

TEKNILLINEN KORKEAKOULU  
Informaatio- ja luonnontieteiden tiedekunta  
Tietotekniikan tutkinto-ohjelma

# LANGATTOMAT LÄHIVERKOT

## Turvaratkaisut

### Kandidaatintyö

## Toni Sallanmaa

Tietoliikenneohjelmistojen ja Multimedian Laboratorio  
Espoo 2008

<b>Tekijä:</b>	Toni Sallanmaa	
<b>Työn nimi:</b>	Langattomat lähiverkot – Turvaratkaisut	
<b>Päiväys:</b>	08. lokakuuta 2008	<b>Sivumäärä:</b> 12 + 27
<b>Pääaine:</b>	Tietoliikenneohjelmistot	<b>Koodi:</b>
<b>Vastuopettaja:</b>	prof. Lauri Savioja	
<b>Työn ohjaaja:</b>	TkL Timo Kiravuo	
<p>Langattomat verkot toimivat radioaalloilla ja koostuvat yhdestä tai useammasta tukiasemasta ja niihin liittyneistä asiakkaista. Lisäksi verkkoon voi kuulua tunnistautumispalvelin, jolle asiakkaat tunnistautuvat. Verkossa on tarpeen suojata verkkoon liittyminen sekä verkossa siirrettävä tietoliikenne. Tämän työn tarkoitus on esitellä menetelmät WLAN-verkon suojaamiseen verkkotasolla ja tutkia niiden toimivuutta erilaisissa esimerkkiympäristöissä.</p> <p>Esitellyistä menetelmistä salattu verkon SSID-nimi, staattisten IP-osoitteiden käyttö sekä MAC-suodatus havaittiin tietoturvaltaan puutteellisiksi ja helposti rikottaviksi. WEP havaittiin huonosti rakennetuksi ja sille löydettiin hyökkäyksiä, joilla verkon salasana voidaan selvittää nopeasti. WPA ja WPA2 huomattiin tehokkaiksi suojautumismenetelmiksi, joita suositeltiin useisiin käyttökohteisiin. Lisäksi käsiteltiin HTTP-todennusta, joka todettiin hyväksi ratkaisuksi, mutta vain tietyissä olosuhteissa.</p> <p>Käyttötapauksissa suojaustekniikkoita tarkasteltiin yleisten esimerkkiympäristöjen näkökulmasta. Kotikäyttöön suositeltiin käytettäväksi WPA-suojausta, mikäli ei ole pakottavaa syytä käyttää WEP-suojausta. Yrityksissä käsiteltiin kolmea esimerkkiä, joista pienyritykselle suositeltiin WPA-suojausta, keskisuurelle IT-yritykselle WPA-suojausta sekä pankille WPA2-suojausta tunnistautumispalvelimen kanssa. Kahviloille suositeltiin WPA-suojausta tai HTTP-todennusta.</p>		
<b>Avainsanat:</b>	wlan, tietoturva, wep, wpa	
<b>Kieli:</b>	Suomi	

TEKNISKA HÖGSKOLAN

SAMMANDRAG AV

Fakulteten för informations- och naturvetenskaper KANDIDATARBETET

Examensprogrammet för datateknik

<b>Utfört av:</b>	Toni Sallanmaa	
<b>Arbetets namn:</b>	Langattomat lähiverkot – Turvaratkaisut	
<b>Datum:</b>	08. lokakuuta 2008	<b>Sidoantal:</b> 12 + 27
<b>Huvudämne:</b>	Tietoliikenneohjelmistot	<b>Kod:</b>
<b>Övervakare:</b>	prof. Lauri Savioja	
<b>Handledare:</b>	TkL Timo Kiravuo	
<b>Nyckelord:</b>	wlan, tietoturva, wep, wpa	
<b>Språk:</b>	Svenska	

HELSINKI UNIVERSITY OF  
TECHNOLOGY

Faculty of Information and Natural Sciences  
Degree Program of Computer Science and Engineering

ABSTRACT OF  
BACHELOR'S THESIS

<b>Author:</b>	Toni Sallanmaa	
<b>Title of thesis:</b>		
<b>Date:</b>	October 10 2008	<b>Pages:</b> 12 + 27
<b>Professorship:</b>	Tietoliikenneohjelmistot	<b>Code:</b>
<b>Supervisor:</b>	Professor Lauri Savioja	
<b>Instructor:</b>	Timo Kiravuo, Lic. Sc. (Tech)	
<b>Keywords:</b>	wlan, security, wep, wpa	
<b>Language:</b>	Finnish	



# Käytetyt lyhenteet

802.3	IEEE 802.3, Ethernet-verkkostandardi
802.11	IEEE 802.11, WLAN-standardi
AP	Access Point, tukiasema verkolle
AAA	Authentication, Authorization, Accounting; Tunnistus, todennus ja kirjanpito
AAD	Additional Authentication Data, lisätodennusdata
BSA	Basic Service Area, Peruspalvelualue
BSS	Basic Service Set, Peruspalvelujoukko
DoS	Denial of Service, Palvelunestohyökkäys
EAP	Extensible Authentication Protocol, raami tunnistusprotokollille
ESS	Extended Service Set, Jatkettu palvelujoukko
IP	Internet Protocol, Internet-protokolla
IPSec	IP Security Architecture, IP:n suojausarkkitehtuuri
MAC	Media Access Control, Median käyttökontrolli
MIC	Message Integrity Code, Viestin eheyskoodi
PSK	Pre-Shared Key, Esijaettu avain
RADIUS	AAA-palvelin ja -protokolla
RSN	Robust Security Network, 802.11i -mukainen verkko
RSNA	Robust Security Network Association
SSID	Service Set Identifier, Verkon nimi
VPN	Virtual Private Network, virtuaalinen lähiverkko
WEP	Wired Equivalent Privacy, Langallista verkkoa vastaava tietoturva
WLAN	IEEE 802.11 Wireless Local Area Network, Langaton lähiverkko
WNIC	Wireless Network Interface Card, Langaton verkkokortti
WPA	Wi-Fi Protected Access

# Sisältö

<b>Käytetyt lyhenteet</b>	<b>iv</b>
<b>1 Johdanto</b>	<b>1</b>
<b>2 WLAN-verkkojen tietoturvaratkaisut</b>	<b>3</b>
2.1 Langattoman tietoturvan perusteet . . . . .	3
2.2 MAC-suodatus . . . . .	4
2.3 Salainen nimi ja staattinen IP-osoite . . . . .	6
2.4 Wired Equivalent Privacy . . . . .	6
2.5 802.1X . . . . .	8
2.6 Wi-Fi Protected Access . . . . .	10
2.6.1 Versio 1 . . . . .	11
2.6.2 Versio 2 . . . . .	12
2.7 HTTP-todennus . . . . .	13
2.8 Yhteenveto . . . . .	15
<b>3 Johtopäätökset</b>	<b>17</b>
3.1 Yleistä käyttötapauksista . . . . .	17
3.2 Kotikäyttö . . . . .	18
3.3 Yrityskäyttö . . . . .	19
3.3.1 Pieni yritys, muu kuin IT-toimiala . . . . .	19
3.3.2 Pieni tai keskisuuri IT-yritys . . . . .	20
3.3.3 Pankki . . . . .	21

3.4 Kahvilat . . . . .	22
<b>4 Yhteenveto</b>	<b>24</b>
<b>Kirjallisuutta</b>	<b>26</b>

# Luku 1

## Johdanto

Tässä luvussa on katsaus langattomien verkkojen ja niiden tietoturvaratkaisuiden perusteisiin. Seuraava luku sisältää valittujen menetelmien tarkastelun. Lopuksi valittuja menetelmiä vertaillaan eri käyttötarkoituksissa.

Langattomat lähiverkot (Wireless Local Area Networks, WLAN) ovat tapa yhdistää laitteita toisiinsa käyttäen radioaaltoja. Laitteen tulee sisältää verkon käyttämää tekniikkaa ja salausta tukeva langaton verkkokortti (Wireless Network Interface Card, WNIC). Tässä työssä asiakkaalla (client) tarkoitetaan laitetta, joka käyttää muita laitteita saadakseen palveluita tuottamatta itse niitä muille.

Kaikkia langattomien verkkojen kanssa toimivia laitteita kutsutaan asemiksi (Station). Laitteita, joihin asiakkaat ottavat yhteyden WLAN-verkkoa hyödyntäen, kutsutaan tukiasemiksi (Access Point, AP). Joukko synkronoituja asemia muodostaa yhdessä langattoman verkon peruspalvelujoukon (Basic Service Set, BSS). Joukon kattama alue muodostaa yhden peruspalvelualueen (Basic Service Area, BSA) ja useampi joukko yhdistelemällä saadaan jatkettu palvelujoukko (Extended Service Set, ESS). Verkkoja on mahdollista luoda myös ilman erityistä tukiasemaa jolloin tuloksena on Ad Hoc -verkko (Ad Hoc -network). Tällaisessä verkossa jokainen asema toimii sekä tukiasemana että asiakkaana. (IEEE 802.11 Working Group, 2007).

Verkot erotetaan toisistaan niiden palvelualueenimen (engl. Service Set Identifier, SSID) perusteella. Eri verkot myös useasti käyttävät eri kanavia välttääkseen taajuusalueen ylikuormituksesta johtuvat ongelmat. Tukiasema yleensä mainostaa lähialueelle verkkoa omalla SSID-nimellään, jotta alueella kuuntelevat asiakkaat löytäisivät sen. Lisäksi mainosviestissä lähetetään informaatiota esimerkiksi siitä onko verkko salattu. (IEEE 802.11 Working Group, 2007).

Kaikki WLAN-verkkoja hyödyntävät laitteet käyttävät 802.3 Ethernet -verkkokorttien

tavoin MAC-koodeja (Medianhallinnointikoodi, engl. Media Access Control) tunnistautumiseen. Tämä koodi on jokaiselle laitteelle uniikki ja koostuu laitteen valmistajan staattisesta osasta sekä laitekohtaisesta tunnisteesta. Langattomat verkot yleisesti käyttävät myös DHCP-protokollaa (Automaattinen asetusmäärittäminen, engl. Dynamic Host Configuration Protocol) tarvittavien asetusten välittämiseen asiakkaille. Nämä tiedot sisältävät reititysinformaatiota sekä esimerkiksi IP-osoitteen.

