TAMPEREEN
AMMATTIKORKEAKOULU

TIETOTURVA LANGATTOMASSA LÄHIVERKOSSA

Tuomas Pajukoski

Opinnäytetyö
Toukokuu 2018
Tieto- ja viestintätekniikka
Tietoverkot ja tietoliikennetekniikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikka
Tietoverkot ja tietoliikennetekniikka

PAJUKOSKI TUOMAS:
Tietoturva langattomassa lähiverkossa

Opinnäytetyö 31 sivua, joista liitteitä 2 sivua
Toukokuu 2018

Opinnäytetyön tarkoituksena oli rakentaa kokonaisvaltainen mielikuva langattoman lähiverkon tietoturvasta. Yksittäisinä osa-alueina tutkittiin langattoman lähiverkon standardoinnin kehityskulkua, langattoman lähiverkon tietoturvaa ja muutamia tavanomaisia hyökkäystapoja langattomia lähiverkkoja kohtaan. Työn tavoitteena oli kehittää osaamista erityisesti tietoturvakysymyksien saralla, mutta myös yleisesti WLAN-teknologiaan liittyen. Tietoa haettiin pääasiassa alan kirjallisuudesta ja verkon asiantuntijalähteistä.

Opinnäytetyön suorittamisesta saatiin koostettua tiivis katselmointi langattoman lähiverkon tietoturvaan ja niihin tekijöihin, jotka ovat muokanneet sitä nykyiseen tilaansa. Tietoturva ja langattoman lähiverkkoliikenteen ominaisuudet ovat jatkuvassa kehityspaineessa langattomuuden suosion kasvaessa, ja tämä kehityskulku selkeni opinnäytetyön tuloksena.

Tietoturvakehityksen ja sen ongelmien tutkimisesta saatiin paljon ajatuksia siitä, miten ihmisten tulisi ottaa langaton tietoturva huomioon jokapäiväisessä työskentelyssään ja langattoman verkon muussa käyttämisessä. Langaton liikenne on muodostunut niin tavanomaiseksi osaksi elämäämme, että tietoliikenteeseen ja tietoturvaan perehtymättömänkin henkilön olisi viisasta käyttää jonkin verran aikaa langattoman liikenteen keskeisimpien turvallisuusominaisuuksien ja haavoittuvuuksien hahmottamiseen.

Asiasanat: langaton lähiverkko, wlan, tietoturva, verkkohyökkäykset

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
ICT Engineering
Telecommunications and Networks

PAJUKOSKI TUOMAS:
Security in Wireless Local Area Network

Bachelor's thesis 31 pages, appendices 2 pages
May 2018

The purpose of this thesis was to construct an overall view on the security of a wireless local area network. Individual subjects that were researched included the history of wireless local area network standardization, the security of a wireless local area network and some of the most common types of attacks on wireless local area networks. The goal was to further expertise especially in the field of network security but also in WLAN technology in general.

From constructing the thesis, a comprehensive view concerning wireless network security and the factors that molded it in to its current state was formed. Network security and the properties of wireless local area network traffic are under constant pressure to evolve as the popularity of wireless networking increases. The view on this cycle of development clarified as result of the research done for the thesis.

The general development of network security and research done on its problems brought forward several ideas about how people should consider wireless security in their everyday work and leisure use of wireless networks. Wireless networking has become such a regular part of our lives that even someone who is not knowledgeable in telecommunications and security should spend some time in developing a general idea on the fundamentals of the properties and vulnerabilities of wireless security.

Key words: wireless local area network, wlan, security, network attacks

SISÄLLYS

LYHENTEET JA TERMIT

802.11	langattoman lähiverkon standardi
802.1X	802.1X Port Based Authentication, porttikohtainen autentikointimenetelmä
ASCII	American Standard Code for Information Interchange, merkistö
AES	Advanced Encryption Standard, salausmenetelmä
CCK	Complementary Code Keying, modulaatiomenetelmä
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, salausprotokolla
DoS	Denial of Service, palvelunestohyökkäys
DDoS	Distributed Denial of Service, hajautettu palvelunestohyökkäys
DSSS	Direct Sequence Spread Spectrum, modulaatiomenetelmä
EAP	Extensible Authentication Protocol, käyttäjän autentikointiin käytettävä tunnistusprotokolla
IEEE	Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan järjestö
IoT	Internet of Things, asioiden internet, internetin laajentuminen esimerkiksi kodinkoneisiin
ISM	Industrial, Scientific and Medical, radiotaajuuskaista, mikä oli alun perin tarkoitettu teolliseen, tieteelliseen ja lääketieteelliseen käyttöön
IV	Initialization Vector, kryptologiassa käytetty alustusvektori
MAC	Media Access Control, verkon varaamisesta ja liikenteestä vastaava järjestelmä
MIC	Message Integrity Code, datan eheyden tarkistamiseen käytetty koodi
MIMO	Multiple-Input and Multiple-Output, tietoliikennetekniikka, missä dataa voidaan lähettää ja vastaanottaa useammalla kuin yhdellä antennilla
MitM	Man-in-the-Middle, tietoturvahyökkäys, missä hyökkääjä asettuu linkiksi kahden viestijän välille.

MU-MIMO	Multi-User-MIMO, ks. MIMO, MIMO-teknologian hyödyntäminen usealle käyttäjälle samaan aikaan
OFDM	Orthogonal Frequency-Division Multiplexing, moduloimenetelmä
OSI-malli	Open Systems Interconnection (model), tietoliikenteen kerroksittainen esitysmalli
PSK	Pre-Shared Key, jaettu avain, millä autentikoidaan käyttäjiä ja salataan liikennettä
RC4	Ron's Code 4, Rivest Cipher 4, salausalgoritmi
SSID	Service Set IDentifier, WLAN-verkon verkkotunnus
TKIP	Temporal Key Integrity Protocol, salausprotokolla
TSC	TKIP Sequence Counter, lähetettävien kehysten sekvensointiin käytettävä laskuri
VoIP	Voice over Internet Protocol, tekniikka, missä puheluita siirretään internetin välityksellä
WEP	Wired Equivalent Privacy, langattoman lähiverkon salaus- ja autentikointimenetelmä
WLAN	Wireless Local Area Network, langaton lähiverkko
WPA	Wi-Fi Protected Access, langattoman lähiverkon salausprotokolla
WPA2	ks. WPA

1 JOHDANTO

Langattomien lähiverkkojen suosio on ollut huimassa kasvussa useiden vuosien ajan. Nykyiset langattomat verkot ovat nopeita ja käyttäjälle vaivattomia ja joustavia. Mobiilidatansiirtoyhteydet ovat kehittyneet langattomien lähiverkkojen rinnalla varteenotettavaksi tavaksi yhdistää internetiin, mutta silti esimerkiksi kaupungilla kulkiessaan löytää jatkuvasti avoimia WLAN-hotspoteja. Tämän suosion kanssa käsi kädessä kulkee kannettavien laitteiden yleistyminen ja perinteisten pöytäkoneiden hidas katoaminen niin kodeista ja kotitoimistoista, kuin yrityksistä ja oppilaitoksistakin.

WLAN-yhteyksien käyttäjille tärkeintä on yhteyden saatavuus sekä yksinkertaisuus ja nopeus. Näiden ohella langattomien verkkojen tietoturvan tulisi olla paras mahdollinen niin verkkoon yhdistettäessä kuin datan liikkuessa tukiaseman ja päätelaitteen välilläkin. Langattomuus tuo mukanaan tiettyjä haavoittuvuuksia ja tietoturvan ammattilaiset sekä teknologian heikkouksia hyväkseen käyttävät hyökkääjät ovat jatkuvassa kilpailussa pysyäkseen toistensa edellä.

Tässä opinnäytetyössä syvennytään ensimmäiseksi langattomien lähiverkkostandardien yleiseen kehityskulkuun ja niiden keskeisimpien ominaisuuksien päivittymiseen versiosta toiseen. Seuraavaksi käydään läpi WLAN-tietoturvan kehitystä kronologisesti, kiinnittäen huomiota puutteisiin ja tietoturvasukupolvien parannuksiin edellisiin nähden. Lopuksi tutkitaan muutamia tyypillisiä hyökkäystapoja langattomia lähiverkkoja kohtaan.

