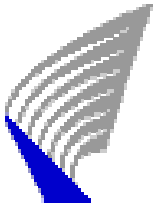


TEKNILLINEN KORKEAKOULU
SÄHKÖ- JA TIETOLIIKENNETEKNIIKAN OSASTO

Marko Ahvenainen

Langattomien Lähiverkkojen Turvallisuus

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi
diplomi-insinöörin tutkintoa varten Espoossa 30.09.2003

Työn valvoja	Professori Jorma Jormakka
Työn ohjaaja	TkL. Markus Peuhkuri

TEKNILLINEN KORKEAKOULU **DIPLOMITYÖN TIIVISTELMÄ**

Tekijä:	Marko Ahvenainen	
Työn nimi:	Langattomien lähiverkkojen turvallisuus	
Päivämäärä:	30. syyskuuta 2003	**Sivumäärä**: 80
Osasto:	Sähkö- ja tietoliikennetekniikan osasto	
Professuuri:	Tietoverkkotekniikka	**Koodi:** S-38
Työn valvoja:	Professori Jorma Jormakka	
Työn ohjaaja:	Markus Peuhkuri, TkL.	

Tässä diplomityössä tutustutaan IEEE 802.11 -standardin mukaisten langattomien lähiverkkojen turvallisuuspiirteisiin. Kirjallisuuslähteiden, spesifikaatioiden ja kokeiden avulla perehdytään eri ratkaisuiden tarjoamiin mahdollisuuksiin ja hyökkäyksiin niitä vastaan. Työn tavoitteena on analysoida eri turvallisuusratkaisuiden soveltuvuutta korkeaa turvallisuustasoa edellyttävän langattoman verkon komponenteiksi.

Työn aluksi käydään lyhyesti läpi IEEE 802.11 -standardin mukaisen langattoman lähiverkon rakenne ja toiminnan periaatteita. Seuraavaksi perehdytään eri turvallisuusratkaisuihin ja analysoidaan niiden toimintaa sekä tehokkuutta. Turvallisuusratkaisuiden esittelyn jälkeen tutustutaan niitä vastaan olemassa oleviin hyökkäyksiin ja kokeellisessa osuudessa suoritetaan muutamia hyökkäyksiä testiverkkoa vastaan.

IEEE 802.11 -standardissa määritellyt turvallisuuskomponentit ovat osoittautuneet heikoiksi. Kehittyneempien ratkaisuiden standardoinnin puute on pitkään vaivannut esiin tulleiden langattomien lähiverkkojen turvallisuusongelmien ratkaisua. Eri valmistajilla on omia vaihtoehtojaan turvallisuuden takaamiseksi ja Wi-Fi Allianssin WPA-ratkaisun kanssa yhteensopivat laitteet tuovat osan kehittyneemmistä turvallisuusmenetelmistä käyttäjien ulottuville jo nyt, mutta ennen IEEE 802.11i -standardin ratifiointia ei ole tarjolla standardoitua vaihtoehtoa. IEEE 802.11i -standardin mukaisten turvallisuusratkaisuiden tehokkuus selviää lopullisesti vasta yhteensopivien laitteiden tultua markkinoille ja ratkaisuiden jouduttua todelliseen testiin.

Avainsanat:	IEEE 802.11, IEEE 802.11i, WLAN, langaton lähiverkko, turvallisuus, WPA

HELSINKI UNIVERSITY OF TECHNOLOGY **ABSTRACT OF THE MASTER'S THESIS**

Author:	Marko Ahvenainen
Name of the Thesis:	Wireless LAN security
Date:	September 30, 2003 **Number of pages:** 80
Department:	Department of electrical and communications engineering
Professorship:	Networking Technology **Code:** S-38
Supervisor:	Professor Jorma Jormakka
Instructor:	Markus Peuhkuri, Lic.Sc.(Tech.)

In this thesis the security features of IEEE 802.11 compliant wireless local area networks are studied. The possibilities of different security solutions and attacks against them are evaluated by conducting a literal study and demonstrations. The objective is to analyse the suitability of different security solutions in a high security WLAN.

The first part of the thesis briefly describes the construction and operation of a IEEE 802.11 compliant wireless network. The next part focuses on different security solutions and analyses their operation and efficiency. After the security solution introduction the attacks against different solutions are described and some of the attacks are performed in the test network.

The security solutions of the IEEE 802.11 standard have proven to be weak. The lack of more advanced security standards has been a problem for a long time when trying to solve the security issues of WLANs. Different manufacturers have their own solutions to ensure security and WI-FI Alliance's WPA solution makes some of the advanced security features available for the users already today but prior the ratification of the IEEE 802.11i standard no standardized solution is available. The security features of the IEEE 802.11i standard are yet to be tested after the standard is ratified and compliant products are available.

Keywords: IEEE 802.11, IEEE 802.11i, WLAN, security, WPA

Alkulause

Tämä diplomityö on tehty Teknillisen Korkeakoulun Tietoverkkolaboratoriossa osana langattomien verkkojen turvallisuutta tutkivaa projektia. Projektissa tekemäni tutkimus on ollut mielenkiintoista ja opettanut minulle paljon uutta tutkimuksen aihepiiristä.

Haluan kiittää työn valvojaa, professori Jorma Jormakkaa, rakentavasta ja erittäin nopeasta palautteesta työn aikana. Haluan lisäksi kiittää työn ohjaajaa, TkL. Markus Peuhkuria, hänen työn aikana antamistaan neuvoista. Markuksen kokemuksesta oli merkittävästi apua testiverkon rakentamisessa sekä työn ongelma-alueiden kartoittamisessa. Kiitokset myös kaikille muille työn valmistumista edesauttaneille tahoille.

Lopuksi haluan vielä kiittää perhettäni ja ystäviäni henkisestä tuesta koko opintotaipaleeni aikana sekä erityisesti Maaritia hänen antamastaan loputtomasta kannustuksesta työn valmistumista odotellessa.

Espoossa 30.09.2003

Marko Ahvenainen

Sisällysluettelo

Lyhenneluettelo

3DES	Triple DES
ACK	Acknowledgement
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AP	Access Point
ARP	Address Resolution Protocol
ATIM	Announcement Traffic Indication Message
BKR	Broadcast Key Rotation
BSS	Basic Service Set
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCM	Counter mode with CBC-MAC
CCMP	CCM Protocol
CRC-32	Cyclic Redundancy Check 32
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTR	Counter mode
CTS	Clear To Send
DCF	Distributed Coordination Function
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DoS	Denial of Service
DS	Distribution System
DSS	Distribution System Services
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
FCS	Frame Check Sequence
FHSS	Frequency Hopping Spread Spectrum
GHz	Gigahertsi
GPS	Global Positioning System
GSM	Global System for Mobile communication
HR-DSSS	High Rate DSSS
http	Hypertext Transfer Protocol
IBSS	Independent Basic Service Set
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IR	Infrared
IV	Initialization Vector
KSA	Key Scheduling Algorithm
L2TP	Layer 2 Tunneling Protocol
LEAP	EAP-Cisco Wireless
LLC	Logical Link Control

MAC	Medium Access Control
MB	Megabyte
Mbps	Megabits per second
MIC	Message Integrity Check
MitM	Man in the Middle
MSDU	MAC Service Data Unit
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OCB	Offset Codebook Block mode
OFDM	Orthogonal Frequency Division Multiplex
OPIE	Open Palmtop Integrated Environment
PC	Personal Computer
PEAP	Protected EAP
PKI	Public Key Infrastructure
PLCP	Physical Layer Convergence Protocol
PRGA	Pseudo Random Generation Algorithm
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial-In User Service
RSN	Robust Security Network
RTS	Request To Send
SIM	Subscriber Identity Module
SNAP	SubNetwork Access Protocol
SS	Station Services
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TSC	TKIP Sequence Counter
TKIP	Temporal Key Integrity Protocol
TLS	Transport Level Security
TTAK	TKIP mixed Transmit Address and Key
TTLS	Tunneled TLS
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless-Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WRAP	Wireless Robust Authenticated Protocol
XOR	Exclusive OR

Lista kuvista

Lista taulukoista

Lista algoritmeista

1 Johdanto

Langattomat lähiverkot (WLAN, Wireless LAN) ovat yleistyneet viime vuosien aikana nopeasti sekä yksityiskäyttäjien että yritysten käytössä. Niiden rakentamisen edullisuus ja langattomuuden tarjoama vapaus liikkua ovat suurimpia innoittajia ajamaan langatonta vallankumousta eteenpäin. Uusimmat laitteet on mahdollista ottaa käyttöön suoraan laittamalla virrat päälle ja verkko toimii ilman monimutkaisia lisäasetuksia. Suorituskyvyltäänkin uusimmat ratkaisut ovat riittäviä kilpailemaan perinteisten lankavaihtoehtojen rinnalla.

Verkolta vaadittavat turvallisuusominaisuudet riippuvat sen käyttökohteesta. Yksityiskäyttäjälle tärkeintä on käytön yksinkertaisuus sopivaa verkkoratkaisua valittaessa. Yritys- ja viranomaiskäytössä monissa sovelluksissa verkon turvallisuusvaatimukset nousevat helppokäyttöisyyden ohi valintakriteereitä mietittäessä. Verkon turvallisuudella tarkoitetaan yleisesti siirrettävän tiedon luottamuksellisuutta ja oikeellisuutta sekä palveluiden saatavuutta. Siirrettävän salaisen liikenteen paljastuminen tai muuttuminen siirron aikana estetään käyttämällä salausta ja eheydentarkastusta sekä rajoittamalla verkkoon pääsyä. Palveluiden saatavuuden varmistamiseksi huolehditaan verkon kapasiteetin riittävyydestä ja palveluiden saatavuutta vastaan kohdistuvien hyökkäyksien torjunnasta.

Langattomassa ympäristössä verkkoa ei voida fyysisesti rajata tiettyyn alueeseen. Siirtomedian tuoma avoimuus asettaa erityisiä haasteita verkon turvallisuuden takaamiselle, jos halutaan saavuttaa langallista ratkaisua vastaava turvallisuustaso. Langattomasti lähetettävä liikenne on kaikkien signaalin kantaman sisäpuolella olevien kuultavissa, joten salauksen merkitys korostuu entisestään. Luvaton verkkoon liittyminen on myös helpompaa kuin lankaverkon tapauksessa ja pääsynhallinnasta on huolehdittava verkon turvallisuuden ja käytössä olevan rajallisen kaistanleveyden riittävyyden varmistamiseksi. Palveluiden saatavuuden varmistamisen kannalta langaton siirtomedia aiheuttaa ongelmia, sillä sen tukkiminen ja palvelunestohyökkäyksien toteuttaminen on yksinkertaisempaa kuin lankaverkossa.

Tämän työn tarkoituksena on tutkia eri langattomien lähiverkkoratkaisuiden tietoturvaominaisuuksia. Työssä keskitytään turvallisuuteen ja hyökkäyksiin protokollatasolla. Hyökkäykset, jotka perustuvat radiosignaalin häirintään on jätetty työn ulkopuolelle. Työn alussa käsitellään kirjallisuuslähteiden ja spesifikaatioiden pohjalta jo tarjolla olevia turvallisuusmekanismeja ja tutustutaan lähitulevaisuudessa markkinoille tuleviin kehittyneempiin ratkaisuihin. Turvallisuusratkaisuihin perehtyminen alkaa toisessa kappaleessa IEEE 802.11 -standardin toiminnan esittelyllä. Kolmannessa kappaleessa käydään ensin läpi standardissa mukana olevat sekä muut yleisesti käytössä olevat turvallisuusratkaisut ja siirrytään käytössä olevien

kehittyneempien ratkaisuiden kautta tulevaisuuden turvallisuusstandardin IEEE 802.11i esittelyyn. Turvallisuusratkaisuita vastaan olemassa olevia hyökkäyksiä ja niiden toteuttamiseen käytettäviä ohjelmistoja käsitellään neljännessä kappaleessa. Viides kappale alkaa langattomia lähiverkkoja hyödyntäviä järjestelmiä vastaan suoritettavien hyökkäysskenaarioiden esittelyllä ja eri skenaarioita torjuvien puolustusmenetelmien suunnittelulla. Kappaleen lopussa esitellään demonstraatioverkossa suoritettavien turvallisuuden perusratkaisuita vastaan kohdistuvien hyökkäyksien toteuttamista. Kuudes kappale kerää työn johtopäätökset yhteenvedoksi.

2 Langattomat lähiverkot

Langattomien lähiverkkojen toteuttamiseen on olemassa useita vaihtoehtoja käyttökohteesta ja ominaisuusvaatimuksista riippuen. Markkinoilla on saatavilla useisiin eri standardeihin ja teknologioihin perustuvia laitteita. Esimerkiksi HiperLAN, HomeRF, Bluetooth ja IEEE 802.11 -standardien mukaiset laitteet ovat löytäneet omat asiakasryhmänsä. Näistä IEEEn [1] Ethernet-standardiin perustuva IEEE 802.11 ja etenkin sen IEEE 802.11b versio on yleistynyt tällä hetkellä suosituimmaksi ratkaisuksi. ETSIn kehittämä HiperLAN [2] on vakavin kilpailija IEEE 802.11 ratkaisuille tarjoten vastaavaa suorituskykyä. HomeRF [3] kärsii pienistä nopeuksista ja Bluetooth [4] kantaman lyhyydestä.

Tässä työssä keskitytään IEEE 802.11 -standardiin perustuviin ratkaisuihin. Seuraavassa käydään lyhyesti läpi ratkaisun toiminnan pääperiaatteet ja sen jälkeen keskitytään ilmenneisiin turvallisuusongelmiin sekä vaihtoehtoihin niiden korjaamiseksi.

2.1 IEEE 802.11 -standardin esittely

IEEE 802.11 -standardi [5] sisältää langattoman lähiverkon MAC-tason (Medium Access Control) ja fyysisen tason määrittelyt. Sen ensimmäinen versio ratifioitiin vuonna 1997. Standardin tavoitteena oli määritellä kilpailukykyinen vaihtoehto lähiverkon toteuttamiseen ilman kaapeleita. IEEE 802.11 -standardin mukaisia laitteita on ollut markkinoilla vuodesta 1998 alkaen ja ne ovat saavuttaneet suurimman suosion langattomien lähiverkkovaihtoehtojen joukossa. Standardi elää jatkuvasti ja uusia osia ratifioidaan vastaamaan muuttuneita tarpeita. Sekä fyysinen rajapinta että turvallisuus ovat saaneet ja tulevat jatkossa saamaan kehittyneempiä vaihtoehtoja omissa lisäosissaan.

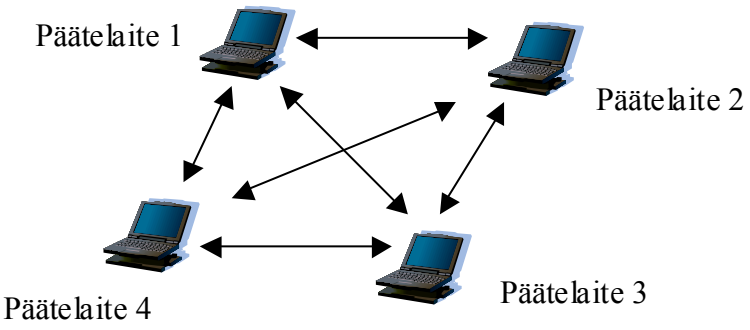
Seuraavissa kappaleissa käydään lyhyesti läpi IEEE 802.11 -standardiin perustuvien verkkojen topologiavaihtoehdot, protokollan tarjoamat palvelut sekä niiden väliset riippuvuudet, MAC-tason perusfunktiot ja fyysisen tason vaihtoehdot.

2.1.1 Verkkoarkkitehtuuri

IEEE 802.11 -standardin mukaiset verkot koostuvat peruspalveluryhmistä (BSS, Basic Service set). BSS on määritelmän mukaan joukko verkon laitteita, jotka voivat keskustella toistensa kanssa joko suoraan tai access pointin (AP) välityksellä. Access point on langattoman verkon rajalla toimiva laite, joka johtaa langattoman verkon toimintaa ja huolehtii yhteyksistä verkon ulkopuolelle. Langattoman verkon muodostavat yleensä useat peruspalveluryhmät, jotka ovat yhteydessä toisiinsa jakelujärjestelmän kautta (DS, Distribution System). Jakelujärjestelmän toteuttamista ei määritellä IEEE 802.11 -standardissa vaan siellä on ainoastaan määriteltyinä palvelut, joita järjestelmän pitää tukea. Langattomat verkot erotellaan toisistaan käyttämällä palveluryhmätunnuksia (SSID, Service Set Identifier). Palveluryhmätunnus on käyttäjän määrittelemä verkkonimi, joka yhdistää samaan loogiseen langattomaan lähiverkkoon kuuluvia laitteita.

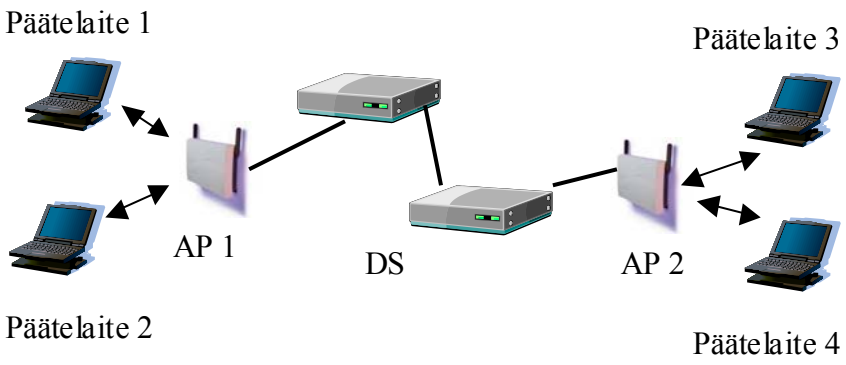
Standardi määrittelee kolme mahdollista verkkotopologiaa, jotka ovat itsenäinen peruspalveluryhmä, infrastruktuuri peruspalveluryhmä ja laajennettu palveluryhmä.

Itsenäinen peruspalveluryhmä (IBSS, Independent Basic Service Set) on yksinkertaisin IEEE 802.11 -standardin mukainen verkko, jota kutsutaan myös Ad-Hoc-verkoksi. IBSS-verkon muodostavat vähintään kaksi päätelaitetta, jotka kommunikoivat keskenään. Liikenne on rajoitettu itsenäisen verkon sisälle ja päätelaitteilla ei ole yhteyttä ulkopuolisiin verkkoihin ja niiden palveluihin. IBSS-verkossa ei ole access pointteja vaan ainoastaan päätelaitteita. IBSS-verkon rakenne on esitettynä kuvassa Kuva 2-1. Itsenäisen verkon ominaisuudet tekevät siitä helpon ja nopean muodostaa, mutta rajoittavat suuresti sen käyttömahdollisuuksia.



