn kaappaus verkkoliikennettä kuuntelemalla? Saadaanko verkon salasana murrettua sanakirjahyökkäyksen avulla?

Kolmannessa vaiheessa tehdään Evil Twin -hyökkäys, jossa luodaan valeyhteyspiste harjoitusympäristön yhteyspisteen tiedot väärentämällä. Kolmannessa vaiheessa tarvitaan ensimmäisen vaiheen deauth-hyökkäystä päätelaitteiden yhteyden katkaisemiseksi. Tämän jälkeen valeyhteyspisteen signaalin ollessa vahvempi kuin harjoitusympäristön yhteyspisteen, yritetään päätelaitteet saada muodostamaan yhteys valeyhteyspisteeseen. Tutkimuskysymys kolmannessa vaiheessa on:

Onnistuuko valeyhteyspisteen luonti väärennetyillä harjoitusympäristön yhteyspisteen tiedoilla eli nimellä (SSID) sekä MAC-osoitteella. Yhdistävätkö päätelaitteet valeyhteyspisteeseen, kun sen signaali on vahvempi kuin harjoitusympäristön yhteyspisteellä?

Kun testisuunnitelman mukaiset hyökkäykset on saatu tehtyä harjoitusympäristössä ja niiden vaikutuksista on tehty havaintoja, pyritään vastaamaan vielä neljänteen tutkimuskysymykseen:

Mitkä ovat suositeltuja toimenpiteitä suojautua WPA2-haavoittuvuuksia vastaan?

7 Skenaariokuvaukset WLAN-verkkoa vastaan tehdyistä hyökkäyksistä yksinkertaisessa harjoitusympäristössä (kotiverkko)

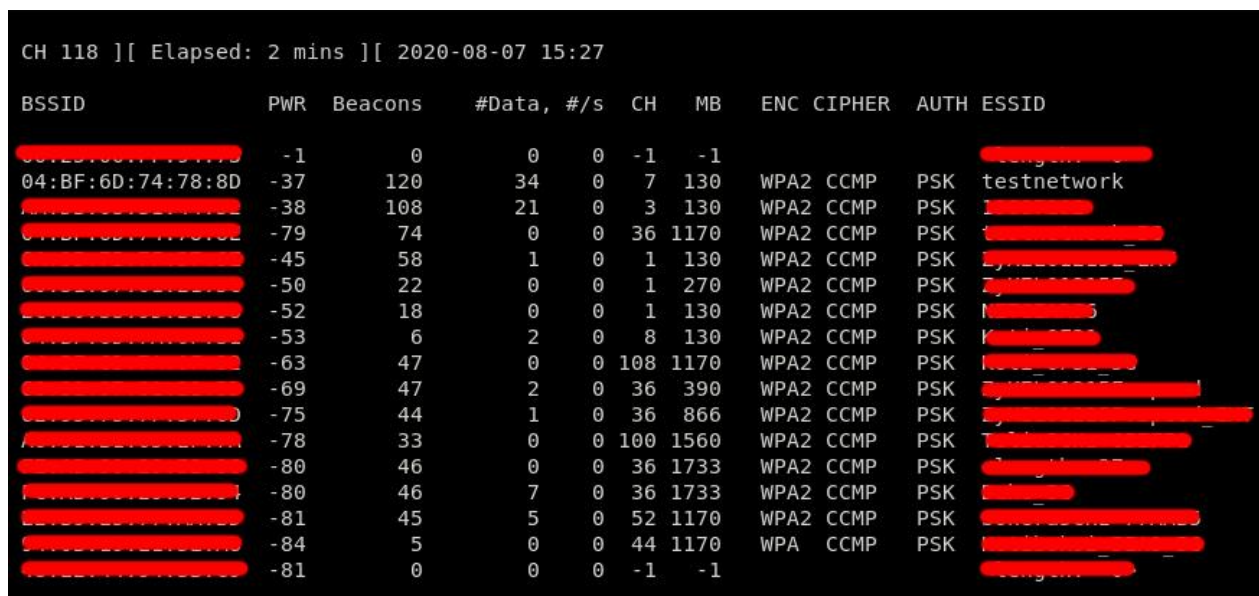
Tutkin työssäni eri hyökkäysten toimivuutta sekä vaikuttavuutta, kun kohteena on tavallinen kotiverkon WLAN-reititin sekä matkapuhelin. Tutkimustulosten on tarkoitus tuoda esille, kuinka helposti hyökkäykset ovat toteutettavissa ohjeita seuraamalla kenelle tahansa aiheesta kiinnostuneelle. Seuraavissa hyökkäyksissä käytetään pelkästään yleisesti saatavilla olevia ohjeita ja ohjelmistoja.

7.1 Skenaario 1 – Deauth

Deauth-hyökkäyksellä voidaan katkaista yhteys laitteilta, jotka on yhdistetty langattomiin verkkoihin. Hyökkäys toimii siten, että kohdeverkon yhteyspisteelle lähetetään väärennetty pyyntö päätelaitteen MAC-osoitteella katkaista suojattu yhteys yhteyspisteeseen. Hyökkäys on mahdollista tehdä liittymättä itse kohdeverkkoon, koska yhteydenmuodostamiseen käytetyt viestinvaihdot päätelaitteen ja yhteyspisteen välillä ovat salaamattomia.

Wi-Fi protokollan 802.11w myötä julkaistiin PMF (Protected Management Frames) -ominaisuus, jonka tarkoitus on estää deauth-hyökkäys varmentamalla deauth-pyyntöjen alkuperä. Jotta PMF toimii, se vaatii tuen yhteyspisteeltä sekä kohdelaitteelta ja tällä hetkellä läheskään kaikki laitteet eivät tue 802.11w-protokollaa.