2 WLAN-STANDARDOINTI

2.1 IEEE

Institute of Electrical and Electronics Engineers (IEEE) on kansainvälinen järjestö, jonka tarkoituksena on teknologian kehittäminen ihmiskunnan hyväksi. Siihen kuuluu yli 423 tuhatta jäsentä yli 160 maassa ja se on taustalla liki kolmanneksessa maailman tietotekniikan, elektroniikan ja sähkötekniikan julkaisuista. IEEE:n tärkeimpiin toimintoihin kuuluu useiden eri teknologioiden standardointi, jotka liittyvät esimerkiksi tietoliikenteeseen, antenniteknologiaan, energiatuotantoon ja kuluttajaelektroniikkaan. (IEEE.)

2.2 Wi-Fi Alliance

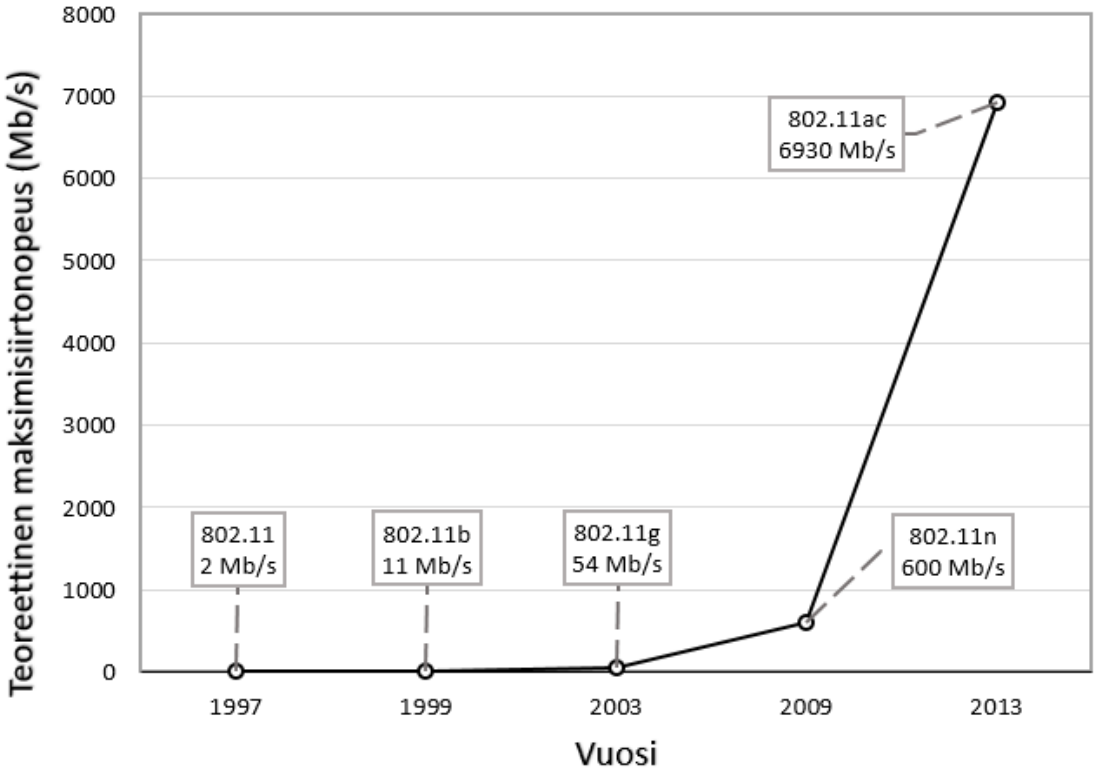
Vuonna 1999 perustettu Wi-Fi Alliancen tärkein tehtävä on eri laitevalmistajien tuotteiden yhteensopivuuden varmistaminen. Wi-Fi Alliance suorittaa laajamittaista yhteensopivuus-, turvallisuus- ja ominaisuustestausta sekä kuluttajaluokan, että yritysluokan laitteille. Sertifiointi on mahdollista myöntää esimerkiksi verkkolaitteille, matkapuhelimille, tietokoneille sekä muulle kuluttajaelektroniikalle. (Wi-Fi Alliance.)

KUVA 1. Wi-Fi sertifioidun tuotteen logo.

Saavuttaakseen oikeuden käyttää Wi-Fi Certified -logoa (kuva 1) tuotteen täytyy läpäistä Wi-Fi Alliancen riippumaton laboratoriotesti. Testin läpäisyyn vaaditaan laaja yhteensopivuus jo sertifioitujen laitteiden kanssa sekä vaadittavien ominaisuuksien ja tarvittaessa tietoturvaominaisuuksien täyttyminen. (Wi-Fi Alliance.)

2.3 IEEE 802.11 -standardit

IEEE:n standardi 802.11 on langattoman lähiverkon (WLAN) de facto standardi, jonka ensimmäinen versio julkaistiin vuonna 1997. Alkuperäisen 802.11-standardin siirtonopeus 2 Mb/s on kasvanut usean version kautta jopa gigabittien siirtonopeuteen sekunnissa ja nopeuden odotetaan yhä kasvavan tulevien standardien mukana. Kuviossa 1 on esitelty muutamien keskeisimpien standardien teoreettiset maksimisiirtonopeudet julkaisuvuosineen. On tärkeää huomioida, että todellinen siirtonopeus riippuu suuresti käytetystä konfiguraatiosta ja realistinen siirtonopeus on huomattavasti teoreettista maksimia pienempi. (Poole, 1-7.)



KUVIO 1. IEEE 802.11 -standardien tiedonsiirtonopeuden kehitys.

Seuraavaksi on esitelty muutamia keskeisimpiä WLAN-standardeja. Esiteltyjen standardien lisäksi IEEE on julkaissut lukuisia muita 802.11x-standardeja, joita on räätälöity erikoistuneempaan käyttöön, kuten esimerkiksi IoT:n (Internet of Things) tarpeisiin.

2.3.1 802.11a

Langattoman verkon standardi 802.11a julkaistiin samaan aikaan 802.11b:n kanssa vuonna 1999. 802.11a toimii 5 GHz:n taajuusalueella, missä sillä on käytettävissä 12 kanavaa 20 MHz:n kanavavälein. Se kykenee teoriassa maksimissaan 54 megabitin siirtonopeuteen sekunnissa, mutta tyypillisessä käyttötilanteessa realistinen siirtonopeus on noin puolet maksimista. Julkaisuajankohtanaan 802.11a tarjosi raakoina lukuina huomattavasti parempaa suorituskykyä, kuin laajemman suosion saanut 802.11b, joka toimii 2,4 GHz:n taajuusalueella. Tämä pienemmäksi jäänyt suosio johtui pääasiassa taloudellisista näkökulmista, sillä 802.11a toimii 5 GHz:n taajuusalueella eli ISM-taajuusalueella (Industrial, Scientific, Medical). Tälle taajuusalueelle tarvittavat piirit olivat kalliimpia valmistaa, joten 802.11a jäi pääasiassa yritysmaailman käyttöön. (Poole, 2.)

2.3.2 802.11b

IEEE 802.11b päätyi kustannustehokkaana ja suorituskyvyltään riittävänä langattomien verkkoyhteyksien suosion kasvun keskipisteeseen. Se toimii 2,4 GHz:n taajuusalueella ja käyttää 20 MHz:n kanavia. Standardin teoreettinen maksimisiirtonopeus on 11 Mb/s ja tyypillisesti sen nopeus jää 5 Mb/s:n tasolle. 802.11b käyttää CCK-koodausta (Complementary Code Keying) yhdessä DSSS-modulaation (Direct Sequence Spread Spectrum). kanssa. Tämä modulaatiovalinta auttoi osaltaan 802.11b:n suosion kehitystä, sillä alkuperäisessä 802.11-standardissa käytettiin DSSS-modulaatiota. Vanhan teknologian yksinkertainen päivittäminen tarkoitti helppoa ja taloudellista siirtymää uuteen standardiin. (Poole, 3.)