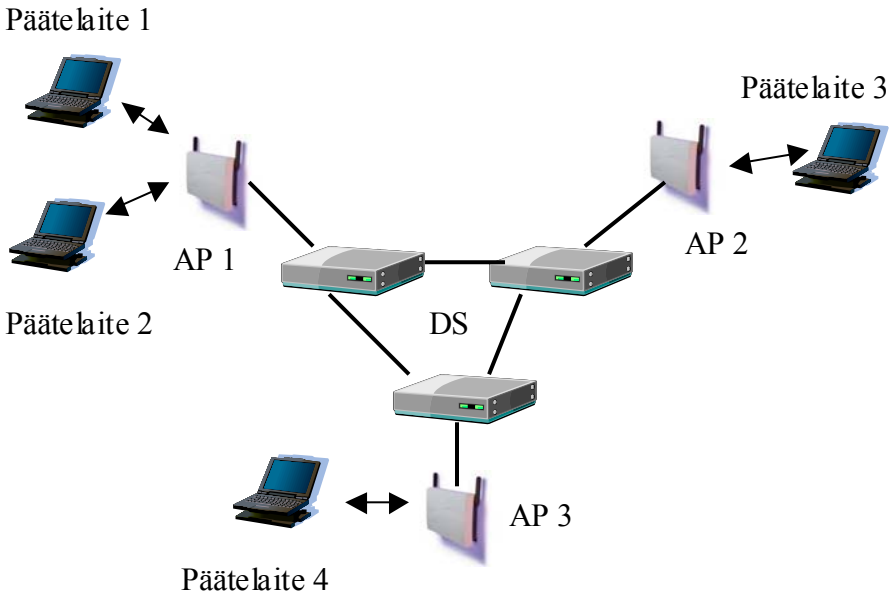
Kuva 2-1 IBSS-verkon topologia

Infrastruktuuri BSS –verkossa (BSS) on vähintään yksi access point. Kaikki verkon päätelaitteet keskustelevat access pointin kanssa. Access point huolehtii päätelaitteiden yhteyksistä sekä toisiinsa että ulospäin verkosta jakelujärjestelmän kautta. Jakelujärjestelmää käytetään yhdistämään eri BSS-verkkoja toisiinsa ja langaton lähiverkko osaksi lankaverkkoa. Kuvassa Kuva 2-2 on esitettynä kaksi BSS-verkkoa kytkettynä yhteen jakelujärjestelmää hyväksikäyttäen.



Kuva 2-2 Infrastruktuuri BSS -verkon topologia

Laajennettu palveluryhmä (ESS, Extended Service Set) koostuu vähintään kahdesta infrastruktuuriverkosta, jotka kytkeytyvät loogiseksi kokonaisuudeksi jakelujärjestelmän avulla. ESS-verkko toimii kuten yksi yhtenäinen infrastruktuuriverkko ja päätelaitteiden on mahdollista siirtyä yhdestä BSS-ryhmästä toiseen. Kuvassa Kuva 2-3 on esitettynä kolmen BSS-ryhmän muodostama ESS.



Kuva 2-3 ESS-verkon topologia

Tässä työssä keskitytään verkkoihin, jotka muodostuvat infrastruktuuriverkoista tai niiden yhdistelmistä. Monet esiin tulevat ratkaisut ja uhat ovat oleellisia myös IBSS-verkoissa, mutta niitä ei tässä työssä käsitellä erikseen.

2.1.2 Palvelut

IEEE 802.11 -standardi määrittelee joukon palveluita, jotka liittyvät arkkitehtuurin eri komponentteihin ja joita MAC-taso käyttää. Palvelut on jaettu kahteen ryhmään

käyttötarkoituksensa mukaan. Palveluryhmät ovat asemapalvelut (SS, Station Services) ja jakelujärjestelmäpalvelut (DSS, Distribution System Services).

2.1.2.1 Asemapalvelut

Jokaisen päätelaitteen ja access pointin on tarjottava standardin määrittelemät neljä asemapalvelua, jotka ovat MSDU-toimitus (MAC Service Data Unit, MAC palvelu data yksikkö), yksityisyys, todentaminen ja todennuksen purku.

MSDU-toimitus on peruspalvelu, jonka tehtävänä on taata luotettava tiedonsiirto langattoman yhteyden ylitse. Muiden palveluiden tehtävänä on auttaa tämän peruspalvelun suorittamisessa.

Yksityisyyspalvelun tavoitteena on suojata verkossa kulkevaa liikennettä. Langattomuus asettaa vaatimuksia salaisen tiedon siirrolle, koska jokainen kuuluvuusalueella oleva päätelaite voi kaapata lähetettävän liikenteen itselleen. Yksityispalvelu toteutetaan WEP-salauksen (Wired Equivalent Privacy) avulla, jota käsitellään tarkemmin kappaleessa 3.1.2.

Todentamispalvelua käytetään rajoittamaan verkkoon pääsyä. Vain todennetut päätelaitteet voivat liikennöidä verkossa. Todentamista varten standardi tarjoaa kaksi vaihtoehtoa, jotka ovat avoin todentaminen ja jaetun avaimen todentaminen. Avoin todentaminen sallii kaikkien päästä verkkoon identiteettinsä toimittamisen jälkeen. Jaetun avaimen todentaminen perustuu WEP-salauksen käyttämiseen ja päästää verkkoon vain salaisen avaimen tuntevat päätelaitteet. WEP-todentaminen toimii haaste-vaste-periaatteen (challenge-response) mukaisesti. Todentamista käsitellään tarkemmin kappaleessa 3.1.1.

Todennuksen purkua käytetään olemassa olevien todennusten päättämiseen. Todennukset puretaan ilmoituksella, joka on pakko hyväksyä.

2.1.2.2 Jakelujärjestelmäpalvelut

Standardi määrittelee jakelujärjestelmälle viisi palvelua, joita sen pitää tukea. Nämä palvelut ovat assosiointi, uudelleenassosiointi, assosioinnin purku, jakelu ja integrointi.

Assosiointipalvelu mahdollistaa päätelaitteen kommunikoinnin jakelujärjestelmän suuntaan. Assosioinnissa päätelaite liitetään tiettyyn access pointtiin ja jakelujärjestelmällä tarjotaan tarvittavat tiedot päätelaitteen saavuttamiseksi. Päätelaite voi kerralla olla assosioituneena vain yhteen access pointtiin.

Uudelleenassosiointia käytetään muuttamaan jo assosioituneen päätelaitteen tietoja. Tämän palvelun avulla voidaan mahdollistaa päätelaitteen siirtyminen yhdestä access pointista toiseen.

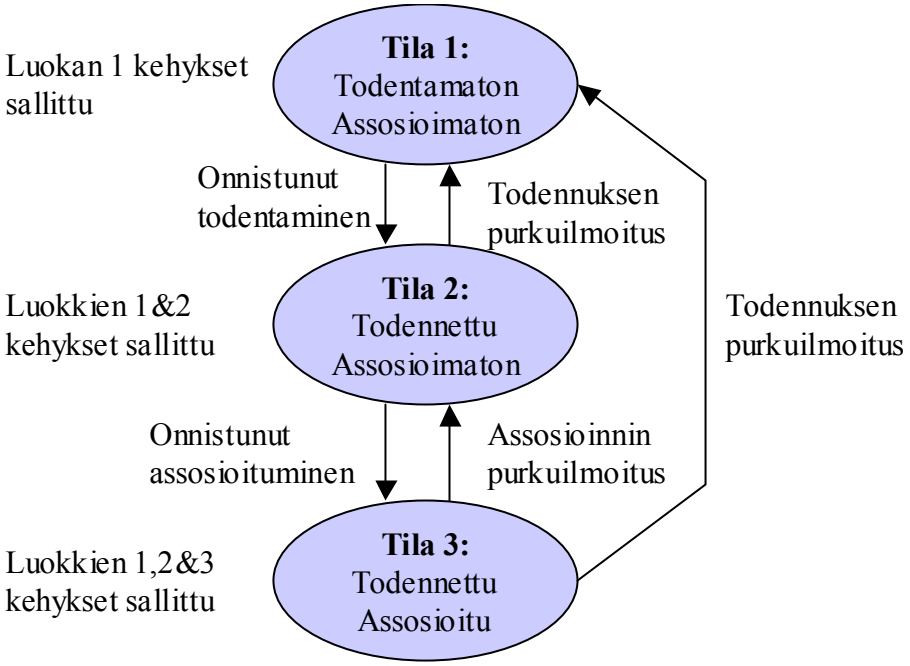
Assosioinnin purkua käytetään purkamaan olemassa olevia assosiaatioita. Purku tapahtuu ilmoituksella, joka on pakko hyväksyä.

Jakelupalvelua käytetään liikenteen lähettämiseen jakelujärjestelmään. Palvelu antaa jakelujärjestelmälle tarvittavat tiedot liikenteen toimittamiseksi oikeaan osoitteeseen.

Integrointipalvelua käytetään kun liikennettä lähetetään jakelujärjestelmän ja IEEE 802.11 -standardista eroavan verkon välillä. Palvelu muuttaa 802.11-kehykset sopivaan muotoon tiedon siirtoa varten.

2.1.2.3 Palveluiden väliset riippuvuudet

Jokainen päätelaite pitää yllä tietoja muista laitteista, joiden kanssa se kommunikoi suoraan. Ylläpidettävät tiedot ovat assosioinnin tila ja todennuksen tila. Eri tilojen väliset siirtymät tapahtuvat kuvassa Kuva 2-4 esitetyn tilakoneen mukaisesti. Ensimmäisestä tilasta siirrytään toiseen kun laite on onnistuneesti todentanut itsensä. Kolmanteen tilaan päästään onnistuneen assosioitumisen jälkeen. Alaspäin siirtyminen tapahtuu todennuksen ja assosioinnin purku -ilmoituksilla. Nämä ilmoitukset ovat ehdottomia, joten purkuviestit mahdollistavat palvelunestohyökkäyksen.



Kuva 2-4 Palveluiden ja tilakoneen väliset riippuvuudet

Laitteen tilasta riippuu mitä kehyksiä se saa lähettää ja vastaanottaa. Kehyksien eri luokilla rajoitetaan todentamattomien ja assosioimattomien laitteiden kykyä liikennöidä verkossa. IEEE 802.11 -standardin määrittelemät kehykset on lueteltuna taulukossa Taulukko 2-1. Hallintapaketteja käytetään yhteyden muodostamiseen päätelaitteiden ja access pointtien välille ja ohjauspaketteja liikenteen siirtoon liittyvään kommunikointiin.

Taulukko 2-1 IEEE 802.11 -standardin mukaiset kehykset [23]

Luokka	Tyyppi	Alityyppi
1	Ohjaus	Lähetyspyyntö (RTS)
1	Ohjaus	Vapaa lähettämään (CTS)
1	Ohjaus	Kuittaus (ACK)
1	Ohjaus	Kilpailuvapaa loppuu
1	Ohjaus	Kilpailuvapaa loppuu + ACK
1	Hallinta	Probe pyyntö/vastaus
1	Hallinta	Majakka (beacon)
1	Hallinta	Todennus
1	Hallinta	Todennuksen purku
1	Hallinta	Ilmoitus liikenteen ilmaisu viesti (ATIM)
1	Data	Data (päätelaitteiden välillä)
2	Hallinta	Assosiointipyyntö/vastaus
2	Hallinta	Uudelleenassosiointipyyntö/vastaus
2	Hallinta	Assosioinnin purku
3	Ohjaus	Tehonsäästökysely
3	Hallinta	Todennuksen purku
3	Data	Data (Jakelujärjestelmien välillä)

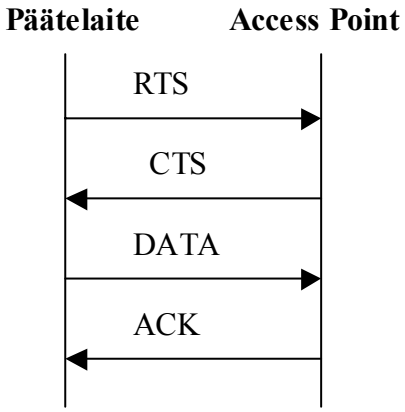
2.1.3 Medium Access Control

MAC-kerroksen tärkein tehtävä on taata luotettava MSDU-pakettien välitys langattoman yhteyden ylitse. MAC-kerros huolehtii myös verkkoon pääsystä ja verkossa liikkuvan tiedon luottamuksellisuudesta.

IEEE 802.11 -standardissa määritellään langattoman median käyttämiseen CSMA/CA-protokolla (Carrier Sense Multiple Access with Collision Avoidance), jonka avulla pyritään välttämään lähetysten törmäykset. CSMA/CA-protokollan mukaisesti laite kuuntelee kanavaa ennen lähetystä ja pyrkii havaitsemaan jo käynnissä olevat lähetykset. Jos kanava on varattu, odottaa laite satunnaisen ajan ennen kuin yrittää uudelleen. Satunnaisen odotusajan tarkoituksena on välttää törmäyksiä tapauksessa, jossa useampi laite odottaa kanavan vapautumista.

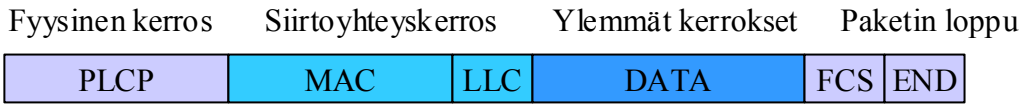
Langattoman median käytössä hyödynnetään hajautettua koordinointifunktiota (DCF, Distributed Coordination Function), jonka toiminta perustuu välittömään kuittaukseen. Viestin vastaanottanut laite lähettää välittömästi viestin jälkeen kuittauksen (ACK, acknowledgement), jotta viestin lähettäjä tietää viestin saapuneen onnistuneesti perille. Jos kuittausta ei tule, ajastaa lähettäjä uudelleenlähetyksen. Langattomassa verkossa kaikki laitteet eivät välttämättä kuule toisiaan ja siten havaitse käynnissä olevia lähetyksiä. BSS-verkossa riittää, että kaikki pystyvät kommunikoimaan access pointin kanssa, joten on mahdollista että piilossa oleva päätelaite on lähettämässä, vaikka toinen päätelaite tulkitsee median vapaaksi. Tällaisen tilanteen välttämiseksi standardi määrittelee hajautettuun koordinointifunktioon kuittausten lisäksi lähetyspyyntöihin perustuvan menetelmän. Lähettämään pyrkivä päätelaite lähettää access pointille lähetyspyynnön (RTS, Request To Send), johon access point vastaa vapaa lähettämään -viestillä (CTS, Clear To Send). Näin kaikki verkon laitteet saavat tiedon, että kanava on

varattuna tietyn aikaa. CTS-viestissä on kerrottuna kuka saa lähettää ja kuinka kauan lähetys kestää. Kuvassa Kuva 2-5 on esitettynä IEEE 802.11 -standardin mukaisten laitteiden käyttämä kättelyprosessi, kun päätelaite lähettää liikennettä access pointille.

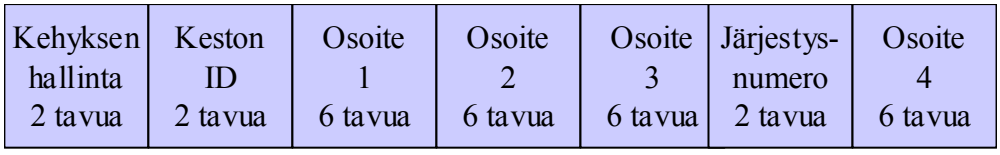


Kuva 2-5 802.11-laitteiden kättelyprosessi

IEEE 802.11b -standardin mukaiset kehykset ovat langattoman ympäristön vuoksi monimutkaisempia kuin vastaavanlaisten lankaverkkojen kehykset. Jaettu dynaaminen media aiheuttaa omat vaatimuksensa ja luotettavan yhteyden luominen edellyttää lisää protokollalta. Kuvassa Kuva 2-6 on esitettynä 802.11b datapaketin rakenne. Paketin alussa on fyysisen kerroksen konvergenssimenetelmä (PLCP, Physical Layer Convergence Protocol), joka sisältää radiokanavan valmistelua varten alustusosan (preamble) ja fyysisen kehyksen. Siirtoyhteyskerroksessa on MAC-otsikko ja valinnainen looginen linkkihallintaosa (LLC, Logical Link Control). MAC-otsikko on esitettynä tarkemmin kuvassa Kuva 2-7. MAC-otsikossa on kehyksenhallintaosa, joka määrittelee minkälainen kehys on kyseessä, ja kehyksen keston pituus. Lisäksi otsikossa on neljä osoitetta ja järjestysnumero pakettien hallintaa varten. Dataosuuden jälkeen on paketin lopusta ilmoittava osuus, jossa on kehyksen tarkistusnumero (FCS, Frame Check Sequence) ja lopetusmerkit.



Kuva 2-6 802.11b-paketin rakenne



Kuva 2-7 802.11b MAC -otsikko

2.1.4 Fyysinen kerros

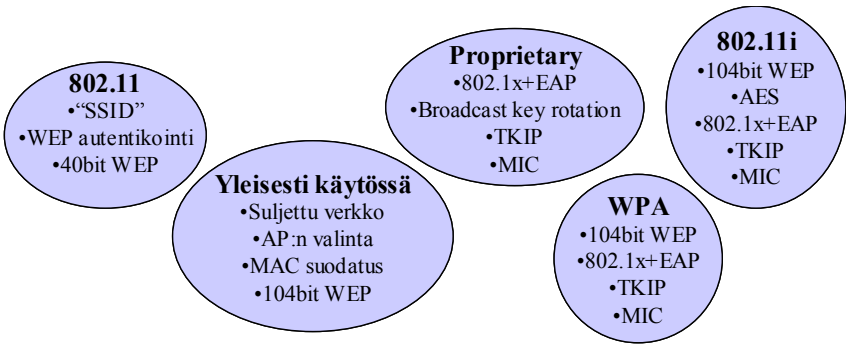
Fyysisen kerroksen tehtävänä on tarjota MAC-kerrokselle palveluita, jotta yhteistoiminta jaetun langattoman median kanssa onnistuu. Fyysinen kerros huolehtii langattoman median varausten havaitsemisesta ja liikenteen lähettämisestä sekä vastaanottamisesta. IEEE 802.11 -standardissa määritellään kolme vaihtoehtoa fyysiselle kerrokselle, jotka ovat taajuushyppelevä hajaspektri (FHSS, Frequency Hopping Spread Spectrum), suorasekvenssi hajaspektri (DSSS, Direct Sequence Spread Spectrum) ja infrapuna (IR, infrared). FHSS ja DSSS toimivat 2,4 GHz lisensoimattomalla taajuusalueella. Kaikki vaihtoehdot tarjoavat 1 ja 2 Mbps nopeuksia. Standardia on laajennettu määrittelemällä siihen lisää fyysisen kerroksen vaihtoehtoja, jotka tarjoavat suurempia nopeuksia. IEEE 802.11a [6] toimii 5 GHz taajuudella ja tarjoaa monikantoaaltomodulointia (OFDM, Orthogonal Frequency Division Multiplex) käyttäen nopeuksia aina 54 Mbps asti. IEEE 802.11b [7] käyttää suurnopeus DSSS (HR-DSSS, high rate DSSS) modulaatiota ja kasvattaa 2,4 GHz alueella toimivan ratkaisun nopeutta 11 Mbps. Lisää fyysisen kerroksen vaihtoehtoja on työn alla omissa työryhmissään ja markkinoilla on jo olemassa laitteita, jotka tukevat näitä luonnosvaiheessa olevia standardeja.