7.1.1 Hyökkäyksen aloitus



BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
04:BF:6D:74:78:8D	-37	120	34	0	7	130	WPA2	CCMP	PSK	testnetwork
	-38	108	21	0	3	130	WPA2	CCMP	PSK	
	-79	74	0	0	36	1170	WPA2	CCMP	PSK	
	-45	58	1	0	1	130	WPA2	CCMP	PSK	
	-50	22	0	0	1	270	WPA2	CCMP	PSK	
	-52	18	0	0	1	130	WPA2	CCMP	PSK	
	-53	6	2	0	8	130	WPA2	CCMP	PSK	
	-63	47	0	0	108	1170	WPA2	CCMP	PSK	
	-69	47	2	0	36	390	WPA2	CCMP	PSK	
	-75	44	1	0	36	866	WPA2	CCMP	PSK	
	-78	33	0	0	100	1560	WPA2	CCMP	PSK	
	-80	46	0	0	36	1733	WPA2	CCMP	PSK	
	-80	46	7	0	36	1733	WPA2	CCMP	PSK	
	-81	45	5	0	52	1170	WPA2	CCMP	PSK	
	-84	5	0	0	44	1170	WPA	CCMP	PSK	
	-81	0	0	0	-1	-1				

Kuva 8. Deauth, skannaus

Aloitin skannaamalla ympärilläni olevia langattomia lähiverkkoja. Tutkimukseni kohdistuu omaan harjoitusympäristöni lähiverkkoon, jonka nimi on testnetwork ja MAC-osoite 04:BF:6D:74:78:8D. Skannaus paljastaa, että kohdeverkossa on käytössä WPA2-PSK-salaus ja verkko toimii WLAN-kanavalla 7. (Kuva 8.)

Skannauksessa havaitut muut verkot on yliviivattu, koska tietyissä tapauksissa niiden fyysinen paikantaminen on mahdollista.

7.1.2 Päätelaitteen yksilöinti

```
CH 7 ][ Elapsed: 5 mins ][ 2020-08-07 15:37
CH 7 ][ Elapsed: 9 mins ][ 2020-08-07 15:41
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
04:BF:6D:74:78:8D	-36	96	5627	7352 1	7	130	WPA2	CCMP	PSK	testnetwork

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
04:BF:6D:74:78:8D	36:34:C1:70:9A:40	-35	1e- 1e	0	6686		

Kuva 9. Deauth-hyökkäyksen kohdistaminen

Seuraavaksi näemme, että testnetwork-verkkoon on yhdistettynä yksi laite, jonka MAC-osoite on 36:34:C1:70:9A:40. (Kuva 9.) Kyseinen laite on harjoitusympäristöni kuuluva OnePlus 5T-puhelin. Tästä eteenpäin kohdistan deauth-hyökkäyksen vain edellä mainittuun puhelimeen. Hyökkäys olisi kuitenkin mahdollista kohdistaa kaikkiin laitteisiin samanaikaisesti, jotka ovat kiinni samassa yhteyspisteessä. Tällä on merkitystä erityisesti silloin, kun deauth-hyökkäystä käytetään vain esivaiheena vakavimmille hyökkäyksille.

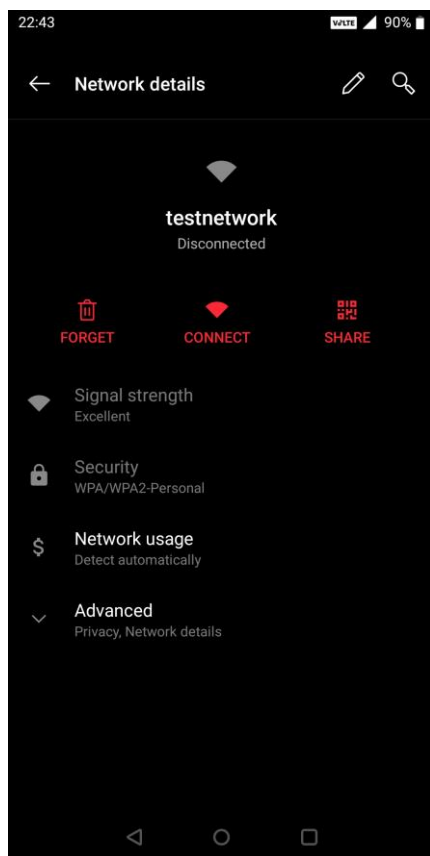
7.1.3 Deauth-pakettien lähetys

```
15:43:45 Sending 64 directed DeAuth (code 7). STMAC: [36:34:C1:70:9A:40] [ 3|53 ACKs]
15:43:46 Sending 64 directed DeAuth (code 7). STMAC: [36:34:C1:70:9A:40] [ 0|62 ACKs]
15:43:47 Sending 64 directed DeAuth (code 7). STMAC: [36:34:C1:70:9A:40] [ 0|65 ACKs]
15:43:47 Sending 64 directed DeAuth (code 7). STMAC: [36:34:C1:70:9A:40] [ 0|67 ACKs]
15:43:48 Sending 64 directed DeAuth (code 7). STMAC: [36:34:C1:70:9A:40] [ 0|61 ACKs]
15:43:49 Sending 64 directed DeAuth (code 7). STMAC: [36:34:C1:70:9A:40] [ 0|65 ACKs]
15:43:49 Sending 64 directed DeAuth (code 7). STMAC: [36:34:C1:70:9A:40] [ 0|63 ACKs]
15:43:50 Sending 64 directed DeAuth (code 7). STMAC: [36:34:C1:70:9A:40] [ 0|64 ACKs]
15:43:51 Sending 64 directed DeAuth (code 7). STMAC: [36:34:C1:70:9A:40] [ 0|63 ACKs]
15:43:51 Sending 64 directed DeAuth (code 7). STMAC: [36:34:C1:70:9A:40] [ 0|64 ACKs]
```

Kuva 10. Deauth pakettien lähetys

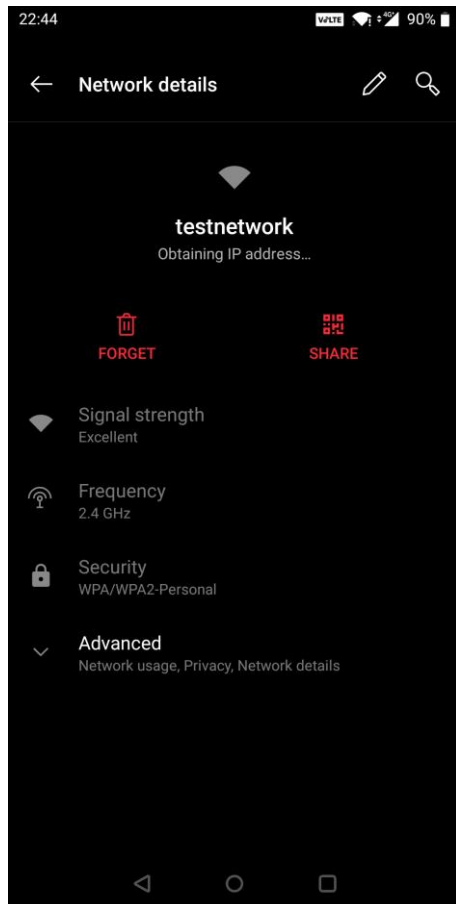
Kohdeverkon yhteyspisteelle lähetetään väärennetty pyyntö päätelaitteen MAC-osoitteella (36:34:C1:70:9A:40) katkaista yhteyspisteeseen muodostettu yhteys. Deauth-pakettien lähetys toistuu valintani mukaisesti kymmenen kertaa, noin yhden sekunnin välein. (Kuva 10.) Deauthia voisi jatkaa periaatteessa myös loputtomasti.

7.1.4 Deauth hyökkäyksen tulos



Kuva 11. Puhelimen katkennut yhteys

Päätelaitteen yhteys yhteyspisteeseen katkeaa välittömästi heti ensimmäisen deauth-paketin lähettämisen jälkeen. (Kuva 11.) Niin kauan kun deauth jatkuu, ei puhelin käytännössä pysty muodostamaan yhteyttä takaisin yhteyspisteeseen, vaan sen muodostama yhteys katkeaa heti uudelleen.



Kuva 12. Yhteyden uudelleen muodostaminen

Päätelaitteena toimiva OnePlus 5T-puhelin yrittää muodostaa automaattisesti yhteyden yhteyspisteeseen uudelleen, kun deauth-hyökkäys päättyy. (Kuva 12.) Toistin saman hyökkäyksen kolme kertaa, jonka jälkeen OnePlus 5T ei enää yhdistänyt yhteyspisteeseen uudelleen. Deauth-hyökkäyksestä voisi halutessaan tehdä jatkuvan ja näin estää haluttujen laitteiden yhteyden muodostamisen yhteyspisteeseen periaatteessa pysyvästi.

7.2 Skenaario 2 – nelivaiheisen kättelyn kaappaus

Deauth hyökkäys toimii myös esivaiheena muille vakavimmille hyökkäyksille. Deauthin tarkoitus on katkaista päätelaitteen yhteys yhteyspisteeseen ja odottaa, että päätelaite muodostaa yhteyden uudelleen. Sillä hetkellä, kun yhteys muodostetaan uudelleen, voidaan yhteyden muodostamisessa käytettävä nelivaiheinen kättely (four-way handshake) kaapata ilmasta. (Kuva 13.)