2.3.3 802.11g

Vuonna 2003 julkaistu 802.11g suunniteltiin korvaamaan 2,4 GHz:n alueella toimiva 802.11b ja tarjoamaan samalla lukuisia parannuksia edeltäjäänsä verrattuna. Sen teoreettinen maksimisiirtonopeus yltää 802.11a:n tasolle, eli 54 Mb/s asti ja samoin sen realistinen maksimisiirtonopeus jää noin puoleen ilmoitetusta teoriamaksimista, eli noin 24 megabittiin sekunnissa. 802.11g on taaksepäin yhteensopiva vanhan 802.11b-järjestelmän kanssa, vaikka 802.11b:n käyttäminen samassa verkossa hidastaakin siirtonopeutta.

Taaksepäin yhteensopivuus taattiin mahdollisuudella vaihtaa modulaatiomenetelmää tarpeen mukaan. Tuetut modulaatiomenetelmät olivat 802.11a:ssa käytetty OFDM, jolla verkko kykeni 6-54 Mb/s tiedonsiirtonopeuksiin ja 802.11b:n kanssa yhteensopiva DSSS-CCK, mitä käyttämällä verkko saattoi toimia 1-11 Mb/s nopeudella. (Poole, 5.)

2.3.4 802.11i

Vuonna 2004 julkaistussa 802.11i-standardissa kiinnitettiin huomiota alkuperäisen 802.11-standardin tietoturvan puutteellisuuteen. Standardilla oli kaksi päätavoitetta: tarjota parempi autentikointimenetelmä verkon ”ovella” ja suojella verkossa liikkuvaa dataa luotettavammin. Standardissa esiteltiin kaksi vaihtoehtoa autentikoinnille: kuluttajakäyttöön sopiva PSK-autentikointi (Pre-Shared Key) ja yritystasolle tarkoitettu 802.1X-standardia hyödyntävä EAP-autentikointi (Extensive Authentication Protocol). (Coleman ym. 2010, 17.)

Radiotiellä liikkuvan datan luottamuksellisuutta parannettiin tehokkaammalla salausmenetelmällä, CCMP:llä (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), jonka taustalla on AES-algoritmi (Advanced Encryption Standard). Standardissa esiteltiin lisäksi uusi valinnainen salausmenetelmä TKIP (Temporal Key Integrity Protocol), joka toimi väliaikaisena korvaajana puutteelliseksi todetulle WEP-salaukselle. (Coleman ym. 2010, 17.)

2.3.5 802.11n

Langattomien lähiverkkojen teknologia on jatkuvassa kehityspaineessa fyysisten dataväylien kyetessä yhä suurempiin siirtonopeuksiin. Vanhojen standardien vakiinnuttua käyttöön IEEE ilmoitti vuonna 2004 aloittaneensa uuden, huippunopean langattoman standardin, IEEE 802.11n:n kehittämisen ja pääominaisuudet uuden standardin ominaisuuksille vahvistettiin vuonna 2006. Tämä antoi laitevalmistajille aikaa suunnitella ja valmistaa verkkolaitteita markkinoille, kun standardi julkaistiin virallisesti vuonna 2009. (Poole, 7.)

802.11n tarjoaa jopa 600 Mb/s siirtonopeuden ja valmiuden toimia sekä 2,4 GHz:n, että 5 GHz:n taajuusalueilla. Standardi mahdollisti perinteisen 20 MHz:n käyttämisen lisäksi myös kahden vastaavan kaistanleveyden hyödyntämisen. Tämä tarkoittaa sitä, että muilla osa-alueilla samalla tavalla konfiguroitu laite kykenee teoriassa kaksinkertaiseen tiedonsiirtonopeuteen, kun kaistanleveys kaksinkertaistuu. Käytännössä 40 MHz:n kaistanleveyttä käytettiin lähinnä vain 5 GHz:n taajuusalueella 2,4 GHz:n alueen ruuhkaisuuden takia. (Poole, 7.)

Toinen 802.11n-standardin tiedonsiirtonopeutta merkittävästi kasvattanut kehitysaskel on MIMO-teknologian hyödyntäminen. MIMO eli Multiple-Input Multiple-Output -teknologia mahdollistaa monitie-etenemisen ja useiden antennien hyödyntämisen tiedonsiirrossa. Teoriassa tämä tarkoittaa tiedonsiirtonopeuden kaksinkertaistumista antennien määrän kaksinkertaistuessa, mutta käytännön hyödyt jäävät heikommiksi. Järjestelmän kyky hyödyntää MIMO-teknologiaa voidaan esittää lauseella a x b : c, missä a on lähettäjän antennien määrä, b on vastaanottajan antennien määrä ja c on yhtäaikaisten datavirtojen maksimimäärä. 802.11n-standardi mahdollistaa jopa neljän yhtäaikaisen datavirran hyödyntämisen, joten tämä maksimi voidaan ilmoittaa edellä olevan kaavan mukaisesti muodossa 4 x 4 : 4. MIMO:n yhteydessä otettiin huomioon myös verkkolaitteiden tehonkulutuksen optimoiminen, sillä jatkuvasti aktiivinen MIMO-järjestelmä nostaa järjestelmän tehoa. Koska tietoliikenne on luonteeltaan purskeista (burst), MIMO-piiri suunniteltiin siten, että se pyritään pitämään lepotilassa, kun sille ei ole tarvetta. (Poole, 7.)

Kuten edeltäjänsä 802.11g, 802.11n on taaksepäin yhteensopiva vanhojen standardien kanssa. Standardiin määritettiin kolme yhteensopivuustilaa:

- yhteensopivuus 802.11a, 802.11b ja 802.11g -standardien kanssa
- yhteensopivuus 802.11a, 802.11b, 802.11g ja 802.11n -standardien kanssa
- vain 802.11n

Viimeisessä yhteensopivuustilassa, eli niin sanotussa Greenfield-tilassa kaikki 802.11n-standardia edeltävä liikenne näyttäytyy tukiasemalle pelkkänä kohinana ja useampien yhteensopivuustilojen käyttäminen päällekkäisillä kantoalueilla voi aiheuttaa ongelmia niin Greenfield-tilassa toimiville laitteille kuin muillekin verkon tukiasemille. (Summit Data 2012).

2.3.6 802.11ac

802.11-perheen siirtonopeus ylitti gigabitin (Gb/s) rajan vuonna 2013, kun 802.11ac julkaistiin. Se käyttää 5 GHz:n taajuusaluetta ja 80 MHz:n kaistanleveyttä, joka on mahdollista laajentaa vielä 160 MHz:iin asti ja sen teoreettinen maksimisiirtonopeus on peräti 6,93 Gb/s. Standardissa vietiin 802.11n-versiossa käyttöön otettu MIMO-teknologia pidemmälle laajentaen sitä niin, että lomittaisia datavirtoja voitiin suunnata useammalle käyttäjälle yhtä aikaa. Tällaista järjestelmää kutsutaan MU-MIMO:ksi (Multi-User MIMO). Tämän lisäksi samanaikaisten yhteyksien määrää kasvatettiin edellisen standardin neljästä kahdeksaan asti. Muita 802.11ac:n merkittäviä ominaisuuksia ovat edeltäjänsä tavoin laaja taaksepäin yhteensopivuus, kaistanleveyden automaattinen säätäminen spektrin ruuhkaisuuden mukaan sekä tehokkaampi virheenkorjaus. (Poole, 8.)