3 WLAN ja turvallisuus

Langattoman lähiverkon turvallisuus koostuu kahdesta osa-alueesta, liikenteen salauksesta ja käyttäjäntunnistuksesta eli todentamisesta. Langattoman siirtomedian luonteen vuoksi tarvitaan lisäksi menetelmiä tiedon eheyden tarkistamiseen.

Kokonaisvaltainen turvallisuusratkaisu muodostuu useista osista, jotka toisiaan täydentäen mahdollistavat turvallisen verkon rakentamisen. Osia sopivasti yhdistämällä pystytään saavuttamaan kuhunkin tilanteeseen soveltuva turvallisuustaso. Nykyiset standardoidut ratkaisut toimivat vain tiettyyn pisteeseen asti ja siitä eteenpäin joudutaan siirtymään valmistajakohtaisiin ratkaisuihin sekä yleensä tinkimään yhteensopivuudesta ja helppokäyttöisyydestä. Uudet turvallisuussovellukset ovat tosin tulossa mukaan uusiin standardeihin ja jo nyt niiden yhteensopivuutta pyritään edistämään monilla tavoin.

Seuraavissa kappaleissa käydään läpi eri vaihtoehtoja langattoman lähiverkon turvallisuusratkaisuiksi lähtien liikkeelle IEEE 802.11 -standardin määrittelemistä vaihtoehdoista ja päätyen valmistajakohtaisien ratkaisujen kautta tulossa olevan IEEE 802.11i -standardin parannettuun turvallisuuteen. Oheinen kuva Kuva 3-1 esittää turvallisuusratkaisuiden kehittymistä.



Kuva 3-1 Langattoman lähiverkon turvallisuusratkaisuita

3.1 IEEE 802.11 -standardin turvallisuus

IEEE 802.11 -standardin sisältämillä turvallisuusratkaisuilla oli tarkoitus taata salaamatonta langallista yhteyttä vastaava turvallisuus langattomaan ympäristöön.

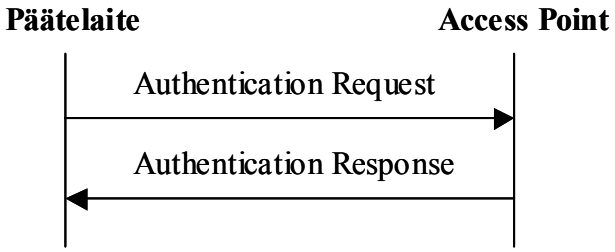
Turvallisuusratkaisua ei ole kuitenkaan määritelty standardissa kokonaan vaan etenkin turvallisuuden hallintaan liittyvät asiat on jätetty standardin ulkopuolelle. Muutenkin helppokäyttöisyyttä on pidetty turvallisuutta tärkeämpänä tavoitteena ja esimerkiksi perusasetukset uusissa laitteissa mahdollistavat verkon käyttöönoton ilman asetuksien muuttamista mutta ilman salausta ja todentamista.

Standardi määrittelee kaksi vaihtoehtoa todentamisen hoitamiseen ja 40-bittisen salauksen. Lisäksi standardissa on pakettien eheyden tarkistamista varten määriteltynä tarkistussumman käyttö.

3.1.1 Todentaminen

Todentamista varten IEEE 802.11 -standardissa on kaksi vaihtoehtoa, avoin todentaminen (open authentication) ja jaetun avaimen todentaminen (shared key authentication). Todentaminen tapahtuu fyysisellä tasolla. [5]

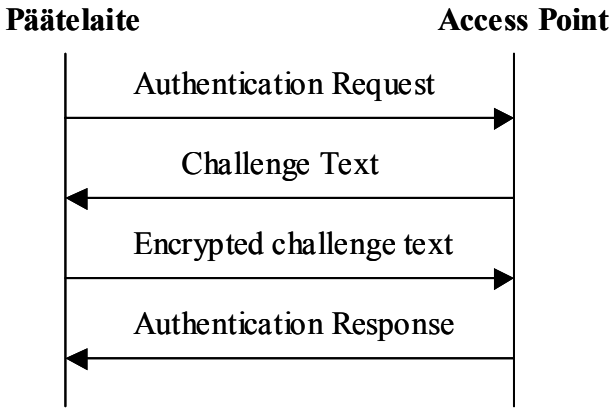
Avoin todentaminen ei oikeastaan ole todentamista ollenkaan vaan kaikki halukkaat pääsevät verkkoon. Avoin todentaminen tapahtuu SSID:n avulla. AP hyväksyy verkkoonsa kaikki halukkaat, joilla on asetettuna sama SSID kuin sillä itsellään. Standardin mukaan lisäksi kaikki päätelaitteet joilla on tyhjä (null) SSID hyväksytään mukaan. Todentaminen tapahtuu kuvan Kuva 3-2 mukaisilla viesteillä.



Kuva 3-2 Avoin todentaminen

SSID ei ole sinällään turvallisuusratkaisu, sillä AP:n lähettämissä majakkapaketeissa (beacon frame) se näkyy salaamattomana. Muutenkin SSID on havaittavissa kaikista hallintapaketeista, joita ei standardin mukaan salata. Osa käyttöjärjestelmistä ja sovelluksista kuuntelee ilmassa kulkevaa liikennettä ja laittaa SSID:n automaattisesti sopivaksi verkkoon liittymistä varten.

Jaetun avaimen todentaminen perustuu WEP-salauksen käyttöön ja on haaste-vaste-tyyppinen todentamismenetelmä. WEP-salauksen periaatteista kerrotaan lisää seuraavassa kappaleessa. Jaetun avaimen todentamisessa AP vastaa todentamispyyntöön lähettämällä haastepaketin, jonka verkkoon haluava päätelaite lähettää WEP-avaimella salattuna takaisin. Jos AP saa purettua salauksen omalla WEP-avaimellaan, on todentaminen onnistunut ja uusi päätelaite liittyy verkkoon. Käyttäjäntunnistusprosessiin liittyvät paketit on esiteltynä kuvassa Kuva 3-3. Jaetun avaimen todentamista käytettäessä vain päätelaitteet, joilla on oikea WEP-avain hallussaan voivat liittyä verkkoon. [5]



Kuva 3-3 Jaetun avaimen todentaminen

3.1.2 Wired Equivalent Privacy

Langaton ympäristö asettaa omat vaatimuksensa tiedon salaukselle, sillä salakuuntelu on huomattavasti helpompaa kuin lankaverkoissa. Salauksen pitää olla tarpeeksi tehokasta kuitenkaan aiheuttamatta huomattavaa verkon suorituskyvyn heikkenemistä. WLAN verkon salauksen hoitamiseen on IEEE 802.11 -standardissa määritelty WEP. WEP on 40-bittinen symmetrinen jonosalausmenetelmä, joka käyttää salaamiseen RSA Data Securityn RC4-algoritmia [8].

RC4 on symmetrinen synkronoitu jonosalausalgoritmi. Samaa avainta käytetään siis sekä tiedon salaamiseen että salauksen purkamiseen. RC4 suorittaa salauksen pienissä osissa bitti kerrallaan. Algoritmin toiminta koostuu kolmesta funktiosta, jotka on esiteltynä algoritmissa Algoritmi 3-1 [9]. Salauksessa käytetään salasanan ja datan lisäksi tilafunktiota, jonka avulla jokainen osa dataa salataan eri tavalla.

$$\text{Tila}_{t+1} = \text{Tilafunktio}(\text{Tila}_t, \text{Salasana}_t)$$
$$\text{Jonoavain}_t = \text{Jonoavainfunktio}(\text{Tila}_t, \text{Salasana}_t)$$
$$\text{Tuloste}_t = \text{Salausfunktio}(\text{Jonoavain}_t, \text{Data}_t)$$

Algoritmi 3-1 Synkronoitu jonosalain

Ensimmäinen käytettävä funktio on KSA (Key Scheduling Algorithm) eli tilafunktio. WEPin tapauksessa, kun käytetään 8-bittistä RC4 algoritmia, lähdetään liikkeelle taulukosta, jossa on 256 8-bittistä arvoa. KSA sekoittaa taulukon salasanan avulla algoritmin Algoritmi 3-2 mukaisesti [9], jolloin saadaan valmis tilamatriisi. Algoritmissa N on 256, S on tilamatriisi, K on salasana ja l on 256.

Alustus :

Kun $i = 0\text{K}\ N-1$

$\text{S}[i] = i$

$j = 0$

Sekoitus :

Kun $i = 0\text{K}\ N-1$

$j = (j + \text{S}[i] + \text{K}[i]) \bmod l$

$\text{Vaihda}(\text{S}[i], \text{S}[j])$

Algoritmi 3-2 KSA

Seuraavana funktiona toimii PRGA (Pseudo Random Generation Algorithm) eli pseudosatunnaisgeneraattori, joka muodostaa jonoavaimen (streaming key) tilamatriisista algoritmin Algoritmi 3-3 mukaisesti [9]. Algoritmissa z on jonoavain ja muut muuttujat kuten KSA:n algoritmissa.

Alustus :

$i = 0$

$j = 0$

Luomissilmukka :

$i = i + 1$

$j = (j + S[i]) \bmod l$

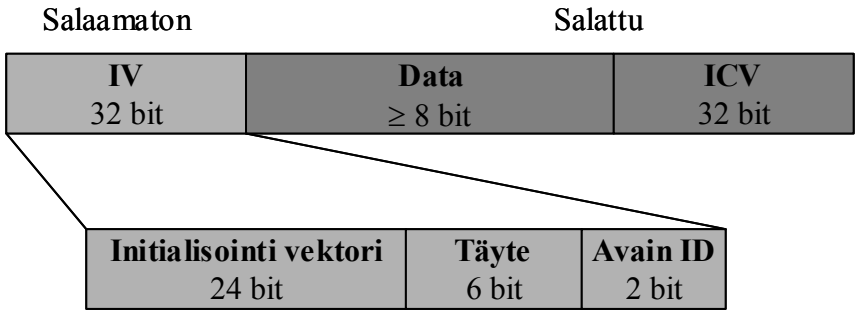
$Vaihda(S[i], S[j])$

$z = S[(S[i] + S[j]) \bmod l]$

Algoritmi 3-3 PRGA

Lopuksi kolmantena funktiona käytetään loogista XOR-operaattoria (exclusive OR), jolla muodostetaan jonoavaimesta ja selväkielisestä viestistä salattu viesti [9]. Salausta purettaessa vastaavasti muodostetaan ensin jonoavain, joka sitten loogista operaattoria käyttäen yhdistetään salattuun tekstiin ja lopputuloksena on jälleen selväkielinen teksti.

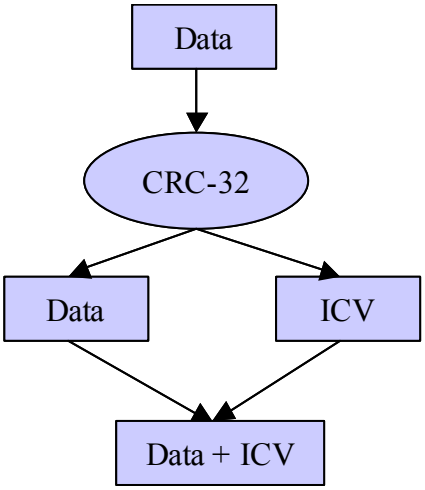
WEPin tapauksessa RC4:n käyttämä salasana on jaetun salaisen avaimen ja alustusvektorin (IV, Initialization Vector) yhdistelmä. Avaimia jokaisessa päätelaitteessa on neljä, joista yhtä kerrallaan käytetään liikenteen salaamiseen ja salauksen purkuun. Vaihtoehtoisesti on mahdollista käyttää jokaiselle yhteydelle omaa avainta. Nämä kohdelähetysavaimet on talletettu jokaiseen päätelaitteeseen taulukkoon kohteen MAC-osoitteiden mukaan järjestettynä. Alustusvektori on 24-bittinen satunnaisluku, joka ketjutetaan salaisen avaimen eteen. IV:n tarkoituksena on parantaa turvallisuutta muuttamalla salaamiseen käytettyä arvoa joka paketille yksilölliseksi. IV kuitenkin lähetetään salaamattomana paketin osoitekentässä. WEP-salatun paketin rungon rakenne on esitettynä kuvassa Kuva 3-4.



Kuva 3-4 WEP-salattu kehys

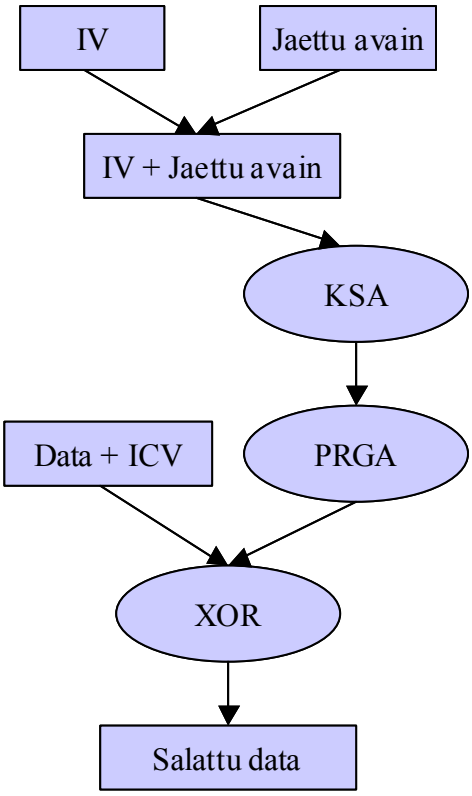
Avainten hallintaa varten IEEE 802.11 -standardissa ei ole esitetty mitään keinoa. Avaimet toimitetaan verkon laitteisiin turvallista standardista riippumatonta tapaa käyttäen. Käytännössä tämä tarkoittaa sitä, että perusratkaisussa avaimet kirjoitetaan käsin jokaiseen päätelaitteeseen ja access pointtiin aina kun niitä vaihdetaan.

WEP prosessi alkaa tarkistussumman laskemisella. Tarkistussumman laskemiseen käytetään lineaarista CRC-32-algoritmia (Cyclic Redundancy Check). Laskettu tarkistussumma liitetään datan perään. Prosessi on kuvattuna kuvassa Kuva 3-5 [9].



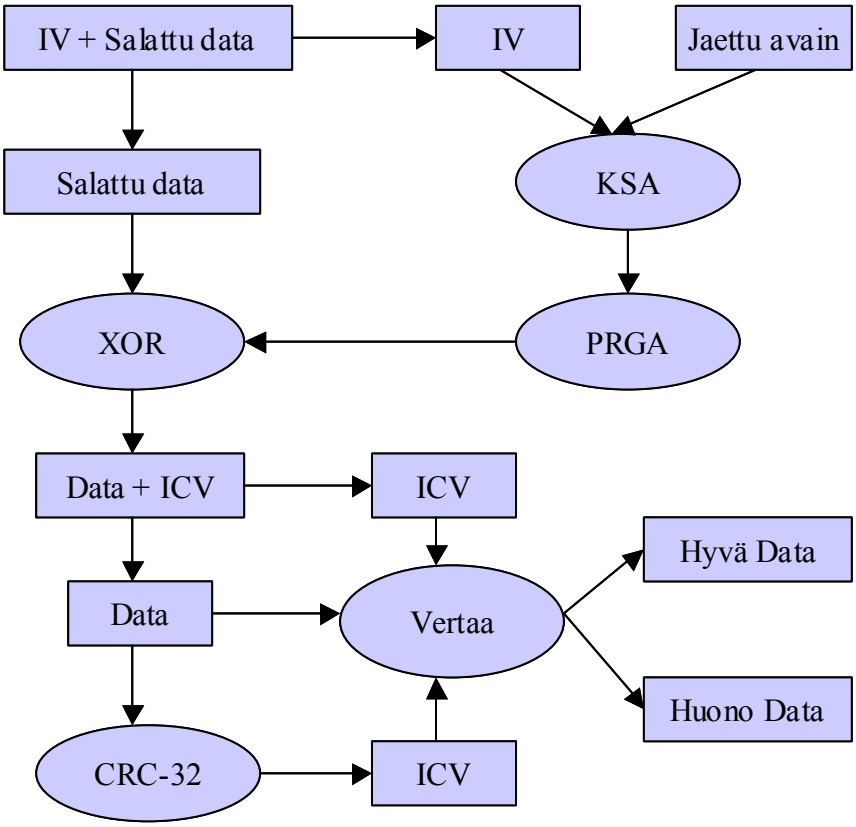
Kuva 3-5 WEP-tarkistussumman laskeminen

Seuraavaksi on vuorossa datan salaus, jota varten muodostetaan jonoavain. Joka paketille valitaan oma alustusvektori, joka liitetään jaetun avaimen eteen. Tämä salasana ajetaan KSA:n läpi, jolloin saadaan tilamatriisi muodostettua. Tilamatriisista PRGA muodostaa jatkuvan muuttuvan jonoavaimen. Salattu data saadaan jonoavaimesta ja datan sekä tarkistussumman yhdisteestä XOR-operaattorin avulla. Tämä vaihe prosessia on esitettynä kuvassa Kuva 3-6 [9].