Verkkotasolla WLAN eroaa 802.3 Ethernet lähiverkosta usealla tavalla. Ensiksi siirtomedia on paljon epäluotettavampi kuin johtoa käytettäessä ja pakettien katoaminen huomattavasti todennäköisempää. Toiseksi yksi verkko ei voi varata koko mediaa, vaan se voidaan joutua jakamaan muiden verkkojen kanssa. Kolmanneksi langattomuus tuo dynaamisuutta verkkoon ja asiakas voi siirtyä verkon sisällä. Tämän takia langattomissa lähiverkoissa viestittäessä ei osoiteta paketteja suoraan asiakkaille vaan tämän käyttämään tukiasemaan. (IEEE 802.11 Working Group, 2007).

IEEE 802.11 Working Group säätelee ja standardisoi WLAN-tekniikkaa ja toistaiseksi standardista on 9 eri versiota. Taulukko 1.1 vertailee yleisempien standardien tärkeimpiä ominaisuuksia.

Taulukko 1.1: Osa langattomien lähiverkkojen standardeista. (IEEE 802.11 Working Group, 2007), (Wi-Fi Alliance, 2008)

Standardi	Julkaisuvuosi	Taajuus	Nopeus
802.11	1997	2.4 GHz	2 Mbps
802.11b	1999	2.4 GHz	11 Mbps
802.11g	2003	2.4 GHz	54 Mbps
802.11n	2008	2.4 GHz ja 5 GHz	248 Mbps

Maksimaalisen lähetysnopeuden nostaminen oli ensin pääasiallisena tavoitteena, mutta 802.11g-standardin julkistamisen jälkeen painotus on siirtynyt entistä enemmän kantomatkan lisäämiseen. Yleisesti standardit eivät ole yhteensopivia keskenään, mutta toteutukset tukevat useampaa kuin yhtä standardia.

Työn tarkoitus on eritellä sekä analysoida nykyään käytössä olevia langattomien verkkojen suojausmenetelmiä sekä pohtia niiden soveltuvuutta eri tilanteisiin. Työ rajautuu erityisesti niihin menetelmiin, joille on valmiita kaupallisia toteutuksia. Lisäksi uusia, mutta vasta kehitystasolla olevia tekniikoita sivutaan.

## Luku 2

# WLAN-verkkojen tietoturvaratkaisut

Tässä luvussa tutustaan ensin langattomien verkkojen tietoturvaan yleisesti, jonka jälkeen käydään läpi laajalti käytössä olevia turvamenetelmiä.

### 2.1 Langattoman tietoturvan perusteet

Langattomat WLAN-verkot aiheuttavat huomattavasti enemmän tietoturvaongelmia kuin perinteiset IEEE 802.3-standardin mukaiset Ethernet-lähiverkot. Langattomasta verkosta puuttuu fyysisen kaapelin tuoma turva, koska siirtomedia leviää tukiaseman kantoalueelle eikä sitä voida hallita. WLAN-verkkojen liikennettä on siis huomattavasti helpompi vastaanottaa ja lähettää luvatta, kuin Ethernet-verkon liikennettä. (Cam-Winget et al., 2003).

Verkon turvattomuudesta nousevia uhkia varten IEEE 802.11 Working Group (2007) määrittelee kaksi eri luokkaa algoritmeja, joilla langaton verkko voidaan turvata. Standardin määrittelemät luokat ovat Pre-RSNA ja RSNA (engl. Robust Security Network Association). RSN (engl. Robust Security Network) on 802.11i-standardin määrittelemä tietoturvalisäys, joka tehtiin korvaamaan jo vanhentunut WEP-suojaus. RSNA-luokka on tehty laajennettavaksi, joten uusien algoritmien lisääminen uusien uhkien löytyessä on mahdollista ja helpompaa kuin aiemmin. Algoritmit määritetään luokkiin standardin mukaan taulukon 2.1 mukaisesti.

Bhagyavati et al. (2004) jakavat algoritmit ensimmäisen ja toisen sukupolven suojauksiin. He argumentoivat että langaton lähiverkko voi olla yhtä turvallinen kuin 802.3 Ethernet -kaapeliverkko, jos turvaohjeita noudatetaan tarkasti ja verkon rakentamisessa on kiinnitetty erityistä huomiota verkon turvallisuuteen. Lisäksi

Taulukko 2.1: Algoritmien jako Pre-RSNA- ja RSNA-luokkiin.

Pre-RSNA	RSNA
WEP IEEE 802.11 Authentication	TKIP CCMP 802.11X Avaimenhallintajärjestelmät

he painottavat toisen sukupolven suojauksiin perustuvien laitteiden käyttöä.

Verkon turvallisuusratkaisu voidaan myös siirtää hierarkiassa ylemmälle tasolle, ohjelmatasolle (engl. application layer), jolloin WLAN-verkko voi olla suojaamaton. Tämä kuitenkin vaatisi suojauksen kehittämisen jokaiselle käytettävälle palvelulle erikseen ja jokainen näistä voi olla erikseen altis tietoturvaongelmille. Tässä työssä nämä menetelmät sivuutetaan, mukaanlukien erilaiset VPN- (Virtual Private Network, engl. Virtual Private Network) ja IPSec-menetelmät (engl. IP Security Architecture), ja keskitytään WLAN-suojauksiin. HTTP-autentikointia kuitenkin tarkastellaan myöhemmin sen suuren levinneisyyden vuoksi.

Verkon toimivuus ja turvallisuus voidaan vaarantaa hyökkäyksillä. Miltei kaikki tunnetut hyökkäykset perustuvat raan verkkoliikenteen kaappaamiseen. Lisäksi suurin osa tunnetuista hyökkäyksistä on saatavilla binäärimuodossa valmiina ohjelmina, joskaan ei kaupallisesti.

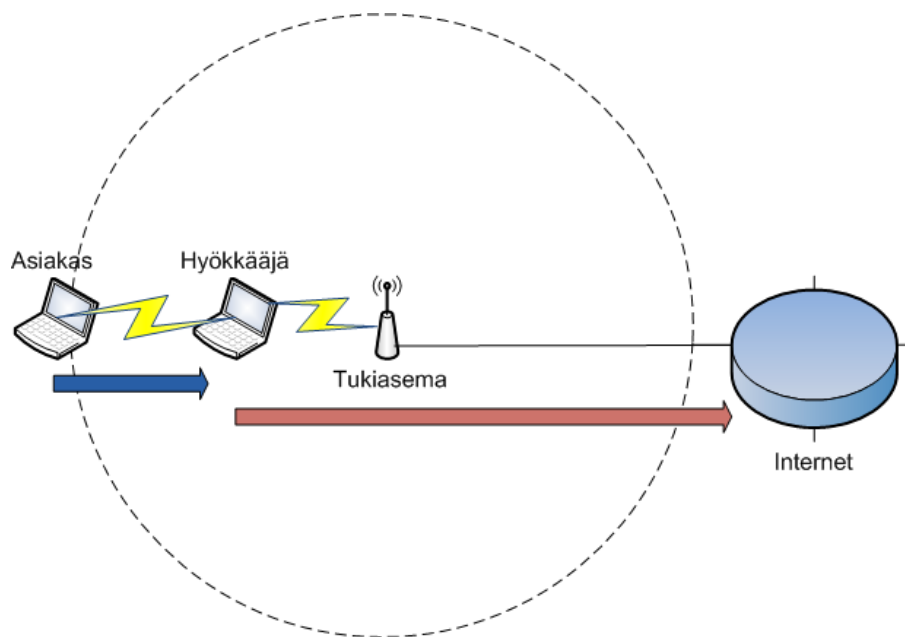
## 2.2 MAC-suodatus

MAC-suodatuksessa (engl. MAC-filtering) käytetään hyväksi kaikkien WLAN-laitteiden sisäänrakennettuja MAC-koodeja (Median käyttökontrolli, engl. Media Access Control) suodattamaan asiakkaita linkkikerroksessa. Tukiasema voidaan asettaa hyväksymään vain tietyillä koodeilla varustetut asiakkaat. Nämä koodit täytyy asettaa tukiasemaan etukäteen, joten käyttäjäjoukko rajautuu huomattavasti ja uusien asiakkaiden lisääminen verkkoon vaikeutuu. MAC-suodatus on ollut mahdollista kaikissa WLAN-standardin versioissa ja se ei varsinaisesti kuulu standardiin vaan valmistajat ovat toteuttaneet sen laitteissaan.

Suojaus on kuitenkin varsin tehoton. Langattomat verkot eivät käytä todentamista lähettäessään ohjausviestejä, joten tämä järjestelmä on hyvin altis ns. MAC Spoofing -hyökkäykselle (MAC-osoitteen väärentämishyökkäys). Hyökkäys yhdistää piirteitä palvelunestohyökkäyksestä (engl. Denial of Service, DoS) ja

identiteettivarkaudesta (engl. Identity theft). Tällaisessa hyökkäyksessä kolmas osapuoli kuuntelee tukiaseman ja luotetun asiakkaan välistä liikennettä ja voi liikenteestä seuloa kummankin MAC-osoitteet. Hyökkääjä väärentää yhteyden katkaisu (engl. deauthentication message) -viestin, johon väärennetään lähettäjäksi tukiasema ja lähettää viestin asiakkaalle. Asiakas toimii viestin edellyttämällä tavalla ja yhteys katkeaa. Hyökkäyksen toista osaa varten hyökkääjä väärentää tukiasemalle lähetettävän tervehtimisviestin oikean luotetun asiakkaan MAC-osoitteella ja tämän avulla tunnistautuu tukiasemalle. Tämän jälkeen tukiasema on hyökkääjän käytössä samalla tavalla kuin se olisi normaalin asiakkaan käytössä. Palvelunestohyökkäystä voidaan käyttää varmistamaan, että oikea asiakas ei voi tehdä mitään tukiasemalle kun hyökkääjä lähettää omia viestejään. (Gill et al., 2006).