```
Reading packets, please wait...
Opening /root/capture-02.cap
Read 18609 packets.

# BSSID ESSID Encryption
1 04:BF:6D:74:78:8D testnetwork WPA (1 handshake, with PMKID)

Choosing first network as target.

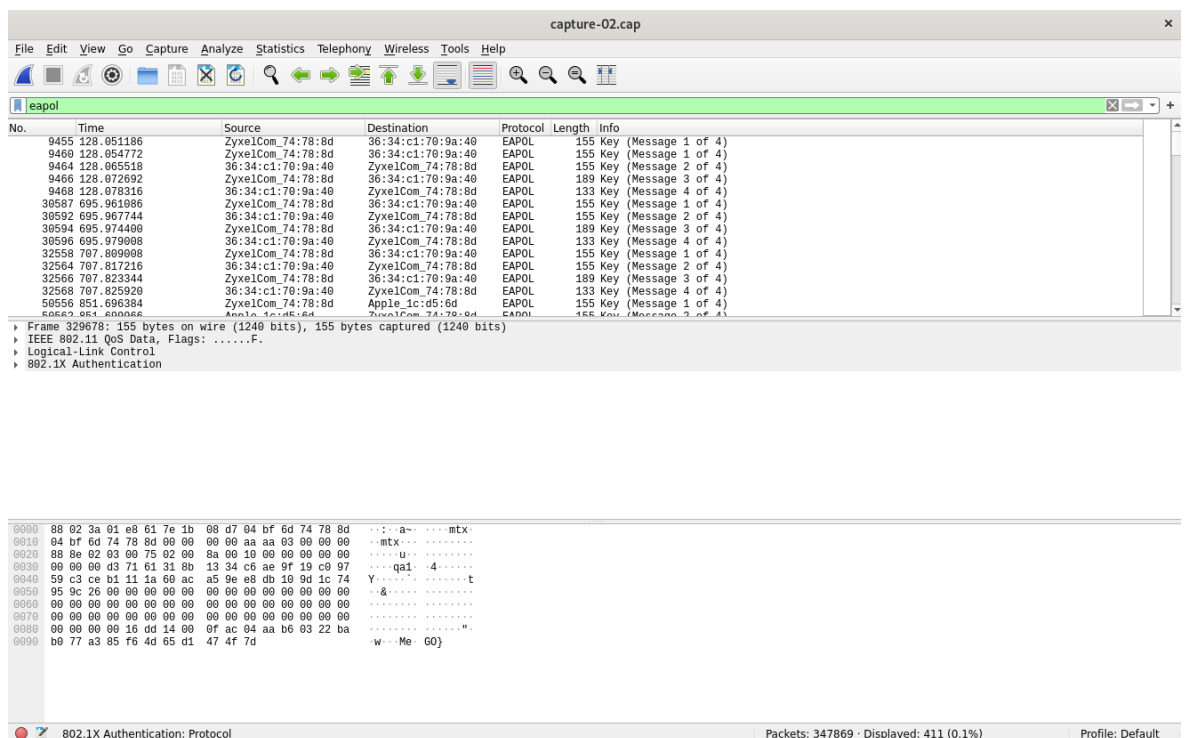
Reading packets, please wait...
Opening /root/capture-02.cap
Read 18609 packets.