Kuva 3-6 WEP-salaus

Vastaanottaja tarvitsee salauksen purkamiseen sekä jaetun salaisen avaimen että käytetyn alustusvektorin. Jaettu avain hänellä on jo hallussaan ja IV lähetetään salatun paketin otsikossa salaamattomana. Vastaanottaja muodostaa itselleen salaukseen käytetyn jonoavaimen ja purkaa salauksen. Tiedon eheys tarkistetaan laskemalla datasta tarkistussumma ja vertaamalla saatua tulosta vastaanotettuun tarkistussummaan. Salauksen purkaminen ja eheyden tarkistus on esiteltynä kuvassa Kuva 3-7 [9].



Kuva 3-7 WEP-salauksen purkaminen

WEP-salaus on standardin mukaisesti toteutettuna osoittautunut heikoksi ja on olemassa valmiita ohjelmia, joilla salauksen purkaminen onnistuu, kunhan tarpeeksi salattua dataa on saatavilla. WEPin heikkouksista lisää seuraavassa kappaleessa ja WEP-hyökkäystä käsittelevässä kappaleessa 4.4.

3.1.3 IEEE 802.11 -standardin turvallisuusratkaisuiden heikkoudet

IEEE 802.11 -standardin turvallisuusratkaisuja on arvosteltu heikoiksi monestakin syystä. Heikkouksia löytyy salauksen toteuttamisesta, avainten hallinnoimisesta ja käyttäjäntunnistuksesta.

Eheyden tarkistamiseen käytettävä lineaarinen CRC-32-tarkistussumma on toiminnaltaan heikko. Yksittäisten bittivirheiden havaitsemiseen se soveltuu hyvin, mutta tahallisesti aiheutettujen DoS-hyökkäysten (Denial of Service) torjumiseen sitä ei voi käyttää kuten DoS-hyökkäyksiä käsittelevässä kappaleessa 4.7 myöhemmin tulee ilmi.

IEEE 802.11 -standardin mukaisessa käyttäjäntunnistuksessa on useita heikkoja kohtia. Standardin määrittelyn mukaan todentaminen tapahtuu fyysisellä tasolla. Käyttäjäntunnistuksen jättäminen pelkästään fyysisen tason tehtäväksi etenkin langattomassa järjestelmässä on vaarallista, sillä hyökkääjä voi käyttää hyväkseen jo todennetun päätelaitteen osoitteita. Tällaisia hyökkäyksiä käsitellään myöhemmin lisää.

Jaetun avaimen todentamisen käyttö vaikeuttaa luvattomien päätelaitteiden pääsyä verkkoon mutta samalla heikentää koko salauksen turvallisuutta käyttämällä haaste-vaste-tyyppistä todentamista. Hyökkääjä voi tällöin salakuuntelulla saada haltuunsa sekä salatun datan että saman datan selväkielisenä. WEP-hyökkäyksestä kertovassa kappaleessa tutustutaan tarkemmin tähän heikkouteen. Todentaminen toteutetaan tilattomasti eli todennettava päätelaite voi itse päättää käyttämänsä alustusvektorit. Näin hyökkääjä voi hyödyntää salakuuntelulla hankkimaansa IV-jonosalain-paria ja tuottaa onnistuneesti salattua liikennettä todentamistarkoitukseen. Lisäksi todentaminen suoritetaan vain yhteen suuntaan eli AP todentaa päätelaitteen. Päätelaitteelle ei tarjota näin ollen mahdollisuutta varmistaa onko se yhteydessä oikean AP:n kanssa.

WEP-salauksen heikkous ei ole RC4-algoritmissa vaan salasanan muodostuksessa. Itse RC4-algoritmi on vahva ja käytössä monissa muissakin sovelluksissa. WEPin heikkouksiksi voidaan luetella etenkin staattisten avaimien käyttö ja alustusvektorien toteutus. Staattisten avainten käyttö on suora seuraamus avainten levittämiseen tarkoitetun menetelmän puuttumisesta. Jaettujen avainten turvallisuutta heikentää myös se, että kaikki käyttävät yleensä samoja avaimia ja näin liikennettä avainta kohden tulee enemmän kuin jos jokaisella yhteysparilla olisi oma avain käytössä. Alustusvektoreiden toteutuksessa on useita kohtia jotka heikentävät turvallisuutta. Ensinnäkin vektorit lähetetään salaamattomana. Lisäksi IV-avaruus on 24 bittiä eli erilaisia vektoreita on olemassa suhteellisen pieni määrä verrattuna siihen, kuinka paljon paketteja lähetetään korkean käyttöasteen verkossa. Kun jokaisella paketilla on oma IV niin vektoreita joudutaan käyttämään uudelleen suhteellisen nopeasti. Jo 10 MB tiedoston siirtäminen voi johtaa vektorin uudelleenkäyttöön. Osa käytettävistä alustusvektoreista on heikkoja siinä mielessä että ne paljastavat osia jaetusta salaisesta avaimesta. WEPin heikkouksia käydään läpi enemmän WEP-hyökkäystä käsittelevässä kappaleessa.

WEP-salauksen heikkoutta lisää salasanan tallentaminen päätelaitteeseen. Päätelaitteen joutuessa vihamielisen käyttäjän käsiin voi hän liikennöidä verkossa kuten normaalit käyttäjät. Verkkoon pääsy onnistuu, koska todentaminen suoritetaan päätelaitetasolla. Lisäksi käytetty salainen avain paljastuu, jos se pystytään lukemaan päätelaitteesta selväkielisenä.

Turvallisuuden kannalta huono asia on myös se, että vain dataliikenne salataan. Ohjaus- ja hallintoliikenne sen sijaan lähetetään selväkielisenä. Tämä mahdollistaa ohjausliikenteen salakuuntelua ja palvelunestohyökkäyksiä.

3.2 WLAN-verkon turvallisuuden parantamisen perusratkaisuja

IEEE 802.11 -standardin mukaisten turvallisuusratkaisuiden heikkouksien tultua julki kehittivät laitevalmistajat uusia keinoja turvallisuuden parantamiseksi. Nämä alkujaan valmistajakohtaiset ratkaisut ovat levinneet nykyään jo lähes kaikkiin laitteisiin. Osa tekniikoista on yksipuolisia eli vastapuolen ei tarvitse tukea ratkaisua pystyäkseen liittymään verkkoon. Vastaavasti joidenkin tekniikoiden kanssa saattaa tulla vastaan yhteensopivuusongelmia. Vaikka kahden valmistajan laitteet periaatteessa käyttäisivätkin samaa ratkaisua, voi toteutuksissa olla ratkaisevissa kohdissa pieniä eroja.

Lucent kehitti ensimmäisenä suljetun verkon -käsitteen (closed network) [10]. Suljetulla verkolla tarkoitetaan IEEE 802.11 -standardissa määritellyn AP:n majakkatoiminnon poiskytkemistä. SSID lähetetään edelleen salaamattomana muun liikenteen otsikoissa, mutta erillisiä säännöllisesti kaikille kuulijoille osoitettuja majakkapaketteja ei enää lähetetä. Verkkotunnus täytyy asettaa käsin jokaiseen päätelaitteeseen, joka haluaa liittyä verkkoon. Liikennettä haistelemalla SSID:n pystyy edelleen selvittämään, joten suljettu verkko ei yksinään riitä turvallisuusratkaisuksi.

WEP-salauksen laajentaminen 104-bittiseksi oli myös Lucentin aloittama parannus [10]. Toiminta pysyy muuten samanlaisena kuin IEEE 802.11 -standardin mukaisessa salauksessa mutta jaetun salaisen avaimen pituus on 104 bittiä 40 bitin sijaan. WEPin laajennus ei auta kehittyneempiä WEP-hyökkäyksiä vastaan, sillä käytössä ovat edelleen 24-bittiset alustusvektorit ja niiden mukanaan tuomat heikkoudet. Laajennettua salausta käyttävän verkon kaikkien laitteiden pitää tukea 104-bittistä salausta voidakseen kommunikoida keskenään.

Lucent on pyrkinyt parantamaan WEP-salauksen turvallisuutta edelleen ottamalla käyttöönsä ORINOCO WEPplus -tekniikan [11]. Siinä alustusvektoreina ei käytetä niin sanottuja heikkoja vektoreita, jotka paljastavat osia salaisesta avaimesta, ja näin WEP-salauksen purkaminen vaikeutuu.

Käyttäjäntunnistukseen on mahdollista käyttää myös päätelaitteiden MAC-osoitteita [10]. Todentamista varten kaikkien päätelaitteiden MAC-osoitteet tallennetaan tietokantaan, joka sijoitetaan joko yhteiselle palvelimelle tai kaikkiin access pointteihin, ja vain tietokannassa olevien päätelaitteiden liikenne sallitaan. MAC-suodatuksella on kaksi heikkoutta. Ensinnäkin tietokannan ylläpitäminen on hankalaa, etenkin jos joka AP:ssa on oma tietokantansa. Toiseksi MAC-osoitteen väärentäminen on helppoa, kunhan ensin on haistellut verkosta tietoonsa sallitun osoitteen.

Väärien access pointtien torjuntaan voidaan käyttää SSID:hen ja MAC-osoitteeseen perustuvaa valintaa päätelaitteissa. Päätelaitteisiin tallennetaan sallittujen access pointtien osoitteet ja assosiointi sallitaan vain niiden kanssa. Turvallisuuden kannalta tällä ratkaisulla on samat heikkoudet kuin MAC-suodatuksella.

Verkon turvallisuutta parantaa laitteiden asetuksien optimointi turvallisuutta silmälläpitäen. Turhat palvelut kytketään pois käytöstä. Esimerkiksi DHCP-palvelun (Dynamic Host Configuration Protocol) käyttäminen voi helpottaa hyökkääjää saamaan käyttöönsä sallittu IP-osoite. Vakiotunnukset ja salasanat on hyvä muuttaa pois oletusarvoistaan. Laitteiden säteilykenttää kannattaa pienentää vähentämällä lähetystehoa ja kiinnittämällä huomiota laitteiden sijoitteluun. Koko langaton järjestelmä asennetaan palomuurin taakse niin sanotulle demilitarisoidulle vyöhykkeelle (DMZ, demilitarized zone). Lisäksi verkon käyttäytymistä kannattaa tarkkailla keräämällä lokitietoa verkon tapahtumista ja siten havaita mahdolliset hyökkäykset verkon turvallisuutta vastaan.

3.3 Kehittyneemmät turvallisuusratkaisut

Seuraava askel kohti turvallista langatonta lähiverkkoa otettiin, kun suuret valmistajat kuten Cisco julkaisivat omat ratkaisunsa WEPin turvallisuusaukkojen paikkaamiseen. Käyttäjäntunnistuksen parantamiseksi käytetään IEEE 802.1X -standardin mukaista arkkitehtuurikehystä ja EAP:ia (Extensible Authentication Protocol). Todentaminen voidaan näin keskittää ulkoiselle palvelimelle ja todentamistavaksi on useita vaihtoehtoja. Salausta parannetaan ottamalla käyttöön dynaamiset avaimet ja vaihtamalla avaimia riittävän usein. Lisäksi eheyden tarkastamiseen tarjotaan uutta vahvempaa vaihtoehtoa lineaarisen tarkistussumman ohelle.

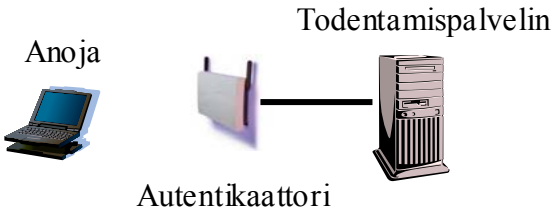
Nämä kehittyneemmät turvallisuusratkaisut ovat yleensä valmistajakohtaisia ja standardoinnin puuttuessa yhteensopivuusongelmia saattaa esiintyä.

3.3.1 IEEE 802.1X -standardi ja EAP

IEEE 802.1X -standardi määrittelee porttipohjaisen todentamiskehyksen, jota voidaan käyttää IEEE 802 -standardien mukaisissa lähiverkoissa [12]. Standardi kehitettiin alunperin langalliseen ympäristöön, mutta se soveltuu hyvin myös langattoman verkon todentamiskehykseksi.

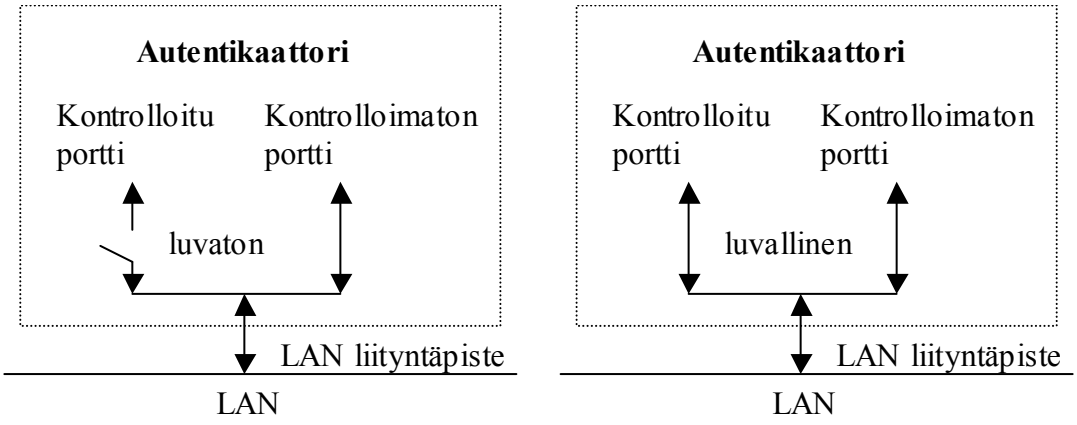
Standardi ei määrittele itse todentamistapaa vaan ainoastaan pohjan, jonka päällä voidaan käyttää useita eri todentamisvaihtoehtoja. Yleensä IEEE 802.1X -standardin kanssa käytetään EAP-protokollaa, joka huolehtii pakettien välityksestä todentamisprosessin aikana ja mahdollistaa ulkoisten todentamispalvelimien käytön [13]. Todentamispalvelimena käytetään yleensä RADIUS-palvelinta (Remote Authentication Dial-In User Service) [14] [15]. Käyttäjäntunnistuksen ohella 802.1X ja EAP mahdollistavat dynaamisten salausavaimien käytön ja parantavat näin WEP-salauksen turvallisuutta.

Porttipohjainen verkon pääsynhallinta toimii MAC-tasolla kontrolloimalla liikennettä avaamalla ja sulkemalla portteja päätelaitteiden tilan mukaan. WLAN ympäristössä porttina toimii päätelaitteen assosiointi access pointin kanssa. Todentamisjärjestelmä koostuu kolmesta komponentista kuvan Kuva 3-8 mukaisesti. Autentikaattori (authenticator), eli yleensä access point, pakottaa anojan (supplicant), eli yleensä päätelaitteen, todentamaan itsensä ennen kuin sallii sen käyttää verkon resursseja. Kolmas komponentti eli todentamispalvelin huolehtii itse todentamisesta. Autentikaattorin tehtävänä todennusprosessissa on vain välittää liikennettä anojan ja palvelimen välillä ja koteloida viestit kulloinkin sopivan protokollan sisään.



Kuva 3-8 802.1X-pohjainen todentamisjärjestelmä

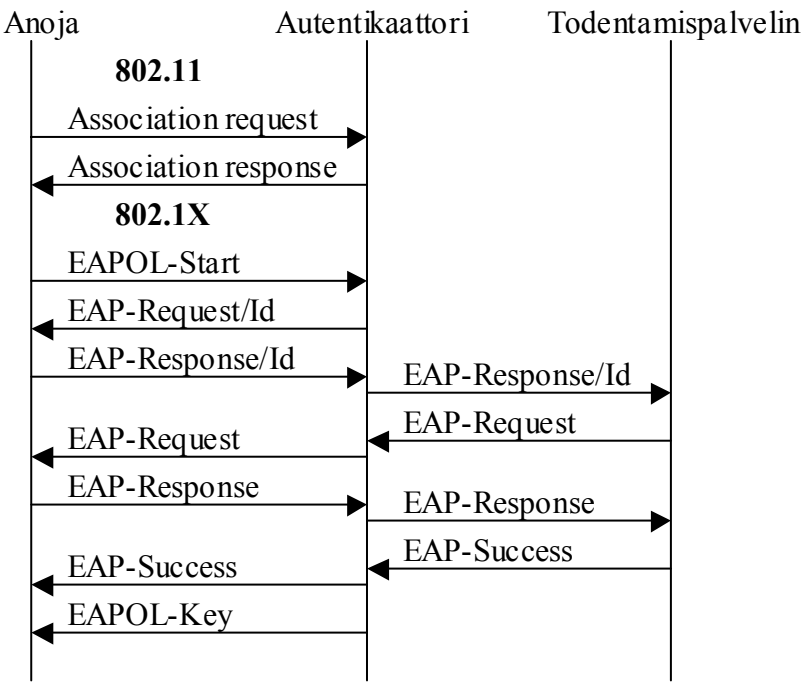
Autentikaattori kontrolloi liikennettä jakamalla LAN-yhteyden kahteen virtuaaliseen porttiin kuvan Kuva 3-9 mukaisesti. Kontrolloimatonta porttia käytetään todentamista varten ja siitä pääsevät läpi vain EAP-paketit. Kontrolloitu portti avataan vasta kun anoja on todennettu onnistuneesti ja pääsy verkkoon voidaan sallia. Normaali liikenne kulkee kontrolloidun portin kautta.



Kuva 3-9 802.1X-autentikaattorin portit

IEEE 802.1X -standardin mukainen todentamisprosessi on kuvattuna kuvassa Kuva 3-10. Todentaminen alkaa päätelaitteen assosioitumisella access pointin kanssa. Assosiointia varten päätelaite ensin todennetaan avointa todentamista käyttäen. Autentikaattori asettaa kontrolloidun portin estotilaan. 802.1X todennuksen toiminta alkaa joko anojan lähettämällä EAPOL-Start-paketilla tai suoraan autentikaattorin lähettämällä EAP-Request-paketilla, jossa pyydetään anojan tunnistetietoja. Anoja vastaa pyyntöön lähettämällä tunnistetietonsa autentikaattorille. Autentikaattori välittää tunnistetiedot todentamispalvelimelle turvallista tietä pitkin.

Todentamispalvelin vastaa tunnistetietoihin lähettämällä haastepaketin anojalle. Paketin rakenne riippuu käytettävästä EAP-menetelmästä ja haastepaketteja voidaan lähettää useampiakin. Anoja lähettää vastauksen haastepakettiin ja palvelin suorittaa todentamisen. Onnistuneen todentamisen seurauksena palvelin lähettää autentikaattorille EAP-Success-paketin menestyksekkään todentamisen merkiksi. Epäonnistuneesta todentamisesta seuraa EAP-Failure-paketin lähetys.