Kuva 2.1 visualisoi kuinka MAC-osoite voidaan väärentää. Hyökkääjä on asiakkaan ja tukiaseman välissä. Hyökkääjän täytyy varmistaa että asiakkaan viestit eivät pääse perille (sininen nuoli) ja että hän voi itse lähettää haluamiaan viestejä verkkoon (punainen nuoli).



Kuva 2.1: MAC osoitteen väärentäminen.

Hyökkäys ei vaadi suurta määrää dataa kerättäväksi, joten aikavaatimus on pieni. Hyökkääjän täytyy vain olla paikalla, kun joku luotettu asiakas käyttää verkkoa. MAC-osoitteet ovat kaikissa ohjauspaketeissa, joten niiden saaminen on helppoa. Gill et al. (2006) esittelevät menetelmiä identiteettivarkauden huomaamiseksi jo

pienellä määrällä virheitä. Heidän testeissään hyökkäykset havaittiin viimeistään noin 1400 802.11-siirtokehyksen jälkeen. Nämä menetelmät eivät poista hyökkäyksen mahdollisuutta vaan keskittyvät nopeaan vasteaikaan hyökkäyksen tapahduttua.

## 2.3 Salainen nimi ja staattinen IP-osoite

Useimmiten verkon SSID-nimi on julkinen verkon löydettävyyden parantamiseksi. Tällöin tukiasema lähettää mainosviestiä palvelustaan kantoalueelleen. On myös mahdollista kytkeä mainosviesti pois päältä, jolloin verkkoa ei näy asiakkaiden hakutuloksissa ja verkkoon kytkeytyäkseen täytyy tietää verkon SSID-nimi. Bhagyavati et al. (2004) kuitenkin huomauttaa että uuden asiakkaan liittyessä tukiasemaan joka käyttää salaista SSID-nimeä, se lähettää nimen ilman salausta tervehtimisviestissään. Liittymisviestien kuunteleminen verkosta on äärimmäisen helppoa hyökkäjälle. Tämän takia salainen nimi ei tietoturvaratkaisuna ole erityisen toimiva.

Kumpaakin menetelmää tai näiden yhdistelmää on ollut mahdollista käyttää kaikissa WLAN-standardin versiossa. Kuten MAC-suodatus, nämäkään menetelmät eivät ole osa standardia vaan pikemminkin sen ympärille rakennettuja suoja-menetelmiä. Jotkin laitevalmistajat tarjoavat vielä lisäoptiota näiden ympärille, esimerkiksi automaattisesti vaihtuva (salainen) SSID-nimi.

DHCP-palvelimen automaattinen IP-osoitteen tarjoaminen (DHCP-palvelu) yleensä kytketään pois päältä salaista nimeä käytettäessä. Tällöin päästäkseen käyttämään tukiaseman palveluita on asiakkaan osattava itse asettaa oma IP-osoitteensa tukiaseman palvelemaan osoiteavaruuteen. Normaalitylanteessa verkon DHCP-palvelin antaa IP-osoitteen asiakkaalle. Tämäkin suojausmenetelmä on haavoituttava verkkoliikenteen salakuuntelulle. Nykyisten asiakkaiden IP-osoitteet voi salakuunnella verkkoliikenteestä, jonka jälkeen voi joko palvelunestohyökkäystä käyttäen estää asiakkaan pääsy tukiasemaan ja esiintyä asiakkaan IP-osoitteella tai vaihtoehtoisesti yrittää kerättyihin IP-osoitteisiin pohjautuen arvata sopivan osoitteen. Kuva 2.1 kuvaa myös tämänkaltaista toimintaa.

## 2.4 Wired Equivalent Privacy

WEP (Lankaverkkoa vastaava turva, engl. Wired equivalent privacy) on alkuperäisen langattomien verkkojen standardin, 802.11-standardin, pääasiallinen suojausalgoritmi. WEP:n tarkoituksena on suojata 802.11-verkko niin hyvin, että

suojaus olisi samalla tasolla 802.3 Ethernet -verkon kanssa. Datan salaamiseen käytetään RC4-virtasalausta (engl. stream cipher) sekä eheyden (engl. integrity) varmistamiseen käytetään CRC32-tiivistealgoritmia. IEEE-standardin määrittelemä WEP käyttää 40 bitin pituista avainta salaukseen, mutta nykyään laitetoteutukset ovat pääasiassa toteutettu 104 bittisellä salausavaimella. Näiden kahden toteutuksen erottelunsa vuoksi käytetään useasti nimiä WEP-40 ja WEP-104. Jotkin valmistajat ovat käyttäneet vielä pidempiä avaimia. Yleensä avaimet toistetaan käyttäjille heksadesimaalijonoina luettavuuden parantamiseksi. (IEEE 802.11 Working Group, 2007).

IEEE 802.11 Working Group (2007) määrittelee tarkasti kuinka WEP-algoritmi toteutetaan. WEP-avain ei ole suoraan avaimena RC4-salaukselle, vaan se yhdistetään (engl. concatenate) 24-bittisen pakettikohtaisen aloitusvektorin (IV, engl. initialization vector) kanssa. Aloitusvektori lisätään WEP-viestin alkuun salauksittomana. RC4 tuottaa avainvirran (key stream) joka viedään salattavan viestin sekä siitä tuotetun eheysarvon kanssa ehdoton tai -funktion (XOR, engl. exclusive or) läpi. Tämä salattu arvo muodostaa loppuosan WEP-viestistä. Salauksen purku toimii vastaavasti, paketista löytyvän IV-arvon sekä WEP-avaimen avulla saadaan sama avainvirta. Standardi tukee neljää avainta, joita käytetään vuorotellen WEP-avaimena, mutta käytännössä näistä käytetään vain yhtä.

WEP ei sisällä avaimenhallintaprotokollaa (engl. Key management protocol), joten avaimet täytyy syöttää kaikille verkon laitteille aina käsin. Tämä ratkaisu tekee verkon uudelleenkonfiguroinnin hyvin vaikeaksi, koska avaimet täytyy myös käydä päivittämässä käsin. Lisäksi koska kaikki käyttävät samaa avainta, on kaikki verkon data suoraan luettavissa mikäli vain yhden koneen WEP-avain paljastuu. Useimmat käyttöjärjestelmät pitävät WEP-avaimet tietokoneen muistissa, jotta niitä ei tarvitsisi joka kerta kirjoittaa uudelleen, mutta tämä tarkoittaa myös että verkon turvallisuus on vaarassa jos yksikin sen kone katoaa tai varastetaan, koska avain on luettavissa koneen kiintolevyiltä. (Cam-Winget et al., 2003).

WEP-salauksen heikkous on sen versio RC4-avaimen luonnista. Sen ensimmäinen ongelma on avaimen uusiokäyttö. Virtasalauksessa samaa avainta ei saa koskaan käyttää uudelleen, koska tämä heikentää salauksen tehokkuutta. 24 bittinen pakettikohtainen osa WEP:n RC4-avainta ei ole riittävän pitkä taatakseen että samaa avainta ei käytettäisi uudelleen ja tämä mahdollistaa viestien muuttamisen. Fluhrer, Mantin ja Shamir julkaisivat aikaisempien hyökkäysten jälkeen oman ns. FMS-hyökkäyksen WEP-salaukselle. Heidän tuloksensa osoittivat että FMS-hyökkäystä käyttämällä WEP-avain voidaan murtaa kuuntelemalla verkosta noin miljoona salattua pakettia (keskimäärin 1,5 gigatavua verkkoliikennettä). Myöhemmin Tews et al. (2007) jatkoivat aikaisempia RC4-algoritmiin kohdistuneita hyökkäyksiä ja loivat WEP-hyökkäyksen, jolla 104-bittisen avaimen voi

ratkaista jo 40000 paketin (keskimäärin 65 megatavua) jälkeen. Heidän menetelmänsä pätee myös pidemmille avaimille. (Cam-Winget et al., 2003).

Nämä hyökkäykset mahdollistavat WEP-salauksen hyötyjen täydellisen poiston hyvin nopealla aikavälillä. Tews et al. (2007) huomauttavat että hyökkääjä voi hiljaisessa verkossa itse luoda liikennettä, jotta salattujen pakettien kaappaus onnistuisi. Heidän kokeensa osoittivat että 802.11g-standardin mukaisessa verkossa käyttämällä uudelleenlähetettyjä paketteja (engl. re-injection) on mahdollista kerätä tarvittavat 40000 pakettia alle minuutissa. Paljon asiakkaita sisältävissä verkoissa hyökkäys on täysin passiivinen, joten sen havaitseminen on mahdotonta. WEP:n käyttämät algoritmit ovat hyviä, mutta salauksen tapa käyttää algoritmeja altistaa sen hyökkäyksille. (Cam-Winget et al., 2003).