2.3.7 802.11ax

Vielä julkaisematon 802.11ax keskittyy toimimaan tehokkaammin ruuhkaisilla alueilla vähentäen eri tukiasemien toisilleen aiheuttamaa häiriötä. Se tulee toimimaan sekä 2,4 GHz:n taajuusalueella sekä 5 GHz:n alueella ja se tulee käyttämään yhtä tehokkaammin edellisissä standardeissa käytettyä MIMO-teknologiaa. Sen odotetaan tuovan mukanaan edeltäjäänsä nähden huomattavasti parantuneen spektritehokkuuden MIMO-OFDMA:n muodossa. Lopullisen standardin julkaisun odotetaan tapahtuvan aikaisin vuonna 2019. (Poole, 12.)

3 TIETOTURVA

Langattoman lähiverkon tietoturvallisuuden huomioon ottaminen on erittäin tärkeää, sillä kaikki liikenne kulkee ilmassa sähkömagneettisena säteilynä. Langattoman liikenteen perusluonne siis altistaa siirrettävän datan haavoittuvuuksille, joiden hyödyntäminen on paljon helpompaa, kuin fyysisissä verkoissa. Kaiken tietoturvan kolme peruspilaria pätevät myös WLAN-liikenteelle:

- luottamuksellisuus: tiedot ovat vain niiden tahojen käytettävissä, joilla on oikeus tietojen näkemiseen
- eheys: tieto ei muutu tai tuhoudu siirron aikana
- saatavuus: palveluiden tai tietojen tulisi olla saatavilla, kun niille on tarvetta

Langattoman lähiverkon salauksen täytyy turvata jokainen perusperiaate, jotta verkossa voidaan kommunikoida turvallisesti. Alkuperäisen 802.11-standardin WEP-salaus oli haavoittuva, eikä verkon tietoturvan taso ollut luotettava. WPA- ja WPA2-luokitukset ovat parantaneet salauksen vahvuutta huomattavasti ja onkin aina suositeltavaa käyttää vahvinta mahdollista salaustekniikkaa niin kotona, kuin oppilaitoksissa ja työpaikoillakin. (Coleman ym. 2010, 16-18.)

3.1 WEP

WEP (Wired Equivalent Privacy) on IEEE:n standardissa IEEE 802.11 määritetty salausjärjestelmä. Nimensä mukaisesti sen on tarkoitus tarjota langattoman verkon päätelaitteen ja tukiaseman välille tietoturvallisuuden taso, joka on vertailukelpoinen vastaavalla topologialla rakennetun langallisen verkkoyhteyden kanssa. WEP-suojattu yhteys estää luvattoman pääsyn verkkoon ja suojaa yhteyttä ulkopuoliselta kuuntelulta. WEP ei kuitenkaan ole turvallinen salauksen taso ja se onkin korvautunut WPA- ja edelleen WPA2-luokituksilla. (Ross 2008, 219.)

3.1.1 Autentikointi ja salaus

WEP-yhteyden autentikoiminen ja verkkoliikenteen salauksen takaaminen perustuvat jaettuun salausavaimeen (Shared Key), jota verkon päätelaitteet käyttävät yhdistyessään tukiasemaan. Langattomassa verkossa lähetettävät datapaketit suojataan käyttäen tätä salausavainta ja vastaanotetuille paketeille suoritetaan eheystarkistus, jotta voidaan varmistaa, ettei lähetetty tieto ole muuttunut matkan aikana. (Ross 2008, 219.) WEP-suojattuun verkkoon liittymisen autentikointi tapahtuu neljässä vaiheessa:

1. Päätelaite lähettää autentikointipyynnön tukiasemalle
2. Tukiasema lähettää vastauksena *selväkielisen* haasteen
3. Päätelaite salaa vastaanottamansa haastetekstin kyseisessä verkossa käytetyn avaimen avulla ja lähettää sen tukiasemalle uutena autentikointipyyntönä
4. Tukiasema purkaa salatun viestin käyttäen paikallisesti asetettua avainta. Tukiasema vertaa alkuperäistä lähettämäänsä haastetta ja uutta, purettua viestiä. Jos viestit ovat samat, voi tukiasema autentikoida päätelaitteen ja päätelaite yhdistää verkkoon. (Jacobs 2008.)

WEP-salaus käyttää RC4-salausalgoritmia, joka on Ronald Rivestin vuonna 1987 kehittämä salaaja. RC4-algoritmilla oli muitakin käyttökohteita, mutta merkittävin käyttökohde oli sen integroituminen WEP-salaukseen. (TechTarget.) WEP-salauksessa voidaan käyttää kahta eri salausavaimen pituutta, 64-bittistä tai 128-bittistä (Ross 2008, 219-220). Kumpaankin salausavaimeen sisältyy 24-bittinen selkokielisenä lähetettävä alustusvektoriosa (Initialization Vector, IV), joka on laitevalmistajan itse määritettävissä. Alustusvektoriosa ei näin ollen ole määritelty standardissa ja se voidaan generoida esimerkiksi satunnaisuuteen perustuen tai tasaisesti muuttuen. (Jacobs 2008.)

Kummankin salausavaimen lopullinen muoto määräytyy määritetyn salasanan perusteella. Yksi ASCII-merkki on 8 bitin kokoinen, joten 64-bittiseen avaimeen niitä mahtuu viisi kappaletta eli 40 bittiä, kun huomioidaan alustusvektoriosan käyttämät 24 bittiä. Samalla tavalla voidaan laskea 128-bittiseen avaimeen mahtuvan 13 kahdeksan bitin ASCII-merkkiä alustusvektoriosan lisäksi. Käyttäjälle tämä näyttäytyy siten, että tukiasemaan konfiguroitava tai päätelaitteella yhteyden autentikointiin käytettävä salasana on 5 tai 13 ASCII-merkkiä pitkä valitusta salausavaimen pituudesta riippuen. (Ross 2008, 219-221.)

3.1.2 WEPin haavoittuvuus

WEP-salaus oli alusta asti haavoittuva, alkaen jo salasanan pituusrajoituksista. WEP-salauksen 24-bittinen alustusvektori suunniteltiin vahvistamaan salauksen turvallisuutta. Käyttämällä alustusvektoria peräkkäiset paketit salataan eri avaimilla, mikä vaikeuttaa salasanan urkkimista. Alustusvektorin käyttäminen teki kuitenkin WEP-salauksesta luonnostaan haavoittuvan, koska 24-bittinen sana tarkoittaa 2^{24} tai noin 16 miljoonaa mahdollista alustusvektoria, jotka loppuvat aktiivisessa verkossa kesken muutamissa tunneissa. 24-bittinen alustusvektori on lisäksi varsin lyhyt ja se liikkuu radiotiellä selkokielisenä jokaisessa 802.11-paketissa. (Jacobs 2008.)

3.2 WPA ja WPA2

WEP oli todettu haavoittuvaksi salausmenetelmäksi jo vuoteen 2001 mennessä, muutaman vuoden virallisen julkaisunsa jälkeen (University of California, Berkeley). IEEE päätyi siten perustamaan työryhmän, jonka päämääränä oli suunnitella uusi tietoturvataso vanhan 802.11-standardin korvaajaksi. Standardin suunnitteluun ja julkaisuun sekä laitekannan päivittymiseen kuluva aika tuli kuitenkin olemaan varsin pitkä, joten työryhmä joutui ottamaan huomioon myös siirtymäajan. Ennen kuin standardi 802.11i julkaistiin virallisesti vuonna 2004, osia siitä otettiin jo käyttöön siirtymäaikana WEP-salauksen heikkouden takia. Wi-Fi Alliance antoi tälle ”esikatselulle” 802.11i-standardista - joka hyödynsi myös 802.1X-standardin tekniikoita - luokituksen WPA (Wi-Fi Protected Access). Wi-Fi Alliancen WPA2-luokitus on kirjaimellinen tulkinta IEEE 802.11i -standardista ja merkittävin eroavuus WPA-luokitukseen on CCMP-salausprotokollan hyödyntäminen. (Coleman ym. 2010, 88.)