Kuva 3-10 802.1X-todentamispakettien vaihto [23]

Onnistuneen todentamisen jälkeen autentikaattori lähettää anojalle EAPOL-Key-viestin, jota käytetään salausavaimien välittämiseen salattuna päätelaitteelle. Salaamisessa on käytössä avaimet sekä kohdelähetystä että levityslähetystä varten. Kohdelähetysavaimia käytetään päätelaitteen ja access pointin väliseen kommunikaatioon ja levityslähetysavaimia kaikille välittyvään liikenteeseen. Ensimmäinen kohdelähetysavain luodaan todentamisprosessin aikana sekä anojassa että todentamispalvelimessa ja palvelin toimittaa avaimen todentamisen onnistuttua autentikaattorille. Tätä avainta käyttäen salataan ensimmäiset EAPOL-Key-paketit ja päivitetään anojan salausavaimet.

EAP on haaste-vaste-periaatteen mukaan toimiva protokolla. WLAN-verkossa EAP-viestit kulkevat suoraan MAC-kerroksen päällä koteloituina EAPOL-kehyksien (EAP over LAN) sisään. Lankaverkossa EAP-paketit koteloidaan vastaavasti esimerkiksi RADIUS-protokollan sisään. Viestien kuljettaminen suoraan MAC-kerroksen päällä mahdollistaa todentamisen ennen kuin korkeampia protokollia on alustettu ja näin verkon resurssien käyttö onnistuu vasta onnistuneen todentamisen jälkeen.

EAP-toteutuksia on useita ja niiden toimintaperiaatteet vaihtelevat suuresti. Eri ratkaisut soveltuvat erilaisiin ympäristöihin riippuen verkon rakenteesta, palveluista, todentamisen viivevaatimuksista ja verkon yhteyksistä ulkoisiin palveluihin. Ohessa on esiteltyinä lyhyesti muutamia EAP-ratkaisuita.

EAP-MD5 [16] käyttää MD5-hajautusalgoritmia todentamiseen. EAP-MD5 ei tarjoa ratkaisua avainten hallintaan eikä siten mahdollista dynaamisten avainten käyttöä. Lisäksi kaksisuuntaisen todentamisen puuttuessa päätelaite ei voi varmistua access pointin oikeellisuudesta. EAP-MD5 ei paranna merkittävästi turvallisuutta perusratkaisuihin verrattuna.

EAP-SIM (EAP- Subscriber Identity Module) [17] ja EAP-AKA (EAP- Authentication and Key Agreement) [18] hyödyntävät GSM (Global System for Mobile communications) ja UMTS (Universal Mobile Telecommunications System) -verkoissa käytössä olevia todentamismenetelmiä. Todentaminen perustuu erillisen älykortin käyttöön ja matkapuhelinverkosta saataviin tunnistepalveluihin. Kaksisuuntainen todentaminen ja dynaaminen avaintenhallinta on toteutettuna näissä ratkaisuissa.

LEAP (EAP-Cisco wireless) on Ciscon standardoima EAP-ratkaisu. Käyttäjäntunnistukseen LEAP käyttää EAP-MD5-toteutuksen lailla salasanoja. Dynaamiset kertakäyttöiset avaimet ja niiden jakaminen on toteutettuna samoin kuin kaksisuuntainen todentaminen. Toteutuksessa on kaksi heikkoutta. Tunnistetietojen välitykseen käytettävässä protokollassa on heikkouksia ja LEAP-verkossa voi olla ainoastaan Ciscon valmistamia laitteita. [10]

EAP-TLS toteutus [19] käyttää TLS-protokollaa (Transport Level Security) [20] ja PKI-tunnisteita (Public Key Infrastructure) käyttäjäntunnistukseen. Dynaamiset kertakäyttöiset avaimet ja kaksisuuntainen todentaminen löytyvät myös tästä ratkaisusta. Heikkoutena on erillisen tunnistepalvelimen tarve ja yhteensopivuuden rajoittuminen Microsoft-pohjaisiin ratkaisuihin.

EAP-TTLS-todentamisprosessi (EAP tunneled TLS) [21] on kaksivaiheinen. Ensimmäisessä vaiheessa muodostetaan tunneli anojan ja todentamispalvelimen välille käyttäen tunnisteita kuten EAP-TLS-protokollassakin. Itse todentaminen tapahtuu toisessa vaiheessa kyseistä tunnelia hyödyntäen. Toisessa vaiheessa todentamismekanismina voidaan käyttää mitä tahansa palvelimen tukemista vaihtoehdoista.

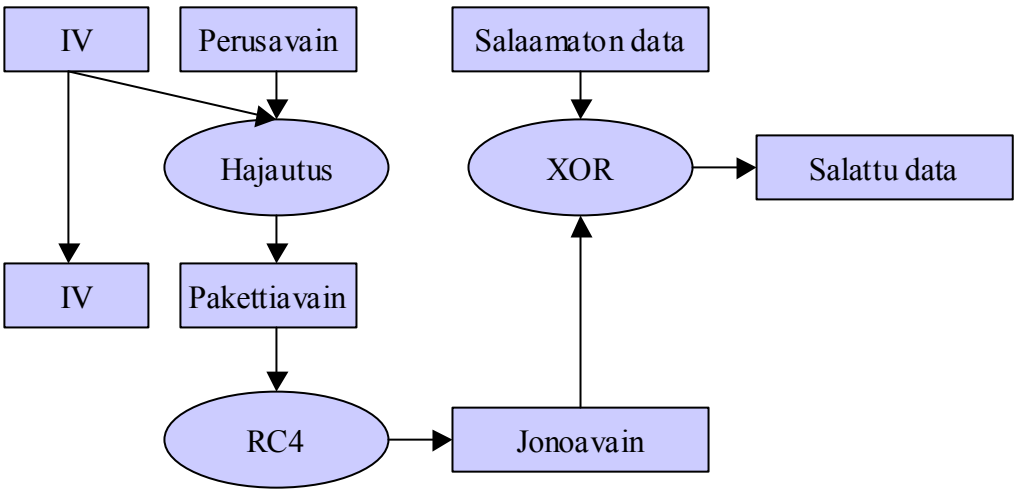
PEAP-menetelmä (Protected EAP) [22] on Microsoftin ja Ciscon kehittämä kilpailija EAP-TTLS:lle. Näiden kahden protokollan toiminta eroaa vain toisessa vaiheessa, jossa PEAP hyväksyy ainoastaan EAP:in mukaiset todentamismenetelmät TTLS:n käyttäessä muitakin menetelmiä.

Tarkempi selvitys IEEE 802.1X -standardista ja eri EAP-protokollien toiminnasta löytyy esimerkiksi Antti Erkkilän diplomityöstä ”IEEE 802.1X Authentication In Operator’s WLAN” [23].

3.3.2 Cisco Wireless Security Suite

Cisco on ollut yksi aktiivisimmista langattomien lähiverkkojen turvallisuuden kehittäjistä. Ciscon tarjoama turvallisuuspaketti on nimeltään ”Cisco Wireless Security Suite” ja se koostuu useista WEP-salausta vahvistavista komponenteista [24]. Ciscon turvallisuuspakettiin kuuluvat eheyden tarkastusta parantava MIC (Message Integrity Check), salausavainten käyttöä tehostavat TKIP (Temporal Key Integrity Protocol) ja BKR (Broadcast Key Rotation) sekä todentamista ja avaintenhallintaa koskeva 802.1X. Monet näistä ratkaisuista ovat päätyneet muidenkin valmistajien laitteisiin ja tuleviin standardeihin.

TKIP eli WEP-avaimen hajautus mahdollistaa jaetun salaisen avaimen suojaamisen hyökkäyksiltä. Ciscon käyttämää ratkaisua kutsutaan Cisco TKIP:ksi erotukseksi standardoitavasta TKIP:stä. Ciscon ratkaisu esitellään tässä kappaleessa ja standardoitu versio myöhemmin WPA-ratkaisua käsittelevässä kappaleessa 3.4. TKIP tarjoaa mahdollisuuden käyttää pakettikohtaisia avaimia ja poistaa näin ennustettavuuden liikenteen salauksesta vaikeuttaen hyökkäyksiä WEP-salausta vastaan. TKIP:n toiminta on kuvattuna kuvassa Kuva 3-11.



Kuva 3-11 Cisco TKIP:n toiminta

Salaukseen ei käytetä tavallisen WEP-salauksen lailla suoraan jaettua avainta vaan jaetusta avaimesta johdettua pakettikohtaista avainta. Jaetusta perusavaimesta ja alustusvektorista muodostetaan hajauttamalla yksilöllinen pakettiavain (temporal key). Alustusvektorin pituus on 24 bittiä ja jaetun avaimen 104 bittiä. Pakettiavain syötetään sitten RC4-algoritmiin josta saadaan salaamiseen käytettävä jonoavain. Salaus ja jonoavaimen muodostaminen tapahtuu kuten tavallisessakin WEP-salauksessa. Onnistunut hyökkäys salausta vastaan voi paljastaa pakettiavaimen mutta itse jaettu avain on turvassa. Jaettu avain pitää vaihtaa riittävän usein alustusvektorien uudelleenkäytön välttämiseksi. Avainten päivittämiseen soveltuvat EAP-todennusprotokollat. [25]

Pakettien eheyden tarkistusta varten TKIP:ssä on määriteltynä MIC. Parannetun eheydentarkastuksen tarkoituksena on torjua toistohyökkäyksiä (reply attack) ja bit-flip hyökkäyksiä. Lineaarisen CRC-32-tarkistussumman käyttö yhdessä tilattoman IV-ratkaisun kanssa muodostaa heikkouden, jota toistohyökkäyksissä hyödynnetään. Lähettäjä generoi itse käytettävät alustusvektorit, joten hyökkääjä pystyy käyttämään yhtä selvittämäänsä IV-jonoavain-paria yhä uudelleen ja lähettää oikein salattua liikennettä tuntematta jaettua avainta. Vastaavasti lineaarista tarkistussummaa käytettäessä on mahdollista muokata salattua pakettia ja laskea uusi tarkistussumma purkamatta salausta. Tällaisia hyökkäyksiä kutsutaan bit-flip-hyökkäyksiksi. MIC ratkaisee nämä heikkoudet ottamalla tarkistussumman laskentaan mukaan lähettäjän ja vastaanottajan MAC-osoitteet sekä joka päätelaitteelle yksilöllinen siemenarvo. Laskentaan MIC käyttää hajautusalgoritmia. [9]

802.1X ja EAP huolehtivat kehittyneemmästä todentamisesta sekä mahdollistavat dynaamisten ja yksilöllisten kohdelähetysavainten käytön. EAP kuitenkin jättää ongelmaksi staattiset levityslähetysavaimet. BKR tarjoaa keinot MAC-kerroksen levitys- ja jakelulähetysviestien salaamiseen käytettävien levityslähetysavainten dynaamisuuteen. Access point laskee uuden avaimen tietyin väliajoin ja lähettää sen terminaaleille vanhalla avaimella salattuna EAPOL-Key-pakettien avulla. BKR edellyttää dynaamiseen avainten johtamiseen kykenevän EAP-ratkaisun, kuten LEAP tai EAP-TLS, käyttöä. EAP ja BKR yhdessä tarjoavat vaihtoehdon TKIP:n käytölle. [26]

3.4 Wi-Fi Protected Access

Wi-Fi Allianssi (Wireless-Fidelity) on ei-kaupallinen yhteisö, joka perustettiin vuonna 1999 edistämään IEEE 802.11 -standardiin perustuvien langattomien lähiverkkojen yhteensopivuutta [27]. Allianssin tavoitteena on reagoida standardointielimiä nopeammin markkinoiden ja laitteistojen tarpeisiin tuottamalla standardinomaisia suosituksia teknologioiden nopean käyttöönoton ja yhteensopivuuden mahdollistamiseksi. Wi-Fi-sertifikaatti laitteessa varmistaa, että laite täyttää tietyt yhteensopivuusehdot ja toimii muiden Wi-Fi-sertifioitujen laitteiden kanssa samassa verkossa.

WPA (Wi-Fi Protected Access) on Wi-Fin ratkaisu WEP-salauksen heikkouksiin. Se tarjoaa standardinomaisen vaihtoehdon valmistajakohtaisille ratkaisuille. WPA kehitettiin parantamaan turvallisuutta ja yhteensopivuutta ennen oikean WLAN turvallisuusstandardin IEEE 802.11i valmistumista. WPA:n vahvuutena on, että laitteita on saatavilla jo nyt [27]. Yhteensopivuus tulevan standardin kanssa on taattu, sillä käytännössä WPA muodostuu standardiin tulevista turvallisuuskomponenteista. WPA:han sisällytetyt komponentit on valittu pitäen mielessä, että vanhojen laitteiden päivitys WPA-yhteensopiviksi pitää pystyä tekemään ohjelmistopäivityksellä. [28]

WPA koostuu neljästä uudesta algoritmista, jotka korjaavat alkuperäisen WEP-toteutuksen heikkoudet. Nämä algoritmit liittyvät salauksen parantamiseen, eheyden tarkistamiseen ja todentamiseen sekä avainten hallintaan. Salausta parantamaan on määritelty TKIP ja laajennettu alustusvektoriavaruus. Eheyden tarkistukseen käytetään TKIP:n sisältämää MIC-tarkistussummaa ja todennukseen sekä avainten hallintaan IEEE 802.1X -standardia ja EAP-protokollia. IEEE 802.1X -standardin käyttöä on käsitelty aiemmin omassa kappaleessaan. Muut parannuskeinot esitellään seuraavassa kappaleessa.

3.4.1 TKIP ja muut WPA:n komponentit

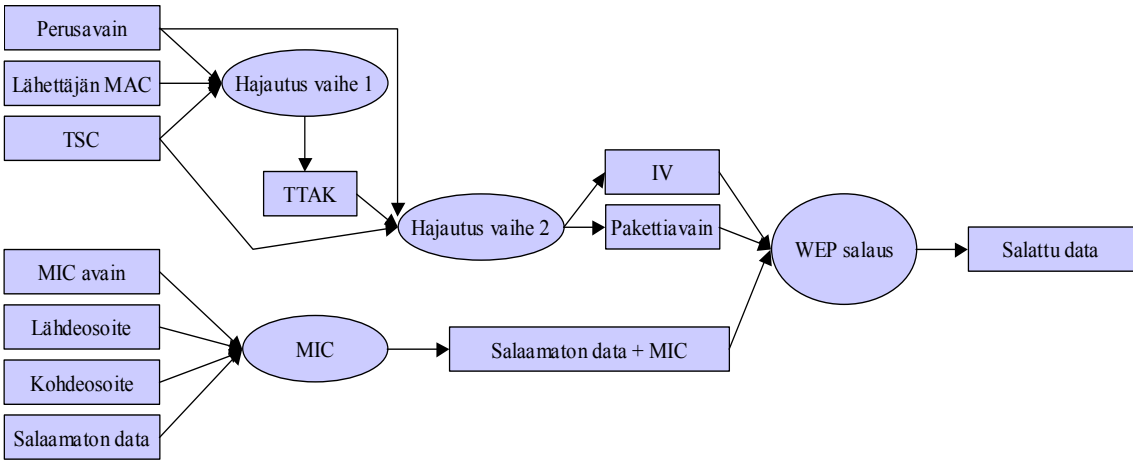
TKIP parantaa langattoman verkon turvallisuutta huomattavasti ottamalla käyttöön pakettikohtaiset salausavaimet. Salaukseen käytetään edelleen RC4-algoritmia mutta salausavaimen pituus on 128 bittiä. Perusavaimien luonnista ja hallinnasta huolehtii todentamispalvelin EAP-protokollien avulla. Perusavaimesta muodostetaan salaukseen

käytettävä pakettiavain kaksivaiheisen prosessin avulla. Itse perusavainta ei käytetä sellaisenaan salaukseen.

WEP salausta vastaan suoritettuja hyökkäyksiä torjumaan TKIP:ssa on toteutettuna useita uusia algoritmeja. TSC (TKIP Sequence Counter) eli sekvenssilaskuri torjuu toistohyökkäyksiä. Jokaisella päätelaitteella on oma laskurinsa ja laskurin arvoa kasvatetaan aina kun uusi kehys salataan ja lähetetään. Sekvenssilaskurin arvo toimitetaan vastaanottajalle WEP-alustusvektorina ja vastaanottaja hylkää paketit, joissa sekvenssilaskurin arvo ei ole odotetusti muuttunut. TSC:n pituus on 48 bittiä eli alustusvektoriavaruutta on kasvatettu vanhasta 24 bitistä ja vektorien törmäyksien tiheyttä on näin saatu pienennettyä.

Eheyden tarkastukseen käytettävä MIC lasketaan lähde- ja kohdeosoitteesta sekä salaamattomasta datasta Michael-algoritmia käyttäen. Vastaanottaja laskee vastaavasti oman MIC-arvonsa ja hylkää paketin, jos arvot eivät täsmää. Lineaarista CRC-32-tarkistussummaa paremmin toimiva hajautusmenetelmä tarvitsee laskentaan lisäksi 64-bittisen MIC-avaimen, joka luodaan pakettiavainten luomisen yhteydessä [29]. Virheelliset MIC-arvot aiheuttavat vastatoimenpiteitä torjumaan oletettavasti käynnissä olevat aktiiviset hyökkäykset. Vastatoimenpiteillä pyritään estämään hyökkääjän tiedonsaanti salaukseen käytettävistä avaimista sekä estämään liian tiheä avainten uusiminen. MIC torjuu tehokkaasti datan muuttamiseen ja osoitteiden manipulointiin liittyviä hyökkäyksiä.

Salaukseen käytettävän pakettiavaimen muodostaminen tapahtuu kahdessa vaiheessa kuvan Kuva 3-12 mukaisesti. Jaettua 128-bittistä perusavainta ei sellaisenaan käytetä salaukseen, joten hyökkäykset eivät voi enää kohdistua suoraan siihen.



Kuva 3-12 TKIP:n toiminta

Ensimmäisessä vaiheessa muodostetaan hajautusalgoritmia käyttäen lähettäjän MAC-osoitteesta, TSC:stä ja perusavaimesta TTAK (TKIP mixed Transmit Address and Key). Perusavaimesta käytetään tässä vaiheessa 80 ensimmäistä bittiä ja sekvenssilaskurista 32 merkitsevintä bittiä. Muodostettava TTAK on 80 bittiä pitkä. TTAK ei ole jokaiselle paketille yksilöllinen, joten samaa avainta voidaan käyttää peräkkäin lähetettäville paketeille.