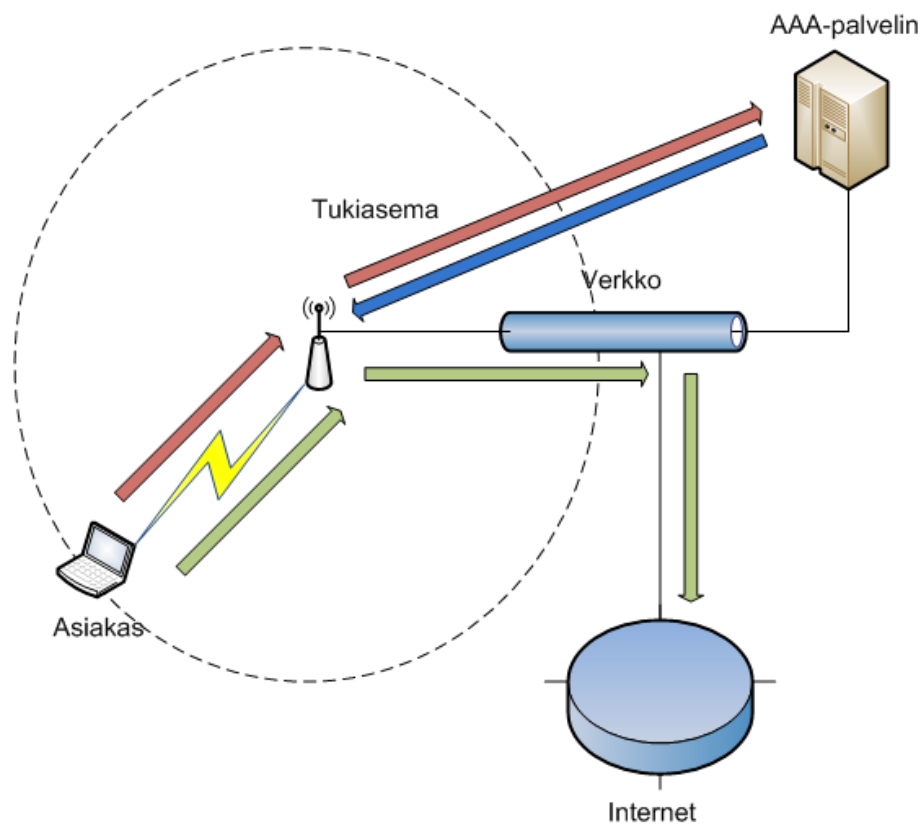
WEP-hyökkäysohjelmia on helposti saatavilla internetistä ilmaiseksi useina eri versiona ja useille käyttöjärjestelmille. Ohjelmien käyttäminen ei vaadi erikoisosaamista, sillä ohjeita on saatavilla ohjelmistojen sivuilta useille eri käyttöjärjestelmille ja verkkokorteille.

## 2.5 802.1X

802.1X on 802.1 -sarjan verkkostandardi, joka käsittelee porttikohtaista verkkotunnistusta. Sen tarkoitus on mahdollistaa tiettyyn laitteen porttiin kiinnitetyn asiakkaan todentaminen ja todennuspalvelimen päätöksen perusteella joko hyväksyä yhteydet (hyväksytty asiakas) tai estää kaikki asiakkaan yhteydet (tunkeilija). 802.11 -standardissa 802.1X -protokolla on osana 802.11i -tietoturvalaajennusta ja siten pakollisena osana WPA2-salausta. Yleensä 802.1X toimii NAS-palvelimena (engl. Network Access Server) ja käyttää erillistä AAA-palvelinta (Todennus, Valtuutus, Kirjanpito; engl. Authentication, Authorization and Accounting) asiakkaiden todentamiseen. Vaihtoehtoisesti NAS-palvelin voi myös todentaa asiakkaita ns. PSK-tilassa (esijaettu avain, engl. Pre-Shared Key), jolloin AAA-palvelinta ei tarvita. (IEEE 802.11 Working Group, 2007).

802.1X on rakennettu EAP-runkoon (laajennettava todennusprotokolla, engl. Extensible Authentication Protocol) perustuen. EAP määrittelee viestimekanismeja, joilla voidaan todentaa asiakas AAA-palvelimelle. Yleisesti ei käytetä tietoturvaltaan heikkoa EAP-protokollaa, vaan esimerkiksi EAP-TLS -protokollaa tai Protected EAP -protokollaa. EAP-TLS protokollassa ensin neuvotellaan suojattu TLS-yhteys AAA-palvelimen ja asiakkaan välille ja tässä suojatussa tunnollisissa siirretään EAP-paketit. Nykyisin AAA-palvelin voi käyttää asiakkaan tietojen todentamiseen ulkoisia lähteitä kuten Kerberosta tai Active Directory -palvelinta. (Steve Riley, 2005).

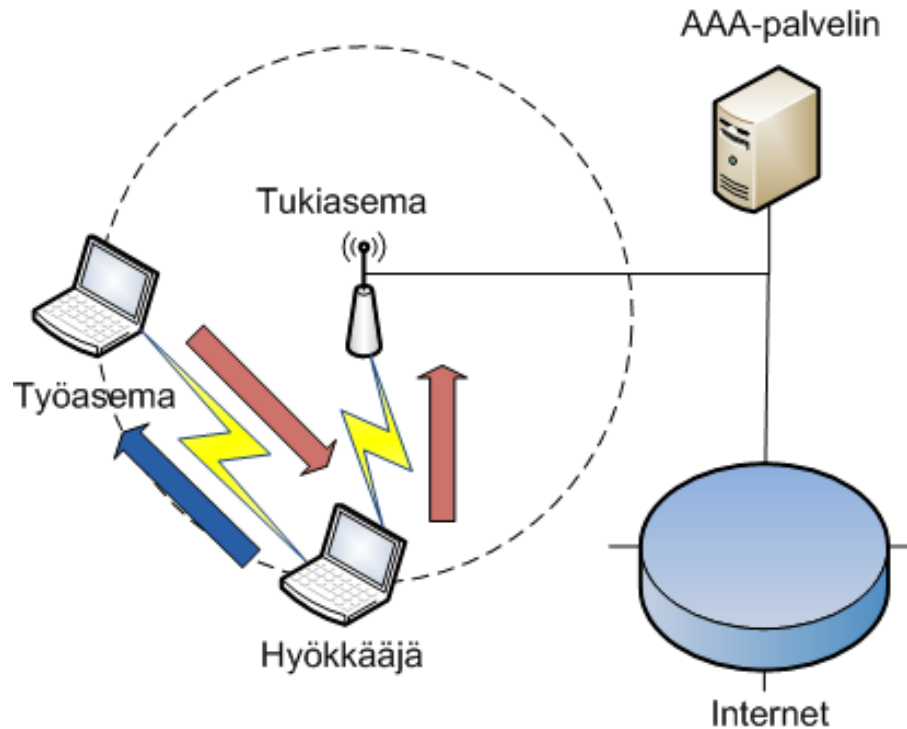
802.1X -autentikaation toiminta AAA-palvelimen kanssa on kuvattu kuvassa 2.2. Asiakas ottaa yhteyden NAS-palvelimeen (tukiasemaan) käyttäen 802.1X kontrolloimatonta porttia. Kaikki liikenne asiakkaalta kontrolloituihin portteihin estetään kunnes autentikaatio on onnistuneesti saatettu loppuun. NAS-palvelin lähettää pyynnön eteenpäin AAA-palvelimelle, joka tekee päätöksen pääsystä verkkoon ja kirjaa tapahtuman lokiin. Yleisesti tähän käytetään RADIUS-protokollaa ja RADIUS-palvelinta. AAA-palvelin todentaa pyynnön asiakkaan kanssa esimerkiksi EAP-protokollaa käyttäen. Hyväksytyt todennuksen jälkeen kaikki liikenne päästetään läpi kontrolloitua porttia pitkin. (IEEE Computer Society, 2004).



Kuva 2.2: 802.1X-todennuksen toiminta.

Steve Riley (2005) huomauttaa, että 802.1X ei ole suojattu MITM-hyökkäyksiä (Mies keskellä, engl. Man-in-the-middle) vastaan. 802.1X todentaa käyttäjän vain yhteydenmuodostuksessa. Kuva 2.3 esittää tätä hyökkäystä. Hyökkääjä esiintyy tukiasemana ja lähettää EAP-yhteydenmuodostusviestit asiakkaalle (sininen nuoli). Tämän jälkeen asiakas lähettää datansa hyökkääjän kautta, joten hän voi kuunnella kaikkea liikennettä (punaiset nuolet). Tätä heikkoutta vastaan Steve

Riley (2005) suosittaa IPSec-tunnelin käyttämistä 802.1X-todennuksen jälkeen, jolloin hyökkäys on mahdoton toteuttaa.



Kuva 2.3: 802.1X-todennus ja Man-in-the-middle -hyökkäys.

Toinen mahdollinen hyökkäys on yhteyden haltuunotto (engl. session hijacking). Tässä hyökkääjä odottaa kunnes 802.1X-todennus on suoritettu ja asiakas voi lähettää dataa verkkoon. Tämän jälkeen hyökkääjä väärentää yhteys katkaistu -pakettin ja lähettää sen asiakkaalle. Asiakas katkaisee yhteyden, mutta tukiasemalla se on vielä voimassa ja hyökkääjä voi nyt käyttää yhteyttä. Tämä ja edellinen haavoittuvuus ovat molemmat mahdollisia, koska 802.1X tekee vain yksipuolisen todennuksen, jos käytetään EAP-protokollaa. Molempipuolisella todennuksella (engl. mutual authentication) tätä hyökkäystä ei voi käyttää, koska pakettien väärentäminen on erittäin vaikeaa.

## 2.6 Wi-Fi Protected Access

WPA/WPA2 (engl. Wi-Fi Protected Access) on tietoturvaprotokolla, jota Wi-Fi -liittouma (Wi-Fi Alliance) kehittää. Alunperin WPA kehitettiin korjaamaan

WEP-salauksen ongelmat nopeammin kuin tuleva 802.11i -tietoturvalisäys. Wi-Fi -liittouma myöntää Wi-Fi Certified -merkkiä laitteille, jotka tukevat WPA- ja WPA2-protokollaa. (Wi-Fi Alliance, 2003).

Syksyllä 2008 venäläinen turvayhtiö ilmoitti, että se onnistui nopeuttamaan WPA- ja WPA2-avainten ns. brute force -hakemista (raaka voima) jopa 10000 prosenttia käyttäen apunaan NVidian GeForce -tehonäytönohjaimia rinnakkaislaskentaan (Global Secure Systems, 2008). Tämä tarkoittaa, että jatkossa heikoilla avaimilla WPA-suojatut verkot voivat murtua yhtä nopeasti kuin WEP-suojatut verkot nykyään murretaan.