Kummassakin WPA-luokituksessa on mahdollista käyttää koti- ja pientoimistoympäristöihin sopivaa WPA/WPA2 Personal -versiota tai suurempien yritysten käyttöön sopivaa WPA/WPA2 Enterprise -versiota. WPA Personal perustuu jaetun avaimen eli PSK:n (Pre Shared Key) avulla tapahtuvaan autentikointiin ja WPA Enterprise hyödyntää 802.1X/EAP -autentikointia. (Coleman ym. 2010, 18.)

3.2.1 TKIP

Standardissa IEEE 802.11i esitelty TKIP (Temporal Key Integrity Protocol) kehitettiin tietoturvaparannukseksi WEP-salauksen tilalle. TKIP suunniteltiin toimimaan vanhemman laitekannan väliaikaisena tietoturvaparannuksena ennen 802.11i standardissa määriteltyjen parempien tietoturvaominaisuuksien virallista julkaisua ja sen suunniteltu käyttöikä oli noin viisi vuotta. Suurimmalle osasta laitteista TKIP-asennus olikin mahdollista suorittaa yksinkertaisen firmware-päivityksen avulla, mutta joidenkin laitevalmistajien tuotteet eivät olleet yhteensopivia päivityksen kanssa. (Coleman ym. 2010, 75.)

TKIP käyttää salaukseen taustalla samaa RC4-algoritmia, kuin WEP, samalla laajentaen ja parantaen sen ominaisuuksia. TKIP-salauksen keskeisimmät parannukset WEP:iin verrattuna ovat:

- lähetettyjen kehysten sekvensointi
- datan eheyden parantuminen
- vahvemmat salausavaimet

TKIP-suojaus laskee kehys kehykseltä TSC-arvoa (TKIP Sequence Counter) lähettämilleen kehyksille. Kehykset vastaanottava asema pudottaa kaikki vastaanottamansa kehykset, jotka saapuvat väärässä järjestyksessä. Tämä auttaa WEP-salauksen haavoittuvuuteen, missä hyökkääjä saattoi injektoida itse generoimiaan kehyksiä liikenteen sekaan. Datan eheys tarkistetaan MIC:n (Message Integrity Code) avulla. TKIP vahvistaa salausavaimia siten, että kahden aseman välinen salaus tapahtuu kyseisille asemille uniikilla salausavaimella. Varsinainen salausprosessi on esitetty liitteessä 1. (Coleman ym. 2010, 75-77.)

3.2.2 CCMP

CCMP-salausprotokolla (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) on IEEE:n standardissa 802.11i esitelty salausprotokolla, joka suunniteltiin WEP:n ja edelleen TKIP:n korvaajaksi. CCMP on pakollinen ominaisuus

kaikille WPA2-luokituksen saaneille laitteille. Se käyttää AES-salausalgoritmia (Advanced Encryption Standard) ja 128 bittiä pitkiä salausavaimia. Salausprosessi on esitetty liitteessä 2.

4 HYÖKKÄYSTAPOJA

WLAN-liikenteen tietoturva on perusluonteeltaan ongelmallista. Kaikki liikenne kulkee ilmassa radioaaltoina ja parhaimmillakin salaustekniikoilla varjellusta liikenteestä on mahdollista saada jonkin verran informaatiota selville. Potentiaalisen hyökkääjän ei tarvitse välttämättä olla edes rakennuksen sisäpuolella aiheuttaakseen vahinkoa, sillä WLAN-signaalit kuuluvat tyypillisesti myös rakennuksien ulkopuolelle. (Cisco Press, 2015.)

Langattoman lähiverkon tietoturvauhat voidaan luokitella kolmeen pääkategoriaan: liikenteen kuunteluun, verkon luvattomaan käyttöön sekä palvelunestoon. Liikenteen passiivisella kuuntelulla on mahdollista saada verkosta tietoja, mitä voidaan käyttää esimerkiksi palvelunestohyökkäyksen toteuttamiseen. Verkon luvaton käyttö on tyypillinen ja usein tahattomasti syntyvä ongelma, jonka mahdollistajana on useimmiten luvaton langaton tukiasema. Palvelunestohyökkäyksessä ei ole välttämättä tarkoituksena aiheuttaa uhrille muuta kuin yhteyden katkeamisesta aiheutuvaa harmia, mutta palvelunestohyökkäyksen päättyessä radioliikenteestä on kuunneltavissa hyökkääjän kannalta potentiaalisesti hyödyllistä tietoa, kun laitteet pyrkivät jälleen yhdistämään toisiinsa. Nämä kaikki ongelmat liittyvät WLAN-liikenteen parhaimpaan ja haavoittuvimpaan ominaisuuteen – langattomuuteen. Tässä luvussa esitellään periaatteet kustakin hyökkäyskategoriasta. (Cisco Press, 2015.)

4.1 Liikenteen kuunteleminen

Eräs langattoman lähiverkkoliikenteen haavoittuvuus on sen helppo kuunneltavuus radiotiellä. Liikenteen kuuntelemisella tarkoitetaan langattoman lähiverkkoliikenteen yhteydessä paketti- ja protokolla-analysaattorien käyttämistä taajuusalueen 802.11-liikenteen seuraamiseen ja analysointiin. Liikenteen kuuntelun ongelmallisuus piilee sen passiivisuudessa – langattoman verkon murtoja havaitsevat laitteet eivät huomaa passiivista, liikennettä kuuntelevaa laitetta. (Coleman ym. 2010, 300-301.)

Kaikesta langattomasta liikenteestä – salatustakin – voi saada jonkin verran tietoa kuuntelemalla sitä sopivalla laitteistolla. Tukiasemien ja niihin yhdistyneiden päätelaitteiden

MAC-osoitteet kulkevat radiotiellä selkokielisenä ja jo näillä tiedoilla voidaan esimerkiksi toteuttaa deautentikointihyökkäys, jota tarkastellaan lähemmin kappaleessa 4.4.2. Jos liitytään verkkoon, missä ei ole käytössä mitään salaustekniikkaa (esim. julkinen hotspot, kuten kahvilan avoin WLAN) on kaikki liikenne altista salakuuntelulle. Tämä tarkoittaa esimerkiksi sitä, että liikettä kuunteleva taho voi suoraan kaapata esimerkiksi sähköpostiviestejä ja VoIP-puheluita tai seurata käyttäjien verkkosivuvierailuja. (Coleman ym. 2010, 301-302.)

Kuten edellä mainittiin, kaikesta langattomasta lähiverkkoliikenteestä voidaan kalastella jonkin verran tietoja, sillä 802.11-liikenne toimii OSI-mallin kerroksilla 1 ja 2 ja salakuuntelua on mahdotonta estää näillä kerroksilla. Liikenteen kuuntelulta suojautuessa tärkeintä on varmistaa vahvan salausmenetelmän käyttäminen verkossa, jotta ylempien kerroksien dataa ei voida purkaa kuunneltavasta liikenteestä. Nykyaikana tämä tarkoittaa WPA2/AES-suojatun yhteyden käyttämistä. (Coleman ym. 2010, 302-303.)

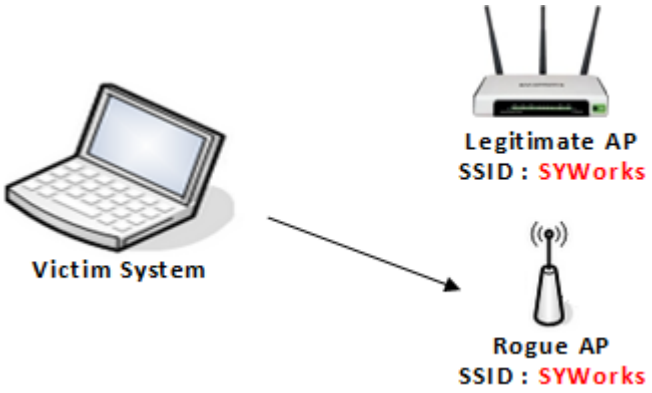
4.2 Rogue Access – luvaton käyttö

Luvattomien laitteiden yhdistäminen verkkoon (Rogue Access) on tapa luoda ikkuna esimerkiksi yrityksen sisäiseen verkkoon ulkopuolisella laitteella, kuten luvattomalla langattomalla tukiasemalla (Rogue Access Point). Luvattomat tukiasemat ovat yksi tyypillisimmistä uhkatekijöistä langattomalle verkkoliikenteelle ja niiden käyttäminen avaa sisäverkon useille haavoittuvuuksille, kuten datavarkauksille, datan tuhoutumiselle ja palvelunestolle. Puutteellisesti valvotussa ja konfiguroidussa ympäristössä hyökkääjän on mahdollista päästä suoraan kiinni sisäverkkoon yksinkertaisella ja halvalla kuluttajaluokan laitteella. Tyypillisin luvaton tukiasema on kuitenkin asennettu ilman aikomustakaan tuottaa harmia tai avata sisäverkkoa ulkopuoliselle tunkeutujalle: yrityksen tai laitoksen työntekijä on tuonut ja ottanut käyttöön oman langattoman tukiaseman tilaan, jossa ei ole ollut langatonta lähiverkkoa. (Juniper Networks.)