Toisessa vaiheessa edelleen hajautusalgoritmia käyttäen muodostetaan perusavaimesta, TTAK:sta ja TSC:stä pakettiavain, joka sisältää alustusvektorin. Perusavaimesta käytetään tässä vaiheessa 24 viimeistä bittiä ja sekvenssilaskurista kaikki 48 bittiä. Syntyvä pakettiavain on 128 bittiä pitkä. Pakettiavain on yksilöllinen ja se lasketaan jokaiselle paketille uudestaan. Vastaanottaja suorittaa saman prosessin voidakseen purkaa salauksen ja tehdä MIC-tarkastuksen. TKIP-salatun datan kehysrakenne on esitettynä kuvassa Kuva 3-13. [30]

Salaamaton		Salattu		
IV 32 bit	**Laajennettu IV** 32 bit	**Data** ≥ 8 bit	**MIC** 64 bit	**ICV** 32 bit

Kuva 3-13 TKIP-salattu kehys

TKIP:n tuomia parannuksia turvallisuuteen voidaan hyödyntää myös pienemmässä ympäristössä ilman todentamispalvelinta käyttämällä etukäteen jaettuja avaimia kuten perus WEP-ratkaisuissa. Salasanat jaetaan tällöin käsin kaikkiin verkon laitteisiin. Tämä PSK-toimintatila (Pre-Shared Key) sisältää perusavaimien vaihtoa lukuun ottamatta samat parannukset kuin täysi TKIP. [28]

3.5 IEEE 802.11i -standardi

IEEE on valmistellut seuraavaa langattomien lähiverkkojen turvallisuutta käsittelevää standardia IEEE 802.11i jo hyvin pitkälle [30]. Standardin ratifioinnin oletetaan tapahtuvan vuoden 2004 ensimmäisen neljänneksen aikana ja yhteensopivia laitteita odotetaan markkinoille toisella vuosineljänneksellä [31]. Standardia kutsutaan myös nimellä WPA2 sillä Wi-Fi:n WPA-ratkaisu koostuu kyseisen standardin osista.

IEEE 802.11i -standardin mukaisia turvallisuusratkaisuita käyttäviä langattomia lähiverkkoja kutsutaan RSN-verkoiksi (Robust Security Network). Standardissa määritellään 802.1X:n mukainen todentamis- ja avaintenhallintakäytäntö sekä parannetut menetelmät tiedon salaukseen. Salaukseen tarjotaan kolmea vaihtoehtoa TKIP, WRAP (Wireless Robust Authenticated Protocol) ja CCMP (Counter mode with Cipher-Block Chaining-Message Authentication Code Protocol), joista viimeinen on ainoa pakollinen salausprotokolla. RSN-turvallisuus tarjoaa kaksisuuntaisen todentamisen ja yksilöllisten avainten käytön myös Ad-Hoc-tilassa olevissa verkoissa, kun aiemmin vahvistettu turvallisuus oli saatavilla vain infrastruktuuritilassa oleviin verkkoihin. [30]

TKIP tarjoaa vaihtoehdoista heikoimman salauksen, mutta on mukana takaamassa yhteensopivuuden vanhojen laitteiden kanssa, kunhan niissä on TKIP-päivitys asennettuna. WRAP ja CCMP käyttävät salaukseen kehittyneempää 128-bittistä AES-algoritmia (Advanced Encryption Standard). AES-algoritmin käyttäminen edellyttää muutoksia laitteistojen toteutukseen eikä sitä ole mahdollista ottaa käyttöön pelkällä ohjelmistopäivityksellä. TKIP sisältää 128-bittisen WEP-salauksen, pakettikohtaisten avainten käytön ja MIC-tarkistussumman. WPA:n yhteydessä toteutettu TKIP on vastaava kuin IEEE 802.11i -standardiin tuleva ja se on esiteltynä tarkemmin jo WPA:ta

käsittelevässä kappaleessa. IEEE 802.1X -standardin todennus ja avainten hallinta on myös esiteltynä omassa kappaleessaan ja 802.11i:n kanssa käytettäväksi soveltuvat kaikki EAP-protokollat, joissa on toteutettuna dynaaminen avaintenhallinta. Seuraavissa kappaleissa tutustutaan kahteen tarjolla olevaan AES-algoritmiin.

3.5.1 Advanced Encryption Standard

Amerikkalainen NIST (National Institute of Standards and Technology) on valinnut AES:in Rijndael-algoritmin seuraavan sukupolven salausalgoritmiksi korvaamaan nykyisiä DES- (Data Encryption Standard) ja 3DES-algoritmia (Triple DES) [32]. Rijndael-algoritmi valittiin seuraavaksi turvallisuusstandardiksi vuosia kestäneen prosessin jälkeen, joka alkoi DES-algoritmin murtamisesta vuonna 1990 [9]. AES-algoritmin tehokkuutta ei ole vielä käytännössä testattu mutta sen uskotaan säilyvän salausstandardina useita vuosia eteenpäin. Algoritmia vastaan kehitetään jatkuvasti uusia hyökkäyksiä ja etenkin algebrallisten hyökkäysten toimivuuden mahdollisuuksia tutkitaan tarkasti. Yhtään todistetusti toimivaa hyökkäystä ei ole kuitenkaan vielä julkaistu.

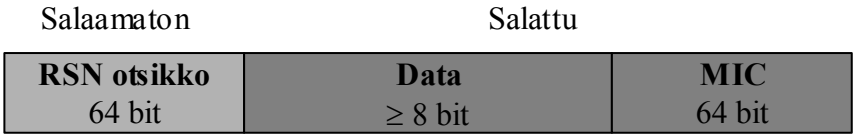
AESin toiminta on täysin erilainen kuin RC4-algoritmin. AES on symmetrinen lohkosalausalgoritmi, joka pystyy käyttämään eripituisia avaimia. Avainvaihtoehtoja ovat 128-, 192- ja 256-bittinen. IEEE 802.11i -standardin yhteydessä käytetään 128-bittistä salausta. AES vaatii enemmän laskentatehoa kuin RC4 ja siitä aiheutuva otsikkokuorma on suurempi. Suuremmasta laskentatehonvaatimuksesta johtuen AESin käyttö vaatii laitteistolta rautakiihdytystä ja siten sen käyttöönotto vaatii laitteiden päivitystä.

IEEE 802.11i -standardissa määritellään kaksi vaihtoehtoa AES-salauksen toteuttamiseen. WRAP käyttää AES-salausta OCB-tilassa (Offset Codebook block mode). WRAP-salauksen tukeminen ei ole pakollista RSN-yhteensopivuuden saavuttamiseksi. WRAP salaa ainoastaan kohdelähetysliikenteen dataosuuden, levityslähetysliikenteen salaus hoidetaan suoraan 802.1X-protokollan avulla saadulla avaimella ja tarkistussummaa ei salata ollenkaan. Salausta varten WRAP-kehyksessä on toistolaskurikenttä, jota käytetään pakettien toiston huomaamiseen ja alustusvektoreiden tapaan salaukseen. Kehys on esitettynä kuvassa Kuva 3-14. OCB-salaus tehdään pakettikohtaisen avaimen ja toistolaskurin sekä kohde- ja lähdeosoitteen muodostaman merkkijonon avulla. Salauksen yhteydessä lasketaan tarkistussummaksi OCB-leima (MIC). Salatun paketin vastaanottaja suorittaa tarkastukset salauksen oikeellisuudelle tutkimalla pakettilaskureitaan, vastaanotetun paketin rakennetta sekä tarkistussummaa. Väärin muotoillut ja väärällä toistolaskurin arvolla saapuneet paketit hylätään ennen salauksen purkamista.

Salaamaton	Salattu	Salaamaton
Toistolaskuri 32 bit	**Data** ≥ 8 bit	**MIC** 64 bit

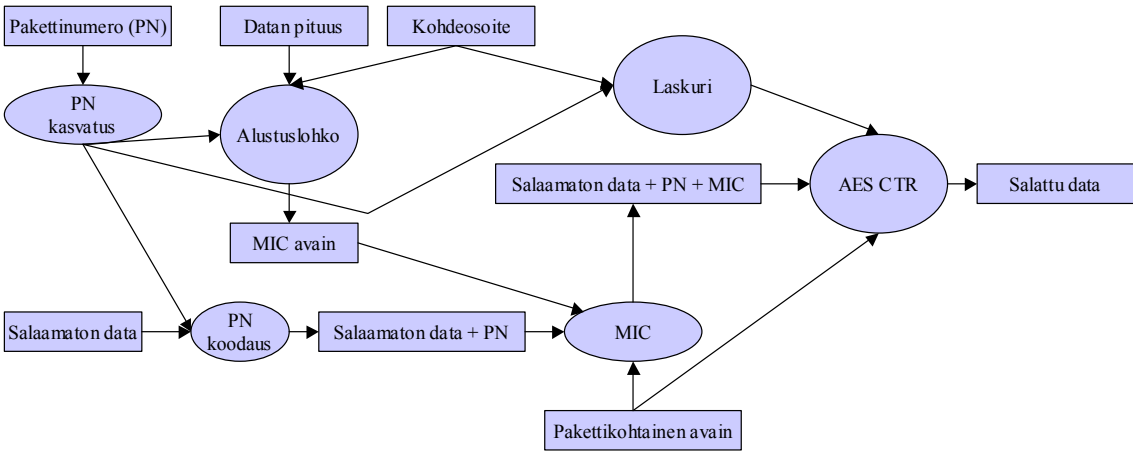
Kuva 3-14 WRAP-kehys

Toinen AES-vaihtoehto on CCMP, jonka tukeminen on edellytyksenä RSN-yhteensopivuudelle. CCMP käyttää AES-salausta CCM-tilassa (Counter Mode/CBC-MAC), joka tarjoaa CTR-muotoisen (Counter) salauksen ja CBC-MAC-muotoisen (Cipher Block Chaining Message Authentication Code) eheydentarkistuksen. CCMP-kehyksen rakenne on esitettynä kuvassa Kuva 3-15. WRAP-kehykseen verrattuna otsikkotietoja on enemmän ja tarkistussumma on salatussa muodossa.



Kuva 3-15 CCMP-kehys

Salaus ja eheyden tarkistus suoritetaan kuvassa Kuva 3-16 esitetyn prosessin mukaisesti. Jokaisella salattavalla paketilla on yksilöllinen pakettinumero, jota käytetään pakettien toiston huomaamiseen. Salausprosessin alussa pakettinumeroa kasvatetaan yhdellä ja uusi pakettinumero koodataan salaamattomaan dataan. Alustuslohkossa muodostetaan eheyden tarkistuksen laskemista varten pakettinumerosta, datan pituudesta ja kohdeosoitteesta MIC-avain. CBC-MAC-algoritmia käyttäen lasketaan salaamattomasta datasta MIC-tarkistussumma pakettikohtaisen avaimen ja MIC-avaimen avulla. Tarkistussumma liitetään datan jatkoksi. Salausta varten muodostetaan laskuriarvo kohdeosoitteesta ja pakettinumerosta. Laskuriarvo vastaa aikaisemmin käytettyä alustusvektoria. AES CTR -algoritmia käyttäen salataan lopuksi pakettiavainta ja laskuriarvoa hyödyntäen data ja tarkistussumma.



Kuva 3-16 CCMP-salauksen suorittaminen

Salauksen purkaminen tapahtuu käänteisessä järjestyksessä. Salatusta paketista erotetaan pakettinumero RSN-otsikosta ja tarkastetaan sen oikeellisuus vertaamalla sitä viimeksi vastaanotettuun pakettinumeroon. Väärällä pakettinumerolla saapuvat paketit hylätään. Salauksen purkamista varten muodostetaan laskuriarvo ja tarkistussumman

laskemista varten MIC-avain. Salaus puretaan ja MIC-vertailun jälkeen todetaan data oikeaksi tai hylätään paketti.

Tarkempi selvitys AES-algoritmien toiminnasta löytyy esimerkiksi IEEE 802.11i -standardista. [30]

3.6 Virtual Private Network

VPN (Virtual Private Network) eli virtuaalinen yksityinen verkko tarjoaa mahdollisuudet laajentaa turvallisesti yksityistä verkkoa turvattoman verkon, kuten Internet, ylitse. VPN-sovellukset ovat laajalti käytössä lankaverkoissa yritysten etäyhteyksien luonnissa tavallisten vuokrattujen linjojen ja soittoyhteyksien korvaajina. VPN-yhteys on virtuaalinen yhteys kahden pisteen välillä. Yhteyden päätepisteet voivat olla yksittäisiä käyttäjiä tai kokonaisia verkkoja. VPN tarjoaa toteutukset tunnelointia, salausta, eheyden tarkistusta, todennusta ja pääsynhallintaa varten.

Yleisesti VPN-ratkaisut ovat ohjelmistopohjaisia sovelluksia. IPsec (Intrnet Protocol Security) on tällä hetkellä suosituin protokollakokoelma VPN-sovelluksen perustaksi. Se perustuu L2TP-protokollan (Layer 2 Tunneling Protocol) käyttöön ja turvattujen linkkikerroksen yhteyksien luontiin. IPsec on arkkitehtuuriprotokolla, joka tarjoaa kehyksen salaus- ja muiden protokollien yhteensovittamista varten. IPsec-protokollan kanssa käytetään yleensä IKE-protokollaa (Internet Key Exchange) avaintenhallintaan ja DES-, 3DES- tai AES-algoritmia salaukseen. [9]

Langattoman lähiverkon yhteydessä VPN toimii kokonaisuudessaan WLAN-kerroksien päällä. VPN mahdollistaa yhteensopivuusongelmien ja WEP-salauksen heikkouksien torjumisen toimivaksi todistetulla ratkaisulla. Etuina VPN-ratkaisuissa ovat laitteistovalmistajariippumattomuus, useat todentamis- ja salausvaihtoehdot, tehokas eheydentarkistus sekä kaksisuuntainen todentaminen. Lisäksi erona langattomien verkkojen omiin turvallisuusratkaisuihin VPN mahdollistaa turvallisuuden yhteyden päästä päähän, WLAN-standardien tarjotessa turvallisuutta vain päätelaitteiden ja access pointtien välillä. Heikkouksiksi VPN-vaihtoehdolle nähdään mahdollinen ylimääräisen prosessoinnin aiheuttama suorituskyvyn lasku. Koska VPN-sovellus toimii WLAN-kerroksien päällä tarvitaan myös erillinen asiakasohjelmisto käyttäjien tietokoneisiin ja vastaavasti palvelin joko access pointin yhteyteen tai syvemmälle verkkoon. Access pointista toiseen liikkuminen ilman yhteyden katkeamista vaikeutuu ja saattaa vaatia valmistajakohtaisia ratkaisuita toimiakseen. VPN-palvelimen sijoittamisen kanssa pitää ottaa huomioon siitä aiheutuvat mahdolliset tietoturvariskit luotaessa suojattua polkua verkon sisälle. [33]

3.7 Yhteenveto

Turvallisuus on noussut yhdeksi kuumimmista puheenaiheista langattomien lähiverkkojen yhteydessä. Yritysmaailma joutuu kamppailemaan hallittavuuden ja turvallisuuden välissä seuraten uusien langattomien turvallisuusratkaisuiden syntymistä

ja kehittymistä kohti standardoituja sovelluksia. IEEE 802.11 -standardin ajoista on tultu jo pitkälle ja turvallisuus on ajanut helppokäyttöisyyden edelle.

Alkuperäisessä standardissa ovat määriteltyinä 40-bittinen WEP-salaus ja jaettuun salaiseen avaimeen perustuva todentaminen. Datan eheyden tarkistamista varten on määriteltynä lineaarisen 32-bittisen tarkistussumman käyttö. Jo pian julkaisunsa jälkeen WEP osoittautui haavoittuvaiseksi ja selvästi riittämättömäksi yritysmaailman käyttöön. Lisäksi heikko todentaminen ja avainten hallinnan puuttuminen kokonaan vaikeuttivat WLAN-tuotteiden läpimurtoa yritysmaailmassa. Laitteistovalmistajat kehittivät omia ratkaisuitaan torjumaan näitä heikkouksia, mutta yhteensopivuusongelmat pakottivat käyttämään vain yhden valmistajan verkkoja.

Todentamiseen käytettäväksi mekanismiksi on vähitellen vakiintumassa lankaverkoista omaksuttu IEEE 802.1X -standardiin perustuva järjestelmä, joka mahdollistaa ulkoisen todentamispalvelimen käytön. Standardin yhteydessä käytetään EAP-protokollaa, joka tarjoaa lisäksi menetelmät avainten hallintaan. Suurista valmistajista etenkin Cisco on ollut voimakkaasti kehittämässä langattomien verkkojen turvallisuutta ja monet alun perin Ciscon kehittämät ratkaisut ovat päätyneet Wi-Fi Allianssin WPA-ratkaisuun.

WPA tarjoaa korjaukset WEP-salauksen heikkouksiin ja sen käyttöönotto onnistuu ohjelmapäivityksellä. Salaukseen käytetään 128-bittistä avainta ja joka paketille luodaan oma yksilöllinen avain. Salasanan toistumista hyödyntävät hyökkäykset vaikeutuvat kun käytettävä alustusvektoriavaruus on kasvatettu 48 bittiin. Eheyden tarkistamiseen käytetään lineaarista menetelmää tehokkaampaa hajautusmenetelmää ja myös otsikkotiedot ovat mukana eheydentarkistuksessa.

WPA ei ole standardi, vaan ainoastaan suositus hyvästä toimintatavasta. WPA-yhteensopivuus laitteissa todennetaan testaamalla ja hyväksytysti testatut laitteet saavat käyttää Wi-Fi Allianssin yhteensopivuusmerkintää. Standardointirintamalla turvallisuutta parantava ratkaisu on IEEE 802.11i -standardi, jota ei ole vielä hyväksytty. Tämä WPA2 tarjoaa samat ratkaisut kuin WPA mutta lisäksi valittavana on kokonaan uudenlainen salausmekanismi AES. AES on salausalgoritmina hyvin erilainen kuin RC4 ja vaatii enemmän prosessointitehoa, joten WPA-laitetta ei voi ohjelmistopäivityksellä muuttaa WPA2-laitteeksi. Oheisessa taulukossa Taulukko 3-1 on koottuna kolmen merkittävimmän turvallisuusratkaisun eroja.