1 potential targets

Please specify a dictionary (option -w).
```

Kuva 13. Kaapattu handshake

Kaapattu handshake tallentuu tiedostoon ja sitä voi tarkastella Wireshark-ohjelmistolla. Kuvasta 14 nähdään, että yhteyspisteen ja päätelaitteen välinen handshake tallentui kokonaisuudessaan (messages 1-4). Kaappaus ei suinkaan aina onnistu ensimmäisellä yrityksellä, vaan sitä täytyy yrittää uudelleen. Kaappauksen onnistumista lisää kohdelaitteiden määrä, jotka ovat yhteydessä yhteyspisteeseen, sillä silloin voidaan katkaista näiden kaikkien laitteiden yhteys ja odottaa, että ne muodostavat yhteyden uudelleen. Näin saadaan kaapattua mahdollisesti useita eri kättelyitä. Onnistuneen kaappauksen jälkeen verkon salasanaa vastaan voidaan hyökätä sanakirjahyökkäyksellä.



Kuva 14. Kaapatun handshake:n katselu Wireshark-ohjelmassa

7.2.1 Sanakirjahyökkäys

Sanakirjahyökkäys (Dictionary Attack) on menetelmä, joka vertaa salasanalistoja murrettavaan salasanaan. Salasanalistat voivat sisältää jopa miljardeja erilaisia merkkijonoja. Näiden lisäksi niihin lisätään jatkuvasti verkkoon vuotavia tietokantoja, jotka sisältävät ihmisten käyttämiä salasanoja eri palveluissa. Salasanalistan vertaaminen murrettavaan salasanaan vie aikaa tehokkaalla tietokoneella listan pituudesta riippuen, sekunneista tunteihin. Vertailuun käytetään raakalaskentaa (Brute Force). (Hashcat.net 2020.)

7.2.2 Raakalaskenta eli Brute Force

Raakalaskenta eli Brute Force on tekniikka, johon hyödynnetään tietokoneiden laskentakapasiteettia. Nykyaikaiset näytönohjaimet ovat tässä avainasemassa, sillä niiden avulla voidaan suorittaa huomattavan paljon enemmän rinnakkaislaskentaa verrattuna tietokoneen prosessoriin. Tämä johtuu siitä, että näytönohjaimissa on enemmän ytimiä kuin prosessorissa. Tyypillisessä tietokoneen prosessorissa on 4-32 ydintä, kun taas näytönohjaimessa ydinten määrä voi olla jopa 10496, kuten NVIDIA:n RTX 3090 -näytönohjaimessa. Tämä tarkoittaa yksinkertaisesti sitä, että näytönohjain voi suorittaa huomattavan paljon enemmän samanaikaisia laskentatehtäviä eli esimerkiksi laskea erilaisia salasanayhdistelmiä salasanaa murrettaessa. (Whitwam 2020.)

Pitkän salasanan murtaminen raa'alla laskentateholla on huomattavan paljon aikaa vievä prosessi. Salasana, joka sisältää yhdeksän merkin edestä isoja ja pieniä kirjaimia sekä numeroita, esimerkiksi Kasvi1980 murtaminen raa'alla laskentateholla vaatii sen, että käydään läpi kaikki isot ja pienet kirjaimet, sekä numerot eli 62^9 . Tällöin erilaisia yhdistelmiä on olemassa 13.537.086.546.263.552. Jos tietokone kävisi läpi sata miljoonaa yhdistelmää sekunnissa, veisi salasanan murtaminen hieman yli 4 vuotta. (Hashcat.net 2020.)

Ihmiset luovat salasanoja kuitenkin usein tiettyjen mallien mukaisesti, joista hyvin yleinen on edellisessä esimerkissäkin käytetty 9 merkkiä pitkä salasana, joka koostuu nimestä ja vuosiluvusta. Hyökkäystä voidaan ohjata kokeilemaan isoja kirjaimia vain ensimmäisen merkin kohdalla, sillä ihmisillä on tapana luoda salasana niin, että ensimmäinen merkki on iso kirjain, harvoin toinen tai kolmas merkki. Murtamiseen vaadittavaa aikaa saadaan lyhennettyä näin ollen $52 \cdot 26 \cdot 26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 \cdot 10$ eli 237.627.520.000 erilaista yhdistelmää. Samalla 100M/s laskentateholla murtamiseen kuluisi vain 40 minuuttia. (Hashcat.net 2020.)

Salasanojen murtamiseen on tehty useita erilaisia työkaluja. Yksi suosittu työkalu on Hashcat. Työkalujen avulla salasanojen murtamiseen vaadittava aika saadaan lyhyemmäksi, kun raa'an laskennan apuna käytetään erilaisia ennalta määrättyjä merkkijonoja, kuten vuosilukuja. (Hashcat.net 2020.)

Sanakirjahyökkäyksen ja raa'an laskennan tekniikoiden yhdistämistä kutsutaan hybridiksi, jossa salasanan murtaminen tapahtuu puoliksi sanasanalistojen sekä laskennan avulla. (Hashcat.net 2020.)

Murrettavaan salasanaan verrattavassa salasanalistassa voisi olla esimerkiksi sanat:

kasvi
kello

..joiden perään lisätään numerot 0-9999, jotka käydään järjestelmällisesti läpi.

kasvi0000
kasvi0001
kasvi0002
.
.
kasvi9999
kello0000
kello0001
kello0002
.
.
kello9999

Näitä yhdistelmiä käytetään siis sen takia, että ihmisillä on tapana luoda tietynlaisia salasanoja, jotka on helppo muistaa. (Hashcat.net 2020.)

Omassa harjoitusympäristössäni käytin Aircrack-ng:n tarjoamaa sanakirjahyökkäystä, joka tosin on hidas verrattuna näytönohjainta hyödyntävään Hashcatiin. Ohjelma yrittää siis murtaa salasanan kaapatun nelivaiheisen kättelyn sisältämistä salausavaimista.

```
Aircrack-ng 1.6

[00:00:00] 219/222 keys tested (3618.32 k/s)

Time left: 0 seconds                                98.65%

KEY FOUND! [ 12345678 ]