4.2.1 Luvattoman käytön uhkatekijät

Äärimmäisimmässä tapauksessa vilpittöminkin perustein asennettu tukiasema avaa tehokkaan hyökkäysvektorin yrityksen tai muun laitoksen sisäverkkoon. Luvattoman tukiaseman asentaja on tavallisesti luotettu, paikallinen käyttäjä tai vierailija. On tyypillistä, että käyttäjät eivät itse tiedä tekevänsä mitään väärää puutteellisen ohjeistuksen ja koulutuksen takia. Toisaalta monet käyttäjät tietävät toimivansa vastoin sääntöjä asentaessaan erillisiä verkkolaitteita, mutta kokevat samalla saamansa hyödyn työskentelyn helpottumisessa tärkeämmäksi, kuin paikallisen IT-tuen tai tietohallinnon kirjalliset ohjeistukset. (Coleman ym. 2010, 293-294.)

Luvattoman tukiaseman käyttäminen mahdollistaa monenlaisen vahingon aiheuttamisen sekä itse verkon turvallisuudelle, että verkon omistavalle yritykselle tai muulle organisaatiolle. Luvaton tukiasema on tehokas väylä esimerkiksi Man-in-the-Middle-hyökkäyksen toteuttamiseen. MitM-hyökkäyksessä ulkoinen osapuoli asettuu verkossa linkiksi käyttäjien välille naamioitumalla luotettavaksi tahoksi. Kuvassa 2 on esitetty tilanne, missä käyttäjä on tietämättään yhdistänyt luvattomaan tukiasemaan, jolla on sama SSID kuin oikealla tukiasemalla. Uhrien välinen kommunikointi on kokonaan hyökkääjän valvottavissa ja hallittavissa. Luvatonta tukiasemaa hyväkseen käyttävä hyökkääjä voi myös toteuttaa palvelunestohyökkäyksen täyttämällä verkon turhalla datalla, jolloin verkon suorituskyky heikkenee merkittävästi. (Juniper Networks.)



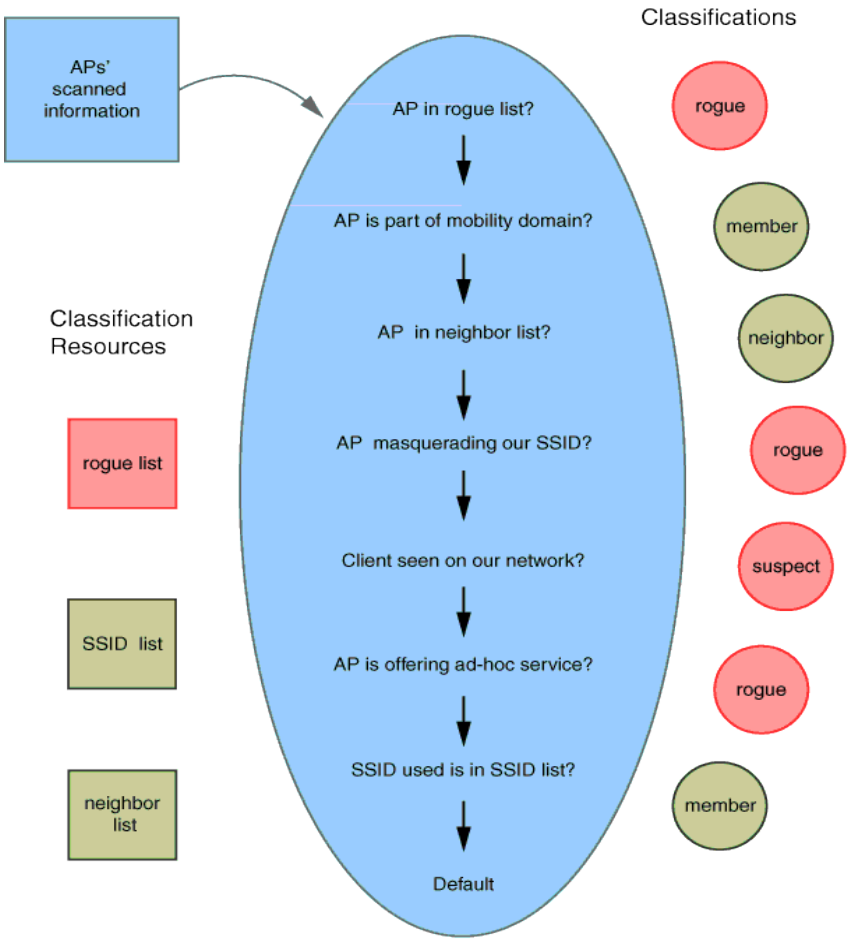
KUVA 2. Käyttäjä on tietämättään yhdistänyt luvattomaan tukiasemaan. (SYWorks)

Yrityksen näkökulmasta pelkkää verkon haavoittuvuutta pahempi tilanne on aste, jossa ulkopuolinen taho on jo päässyt käsiksi paikalliseen verkkoon tallennettuun dataan. Tällaista dataa voivat olla yrityksen liikesalaisuudet, jotka saattavat kattaa tietoja yrityksen

talouteen liittyvistä asioista, yksityiskohtaisia teknisiä tietoja yrityksen tuotteista tai käyttämistä laitteista tai tulevista tai käynnissä olevista projekteista. Lisäksi tunkeutuja voi päästä käsiksi asiakkaiden ja yhteistyötahojen luottamuksellisiin tietoihin. Yksilön kannalta ongelmallisinta on tarkasti yksilöivien ja henkilökohtaisten tietojen, kuten terveystietojen luottamuksellisuuden vaarantuminen. Tietojen varastamisen lisäksi hyökkääjällä on mahdollisuus muokata tai tuhota dataa ja ladata verkkoon haittaohjelmia, joilla voidaan pitkittää haavoittuvuudesta aiheutuneita ongelmia. (Coleman ym. 2010, 295-296.)

4.2.2 Luvattoman tukiaseman tunnistaminen

Luvattoman tukiaseman tunnistamisessa voidaan edetä esimerkiksi vaiheittain. Juniper Networks esittelee kahdeksanasteisen menetelmän verkosta skannatun tukiaseman luokitteluun (kuva 3). Tämän vaiheittain etenevän seulonnan perusteella voidaan päätellä, onko verkkoon kytketty tukiasema verkon jäsen, naapuri, epäilty luvaton laite vai varma luvaton laite. Luvattomaksi laitteeksi luokitteluun voi johtaa positiivinen vastaus kysymyksiin ”Onko tukiasema naamioitunut luotetuksi laitteeksi SSID:n avulla?” tai ”Tarjoaako laite ad hoc -yhteyksiä?”.