Taulukko 3-1 Turvallisuusstandardien vertailu [31]

	WEP	WPA	WPA2
Algoritmi	RC4	RC4	AES
Salausavain	40 bit	128 bit	128 bit
IV avaruus	24 bit	48 bit	48 bit
Eheys	CRC-32	Michael	CCM
Otsikon eheys	Ei ole	Michael	CCM
Avainten hallinta	Ei ole	EAP	EAP

Langattoman lähiverkon turvallisuutta voidaan parantaa myös ottamalla käyttöön VPN ja kokonaan erilainen lähestymistapa. VPN ei itsessään liity langattomiin verkoihin vaan on sovellus, jota käytetään langattomien ratkaisuiden päällä. VPN on turvallinen,

mutta sen soveltuvuus langattomaan ympäristöön jakaa mielipiteitä. VPN on suunniteltu langalliseen ympäristöön, joten langattoman verkon suorituskyky ja käytettävyys heikkenee turvallisuuden parantumisen myötä.

4 Hyökkäykset WLAN-verkkoja vastaan

Langattomia lähiverkkoja vastaan kohdistuvat hyökkäykset ovat periaatteessa samanlaisia kuin lankaverkoissa esiintyvät hyökkäykset. Langaton ympäristö avaa vain uusia mahdollisuuksia hyökkääjille ja aiheuttaa pieniä muutoksia hyökkäysmenetelmiin. Edelleen langattomiin verkkoihin voidaan hyökätä perinteisillä lankaverkon menetelmillä, jos langaton verkko on kytkettynä osaksi lankaverkkoa.

Langattomille verkoille on ominaista helppo asennettavuus, mutta turvallisuuden varmistaminen vaatii enemmän panostusta kuin lankaverkoissa. Usein langaton verkko on liitetty lankaverkon jatkoksi, jolloin hyökkäyksien tavoitteena voikin olla pääsyn saavuttaminen lankaverkkoon ja sen resursseihin. Huonosti asennettu langaton lähiverkko voi vaarantaa muuten suojatun lankaverkon turvallisuuden.

Hyökkäykset tapahtuvat kolmea verkon perusominaisuutta vastaan. Nämä ovat luottamuksellisuus, eheys ja käytettävyys. Luottamuksellisuutta vastaan hyökättäessä pyritään kaappaamaan siirrettävää tietoa, selvittämään tunnistetietoja tai purkamaan salausavaimia. Tavoitteena on saada haltuun luottamuksellista tietoa tai keinoja sen saamiseen. Eheyttä vastaan hyökätään muuttamalla siirrettävää tietoa tai verkossa olevia laitteita. Voidaan sijoittaa vihamielinen päätelaite yhteyden päätepisteiden väliin ja sen avulla kaapata, muuttaa ja lähettää vastaanottajalle tietoa. Käytettävyyttä vastaan hyökätään palvelunestohyökkäyksillä.

WLAN-verkon turvallisuuden perusratkaisuita vastaan on olemassa lukuisia hyökkäyksiä ja valmiita ohjelmia toteuttamaan niitä. Hyökkäyksien toteuttamisen helppous ja niihin tarvittavien laitteiden edullisuus lisäävät tarvetta käyttää kehittyneempiä ratkaisuja verkon turvallisuuden varmistamiseksi. Kehittyneemmätkään turvallisuusratkaisut eivät ehkäise hyökkäyksiä, jotka perustuvat esimerkiksi salaamattomaan ohjausliikenteeseen tai jaettuun langattomaan siirtomediaan. Seuraavissa kappaleissa käydään läpi mahdollisia hyökkäyksiä ja esitellään keinoja niiden vaikeuttamiseen sekä torjuntaan.

4.1 Verkon löytäminen

Verkkoon tunkeutuminen alkaa luonnollisesti verkon paikallistamisella. Verkon löytäminen (network discovery) onkin yleisin hyökkäys langattomia lähiverkkoja vastaan. Verkkojen etsinnästä käytetään usein hakkeroinnin historiasta periytyvää

nimitystä ”War Driving”. Tällaisen hyökkäyksen suosiota kasvattaa myös sen helppous ja vähäiset laitteistovaatimukset. Hyökkäyksen toteuttamiseen tarvitaan kannettava tietokone, langaton verkkokortti ja sopiva ohjelma, joita saa ilmaiseksi Internetistä. Lisäksi voidaan käyttää ulkoisia antenneja kasvattamaan toimintasädettä ja GPS-laitteita (Global Positioning System), jotka on mahdollista integroida toimimaan ohjelman kanssa, helpottamaan kerättyjen tietojen analysointia.

Hyökkäyksen toteuttamiseen soveltuvia ohjelmia on runsaasti tarjolla. Jo langattoman verkkokortin mukana tulevalla ohjelmistolla pääsee alkuun ja saa kerättyä perustietoa alueella olevista verkoista. Käyttöjärjestelmistä Microsoft Windows XP [34] sisältää langattomia lähiverkkoja varten käyttökelpoisia työkaluja. XP kertoo langattomien verkkotietojen lisäksi hyödyllistä tietoa verkkotopologiasta ja verkossa olevista aktiivisista palveluista. NetStumbler [35] on yksi suosituimmista verkon löytämiseen soveltuvista ohjelmista, jonka saa ilmaiseksi ladattua Internetistä. NetStumbler kertoo käyttäjälle tarvittavat tiedot verkon langattomista asetuksista. Ohjelma tukee GPS-laitteen käyttöä, joka helpottaa tulosten analysointia jälkikäteen. NetStumblerin ympärille on kehittynyt yhteisö, joka ylläpitää internetsivuillaan tietokantaa ohjelmalla havaituista verkoista ja niiden asetuksista.

Verkon löytämiseen käytettävien ohjelmien toiminta perustuu majakkapakettien kuuntelemiseen. Access pointit lähettävät säännöllisesti majakkapaketteja, joilla ne mainostavat itseään päätelaitteille ja kertovat muille access pointeille itsestään. Majakkapaketeissa kerrotaan tiedot verkon asetuksista siihen liittymistä varten. Majakkatoiminnon poiskytkeminen suojaa verkkoa yllämainituilta ohjelmilta, mutta haistelijaohjelmilla voidaan edelleen havaita verkko ja selvittää vastaavat verkkoasetukset. Haistelijoita käsitellään tarkemmin salakuuntelua koskevassa kappaleessa 4.3. Salauksella ei pystytä vaikeuttamaan verkon havaitsemista, sillä otsikkotietoja ja ohjausliikennettä ei salata. Verkon löytämiseen käytettävät ohjelmat voivat toimia täysin passiivisesti, jolloin niiden havaitseminen on vaikeaa, tai ne voivat aktiivisesti lähettää verkkoon pyyntöjä (probe). Tällaisten hyökkäyksien torjuntaa vaikeuttaa myös langattomien verkkojen ulottuminen rakennuksen seinien ulkopuolelle. Huonosti sijoitettujen access pointtien ja suunta-antennien käytön ansiosta hyökkääjä voi havaita verkkoja kaukaakin.

Verkkojen paikallistamisen motiivina voi olla pelkkä uteliaisuus eikä verkon löytämisestä itsessään ole harmia. Tavoitteena voi kuitenkin olla perustietojen hankkiminen muiden vaarallisempien hyökkäyksien toteuttamista varten. Tavoitteena voi olla myös ilmaisen internetyhteyden saaminen suojaamattomien verkkojen kautta.

4.2 Roque Adapter

Verkon löytämisestä seuraava askel on löydetyn verkon hyödyntäminen eli luvattoman päätelaitteen (roque adapter) kytkeminen verkkoon. Verkkoon kytkeytymisen tavoitteena voi olla ilmaisen internetyhteyden hyödyntäminen tai luottamuksellisen tiedon etsiminen verkon sisältä. Hyökkäyksen toteuttamiseen riittävät helpoissa tapauksissa samat laitteet kuin verkon löytämiseenkin eli tietokone, langaton verkkokortti ja verkon löytämiseen soveltuva ohjelma.

Jotta verkkoon liittyminen onnistuisi, pitää tietää oikeat asetukset access pointtiin assosioitumista ja IP-osoitteen hankkimista varten. Assosioitumista varten tarvitaan verkon SSID ja kanava, joiden selvittämiseen käytetään edellisestä kappaleesta tuttuja ohjelmia. Majakkatoiminnon ollessa päällä verkkoon liittyminen voidaan suorittaa suoraan valitsemalla listasta sopiva verkko. Majakkatoiminnon puuttuessa joudutaan SSID ja mahdollisesti kanava syöttämään käsin. MAC-suodatuksen ollessa päällä joudutaan selvittämään luvallinen MAC-osoite haistelijalla ja muuttamaan oma MAC-osoite vastaamaan sitä. WEP-salauksen ollessa aktivoituna pitää lisäksi selvittää käytetty salausavain. Salausavaimen purkamista käsitellään kappaleessa 4.4.

Assosioitumisen jälkeen tarvitaan vielä sopivat IP-asetukset, jotta verkossa voitaisiin toimia. Jos verkossa on käytössä DHCP-palvelu, saadaan tarvittavat asetukset sen kautta automaattisesti. DHCP-palvelun puuttuessa pitää oikeat osoitteet selvittää käsin haistelijan avulla. Päätelaitteen IP-osoitteen lisäksi tarvitaan oletusyhdyskäytävän osoite, jos halutaan liikennöidä verkosta muihin verkkoihin.

Verkkoon liittymistä voidaan vaikeuttaa kytkemällä majakkatoiminto ja DHCP-palvelin pois päältä sekä ottamalla MAC-suodatus ja WEP-salaus käyttöön. Kuten demonstraatiossa myöhemmin huomataan, eivät nämä keinot kuitenkaan ole riittäviä takaamaan verkon turvallisuutta.

4.2.1 MAC-osoitteen väärentäminen

MAC-osoitteen väärentämisellä (MAC address spoofing) tarkoitetaan verkkokortille valmistajan asettaman MAC-osoitteen muuttamista. Osoitteen muuttamista käytetään hyväksi monissa eri hyökkäyksissä, kuten verkkoon kytkeytymisessä ja Man-in-the-Middle-hyökkäyksissä. Osoitteen väärentäminen on useilla WLAN-tuotteilla erittäin helppoa. Jopa laitteiden mukana tulevilla ohjelmilla on mahdollista vaihtaa MAC-osoite haluamakseen.

MAC-osoitteen vaihtamisen tarkoituksena voi olla oman läsnäolon salaaminen verkkoa valvovilta hyökkäystentunnistusohjelmilta, pääsynhallintalistojen ohittaminen tai laillisesti todennetuksi käyttäjäksi tekeytyminen [36]. Hyökkäyksentunnistusohjelmat (NIDS, Network Intrusion Detection System) valvovat usein verkkoa MAC-osoitteiden perusteella ja tutkimalla yksittäisistä osoitteista tapahtuvaa liikennöintiä. Vaihtamalla MAC-osoitetta säännöllisesti hyökkääjä voi toteuttaa hyökkäyksiä valvonnan sitä huomaamatta. Verkkoon pääsyä voidaan rajoittaa MAC-osoitteiden perusteella sallimalla pääsy vain tietyille osoitteille. Hyökkääjä voi helposti selvittää haistelijalla sallittuja osoitteita ja sen jälkeen päästä verkkoon väärentämällä oman osoitteensa. Osa langattoman verkon todennusmenetelmistä käyttää MAC-osoitteita erottelemaan todennetut laitteet todentamattomista. Todentamattomista osoitteista ei ole pääsyä, mutta jo todennettujen laitteiden MAC-osoitteista tuleva liikenne päästetään verkkoon. Hyökkääjä voi ottaa käyttöönsä jo todennetun laitteen MAC-osoitteen ja siten päästä verkkoon ilman todentamista.

MAC-osoitteen väärentämisen havaitsemiseen on olemassa useita keinoja. IEEE määrittelee eri valmistajille omat MAC-avaruudet, joista ne jakavat MAC-osoitteita valmistamilleen laitteille. Nämä osoitelistat ovat yleisesti saatavilla ja listoilta

puuttuviin MAC-osoitteisiin törmääminen osoittaa yleensä osoitteen väärentämisen tapahtuneen. Lisäksi voidaan havaita tietyn valmistajan laitteen käyttävän eri valmistajan osoiteavaruutta, jolloin osoite voidaan taas päätellä väärennetyksi. Osoitetta säännöllisesti vaihtamalla toteutetut hyökkäykset voidaan havaita seuraamalla IEEE 802.11 -standardin mukaisten pakettien järjestysnumeroiden muuttumista. [36]

4.3 Salakuuntelu

Salakuuntelulla tarkoitetaan verkossa kulkevan tiedon kaappaamista. Kerätystä tiedosta voidaan etsiä tunnistetietoja, verkkoinformaatiota sekä muuta hyökkääjää kiinnostavaa informaatiota. Salakuuntelu on myös osana monia muita hyökkäyksiä, jotka tarvitsevat kaapattua tietoa toteutukseensa.

Salakuuntelun toteuttamiseen tarvitaan tietokoneen ja langattoman verkkokortin lisäksi kaappausohjelma eli haistelija (sniffer). Verkkokortille on vaatimuksena mahdollisuus asettaa se joko promiscuous- tai monitor-tilaan, jotta se kaappaisi muille tarkoitettua liikennettä. Normaalissa tilassa langaton verkkokortti hylkää muille kuuluvan liikenteen eikä käyttäjä pääse siihen käsiksi. Promiscuous-tilassa kortti assosioituu access pointin kanssa ja kaappaa sen jälkeen verkon liikennettä. Monitor-tilassa toimitaan täysin passiivisesti ilman assosioitumista. Haistelijat voivat kaapata kerrallaan kaiken yhdellä kanavalla siirtyvän liikenteen tai hyppiä kanavalta toiselle ja kaapata liikennettä kaikilta kanavilta, joilla sitä on.

Langattomia haistelijaohjelmia on saatavana ilmaiseksi Internetistä ja myös kaupallisia ratkaisuita on tarjolla. Ilmaisia ohjelmia ovat esimerkiksi Kismet [37] ja Ethereal [38]. Näistä Kismet suorittaa vain tiedon kaappausta. Ethereal suorittaa tiedon kaappauksen ohella sen analysointia. Esimerkki kaupallisesta ohjelmasta on AiroPeek NX [39].

WEP salauksen käyttäminen vaikeuttaa salakuuntelua muttei tee siitä mahdotonta. Salatut paketit pystytään kaappaamaan samalla tavalla kuin salaamattomatkin, mutta niiden avaamista varten pitää selvittää käytetty salausavain. Promiscuous-tilassa olevan haistelijan pystyy havaitsemaan seuraamalla access pointteihin assosioituneita päätelaitteita. Täysin passiivisen monitor-tilassa olevan haistelijan havaitseminen on protokollatasolla mahdotonta. Sen havaitseminen tutkimalla laitteista lähtevää radiosäteilyä on riittävän herkillä vastaanottimilla mahdollista, sillä vastaanottotilassakin laitteista vuotaa säteilyä niin sanottuna lokaalivuotona ja suunta-antennin käyttö voi vahvistaa vuotavan säteilyn voimakkuutta merkittävästi.

4.4 WEPin purkaminen

WEP-salauksen heikkoudet perustuvat huonoon alustusvektoritoteutukseen. RC4-algoritmia itsessään pidetään edelleen tehokkaana ja sitä käytetään lukuisissa sovelluksissa. Salaus perustuu kahden muuttujan käyttöön, joten jos toinen muuttujista tiedetään voidaan toinen ratkaista. Tuntemalla sekä salatun että salaamattoman informaation voi hyökkääjä helposti ratkaista käytetyn jonoavaimen. Salattu informaatio voidaan helposti kaapata siirron aikana, joten ensimmäinen ongelma hyökkäyksen

suorittamisessa on salattua informaatiota vastaavan selväkielisen informaation keksiminen.

Selväkielisen informaation keksimistä voidaan helpottaa lähettämällä ennakoitavaa liikennettä, joka sisältää ainoastaan yhtä merkkiä. Otsikkotiedoissa on myös paljon suhteellisen helposti arvattavaa muuttumatonta tietoa, kuten osoitetiedot. Pitkien selväkielisten viestien arvaaminen on tosin hankalaa, koska protokollat lisäävät viesteihin omia tietojaan. SNAP-otsikko (SubNetwork Access Protocol) on ensimmäisenä lähes jokaisen WLAN-verkossa liikkuvan salatun paketin otsikkokentässä. SNAP-otsikon ensimmäisenä tavuna on aina 0xAA, joten sitä voidaan käyttää, jos tarvitaan ainoastaan paketin ensimmäinen salattu tavu, kuten on tilastollisen hyökkäyksen tapauksessa [40].

Selväkielisen viestin arvaamiseen voidaan käyttää myös lineaarisen CRC-32-tarkistussumman mahdollistavaa bitinsiirtohyökkäystä (bit flip). Hyökkääjä kaappaa salattua liikennettä ja muuttaa sitä hieman. Myös tarkistussumma on salattuna, mutta hyökkääjän on mahdollista laskea muutoksen aiheuttama vaikutus tarkistussummaan ja siten saada tarkistussumma oikeaksi. Toisen tason eheydentarkistuksesta muokattu paketti menee läpi salauksen purkamisen jälkeen ja se lähetetään edelleen kolmannen tason sovellukselle. Kolmannen tason sovellukset huomaavat virheen, hylkäävät paketin ja lähettävät ennakoitavan vastauksen. [24]

Voidakseen hyökätä WEP-salausta käyttävään verkkoon ei tarvitse välttämättä ratkaista itse salaista avainta. Salaukseen käytettävän jonoavaimen selvittäminen tietyllä alustusvektorilla riittää, jos halutaan vain lähettää tietoa verkkoon. Tätä hyökkäystä kutsutaan jonoavaimen uudelleenkäytöksi ja se on mahdollinen koska WEP on tilaton protokolla. Keräämällä riittävästi eri alustusvektoreita vastaavia jonoavaimia voidaan myös purkaa salattua liikennettä. Jonoavaimen uudelleenkäyttöä hyödyntämällä suoritettavan hyökkäyksen toteuttaminen ei ole kannattavaa tehokkaampien hyökkäyksien löytymisen jälkeen ja pitkien selväkielisten viestien arvaamisen vaikeuden vuoksi.