### 2.6.1 Versio 1

WPA (WPAv1, WPA versio 1) julkaistiin ennen kuin 802.11i -tietoturvalaajennus oli valmis ja se kehitettiin yhteistyössä IEEE:n kanssa. WPA2-nimi oli jo suunniteltu lanseerattavaksi kun 802.11i -laajennus oli ratifioitu. WPA sisälsi suurimman osan 802.11i -laajennuksen uudistuksista sekä lisäsi WEP-protokollasta puuttuneen käyttäjien todennuksen (engl. user authentication). Lisäksi tarkoituksena oli poistaa tarve käyttää esimerkiksi VPN-tunneleita WLAN-verkon päällä. Kodeille ja pienyrityksille lisättiin mahdollisuus käyttää WPA:ta ilman erillistä todennuspalvelinta (802.1X) käyttäen esijaettuja avaimia (engl. pre-shared key). (Wi-Fi Alliance, 2003).

WPA toimii vanhoilla WEP-laitteilla ohjelmistopäivityksellä, koska algoritmeja ei ole muutettu. Kaiken pohjana on edelleen WEP, mutta sen päälle on rakennettu uusia osia, joilla on korvattu osa vanhoista ohjelmistossa tapahtuvista osista. Näillä muutoksilla on poistettu kaikki vanhat ongelmat ja säilytetty yhteensopivuus vanhempien laitteiden kanssa.

Käytännössä WPA käyttää 802.11i-laajennuksen määrittelemää TKIP-protokollaa (engl. Temporal Key Integrity Protocol) salaukseen. TKIP tuo uuden eheystarkastuksen (MIC, engl. Message integrity code), joka on nimeltään Michael. Jo olemassa olevat algoritmit olivat liian raskaita vanhoille tukiasemille, joten uusi Michael rakennettiin laskutoiminnallisuudeltaan kevyeksi. Michael tarjoaa noin 20 bitin verran turvaa, mutta TKIP vaatii uuden avaimen (engl. rekeying) kun MIC:ssa havaitaan virhe. Lisäksi TKIP lisää pakettien sekvenssinumeroinnin, jotta uudelleenlähetykset pystytään havaitsemaan ja poistamaan. Lisäksi WEP:n heikkoa RC4-avainrakennetta muutettiin. TKIP-protokollan RC4-avain koostuu sekoitusfunktioista, joka ottaa syötteenään WPA-avaimen (vrt. WEP-avain), paketin sekvenssinumeron sekä lähettäjän MAC-osoitteen. TKIP käyttää kahta avainta, 128-bittistä RC4-avainta sekä 64-bittistä eheysavainta Michaelille. Näiden hallintaan käytetään 802.11X-protokollaa. (Cam-Winget et al., 2003).

Moen et al. (2004) osoittavat, että käytettäessä WPA-protokollaa on tärkeää pitää salaisena sekä WPA-avain (kutsutaan myös nimellä Temporal key, TK) sekä siitä generoidut RC4-avaimet. Jo yhden RC4-avaimen kaappaamisella hyökkääjä voi muuttaa paketin MIC-koodeja ja tehdä haluamansa paketin, kunhan alkuperäinen paketti ja sitä seuraavat paketit eivät päädy oikealle vastaanottajalle ennen väärennettyä pakettia. Mikäli hyökkääjällä on käytössään kaksi tai useampi saman IV32-arvon (Alustusvektorin 32 eniten merkitsevää bittiä) kanssa generoituja RC4-avaimia, voi hän purkaa (pitemmän ajan kuluessa) kaikki tuon WPA-avaimen viestit. Moen et al. (2004) käytännön kokeilut osoittivat, että neljän tai useamman RC4-avaimen kanssa purkaminen tapahtuu alle 7 minuutissa. Pienemmällä RC4-avaimien määrillä purkaminen kestää huomattavasti kauemmin.

## 2.6.2 Versio 2

WPA2, tunnetaan myös nimellä RSN (engl. Robust Security Network), on Wi-Fi -liittouman kehittämä toteutus 802.11i -laajennukselle ja se vaaditaan toteutettavaksi kaikkiin Wi-Fi Certified -laitteisiin. RSN-verkot perustuvat RSNA-turvalliitoksiin (Security Relationship). Kun jokaisella asiakkaalla ja tukiasemalla on oma RSNA-liitos, voidaan CCMP-protokollaa käyttäen varmistaa kaiken liikenteen salaaminen sekä pakettien alkuperä ja eheys. WPA on laajennuksen osatoteutus ja WPA2 on tehty korvaamaan se uudemmissa laitteissa. Tämän vuoksi WPA2 vaatii uusia ominaisuuksia laitealustalta, joten vanhoja laitteita ei voida päivittää toimimaan sen kanssa. Suurimpina uudistuksina on RC4-salauksen vaihtaminen AES-salaukseen (edistynyt salausstandardi, engl. Advanced Encryption Standard), MIC-toteutuksen vaihtaminen CCMP-protokollaan (engl. Counter Mode CBC MAC Protocol) sekä neljävaiheisen yhteyden avaamisen lisääminen. WPA2 laitteet osaavat sopia mitä salausta käytetään, joten se on laajennettava myös tulevaisuudessa uusilla salauksilla ja voi käyttää WPA:n TKIP-protokollaa tarvittaessa. (Bulbul et al., 2008).

WPA2 tarjoaa suojaan tukiaseman ja asiakkaan välille, tukiasemasta eteenpäin suojaus on hoidettava jollakin toisella menetelmällä. RSN-verkossa yhteydet muodostetaan neljäosaisella tervehdyksellä (engl. 4-way handshake), jonka jälkeen molemmilla osapuolilla on PMK-avain (Parittainen pääavain, engl. Pairwise Master Key) ja salausalgoritmien käytöstä on sovittu. PMK muodostetaan joko PSK-avaimesta tai AAA-palvelimelta saadusta avaimesta (yleensä muodostetaan EAP-protokollaa käyttäen), mikäli käytössä on AAA-palvelin. PMK-avainta käytetään muiden tarvittavien avainten, mm. TK-avaimen ja EAPOL-avaimien, muodostamiseen. PSK-avainta käytettäessä on otettava huomioon, että mikäli käytössä on vain yksi avain jokaista SSID-tunnistetta kohti niin avaimen paljastuessa

hyökkääjät voivat purkaa kaiken verkossa liikkuvan datan riippumatta suojauksesta. (Frankel et al., 2007).

RSN-verkossa käytetään useata eri avaintyyppiä ja jokaisesta tyypestä on useita eri avaimia yhtä aikaa käytössä. Tyyppejä ovat juuriavain (engl. root key), generointiavain (engl. key generation key), liikenneavain (engl. traffic key), eheysavain (engl. message integrity key) sekä avaimien salausavain (engl. key encryption key, KEK). Näiden lisäksi on erityinen PTK-avain (parittainen hajoava avain, engl. pairwise transient key) joka on koottu muista avaimista. (Frankel et al., 2007).

WPA2 käyttää liikenteen eheyden ja salassapidon varmistamiseen TKIP-protokollan sijaan CCMP-protokollaa. CCMP on suunniteltu suojaamaan datapakettien otsake- sekä dataosio. Protokolla käyttää salaukseen AES-salausta laskurtilan (engl. counter mode) ja osiolinkityksen kanssa (engl. block chaining). Suojauksen avaimena käytetään 128-bittistä TK-avainta. CCMP lisää paketteihin 48-bittisen pakettinumeron, jolla estetään toistohyökkäykset. CCMP-protokollan syötteenä käytetään paketin dataa, pakettinumeroa ja lisätodennusdataa (Additional Authentication Data, AAD). AAD sisältää muun muassa paketin lähtöosoitteen sekä laadunvarmennustietoja. Protokolla on suunniteltu erityisesti vaatimaan vähän resursseja ja käyttämään vain yhtä salausavainta tehokkuuden nostamiseksi. WLAN-ympäristöissä käytettäessä CCMP käyttää kahdeksaa bittiä kuvaamaan MIC-koodia. (Frankel et al., 2007).

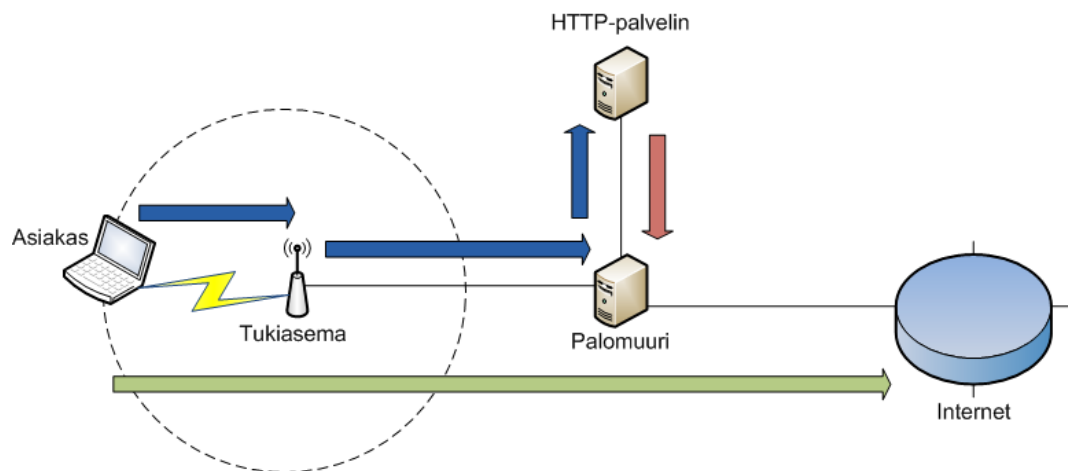
WPA2:lle ei ole Google-haun perusteella julkaistu muunlaisia hyökkäyksiä kuin brute force -menetelmiä sekä avainvalinnan todentamiseen tarkoitettuja sanakirjahyökkäysohjelmistoja (engl. dictionary attack). Ohjelmille on saatavilla valmiiksi laskettuja tiivistetaulukoita (engl. hash table) yleisille SSID-nimille ja salasanoille. Ohjelmat vaativat toimiakseen kaapattua verkkoliikennettä, joka sisältää WPA2-tervehdyksen.