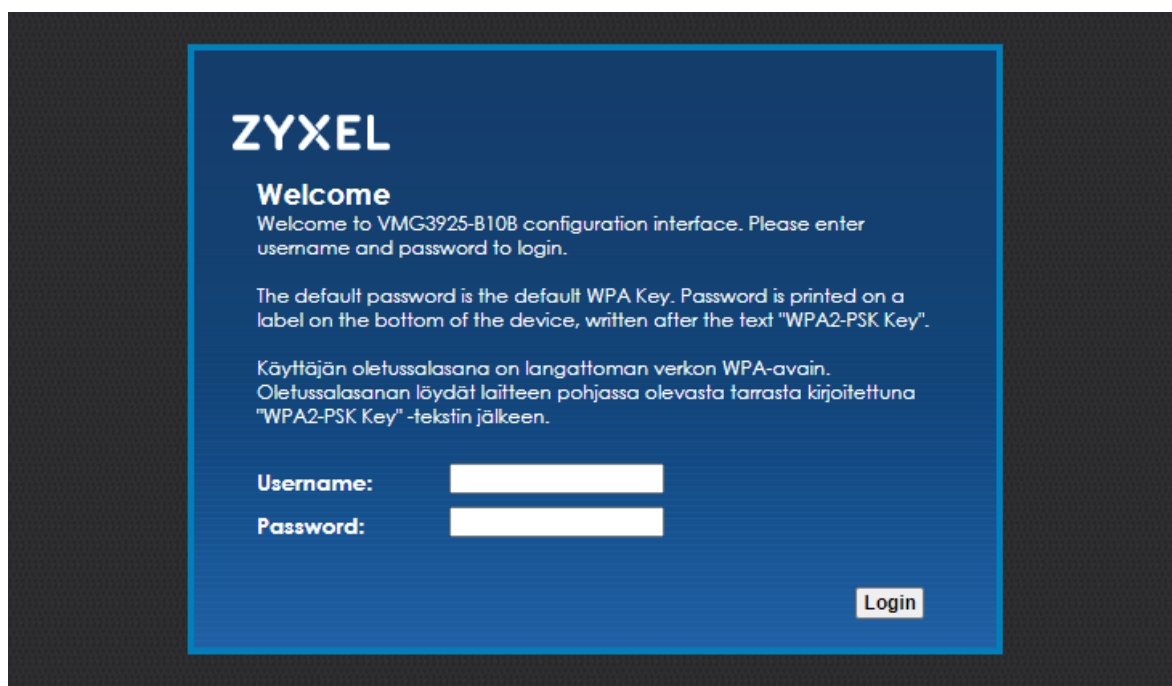
Master Key      : 3E 23 CB 6D DF 5F 1D 28 B4 FA C3 FF FA 4D 5C A2
                  F0 02 16 93 E2 66 7B EA F4 AD 2B 25 C1 AC 91 04

Transient Key   : 4E 3B 14 F9 DD E5 83 C4 46 50 5B 10 F4 63 B2 E2
                  DB 7D 54 07 1B 03 9C 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 8F 10 BC 50 E9 3D 3A B1 82 47 2B 26 68 63 7D DD
```

Kuva 15. Onnistunut sanakirjahyökkäys

Kuva 15 kertoo, että salasanan murtaminen onnistui ja reitittimelle asettamani salasana oli hyvin yksinkertainen: 12345678. Kyseinen salasana löytyi valmiina Kali Linuxin salasanalistaista. 222-sanan listan läpikäymiseen kului aikaa alle sekunti.



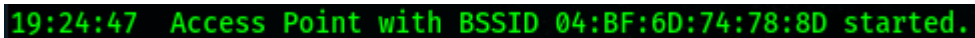
Kuva 16. Zyxel-reittimen kirjautumissivu

Kun yhteyspisteen salasana on murrettu ja verkkoon päästy liittymään, on seuraavaksi mahdollista yrittää kirjautua yhteyspisteen asetuksiin (Kuva 16.). Joidenkin Zyxel-merkkisten modeemien kirjautumistunnukset ovat oletuksena admin ja salasana 1234, kun taas osa laitteista on suojattu hieman paremmin ja salasana löytyy modeemin taakse kiinnitetystä tarrasta. Oletussalasana kannattaa kuitenkin käydä vaihtamassa tarpeeksi pitkäksi ja monimutkaiseksi, varsinkin jos se oletuksena on admin/1234.

Modeemin asetuksiin päässyt hyökkääjä voi tehdä monenalaista haittaa, esimerkiksi muuttaa DNS eli nimipalvelimen hyökkääjän hallussa olevaan. DNS-palvelin muuntaa URL-osoitteet IP-osoitteiksi, esim. iltalehti.fi -> 13.226.202.128. Hyökkääjä voisi luoda aidon näköisen kopion esimerkiksi Nordean nettipankista ja ohjata uhrin liikenteen oman DNS-palvelimen avulla väärennetyille sivulle, kun uhri syöttää selaimen osoitekenttään nordea.fi.

7.3 Skenaario 3 – Evil Twin -hyökkäys

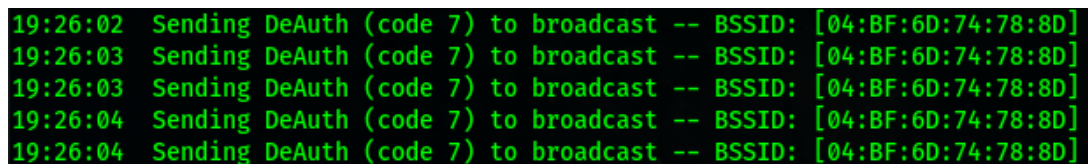
Evil Twin -hyökkäyksessä ideana on luoda väärennetty WLAN-yhteyspiste jonkin lähistöllä olevan aidon WLAN-yhteyspisteen tiedoilla. WLAN-yhteyspisteen nimi ei kerro mitään sen todellisesta ylläpitäjästä, koska kuka tahansa voi nimetä WLAN-yhteyspisteen millä tahansa nimellä. Tämän jälkeen väärennetyn yhteyspisteen lähetystehoa voidaan nostaa ja aidon WLAN-yhteyspisteen yhdistetyille laitteille lähetetään deauth-paketteja yhteyden katkaisemiseksi. Tavoitteena on saada laitteet yhdistämään nyt väärennettyyn WLAN-yhteyspisteeseen, sillä monet laitteet eivät erota aitoa ja väärennettyä yhteyspistettä, kun niillä on sama nimi (SSID).



```
19:24:47 Access Point with BSSID 04:BF:6D:74:78:8D started.
```

Kuva 17. Evil Twin -yhteyspisteen perustaminen

Aloitin luomalla väärennetyn yhteyspisteen samalla nimellä ja MAC-osoitteella, kuin testiympäristössä oleva testnetwork. (Kuva 17.)