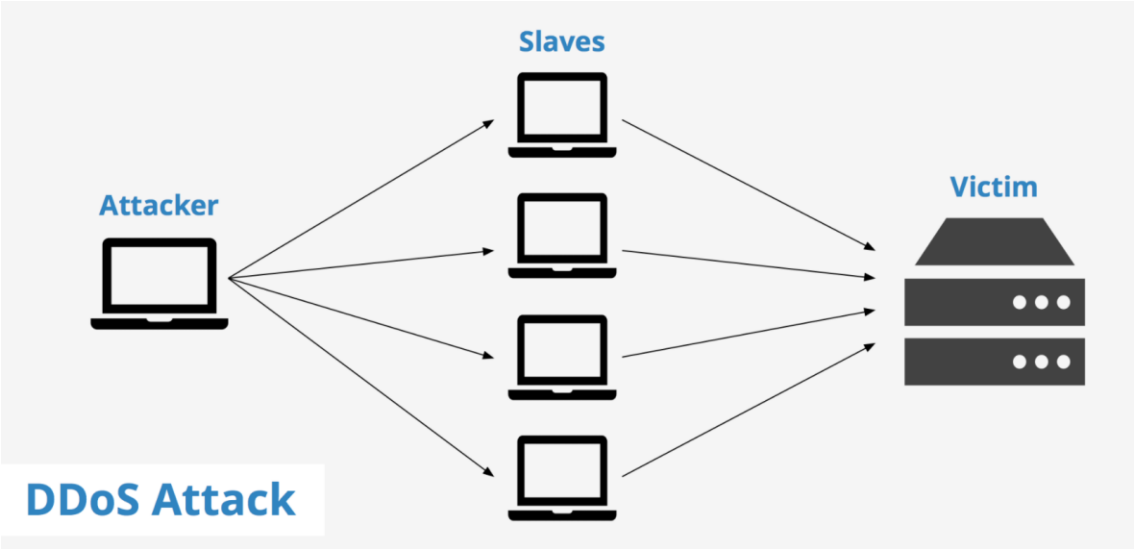
KUVA 3. Tukiaseman vaiheittainen luokittelu. (Juniper Networks)

4.3 Palvelunestohyökkäys

Palvelunestohyökkäys, eli DoS-hyökkäys (Denial of Service) on hyökkäystapa, jossa ulkopuolisen tahon tavoitteena on lamauttaa jokin verkko tai laite, jolloin sen tavanomainen käyttö vaikeutuu tai on kokonaan mahdotonta. Palvelunestohyökkäyksessä laitteelle tai verkolle lähetetään tavallisesti niin paljon turhaa liikennettä, että se ei kykene enää vastaamaan normaalisti sitä käyttävien tahojen yhteyksiin, kuten esimerkiksi verkkosivun vierailijoiden tai yrityksen sähköpostipalvelinta käyttävien työntekijöiden pyyntöihin. Tietojen varastamisen tai tuhoamisen sijaan palvelunestohyökkäyksessä pyritään tyypillisesti mahdollisimman suuren huomion saavuttamiseen kaatamalla esimerkiksi suosittuja internetsivuja. (Cloudflare.)

4.3.1 Keskitetty palvelunestohyökkäys

Keskitetyssä palvelunestohyökkäyksessä (DDoS, Distributed Denial of Service) hyökkääjä käyttää yhtä aikaa useita laitteita palvelunestohyökkäyksen toteuttamiseen (kuva 4). Tällaista saastuneiden laitteiden verkostoa kutsutaan botnetiksi ja yksittäistä laitetta zombiksi (eng. zombie). (Cloudflare.)



KUVA 4. DDoS-hyökkäys. (KeyCDN)

4.3.2 Langattoman verkon palvelunestohyökkäys

Erityisesti langattomaan verkkoon kohdistuvia palvelunestohyökkäyksiä on myös mahdollista toteuttaa. Nämä hyökkäykset keskittyvät varsinaisen WLAN-signaalin häirintään sekä tukiaseman ja langattomaan verkkoon liittyvän laitteen välille ja niiden toteutus perustuu OSI-mallin kerrosten 1 ja 2 heikkouksien hyväksikäyttämiseen. Langattoman lähiverkon palvelunestolta ei ole helppo suojautua ja tämä haavoittuvuus onkin keskeinen näkökulma verkon rakennetta suunniteltaessa: tärkein liikenne olisi pidettävä langallisena. (Coleman ym. 2010, 305-306, 310.)

Yksinkertaisin hyökkäys kohdistuu langattoman verkon kulkuun radiotiellä – tietyllä taajuusalueella kulkevaa langattoman verkon signaalia voidaan yksinkertaisesti häiritä

muilla signaalilähteillä. On mahdollista, että esimerkiksi 2,4 GHz:n taajuusalueella suurella teholla lähettävä laite häiritsee tahattomasti langatonta verkkoa, mutta hyökkääjän on myös helppo käyttää samaa haavoittuvuutta hyväkseen. Langattomassa verkossa liikennettä vastaanottavalle laitteelle signaalitaso -60 dBm on jo niin hyvä, että sitä voidaan pitää yhteyden kannalta luotettavana. Kuvan 5 signaalijammerin lähetysteho on noin 10-13 W, mikä tarkoittaa noin 40 dBm lähetystehoa. (Coleman ym. 2010, 306.)

KUVA 5. SPEC5-signaalijammeri. (Jammer-Store)

Tällaisella teholla toimiva signaalijammeri nostaa taajuusalueen kohinatasoa jo niin paljon, että WLAN-liikenne hukkuu siihen kokonaan ja kommunikointi verkon laitteiden välillä on mahdotonta. Päätelaitteen ja tukiaseman välille muodostuneen yhteyden häiritseminen tällä tavalla avaa WLAN-yhteyden muille uhkakuville: häirinnän loppuessa laitteet aloittavat autentikointiprosessin yhteyden uudelleenmuodostamiseksi ja hyökkääjä voi kuunnella tätä liikennettä. (Coleman ym. 2010, 310.)

Eräässä hienostuneemmassa hyökkäyksessä pyritään äkkinäisesti katkaisemaan päätelaitteen tai päätelaitteiden yhteys tukiasemaan. Tällaiselta deauthentication-hyökkäykseltä on vaikea suojautua ja se on helppo toteuttaa vaatimattomallakin laitteistolla. Hyökkäyksen voi toteuttaa esimerkiksi Aircrack-ng penetraatiotestauspaketilla, joka toimii useilla käyttöjärjestelmillä. Kuvassa 6 on esitetty komentoriville kirjoitettavassa muodossa deautentikointikomento, joka katkaisee päätelaitteen yhteyden tukiasemaan. Parametri -0 ker-

too kyseessä olevan deautentikointi, jonka jälkeen luku 1 kertoo lähetettävien deautentikointiviestien määrän. Parametri -a on tukiaseman MAC-osoite ja parametri -c hyökkäyksen kohteena olevan laitteen MAC-osoite. Hyökkääjä voi deautentikoida kaikki tukiasemaan liittyneet päätelaitteet jättämällä -c-parametrin pois komennosta. Viimeinen parametri ath0 kertoo paikallisen verkkosovittimen nimen. (Aircrack-ng.)

```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 ath0
```

KUVA 6. Deautentikointikomento Aircrack-ng:ssä. (Aircrack-ng)

Deautentikointihyökkäys on uhrin kannalta ongelmallinen, sillä deautentikointiviesti ei ole pyyntö, vaan kehoite, jonka päätelaite suorittaa heti käskyn saatuaan (Coleman ym. 2010, 311).

5 POHDINTA

Langattomasta viestinnästä on tullut keskeinen osa arkeamme. Käytämme langattomia verkkoyhteyksiä päivittäin huviin ja hyötyyn ja tilannetta ilman nykyistä langatonta infrastruktuuria on vaikea enää edes kuvitella. Lähes kaikilla on nykyään mukanaan datansiirtoliittymällä varustettu älypuhelin ja perinteiset, yhteen paikkaan sidotut pöytäkoneet ovat vaihtuneet kannettaviin tietokoneisiin ja tabletteihin. Nykyaikainen tietotekniikan käyttäjä arvostaa vaivattomuutta ja liikuteltavuutta – yhteyksien tulisi toimia juuri siellä missä niitä kulloinkin tarvitaan.