## 2.7 HTTP-todennus

HTTP-todennuksessa hyödynnetään jo olemassa olevia HTTP-palvelimia sekä mahdollisuutta käyttää suojattuja SSL/TLS-yhteyksiä. Yleensä tällaista suojausmenetelmää käytetään, kun verkkoon saapuu paljon vierailijoita, joista halutaan pitää kirjaa ja AAA-pohjainen ratkaisu olisi liian raskas. Esimerkkejä käyttökohteista ovat kahvilat ja lentoasemat. Asiakkaalla on joko henkilökohtainen tunnus verkon käyttöön tai yleistunnus, joka ei ole yleisesti saatavilla. Lisäksi tämä lähestymistapa tekee verkon jatkamisesta helpompaa, koska vanhemmatkin tukiasemat tukevat suojaamattomien verkkojen jatkamista.

Kuva 2.4 esittää yhtä mahdollista kokoonpanoa HTTP-todennukselle. Asiakas ot-

taa langattoman yhteyden tukiasemaan, joka yleensä on jätetty ilman suojausta. Tukiasema on yhdistetty suoraan palomuriin. Asiakas saa IP-osoitteen DHCP-palvelimelta, joka voi olla esimerkiksi samassa koneessa HTTP-palvelimen kanssa. Palomuri uudelleenohjaa kaiken HTTP(S)-liikenteen HTTP-palvelimeen ja estää muun liikenteen kokonaan (sininen nuoli). Asiakkaan täytyy kirjautua omilla tunnuksillaan HTTP-palvelimella, jolloin se lähettää viestin palomuurille avata liikenne asiakkaan käyttämälle IP:lle (punainen nuoli). Tämän jälkeen asiakkaan liikenne kulkee suoraan internetiin palomuurin läpi (vihreä nuoli).



Kuva 2.4: WLAN HTTP-todennus.

Hyvänä puolena tällaisessa järjestelmässä on kokoonpanon helppous sekä mukautettavuus. Toiminta on hieman EAP/AAA-palvelin -mallin tapaista, mutta toteutus on paljon kevyempi ja muistuttaa enemmän WEP-toteutusta useammilla esijae- tuilla avaimilla, joilla on eri oikeudet. Lisäksi palomuriin voi helposti asettaa rajoituksia, jolloin esimerkiksi tietyn siirtomäärän tai ajan ostaminen internet- palveluun on mahdollista. Huonoina puolina on liikenteen salaamattomuus sekä vaatimus HTTP(S)-tuesta asiakaslaitteessa. Tällaiseen verkkoon ei voi käytän- nössä liittyä kuin tietokoneilla ja älypuhelimilla, jotka tukevat HTTP-liikennettä. Verkko itsessään ei tarjoa minkäänlaista turvaa, joten asiakkaan täytyy itse huo- lehtia siitä sovellustasolla, esimerkiksi käyttämällä IPsec-tunnelia tai VPN-sovellusta.

Tällainen lähestymistapa on haavoittuva IP- ja MAC Spoofing -hyökkäyksiä vas- taan. Lisäksi istunnon kaappaaminen on yleisimmissä toteutuksissa mahdollista. Yleensä palomuurin avaaminen datalle perustuu joko asiakkaan IP-osoitteeseen tai MAC-tunnukseen. Kumpaakin näistä voi kuitenkin väärentää, joten hyökkääjä voi tätä kautta käyttää hyväksytyt käyttäjän istuntoa hyväkseen. Palvelut si- sältävät yleensä myös uloskirjautumistoiminnon, jota käyttämällä käyttäjän ai-

ka lopetetaan ja palomuuuri suljetaan uudestaan. Käyttäjät kuitenkin unohtavat käyttää tämän kaltaisia mahdollisuuksia, joten hyökkääjä voi oikean käyttäjän poistumisen jälkeen käyttää tämän yhteyttä. Tämä on erityisesti helppo toteuttaa, jos suodatus palomuurissa peustuu vain IP-osoitteisiin.

## 2.8 Yhteenveto

Taulukko 2.2: Käsitellyt suojausmenetelmät 802.11-verkoille.

	MAC	SSID	WEP
Yhteensopivuus	Kaikki	Kaikki	Kaikki
Liikenteen salaus	Ei ole	Ei ole	On
Salausalgoritmi	Ei ole	Ei ole	RC4
Eheysalgoritmi	Ei ole	Ei ole	CRC32
Vaativuus käyttäjälle	Matala	Korkea	Keskitasoinen
Vaativuus ylläpidolle	Korkea	Korkea	Matala
Hyökkäykset	Session hijack, MAC spoofing	Session hijack	FMS, Tews
	WPA	WPA2	HTTP(S)
Yhteensopivuus	Päivitys	Uudet laitteet	HTTP-laitteet
Liikenteen salaus	On	On	Ei ole
Salausalgoritmi	RC4	AES	Ei ole
Eheysalgoritmi	Michael	CCMP	Ei ole
Vaativuus käyttäjälle	Matala	Matala	Keskitasoinen
Vaativuus ylläpidolle	Matala	Matala	Korkea
Hyökkäykset	Brute force	Brute force	IP- ja MAC spoofing, Session hijack

Taulukko 2.2 sisältää yhteenvedon turvamenetelmien ominaisuuksista. Taulukos-

sa vaativuudella tarkoitetaan tarvittavan ajan sekä tietotaidon yhdistelmää. Lisäksi SSID-suojauksella tarkoitetaan salattua SSID-nimeä ja staattisia IP-osoitteita yhdessä. HTTP-laitteilla tarkoitetaan kaikkia laitteita, joissa voi suorittaa HTTP(S)-autentikoinnin.

# Luku 3

## Johtopäätökset

Tässä luvussa tarkastellaan suojausmenetelmien soveltuvuutta eri ympäristöissä ja erilaisissa esimerkkikäyttötapauksissa. Käyttötapaukset on valittu niiden yleisyyden ja kattavuuden pohjalta, mutta on muistettava että jokainen ympäristö on erilainen.

### 3.1 Yleistä käyttötapauksista

Tutkittaessa mikä suojausmenetelmä sopisi parhaiten mihinkin käyttötapaukseen ja -ympäristöön on otettava huomioon tarvittava tietoturvan taso. Tämä yleensä johdetaan suoraan verkossa siirrettävän datan arvosta ja salassa pidettävyydestä. Lisäksi on otettava huomioon mahdollisesti yrityksen imagolle aiheutuvat haitat mikäli verkkoon murtaudutaan. On muistettava, että mikään WLAN-suojaus ei ole murtamaton. Turvatason saa hyvin korkealle, mutta kaikille nykyään käytössä oleville suojuuksille on löydetty (tarpeellisella laskentateholla) toteutettavissa olevia hyökkäyksiä.

Taulukko 3.1 esittää kolme salaukseen perustuvaa suojaustapaa ja niiden ominaisuuksia. Tulokset osoittavat jokseenkin selvästi, että uudemmat suojausmenetelmät tarjoavat huomattavasti enemmän turvaa kuin aiemmat, joskin lisäturvan hankkimiseksi on tehtävä laitteistoinvestointeja. Lisäksi uudemmat suojaukset eivät toimi vanhemmilla verkkokorteilla eivätkä vanhemmissa käyttöjärjestelmissä (Windows-perheestä XP tukee ensimmäisenä WPA2-suojausta ilman päivityksiä). WEP:n käyttö enää nykyään ei ole suositeltavaa, jollei siihen ole erityisen pakottavaa syytä, esimerkiksi vanhoja laitteita. WEP ei käytännössä suojaa verkkoa mitenkään, vaan perustaidoilla varustettu tietokoneenkäyttäjä pystyy murtamaan suojuksen valmiilla internetistä saatavilla työkaluilla.

Taulukko 3.1: Verkkoliikennettä salaavat suojaukset. (Bulbul et al., 2008).

	WEP	WPA	WPA2 (RSN)
Salausalgoritmi	RC4	RC4 ja TKIP	AES ja CCMP
Salausavaimen koko	40 bittiä	128 bittiä	128 bittiä
Avaintenhallinta	Ei ole	802.1X	802.1X
Salausavaimen vaihdot	Ei ole	Pakettikohtaiset avaimet	Ei tarvetta
Todennus	PSK	802.1X	802.1X
Eheystarkistukset	CRC32 ICV	MIC	CCMP
Otsakkeen eheystarkistus	Ei ole	MIC	CCMP
Toistohyökkäysten esto	Ei ole	Pakettinumerointi	Pakettinumerointi

Taulukko 3.1 ei sisällä muita menetelmiä, koska ne eivät tarjoa liikenteen salausta. HTTP-autentikaatio ei salaa liikennettä, vaan jättää sen asiakkaan vastuulle. Salainen nimi, salainen IP-osoite tai MAC-suodatus eivät myöskään suojaa liikennettä mitenkään. Jälkimmäiset tähtäävät vain yhteyden luonnin vaikeuttamiseen.

Kuten Bhagyavati et al. (2004) toteavat, mitä tahansa suojausta käytettäessä on huomioitava toimintatavat ja prosessit joita yritys tai yhteisö käyttää. Hyväkin suojaus on helpommin murrettavissa jos tietoturvapoliittikkaa laiminlyödään valitsemalla huonoja tai ennalta-arvattavia avaimia (PSK-tilassa) tai omat tunnistetiedot tallennetaan omaan päätelaitteeseen.

## 3.2 Kotikäyttö

Yleinen oletus on, että kotikäyttäjän ympäristössä ei ole juurikaan salattavaa dataa. Olemassa oleva data halutaan kuitenkin pitää eheänä. Lisäksi kotona käytettävät salattavat palvelut ovat yleensä jonkin ohjelmistotason toteutuksen piirissä (esimerkiksi pankkiyhteydet suojataan SSL/TLS-salauksella). Tärkeää on kuitenkin pitää verkko käytettävänä kaikille hyväksytyille käyttäjille, mukaan lukien vieraat. Tämä edellyttää, että ulkopuolisilta estetään pääsy verkkoon, jotta verkon kuormitus pysyy pienenä ja resursseja on käytettävissä hyväksytyille käyttäjille. Lisäksi kotikäyttäjillä on harvoin halua tai mahdollisuuksia hankkia ylläpitopalveluja, joten verkon täytyy olla helposti hallittavissa myös peruskäyt-

täjälle. Käyttäjä ei yleensä halua maksaa paljon verkon rakentamisesta, joten laitteistoinvestoinnit täytyy pitää minimissään, yleensä vain yhdessä tukiasemassa.