```
19:26:02 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BF:6D:74:78:8D]
19:26:03 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BF:6D:74:78:8D]
19:26:03 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BF:6D:74:78:8D]
19:26:04 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BF:6D:74:78:8D]
19:26:04 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BF:6D:74:78:8D]
```

Kuva 18. Deauth-pakettien lähetys aidon yhteyspisteen laitteille

Väärennetty yhteyspiste on nyt perustettu ja on aika lähettää deauth-paketteja aitoon yhteyspisteen yhdistetyille laitteille. (Kuva 18.) Deauthin tarkoitus on siis katkaista yhteys laitteilta ja toivoo, että ne päättävät sen jälkeen muodostaa yhteyden meidän luomaan väärennettyyn yhteyspisteeseen, joka on laitteiden näkökulmasta houkutteleva sen vahvemman lähetystehon ja saman SSID:n vuoksi.

```
19:26:07 Client E8:61:7E:1B:08:D7 associated (WPA2;CCMP) to ESSID: "testnetwork"
19:26:18 Client E8:61:7E:1B:08:D7 associated (WPA2;CCMP) to ESSID: "testnetwork"
19:26:29 Client E8:61:7E:1B:08:D7 associated (WPA2;CCMP) to ESSID: "testnetwork"
19:26:40 Client E8:61:7E:1B:08:D7 associated (WPA2;CCMP) to ESSID: "testnetwork"
19:27:02 Client E8:61:7E:1B:08:D7 associated (WPA2;CCMP) to ESSID: "testnetwork"
19:27:14 Client E8:61:7E:1B:08:D7 associated (WPA2;CCMP) to ESSID: "testnetwork"
19:27:17 Client 36:34:C1:70:9A:40 associated (WPA2;CCMP) to ESSID: "testnetwork"
19:27:25 Client E8:61:7E:1B:08:D7 associated (WPA2;CCMP) to ESSID: "testnetwork"
19:27:37 Client E8:61:7E:1B:08:D7 associated (WPA2;CCMP) to ESSID: "testnetwork"
19:28:00 Client E8:61:7E:1B:08:D7 associated (WPA2;CCMP) to ESSID: "testnetwork"
```

Kuva 19. Laitteet yhdistävät väärennettyyn yhteyspisteeseen

Kuvasta 19 nähdään, että välittömästi deauth-hyökkäyksen jälkeen laitteet muodostivat yhteyden luomaani väärennettyyn yhteyspisteeseen.

Evil Twin -hyökkäystä käytetään yleensä tietojenkalasteluun ihmisiltä. Monet hotellien WLAN-verkot vaativat hotelliasiakkaita kirjautumaan web-portaalin kautta WLAN-verkkoon. Evil Twin -hyökkäyksessä voidaan luoda kopio vastaavasta kirjautumisportaalista, johon uhri ohjataan syöttämään aidon hotellin WLAN-verkon kirjautumistiedot. Väärennetyn yhteyspisteen luonut näkee syötetyt tiedot selkokieleisenä.

8 Johtopäätökset

Työssä tutkittiin langattoman lähiverkon WPA2-salausprotokollaan kohdistuvia hyökkäyksiä yksinkertaisessa harjoitusympäristössä. Hyökkäykset oli jaettu kolmeen osaan:

1. Deauth eli langaton palvelunestohyökkäys
2. Nelivaiheisen kättelyn (handshake) kaappaus
3. Evil Twin -valeyhteyspiste

Ensimmäisestä vaiheesta tehtiin seuraavanlaisia havaintoja: deauth-hyökkäys on merkitävä uhka langattomille verkoille, koska se katkaisee päätelaitteen muodostaman yhteyden yhteyspisteeseen. Hyökkäys onnistui liittymättä itse kohdeverkkoon, koska yhteydenmuodostamiseen käytetyt viestinvaihdot päätelaitteen ja yhteyspisteen välillä ovat salaamattomia. Hyökkäyksen vaikutukset nähtiin reaaliajassa: päätelaitteen muodostama yhteys katkesi välittömästi, kun ensimmäinen deauth-paketti lähetettiin. Deauth-hyökkäystä on myös mahdollista jatkaa periaatteessa loputtomasti, jolloin päätelaitteen yhteyden muodostaminen voidaan paikallisesti estää kokonaan. Deauth-hyökkäyksiltä suojautuminen on lähes mahdotonta, ellei langatonta lähiverkkoa suunnitella 802.11w -standardin mukaiseksi.

Toisessa vaiheessa hyödynnettiin ensimmäisen vaiheen deauth-hyökkäystä, kun päätelaitteen ja yhteyspisteen välinen nelivaiheinen kättely onnistuttiin kaappaamaan verkkoliikennettä kuuntelemalla. Deauth-hyökkäyksellä katkaisiin ensin päätelaitteen muodostama yhteys, jonka jälkeen odotettiin päätelaitteen yhteyden uudelleenmuodostamista. Samalla hetkellä, kun päätelaite muodosti uudelleen yhteyden yhteyspisteeseen, saatiin verkkoliikenteestä kaapattua nelivaiheinen kättely (handshake).

Nelivaiheisen kättelyn sisältämiin salausavaimiin käytettiin Aircrack-ng -ohjelmiston tarjoamaa sanakirjahyökkäystä. Harjoitusympäristön langattoman verkon salasana oli helppo murtaa, koska se tunnistettiin Kali Linuxissa valmiina olevasta salasanalistasta. Tästä voidaan todeta, että käyttämällä tarpeeksi pitkää ja monimutkaista salasanaa kuten esimerkiksi S*Z9JAg},#cJ"]_68wc, voidaan sanakirjahyökkäykseltä suojautua melko hyvin, koska monipuolisen salasanan löytyminen salasanalistaista on epätodennäköistä.

Kolmannessa vaiheessa tehtiin Evil Twin -hyökkäys luomalla valeyhteyspiste väärennetyillä, harjoitusympäristön yhteyspisteen tiedoilla eli nimellä (SSID) ja MAC-osoitteella. Valeyhteyspisteen luominen onnistui ja sen signaali oli vahvempi kuin harjoitusympäristön yhteyspisteellä. Tämän jälkeen käytettiin deauth-hyökkäystä katkaisemaan harjoitusympä-

ristön päätelaitteen yhteys yhteyspisteeseen. Yhteyden katkeamisen jälkeen päätelaite muodosti yhteyden valeyhteyspisteeseen onnistuneesti.

Kaikki testaussuunnitelman mukaiset hyökkäykset onnistuivat ja niille asetetuille tutkimuskysymyksille saatiin vastaukset. Kaikilla hyökkäyksillä oli odotusten mukaisia vaikutuksia. Samat hyökkäykset voidaan toteuttaa myös muissa ympäristöissä, samanlaisella laitteistolla.