IEEE:n standardi 802.11 vakiinnutti asemansa aikaisin langattoman lähiverkkoliikenteen ykkösstandardiksi, eikä tämä asema ole lähitulevaisuudessa horjumassa. Alkuperäisen standardin vaatimattomat siirtonopeudet ovat kehittyneet sille tasolle, että voidaan puhua jo gigabiteistä sekunnissa. Samalla kun fyysiset tiedonsiirtomenetelmät kehittyvät yhä pidemmälle, pyrkii WLAN-liikennekin saavuttamaan yhä korkeampia tiedonsiirtonopeuksia. Tämän lisäksi tuotamme jatkuvasti enemmän dataa tiedonsiirtoväylille, kun kotimme laitteet alkavat hiljalleen yhä enemmän olla yhteydessä internetiin IoT:n yleistyessä. Langaton lähiverkkoliikenne on tämän kehityksen keskiössä, kun tavanomaisten verkkoon liittyvien laitteiden lisäksi esimerkiksi perinteisemmät kodinkoneet kommunikoivat langattomasti.

WLAN-teknologian langattomuus tuo mukanaan samalla sen parhaimmat, mutta myös heikoimmat puolet, sillä ilmassa liikkuva signaali on aina altis häiriöille ja jossain määrin myös ulkopuoliselle urkinnalle. Langattoman lähiverkkoliikenteen salauksen tasoa voidaan kuitenkin pitää nykyään hyvänä, kunhan käytössä on parhaimmat mahdolliset salaustekniikat. Vuoden 2018 aikana on vielä tulossa lisätietoa Wi-Fi Alliancen suunnitteilla olevasta WPA3-luokituksesta, jonka odotetaan parantavan WPA2-luokituksen ominaisuuksia ja lisäksi tuovan uutta turvaa esimerkiksi avoimien verkkojen käyttöön. Samoin kuin varsinainen tiedonsiirron nopeus, on tietoturvakin jatkuvan kehitystyön alaisena yhä useamman laitteen ollessa yhteydessä internetiin.

LÄHTEET

Aircrack-ng. Deauthentication. Luettu 26.4.2018.
http://www.aircrack-ng.org/doku.php?id=deauthentication

Cisco Press. Wireless LAN Implications, Problems and Solutions. Luettu 30.4.2018.
http://www.ciscopress.com/articles/article.asp?p=2351131

Cloudflare. What is a DDoS Attack?. Luettu 25.4.2018.
https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Coleman, D., Westcott, D., Harkins, B., Jackman, S. 2010. CWSP: Certified Wireless Security Professional Official Study Guide. Indianapolis, Indiana: Wiley Publishing, Inc.

IEEE. 802.11-2016 - IEEE Standard for Information technology. Luettu 6.5.2018.
https://ieeexplore.ieee.org/document/7786995/

IEEE. IEEE at a Glance. Luettu 30.4.2018.
https://www.ieee.org/about/today/at-a-glance.html?WT.mc_id=lp_ab_iaa

Jacobs, D. 2008. Wireless security – How WEP encryption works. TechTarget. Luettu 9.4.2018.
https://searchnetworking.techtarget.com/tip/Wireless-security-How-WEP-encryption-works

Jammer-Store. SPEC5 Desktop 2.4GHz, 5 GHz WIFI jammer. Luettu 24.4.2018.
https://www.jammer-store.com/spec5-5ghz-wifi-jammer.html

Juniper Networks. Understanding Rogue Access Points. Luettu 9.4.2018.
https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.1/topics/concept/wireless-rogue-ap.html

KeyCDN. DDoS Attack. Luettu 24.4.2018.
https://www.keycdn.com/support/ddos-attack/

Poole, I. IEEE 802.11 Wi-Fi Standards. Radio-Electronics.com. Luettu 9.4.2018.
http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php

Ross, J. 2008. The Book of Wireless: A Painless Guide to Wi-Fi and Broadband Wireless. Toinen painos. San Francisco: No Starch Press.

Summit Data. 2012. Wi-Fi® and Greenfield Mode Functionality. Luettu 10.4.2018.
http://www.summitdata.com/blog/wi-fi-and-greenfield-mode-functionality/

SYWorks Programming. Wireless IDS [Intrusion Detection System] - Tutorial / Explaination. Luettu 30.4.2018.
http://syworks.blogspot.fi/2014/01/wireless-ids-intrusion-detection-system.html

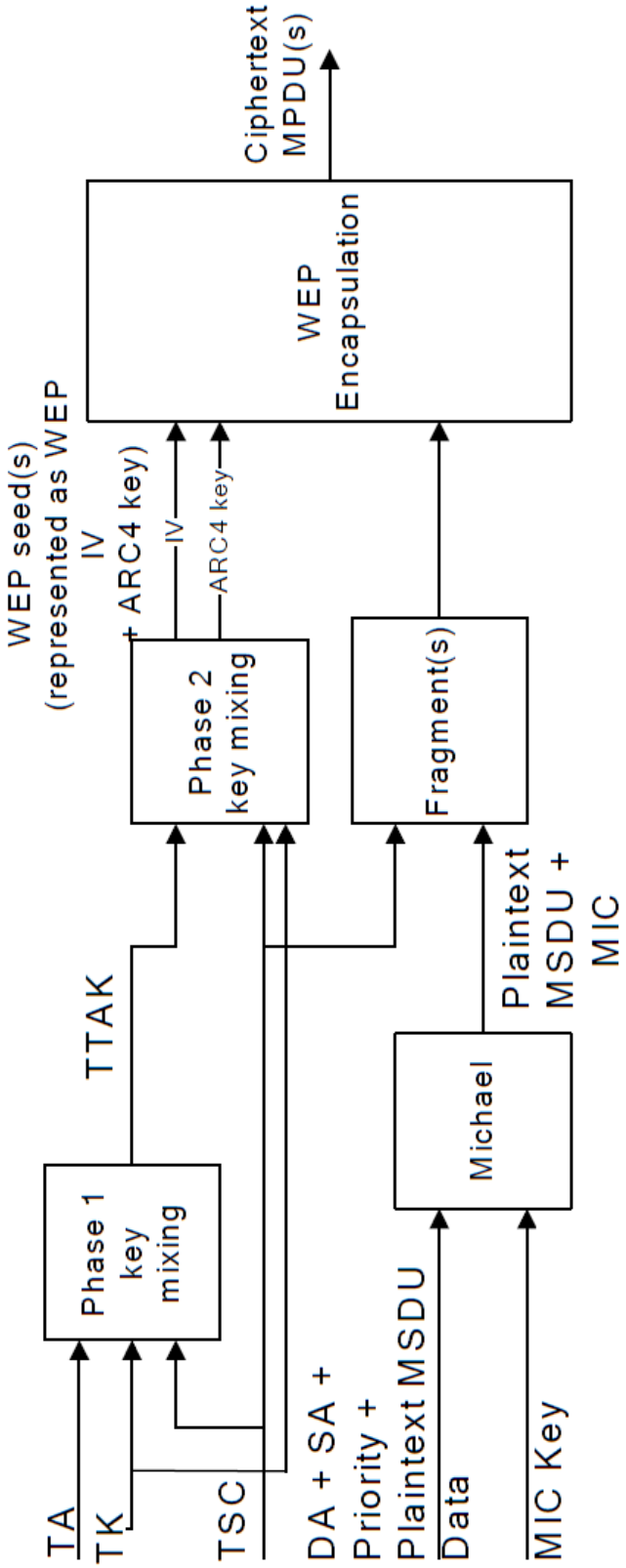
TechTarget. What is RC4?. Luettu 9.4.2018.
https://searchsecurity.techtarget.com/answer/What-is-RC4

University of California, Berkeley. Security of the WEP algorithm. Luettu 9.4.2018. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Wi-Fi Alliance. Certification. Luettu 30.4.2018. https://www.wi-fi.org/certification

LIITTEET

Liite 1. TKIP-salaus (IEEE 2016, 1954)



Liite 2. CCMP-salaus (IEEE 2016, 1969)