Annettujen ehtojen kautta on selvää, että ainoastaan esijaetun avaimen menetelmät ovat toteutettavissa. 802.1X -palvelimet ja HTTP(S)-menetelmät ovat ylimitoitettuja tällaiseen käyttöön. MAC-suodatus täyttää ehdot, mutta se vaatii jatkuvaa ylläpitoa mikäli verkossa käy paljon laitteita. Salainen SSID-nimi riittää sen sijaan vaatimusten täyttämiseen, mutta tällöin otettava riski että osaavat tietokoneenkäyttäjät pääsevät helposti liittymään verkkoon. Ratkaisun hyvinä puolina on, että käyttäjien on muistettava ainoastaan verkon nimi eikä ylläpitoa tarvitse juuri ole.

Salauksen käyttäminen on luontevaa, jotta verkkoon ei pääse liittymään vahingossa. Salaisen SSID-nimen kanssa verkkoon voi päätyä vahingossa, mikäli nimenä käytetään jotakin yleistä verkkonimeä. Tällaista mahdollisuutta ei ole WEP- eikä WPA-suojauksella käytettäessä. WEP on periaatteessa tarpeeksi tehokas suojaus pitämään satunnaiset käyttäjät pois verkosta, mutta koska työkalut salauksen purkamiseen ovat vapaasti saatavilla ei tämä lähestymistapa ole suositeltava. WPA toimii kaikilla nykyisillä käyttöjärjestelmillä ja useimmat kotikäyttöön suunnatut WLAN-tukiasemat ja -reitittimet tukevat sitä, joten ei ole syytä olla käyttämättä WPA:ta, mikäli ei tarvitse tukea vanhemmille laitteille. WPA-suojauksen murtaminen kestää niin kauan, että tavoite pitää satunnaiset käyttäjät pois täytyy.

### 3.3 Yrityskäyttö

Yritysten tietoverkko- ja salaustarpeet vaihtelevat paljon. Seuraavassa käsitellään kolme esimerkkiyritystä ja etsitään tarpeiden pohjalta sopivia ratkaisuja WLAN-verkon turvaamiseen.

#### 3.3.1 Pieni yritys, muu kuin IT-toimiala

Yrityksessä ei ole juurikaan salattavaa materiaalia. Työmenetelmät, tekniikat ja laitteet ovat yleistä tietoa ja työntekijät ovat yrityksen pääasiallinen voimavara. Yrityksessä on kuitenkin tärkeää että verkko on käytettävissä aina kun työntekijä sitä tarvitsee, sillä hitaus ja odottelu kuluttavat työaika. Lisäksi, jos käytössä on esimerkiksi internet-pohjainen tilausjärjestelmä on tärkeää että tilaukset säilyvät järjestelmässä muuttumattomina (eheys) ja että tilauksia voi jättää ajasta riippumatta. Yrityksellä ei ole yleensä erillistä ylläpitoa, joten verkon huolto täy-

tyy olla helppoa. Lisäksi pienellä yrityksellä, jolla verkko ei ole suoraan liitoksissa päätoimialaan, ei ole halua maksaa paljota verkon rakentamisesta.

Erilliset autentikaatiopalvelimet (802.1X ja HTTPS) ovat liian kalliita ratkaisuja esimerkiksi yritykselle sekä niiden aiheuttama ylläpitotonta on liian iso. Yritys ei kuitenkaan halua olla ilman suojausta, koska verkon täytyy olla käytettävissä omille työntekijöille ja verkossa on dataa, jota ei haluta muiden saataville (esimerkiksi yrityksen tilauskanta). Salattu SSID-nimi ja MAC-suodatus ovat helppoja ratkaisuja, mutta ensimmäisen suojattomuus ja jälkimmäisen ylläpitokustannukset eivät tee niistä hyviä ratkaisuja.

WEP- tai WPA-suojaukset ovat tarpeisiin nähden hyviä ratkaisuja. Kumpaakaan ei tarvitse ylläpitää usein ja esijaetun avaimen vaihtaminen määrääjoin riittää. Yrityksillä on harvemmin WPA-suojausta tukemattomia laitteita, joten WPA on selkeästi parempi vaihtoehto WEP-suojauksen helpon murrettavuuden takia. Yrityksen kannattaa vaihtaa laitteet, jotka eivät tue WPA-suojausta mikäli niitä on vielä jäljellä.

### 3.3.2 Pieni tai keskisuuri IT-yritys

IT-yrityksissä ylläpitotehtävissä on yleensä ainakin yksi henkilö, jonka vastuulle voidaan asettaa myös yrityksen WLAN-verkko. Yritys toimialana on tietoteknisten ratkaisujen suunnittelu, joten sillä on paljon salattavaa tietoa digitaalisessa muodossa palvelimilla ja työasemilla (esimerkiksi ohjelmien lähdekoodia). Verkkoliikenne täytyy myös suojata, koska yrityksen tärkeää tietoa liikkuu verkossa usein. Lisäksi on tärkeää, että ulkopuoliset tahot eivät voi muuttaa yrityksen tietoja tai aiheuttaa häiriötä verkon toimintaan. Verkkoa rakennettaessa on yleensä käytössä enemmän rahaa ja tietotaitoa kuin muilla toimialoilla.

Salattu SSID-nimi, MAC-suodatus sekä staattinen IP ovat kaikki liian turvattomia menetelmiä verkon suojaukseen eivätkä ne suojaavat verkkoliikennettä. HTTP(S)-autentikaation käyttäminen olisi mahdollista, mutta sekään ei suojaavat verkkoliikennettä. Menetelmistä jäävät jäljelle WEP, WPA ja WPA2. Kaikki näistä tukevat 802.1X -autentikaatiopalvelimen käyttöä, joka voi olla IT-yritykselle kannattava hankinta. Vaihtoehtoisesti autentikaatiopalvelimen voi myös yhdistää jonkin jo olemassa olevan palvelimen kanssa samaan laitteeseen.

Yrityksen ei kannata käyttää WEP-suojausta edes 802.1X-palvelimen kanssa, koska WEP:n käyttämä yksisuuntainen tunnistus altistaa sen helposti toteutettaville hyökkäyksille. Esijaetun avaimen WEP ei myöskään ole tarpeeksi tehokas suojaus. WPA ja WPA2 esijaetulla avaimella tai autentikaatiopalvelimella ovat tarpeeksi tehokkaita, mutta palvelin tarjoaa lisäksi oheispalveluja. Autentikaatiopalvelin-

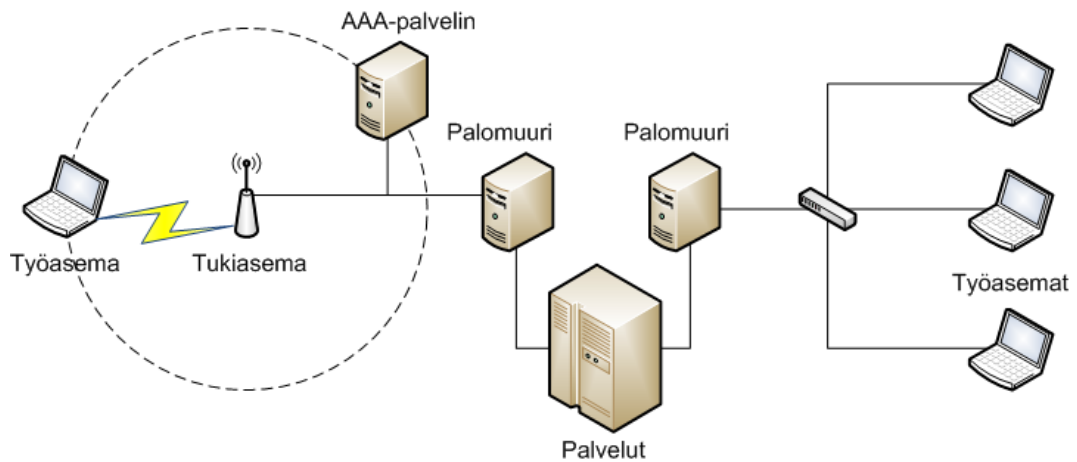
ta käytettäessä yksittäinen käyttäjä on tunnistettavissa myös WLAN-verkossa ja hänen toimenpiteitään voidaan seurata ja myöhemmin todentaa. Ylläpito joutuu kuitenkin lisäämään jokaisen uuden kävijän palvelimeen. Esijaetulla avaimella ylläpidon taakka on kevyempi ja alkuinvestoinnit eivät ole yhtä suuret kuin palvelinta käytettäessä. Käytännössä WPA2-yhteensopivat laitteet ovat olleet markkinoilla jo niin kauan, että yrityksen ei kannata ottaa riskiä ja käyttää jotakin muuta heikompaa suojausta.

### 3.3.3 Pankki

Pankilla on paljon hyvin luottamuksellista tietoa, joka on pidettävä salaisena ja muuttumattomana. Lisäksi tietomurto pankin palveluihin olisi isku sen imagolle ja voisi aiheuttaa sille rahallista haittaa. On siis ensiarvoisen tärkeää pitää ulkopuoliset poissa verkosta. Verkon saatavuutta voidaan heikentää, jos se vähentää hyökkäyksien riskiä (esimerkiksi estää verkon laajentaminen niin, että se on havaittavissa pankin rakennuksen ulkopuolella). Verkon liikenne on myös salattava, koska siinä käsitellään salaisia tiedostoja. Yrityksellä on käytössään ylläpitohenkilökuntaa myös WLAN-verkon ylläpitoon ja rahaa verkon rakentamiseen ja laitteiston ylläpitoon.