Hyökkäyksissä käytetty laitteistobudjetti oli noin 500 euroa, joka koostui pääosin kannettavasta tietokoneesta ja Alfa AC1200 verkkokortista. Hyökkäykset olisi mahdollista toteuttaa vieläkin halvemmalla, noin 200 eurolla. Voidaankin siis todeta, että laitteiston hankintakulut eivät ole este motivoituneelle hyökkääjälle.

Ohjeet hyökkäysten tekemiseksi löytyivät Internetin avoimista lähteistä. Ohjeet olivat hyvin yksityiskohtaisia ja niitä oli helppo noudattaa.

9 Suositellut toimenpiteet lähiverkkoyhteyden turvaamiseksi

Oma lähiverkko kannattaa suojata vahvasti heti käyttöönoton yhteydessä, sillä motivoitunut hyökkääjä pystyy pahimmillaan asentamaan reitittimen laiteohjelmiston (firmware) tilalle oman, muokatun ohjelmiston, jonka avulla hyökkääjä saa kontrollin koko verkosta ja sen käyttäjistä. (Puska 2005, 67.)

WLAN-yhteyspisteen oletusasetuksista vähintään verkon- sekä verkon hallintapaneelin salasana kannattaa vaihtaa käyttöönoton yhteydessä riittävän pitkäksi ja monipuoliseksi. Salasanan pituudeksi kannattaa valita 20 merkkiä ja salasanaan on hyvä sisältyä sekä isoja, että pieniä kirjaimia, numeroita ja erikoismerkkejä. Tällöin sen murtaminen Brute Force -menetelmällä on epätodennäköistä tai erittäin paljon aikaa vievää. Samaa salanaa ei kannata käyttää useassa paikassa, sillä salasanan paljastuessa kaikki samalla salasanalla suojatut palvelut ja laitteet vaarantuvat.

Vahvan salasanan lisäksi reitittimestä on syytä kytkeä pois WPS (Wi-Fi Protected Setup). WPS:n tarkoituksena on helpottaa langattomien laitteiden yhteyden muodostamista käyttämällä reitittimen WPS-painiketta, joka yhdistää asiakaslaitteen reitittimen kanssa tai vaihtoehtoisesti 8-numeroisen PIN-koodin avulla. WPS sisältää kuitenkin kriittisen haavoittuvuuden, jonka avulla sen PIN-koodi voidaan murtaa kohtuullisessa ajassa raakalaskennalla eli Brute Force -tekniikalla. (Viehböck 2011.)

Suositteltu salaus langattomille lähiverkkoyhteyksille tällä hetkellä on WPA2, sen haavoittuvuuksista huolimatta. WLAN-yhteyspisteen asetuksissa WPA2 saattaa esiintyä termeillä "WPA2+PSK (AES)" tai "WPA2-Personal". (TRAFICOM 2014.)

Jos WLAN-yhteyttä on pakko käyttää esimerkiksi ulkomailla työhön liittyvässä konferenssissa, on suositeltavaa asentaa omalle koneelle virtuaalinen erillisverkko (VPN) salaamaan oma verkkoliikenne vahvasti. (TRAFICOM 2014.)

Yritystasolla hyvän tietoturvan toteuttaminen vaatii järjestelmällistä suunnittelua, toteutusta ja seurantaa, jonka lähtökohtana on kirjoitettu tietoturvapoliittikka. Siinä määritellään yrityksen tietoturvatavoitteet, turvattavat resurssit, kaikki verkkolaitteet sekä noudatettavat menettelytavat. Yritys toteuttaa tietoturvapoliittikan perusteella tarvittavia toimenpiteitä kuten laite- ja ohjelmistohankintoja, ohjeita ja määrittelyjä. Tehtyjen toimenpiteiden jälkeen seurataan järjestelmien ja verkkojen käyttöä hyökkäysten, väärinkäytösten ja virheellisten toimien havaitsemiseksi. Jatkuva seuranta on edellytys tietoturvan toteutumiseksi. Järjestelmien ja verkkojen tietoturvaa on myös syytä testata ajoittain. Seuranta ja testaus ovat välttämättömiä, jotta tietoturvaratkaisuja voidaan parantaa. (Puska 2005, 70.)

10 Pohdinta

Samat tietoturvaongelmat ovat piinanneet WLAN-verkkoja jo vuosikaudet ja hyökkääjät hyödyntävät salausprotokollien haavoittuvuuksia jatkuvasti. 17.9.2020 julkaistussa The Register -sivuston artikkelissa todetaan, että Yhdysvaltain sisäministeriö ei läpäissyt tietoturva-auditointia pääosin puutteellisten WLAN-verkkojen suojausten vuoksi. (Nichols 2020.)

Artikkelin mukaan sisäasiainministeriön WLAN-verkot murrettiin alle 200 dollaria maksavalla laitteistolla, johon kuului matkapuhelin sekä vastaavanlainen verkkokortti kuin tässä opinnäytetyössä. Tietoturvatestaajat toteuttivat virastojen läheisyyteen Evil Twin-hyökkäyksen, jonka avulla he saivat haltuunsa sisäasiainministeriön työntekijöiden käyttäjätunnuksia ja salasanoja. Näiden tietojen avulla tietoturvatestaajat pääsivät jopa sisäasiainministeriön käyttämiin sisäverkkoihin. (Nichols 2020.)

Tässä työssä tehdyt hyökkäykset testiympäristöön onnistuivat hyvin ja niiden toteuttaminen oli kohtalaisen helppoa avoimista lähteistä löytyvien ohjeiden avulla. Hyökkäysten ymmärtäminen auttaa osaltaan myös suojautumaan niitä vastaan. Käytännössä pienelläkin budjetilla, jopa alle 100 eurolla, on mahdollista aiheuttaa paljon harmia erilaisissa verkkoympäristöissä. Langatonta verkkoliikennettä on helppo häiritä, joten sen varassa olevat toiminnot eivät voi olla kovinkaan kriittisiä.

WPA2-protokolla on melko turvallinen, kun langattoman verkon salasana on riittävän pitkä ja monimutkainen. Laitteet on myös syytä pitää päivitettynä laitevalmistajan tarjoaman uusimman firmwaren osalta. WPS-ominaisuus kannattaa myös kytkeä pois päältä, sillä sen murtaminen on erittäin helppoa. Langallista yhteyttä kannattaa suosia langattoman sijaan, silloin kun se on käytön kannalta järkevää.

Wi-Fi Alliance julkaisi kesäkuussa 2018 WPA3-protokollan. Sen luvataan tuovan parempaa tietoturvaa edelliseen WPA2-protokollaan verrattuna. Tutkijat ovat löytäneet kuitenkin jo nyt monia haavoittuvuuksia myös WPA3-protokollasta. Mathy Vanhoef ja Eyal Ronen julkaisivat 2019 tutkimuksensa Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd, joka käsittelee WPA3 sekä EAP-pwd protokollien haavoittuvuuksia. Vanhoefin perustamalla sivustolla pelkästään WPA3-protokollan haavoittuvuuksia on havaittu ainakin seuraavat:

- CERT ID #VU871675: Downgrade attack against WPA3-Transition mode leading to dictionary attacks.

- CERT ID #VU871675: Security group downgrade attack against WPA3's Dragonfly handshake.
- CVE-2019-9494: Timing-based side-channel attack against WPA3's Dragonfly handshake.
- CVE-2019-9494: Cache-based side-channel attack against WPA3's Dragonfly handshake.
- CERT ID #VU871675: Resource consumption attack (i.e. denial of service) against WPA3's Dragonfly handshake. (Vanhoeft 2019)

WPA3-protokollan suunnittelijoita yritettiin saada muuttamaan protokollan käyttämää Dragonfly kättelyä, mutta jostain syystä näitä ehdotettuja korjauksia ei toteutettu. (Vanhoeft & Ronen, 2019.)

Tulevaisuus näyttää siltä, että WPA3-protokolla tulee yleistymään jossain vaiheessa, mutta toistaiseksi valtaosa laitteista käyttää WPA2-protokollaa. WPA3 tulee sisältämään useita haavoittuvuuksia, joille suurin osa laitteista altistuu. Laittevalmistajat eivät tunnetusti tuo vanhoille laitteille kovinkaan usein uusia tietoturvapäivityksiä.

Lähteet

Abramovitz, J. 2019. Wi-Fi Alliance®, then and now. Luettavissa: <https://www.wi-fi.org/beacon/jeff-abramowitz/wi-fi-alliance-then-and-now>. Luettu: 12.12.2020.

Aircrack-ng.org. 2010. Tutorial: How to Crack WPA/WPA2. Luettavissa: https://www.aircrack-ng.org/doku.php?id=cracking_wpa. Luettu: 14.12.2020.

Alexandre, C. 2019. How does WPA/WPA2 WiFi security work, and how to crack it? Luettavissa: <https://cylab.be/blog/32/how-does-wpawpa2-wifi-security-work-and-how-to-crack-it> Luettu: 30.7.2020.

Berkeley, I., Borisov N., Goldberg, I. & Wagner D. 2001. Security of the WEP algorithm. Luettavissa: <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>. Luettu 11.12.2020.

Cisco. 2018. 802.11ac: The Fifth Generation of Wi-Fi. Luettavissa: <https://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-3600-series/white-paper-c11-713103.pdf>. Luettu: 11.12.2020.

Colbach, G. 2019. The WiFi Networking Book WLAN Standards: IEEE 802.11 bgn, 802.11n, 802.11ac and 802.11ax. ISBN: 1073328422. Amazon.com.

Halvorsen, F. & Haugen, O. 2011. Cryptanalysis of IEEE 802.11i TKIP. Luettavissa: http://wiki-files.aircrack-ng.org/doc/tkip_master.pdf. Luettu 11.12.2020.

Hashcat.net. 2020. Mask Attack. Luettavissa: https://hashcat.net/wiki/doku.php?id=mask_attack Luettu 1.11.2020.

The four-way handshake in 802.11i, 2007. Luettavissa: <https://commons.wikimedia.org/wiki/File:4-way-handshake.svg> Luettu: 30.7.2020.

Nichols, S. 2020. Feeling bad about your last security audit? Check out what just happened to the US Department of Interior. Luettavissa: https://www.theregister.com/AMP/2020/09/17/dot_pentesers_expose_wifi. Luettu 19.9.2020.

Norman, A. 2018. Hacked: Kali Linux and Wireless Hacking Ultimate Guide With Security and Penetration Testing Tools, Practical Step by Step Computer Hacking Book. CreateSpace Independent Publishing Platform. Amazon.com.

Piessens, F. & Vanhoef, M. 2017. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. Luettavissa: <https://papers.mathyvanhoef.com/ccs2017.pdf>. Luettu: 3.3.2020.

Puska, M. 2005. Langattomat verkot. Gummerus kirjapaino. Jyväskylä.

Ronder, A. 2020. The 4-way handshake WPA/WPA2 encryption protocol. Luettavissa: <https://medium.com/@alonr110/the-4-way-handshake-wpa-wpa2-encryption-protocol-65779a315a64>. Luettu: 12.12.2020.

Sandler, E. 2002. Understanding 802.11 Frame Types. Luettavissa: <https://www.wi-fiplanet.com/understanding-802-11-frame-types>. Luettu 9.8.2020.

STUK, 2020. Langaton lähiverkko. Luettavissa: <https://www.stuk.fi/aiheet/kodin-jatoimiston-sateilevat-laitteet/langaton-lahiverkko>. Luettu: 2.12.2020

TRAFICOM, 2014. WLAN-salaus salaa vain radioliikenteen. Luettavissa: <https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/09/ttn201409091046.html>. Luettu: 30.7.2020

Vanhoef, M. 2017. Key Reinstallation Attacks, Breaking WPA2 by forcing nonce reuse. Luettavissa: <https://www.krackattacks.com>. Luettu: 3.3.2020.

Vanhoef, M. & Ronen, E. 2019. DRAGONBLOOD, Analysing WPA3's Dragonfly Handshake. Luettavissa: <https://wpa3.mathyvanhoef.com>. Luettu 1.11.2020.

Viehböck, S. 2011. Brute forcing Wi-Fi Protected Setup. Luettavissa: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf. Luettu: 14.12.2020.

Whitwam, R. 2020. The Nvidia RTX 3090 GPU Can Probably Crack Your Passwords Luettavissa: <https://www.extremetech.com/extreme/316266-the-nvidia-rtx-3090-gpu-can-probably-crack-your-passwords>. Luettu: 14.12.2020.