Kun kyseessä on yritys, jolla on näin paljon äärimmäisen salaista tietoa on yksi ratkaisumalli WLAN-verkon rakentamiseen se, että verkko jätetään kokonaan rakentamatta. Tämä on mahdollista, jos yritys kokee että verkko ei tuo tarpeeksi arvoa sen tuomiin riskeihin nähden. Toinen lähestymistapa on jättää verkko täysin avoimeksi ja estää palomuurein kaikki muu kuin VPN- ja IPSec-verkkoliikenne. Tällöin verkon turva voidaan ohittaa ja tutkia vain näiden menetelmien antamaa turvaa tilanteissa, jossa liikennettä voidaan kuunnella. WLAN-suojauksia käytettäessä on kuitenkin syytä jakaa verkko osiin, jossa WLAN-verkosta on pääsy vain tarkkaan rajoitettuihin palvelimiin ja palveluihin. Kuva 3.1 havainnollistaa verkkojakoa.

Pankki ei voi käyttää salaista SSID-nimeä, staattisia IP-osoitteita, MAC-suodatusta tai WEP-suojausta verkkonsa suojaamiseen, sillä ratkaisujen tietoturva ei ole pankin edellyttämällä tasolla ja ne ovat liian helposti murrettavissa. Yrityksellä on lisäksi selvä tarve 802.1X-palvelimelle, jotta verkossa tehtäviä toimenpiteitä voidaan valvoa yksilötasolla. 802.1X-palvelin lisää ylläpidon työmäärää, koska he joutuvat luomaan käyttäjiä palveluun, mutta pankin tapauksessa on suotavaa että verkkoon ei päästetä kuin henkilöitä joilla on siihen tarvittava lupa. Jos pankki käyttää WLAN-verkkoa, on sillä myös varaa päivittää WPA2-yhteensopimattomat laitteet, jotta se voi käyttää WPA2-suojausta. WPA2 käyttää AES-salausalgoritmia, joten kaapatun verkkoliikenteen purkaminen ilman avain-



Kuva 3.1: Yrityksen WLAN-verkko palveluineen.

ta on vaikeaa.

### 3.4 Kahvilat

Kahvilat ovat erillinen tapaus, koska ne voivat tarjota internet-käyttöä oheispalveluna (mahdollisesti ilmaiseksi), mutta eivät ole riippuvaisia siitä. Kahvilan verkossa ei ole salattavaa tietoa. Kahvilalle on tärkeää että verkkoon on asiakkaalle yksinkertaista liittyä ja verkko on saatavilla vain kahvilan alueella. Verkon liikenteen salaaminen ei ole pakollista, vaan voidaan jättää asiakkaiden tehtäväksi. Liikenteen rajoittaminen voi tulla kysymykseen, jotta yksi asiakas ei käytä koko palvelun kaistaleveyttä. Verkkoon liittymistä on kuitenkin tarpeen valvoa, jotta maksamattomat asiakkaat eivät pääse verkkoon. Kahvila ei halua maksaa verkosta paljoa, koska se on sille vain oheispalvelu eikä kahvilalla ole erillistä henkilökuntaa verkon ylläpitämiseen. Samalla periaatteella toimivat myös hotellit ja muut vastaavat palveluyritykset.

Kahvilalle ei käy salainen SSID-nimi, staattinen IP-osoite eikä MAC-suodatus. Ensimmäinen ei suojaa verkkoa maksamattomilta käyttäjiltä, toinen vaatii liikaa käyttäjältä ja viimeinen lisää liikaa töitä kahviloiden henkilökunnalle. Autentikaatiopalvelin tuo liikaa ominaisuuksia, joita verkko ei tarvitse (mm. käyttäjäkohtaiset avaimet) ja maksaa enemmän kuin muut toteutustavat.

WEP on hyvä ratkaisumalli tällaiselle verkolle, jossa liikenteen salaamista ei tarvita. Haittapuolena verkkoavain on helppo selvittää verkkoliikenteestä luvattoman

pääsyn mahdollistamiseksi verkkoon. Jos verkkoavainta vaihdetaan säännöllisesti, esimerkiksi päivittäin, ja satunnainen maksamaton asiakas hyväksytään niin WEP riittää kahvilan verkon suojaukseksi. Kuitenkin WPA ja WPA2 esijae-tulla avaimella ovat parempia ratkaisutapoja, koska maksamattomat asiakkaat eivät voi selvittää verkkoavainta verkkoliikenteestä. Käyttönoton hinta WPA:ta käytettäessä on sama kuin WEP:llä ja lähes kaikkien käyttäjien laitteet tukevat WPA-suojauksia, joten kahvilalla ei kuitenkaan ole syytä käyttää WEP-suojauksia WPA-suojauksen sijaan.

HTTP-autentikointi on paras ratkaisu kahviloille, jotka myyvät internet-käyttöaika-aa. Se mahdollistaa käyttäjäkohtaisen seurannan, jolloin yhteydet voidaan sulkea kun aika tai siirtoraja on kulutettu loppuun. Lisäksi WLAN-verkko voidaan jättää avoimeksi, jolloin se ei aseta rajoitteita laitteille. Järjestelmä kuitenkin vaatii enemmän ylläpitoa ja laitehankintoja kuin WLAN-verkon suojaaminen sen omil-la menetelmillä, jolloin järjestelmä on kannattava vain kun verkkoaikaa myydään asiakkaille.

# Luku 4

## Yhteenvedo

Langattomien verkkojen yleistyessä on syytä tarkastella myös niiden tietoturva, jotta vihamieliset käyttäjät eivät voi käyttää verkkoa luvatta. Lisäksi verkkoon tunkeutujille avautuu useimmiten pääsy arkaluontoiseen dataan ja tietomurto voi olla riski imagolle.

Kaikista menetelmistä huomattiin että niille on teoreettisia hyökkäyksiä ja edellytys hyvälle turvatasolle on valitun tietoturvapolitiikan ja hyvien tietoturvaprosessien noudattaminen. Käsitellyistä menetelmistä ainoastaan WEP, WPA sekä WPA2 keskittyvät kaiken verkkoliikenteen suojaamiseen kättelymenetelmän jälkeen. Kaikki tukevat sekä esijaettuja avaimia että AAA-palvelinten käyttöä. WEP ei kuitenkaan tarjoa lähellekään samantasoisia turvaa kuin seuraajansa ja se on purettavissa yksinkertaisilla internetissä tarjottavilla työkaluilla yleensä minuuteissa.

WPA kehitettiin parannukseksi, kun WEP-suojauksen viat havaittiin. Se poistaa löydetty haavoittuvuudet ja on silti toteutettavissa samalla laitealustalla kuin WEP. Itse algoritmit ovat pysyneet samoina, ainoastaan niiden käyttötapaa on muutettu. WPA2 taas kehitettiin puhtaalta pöydältä tarjoamaan enemmän turvaa käyttämällä kehittyneempää salausta (AES RC4-salauksen sijaan), liikenteen seuranta ja todennusta (CCMP-protokolla). Vaikka WPA ja WPA2 ovat viimeaikoina saaneet osakseen negatiivista huomiota, ovat ne silti käytännössä murtamattomia oikein käytettynä.

Eri käyttökohteisiin on tarpeen erilaiset menetelmät. Koteihin ja pienyrityksiin esijaetun avaimen WPA voi olla täysin riittävää turvaa, mutta suuryritysten täytyy miettiä halutaanko verkkoa altistaa lainkaan langattomien verkkojen tuomille uhille. Tällaisessa ympäristössä WPA2 erillisillä AAA-palvelimilla on turvallisin vaihtoehto. Kahvilat ja vastaavat yritykset eivät välttämättä tarvitse liikenteen suojaamista, jolloin HTTP(S)-pohjainen autentikaatio on paras lähtökohta. Lisäk-

si on myös syytä käydä läpi verkon tuoma hyöty sen kustannuksiin ja riskeihin nähden.

# Kirjallisuutta

- Bhagyavati, Wayne C. Summers ja Anthony DeJoie. Wireless security techniques: an overview. *Proceedings of the 1st annual conference on Information security*, sivut 82–87, 2004.
- Halil Ibrahim Bulbul, Ihsan Batmaz ja Mesut Ozel. Wireless network security: comparison of wep (wired equivalent privacy) mechanism, wpa (wi-fi protected access) and rsn (robust security network) security protocols. *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, 2008.
- Nancy Cam-Winget, Russ Housley, David Wagner ja Jesse Walker. Security flaws in 802.11 data link protocols. *Communications of the ACM*, 46(5):35–39, toukokuu 2003.
- Sheila Frankel, Bernard Eydt, Les Owens ja Karen Scarfone. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Tekninen raportti, National Institute of Standards and Technology, 2007.
- Rupinder Gill, Jason Smith ja Andrew Clark. Experiences in passively detecting session hijacking attacks in iee 802.11 networks. *ACM International Conference Proceeding Series; Vol. 167*, sivut 221–230, 2006.
- Global Secure Systems. WiFi is no longer a viable secure connection, 2008. URL <http://www.gss.co.uk/news/article/5503/>. Global Secure Systems WWW-uutisarkisto. Viitattu 15.11.2008.
- IEEE 802.11 Working Group. IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements, kesäkuu 2007.
- IEEE Computer Society. IEEE Std 802.1X - 2004 – Port-Based Access Control, maaliskuu 2004.

Vebjørn Moen, Håvard Raddum ja Kjell J. Hole. Weaknesses in the temporal key hash of wpa. *ACM SIGMOBILE Mobile Computing and Communications Review*, 8(2):76–83, huhtikuu 2004.

Steve Riley. Mitigating the Threats of Rogue Machines – 802.1X or IPsec?, 2005. URL <http://technet.microsoft.com/en-us/library/cc512611.aspx>. Microsoft TechNet WWW-arkisto. Viitattu 15.11.2008.

Erik Tews, Ralf-Philipp Weinmann ja Andrei Pyshkin. Breaking 104 bit WEP in less than 60 seconds. Tekninen raportti, Darmstadt Technical University, 2007. URL <http://eprint.iacr.org/2007/120.pdf>.

Wi-Fi Alliance. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks, huhtikuu 2003.

Wi-Fi Alliance. Wi-Fi Alliance to Certify Pre-Standard IEEE 802.11n Products Next Year, 2008. URL <http://www.wi-fi.org/news/pressrelease-082906-80211n/en/>. Wi-Fi Alliance Press Room. Viitattu 21.11.2008.