Koko salaisen avaimen purkamiseen on olemassa kolmenlaisia hyökkäyksiä: sanakirjahyökkäys, voimahyökkäys ja tilastollinen hyökkäys [41]. Sanakirjahyökkäys käyttää hyväkseen valmiita sanalistoja, joilla yritetään arvata oikeaa salasanaa. Useiden valmistajien langattomien lähiverkojen laitteet mahdollistavat salasanojen muodostamisen käyttäjän antaman fraasin perusteella sen sijaan että salasanat pitäisi kirjoittaa manuaalisesti. Tämä helpottaa sanakirjahyökkäyksen käyttämistä, jos käyttäjien määrittelemät fraasit eivät ole tehokkaasti valittuja. Lisäksi useiden valmistajien salasananmuodostusgeneraattorit toimivat heikosti, johtaen huomattavasti pienempään entropiaan kuin 2^{40} [42]. Tilastollisen hyökkäyksen mahdollistavat alustusvektorien lähettäminen salaamattomana sekä niiden luonnista löytyneet heikkoudet kuten seuraavassa selviää. Voimahyökkäys ja sanakirjahyökkäys perustuvat oikean salasanan arvaamiseen ja oikean arvauksen verifiointiin kaapattujen pakettien avulla. Tilastollinen hyökkäys sen sijaan ratkaisee salasanan tavu kerrallaan.

WEPin tilafunktiolla (KSA) on kaksi merkittävää heikkoutta. Ensinnäkin on olemassa suuri joukko heikkoja alustusvektoreita, joita käytettäessä pieni osa salaista avainta määrittelee suuren osan tilafunktion tuloksesta. Toinen heikkous johtuu alustusvektorin lähettämisestä salaamattomana ja siitä seuraten samaa salaista avainta joudutaan

käyttämään monien hyökkääjälle näkyvien alustusvektoreiden kanssa. Yhdessä nämä heikkoudet mahdollistavat tilastollisen hyökkäyksen suorittamisen WEP-avaimen selvittämiseksi. [43]

Tilastollinen hyökkäys WEP-salausta vastaan tapahtuu seuraavan prosessin mukaisesti. Hyökkäyksen tarkempi kuvaus löytyy C. Peikarin ja S. Fogien kirjasta ”Wireless Maximum Security” [9] ja hyökkäyksen johtaminen ja matemaattinen todistus S. Fluhrerin ja kumppaneiden ”Weaknesses in the Key Scheduling Algorithm of RC4” dokumentista [43]. Lähtötiedoksi tarvitaan ensimmäinen salattu tavu selväkielisenä, jonka avulla ryhdytään ratkaisemaan salaista avainta tavu kerrallaan. Seuraavaksi pitää löytää heikko alustusvektori. Heikot alustusvektorit ovat algoritmin Algoritmi 4-1 mukaista muotoa, jossa B on salasanan arvattava tavu, N on tilataulukon suuruus eli 256 ja X jokin luku 0-255. On olemassa myös muita heikkoja alustusvektoreita, mutta niiden todennäköisyys paljastaa salasanan tavu on pienempi.

$$3 + B : N - 1 : X$$

Algoritmi 4-1 Heikko alustusvektori

Salasanan ratkaiseminen perustuu 5 % mahdollisuuteen, että tilataulukon neljä ensimmäistä arvoa eivät muutu tilafunktion neljän ensimmäisen kierroksen jälkeen [43]. Edellisen pätiessä tilafunktion neljäs kierros siirtää aina tilataulukon neljänteen kohtaan (S[3]) arvattavaan salasanantavuun liittyvän arvon ja pseudosatunnaisgeneraattori muodostaa siitä salaukseen käytettävän avaimen ensimmäisen tavun [9].

Hyökkääjä kaappaa salattua liikennettä ja ratkaisee jonoavaimen ensimmäisen tavun arvaamalla salatun viestin ensimmäisen tavun selväkielisen vastineen. Jonoavaimen ensimmäinen tavu saadaan selville suorittamalla looginen XOR-operaatio salatulle ja salaamattomalle tavulle. Seuraavaksi oletetaan jonoavaimen ensimmäisen tavun olevan tilataulukon neljännen kohdan arvo ja suoritetaan tilafunktion kolme ensimmäistä iterointikierrosta. Iterointikierrokset voidaan suorittaa kaapattujen alustusvektoreiden avulla tietämättä käytettyä salasanaa. Neljäs tilafunktion silmukka voidaan ratkaista taaksepäin tietämällä sen tulos, eli salaukseen käytetty tavu, ja kolmannen silmukan tulos. Neljännestä silmukasta selviää siten salaisen avaimen yksi tavu. Hyökkäyksen onnistumiseen on 5 % mahdollisuus. Yhdellä hyökkäyskierroksella voidaan selvittää salasanan yhden tavun arvo. Kaappaamalla tarpeeksi liikennettä ja ratkaisemalla mahdolliset heikot alustusvektorit voidaan koko salasana lopulta ratkaista tutkimalla paljastuneiden tavujen jakaumia. Salasanan ratkaisuun vaaditaan usean tuhannen heikon alustusvektorin analysointia, joka onnistuu noin viiden miljoonan paketin kaappaamisen jälkeen. [9]

Seuraavassa on esitettynä salasanan ensimmäisen tavun selvittämistä tilastollista hyökkäystä hyväksi käyttäen. Esimerkissä ratkaistaan yksi tavu salasanasta tunnettua heikkoa alustusvektoria hyödyntäen. Taulukossa Taulukko 4-1 on listattuna tarvittavat esitiedot. Esitiedoissa N on tilataulukon suuruus eli 256, B on ratkaistava salasanan tavu eli 0 ja l on salasanan pituus alustusvektorin kanssa eli 8. Näistä saadaan muodostettua heikko alustusvektori 3:255:7 (K[0]:K[1]:K[2]). Ratkaistava salasanan ensimmäinen tavu on 2 (K[3]). [9]

Taulukko 4-1 Esimerkissä käytettävät esitiedot

N	B	l	K[0]	K[1]	K[2]	K[3]
256	0	8	3	255	7	(2)

Ensiksi lasketaan salauksen suorittamista varten tilafunktion arvot kolmella ensimmäisellä kierroksella. Tilafunktion toiminta on selitetty algoritmissa Algoritmi 3-2. Kolmen ensimmäisen kierroksen laskemiseen ei tarvita muuta tietoa kuin käytetty alustusvektori, jonka hyökkääjä saa kaappaamastaan paketista. Tilafunktion tulokset näkyvät taulukossa Taulukko 4-2.

Taulukko 4-2 Tilafunktion kolme ensimmäistä kierrosta

KSA	i	j	S[0]	S[1]	S[2]	S[3]	n	S[n]
0		0	0	1	2	3		
1	0	3	3	1	2	0		
2	1	3	3	0	2	1		
3	2	12	3	0	12	1	12	2

Salausalgoritmi tarvitsee lisäksi tilafunktion neljännen kierroksen tuloksen, mutta hyökkääjä ei enää pysty laskemaan tätä suoraan. Neljännen kierroksen tulos on taulukossa Taulukko 4-3.

Taulukko 4-3 Tilafunktion neljäs kierros

KSA	i	j	S[0]	S[1]	S[2]	S[3]	n	S[n]
4	3	13+K[3]				S[13+K[3]]	13+K[3]	1
4	3	15	3	0	12	15	15	1

Hyökkäyksen onnistumisen kannalta joudutaan tekemään oletus että neljä ensimmäistä tilataulukon arvoa eivät enää muutu tilafunktion loppuun suorituksen aikana. Tällaisen tilanteen todennäköisyys on heikoilla alustusvektoreilla aikaisemmin mainittu 5 %. Tilataulukon muilla arvoilla ei ole merkitystä esimerkin kannalta.

Pseudosatunnaisgeneraattori muodostaa tilataulukon arvojen avulla jonoavaimen ensimmäisen tavun taulukon Taulukko 4-4 mukaisesti. Pseudosatunnaisgeneraattorin toiminta on esitettynä algoritmissa Algoritmi 3-3.

Taulukko 4-4 Jonoavaimen ensimmäinen tavu

PRGA	i	j	S[0]	S[1]	S[2]	S[3]	z
0	0	0	3	0	12	15	
1	1	0	0	3	12	15	15

Jonoavainta käytetään edelleen selväkielisen tekstin salaukseen. Ensimmäisenä tavuna on SNAP-otsikon ensimmäinen tavu 0xAA. Salaustapahtuma on kuvattuna taulukossa Taulukko 4-5.

Taulukko 4-5 Selväkielisen tekstin salaus

Selväteksti	z	Salattuteksti
0xAA	15	165

Hyökkääjä aloittaa hyökkäyksen kaappaamalla salattua liikennettä. Hän olettaa ensimmäisen tavun olevan 0xAA ja saa ratkaistua jonoavaimen ensimmäisen tavun, joka on 15. Hyökkääjä olettaa lisäksi avaimen ensimmäisen tavun olevan samalla tilataulukon neljäs arvo S[3]. Hyökkääjä suorittaa tilafunktion kolme ensimmäistä kierrosta kaapatusta paketista löytyvän informaation avulla. Tilafunktion neljäs kierros ratkaistaan etenemällä taaksepäin lopputuloksesta algoritmin Algoritmi 4-2 mukaisesti.

$$S[3] = z = 15$$
$$S[15] = S[3]_{(t-1)}$$
$$\rightarrow S[15] = 1$$
$$Vaihda(S[3], S[15])$$
$$\rightarrow S[3] = 1,\ S[15] = 15$$
$$j = 15,\ i = 3$$
$$15 = 12 + S[3] + K[3] = 13 + K[3]$$
$$\rightarrow K[3] = 15 - 13 = 2$$

Algoritmi 4-2 Tilafunktion neljännen kierroksen ratkaiseminen taaksepäin

WEP-salauksen purkamiseen on olemassa useita valmiita ilmaisohjelmia. WepAttack [44] käyttää hyväkseen sanakirjahyökkäystä. WEPCrack [45] ja AirSnort [46] käyttävät tilastollista hyökkäystä. Eri ohjelmien tehokkuutta on kasvatettu lisäämällä mahdollisten heikkojen alustusvektorien määrää ja kehittämällä tehokkaita algoritmeja suorittamaan avaimen arvausprosessia. WEP-salauksen purkamista voidaan vaikeuttaa vaihtamalla jaettua salaista avainta riittävän usein tai ottamalla käyttöön dynaamisia avaimia käyttäviä WEPin laajennuksia. WEP-salauksen 104-bittisen version käyttäminen ei sen sijaan auta tilastollisen hyökkäyksen torjunnassa [47].

4.5 Roque Access Point

Kielletyllä access pointilla (Roque Access Point) voidaan tarkoittaa kahta asiaa. Ensinnäkin kyseessä voi olla luvallisen käyttäjän luvaton access point, joka voi huonosti asennettuna muodostaa aukon koko verkon turvallisuuteen. Toinen vaihtoehto on vihamielisen luvattoman access pointin tapaus, jota tässä käsitellään.

Vihamielisen access pointin tarkoituksena voi olla aiheuttaa palvelunestohyökkäys. Päätelaitteet assosioituvat vahvimman access pointin kanssa. Käyttäjä voi yleensä määritellä vain verkon nimen, jonka jälkeen verkkokortti valitsee vahvimman signaalin omaavan yhteyden. Asettamalla suurella lähtöteholla ja suunta-antenneilla varustetun access pointin oikeaan paikkaan voi hyökkääjä saada ainakin osan verkon päätelaitteista

kadottamaan toimivan verkkoyhteytensä. Hyökkäykseen tarvittavan verkkoinformaation voi helposti selvittää haistelijan avulla.

Vastaavasti vihamielistä access pointtia voidaan käyttää lähetettävän tiedon kaappaamiseen ja muuttamiseen tekemällä Man-in-the-Middle-hyökkäys. Hyökkääjä saa käyttäjät assosioitumaan omaan laitteeseensa ja kaappaa kaiken lähtevän liikenteen. Halutessaan hyökkääjä voi muokata kaappaamaansa tietoa ja lähettää sen edelleen alkuperäiseen kohdeosoitteeseen. Näin käyttäjät eivät edes huomaa välissä toimivaa hyökkääjää. Man-in-the-Middle-hyökkäystä voidaan vaikeuttaa käyttämällä vahvempia todentamismenetelmiä langattoman lähiverkon perusratkaisuna tarjottavien yhdensuuntaisten todennusmenetelmien sijaan.

Vihamielisten access pointtien havaitsemista varten on olemassa ohjelmia, kuten AirMagnet [48] ja myös aikaisemmin esitellyistä hyökkääjien käyttämistä verkonhavaitsemisohjelmista on hyötyä vihamielisiä laitteita etsittäessä.

4.6 Man-in-the-Middle

Man-in-the-Middle- hyökkäyksessä (MitM) hyökkääjä asettuu yhteyden päätepisteiden väliin ja kaikki liikenne kulkee hänen kauttaan. Hyökkääjä voi oikeiden käyttäjien huomaamatta muokata liikkuvaa tietoa. MitM-hyökkäyksissä voidaan käyttää menetelminä ARP- myrkyttämistä (Adress Resolution Protocol) tai huonosti suojatuissa verkoissa yksisuuntaisen todentamisen luomaa tietoturva-aukkoa. Vihamielisen access pointin käyttämistä käsiteltiin aikaisemmassa kappaleessa. Tämä kappale keskittyy ARP-myrkyttämisen käyttämiseen.

ARP-myrkyttäminen perustuu IP- ja Ethernet-protokollien yhteistoimintaan ja tapahtuu MAC-tasolla. Ethernet-protokolla käyttää MAC-osoitteita pakettien lähettämiseen paikasta toiseen. Sovellukset taas käyttävät IP-protokollan osoitteita. Kohteen IP-osoitetta vastaava MAC-osoite selvitetään lähettämällä levityksenä ARP-request-paketti kaikille saman lähiverkon laitteille. Pyynnössä olevan IP-osoitteen omaava laite vastaa kysyjälle ARP-reply-paketilla, jossa se kertoo oman MAC-osoitteensa. Osoitteet talletetaan välimuistiin myöhempää käyttöä varten. ARP on tilaton protokolla, joten välimuistin tietoja päivitetään aina kun vastaus tulee riippumatta siitä onko kyselyä lähetetty. ARP-myrkyttämisessä lähetetään väärennettyjä vastauspaketteja ja saadaan ARP-taulukoiden arvot hyökkäykselle sopivaan muotoon. [49]

ARP-myrkyttäminen onnistuu vain saman lähiverkon laitteiden välillä. Access pointit toimivat yleensä MAC-tason siltoina, jolloin ARP-paketit kulkevat langattoman verkon ja lankaverkon välillä. ARP-myrkytys hyökkäyksen toteuttaminen langattomasta verkosta käsin on mahdollista suorittaa siis myös lankaverkossa oleville laitteille, jos access point toimii siltana. Hyökkäys tapahtuu lähettämällä normaalisti keskenään kommunikoiville laitteille uudet ARP-reply-paketit. Näissä paketeissa vastapuolen IP-osoitetta vastaavaksi MAC-osoitteeksi ilmoitetaan hyökkääjän osoite. Laitteet päivittävät taulukkonsa, koska olettavat lähettäneensä joskus pyynnön johon nyt vastattiin. Hyökkääjä vastaanottaa nyt molempien uhrien toisilleen lähettämän liikenteen ja halutessaan muokkaa sitä ennen eteenpäin lähetystä. Hyökkäys voidaan toteuttaa samaan access pointtiin assosioituneille laitteille tai eri access pointteihin

assosioituneille laitteille sekä lankaverkon laitteille, kunhan ARP-pakettien lähettäminen niiden välillä onnistuu. [50]

ARP-myrkyttämiseen ja MitM-hyökkäyksien toteuttamiseen löytyy valmiita ohjelmia. Dsniff [51], Ettercap [52] ja AirJack [53] ovat monipuolisia työkaluja, jotka osaavat hyökätä muun muassa SSH-yhteyksiä ja WEB-yhteyksiä vastaan. MitM-hyökkäys on mahdollista toteuttaa myös VPN-yhteyksiä vastaan. ARP-myrkyttämistä voidaan torjua sijoittamalla palomuuri langattoman verkon ja lankaverkon väliin. Tämä rajoittaa hyökkäykset langattomien laitteiden välille. Langattoman yhteyden suojaamiseksi voidaan käyttää vahvoja salausalgoritmeja suojaamaan tietoa. ARP-myrkyttämisen havaitsemiseen voidaan käyttää Arpwatch [54] ohjelman kaltaisia sovelluksia, jotka valvovat IP- ja MAC-osoitteiden välisten sidosten muuttumista.

4.7 Palvelunestohyökkäykset

Palvelunestohyökkäyksen tarkoituksena on estää laillisilta käyttäjiltä pääsy verkkoon ja sen resursseihin. DoS-hyökkäyksiä voidaan toteuttaa eri tasoilla aina fyysisestä tasosta sovellustasoon asti. Langattomia verkkoja vastaan voidaan hyökätä lankaverkoista tutuilla DoS-hyökkäyksillä ja lisäksi langattomia verkkoja vastaan on olemassa omat hyökkäyksensä. Pelkästään langattomia verkkoja koskevat DoS-hyökkäykset tapahtuvat kolmella alimmalla tasolla eli fyysisellä, siirtoyhteys- ja verkkotasoilla. Tässä keskitytään enemmän langattomalle verkolle tyypillisiin hyökkäyksiin ja perinteiset hyökkäykset mainitaan vain lyhyesti.

Sovellustason ja kuljetustason hyökkäykset ovat samanlaisia kuin lankaverkossa. Palvelin voidaan esimerkiksi saada käyttäjien ulottumattomiin generoimalla liikaa sallittuja pyyntöjä, joita palvelin ei ehdi käsitellä. TCP-protokollan (Transmission Control Protocol) ominaisuuksia hyödyntävällä SYN-hyökkäyksellä voidaan aiheuttaa palvelimelle tai päätelaitteelle tulva TCP-yhteyspyyntöjä, jotka johtavat sen puskureissa ylivuotoon ja kaikkien yhteyksien katkeamiseen. Kaistan ruuhkauttaminen estää käyttäjiltä verkon normaalin käytön. Ruuhkauttaminen voidaan toteuttaa esimerkiksi hajautetusti smurf-hyökkäyksellä, joka perustuu IP-osoitteen väärentämiseen ja ICMP-pyyntöjen (Internet Control Message Protocol) lähettämiseen. Langattoman verkon tapauksessa käytettävää kaistaa on suhteellisen vähän joten sen ruuhkauttaminen on helppoa. [55]

Fyysisen tason hyökkäykset perustuvat käytettävän jaetun median ominaisuuksiin. Langattomassa ympäristössä on käytössä vain rajallinen määrä taajuuksia ja niiden tukkiminen onnistuu esimerkiksi kohinatasoa nostamalla. IEEE 802.11b -standardin mukaiset laitteet käyttävät samaa taajuusaluetta johdottomien puhelimien, mikroaaltouunien ja bluetooth-laitteiden kanssa. Näiden laitteiden käyttäminen WLAN-laitteiden läheisyydessä voi aiheuttaa kanavan tukkeutumisen. Hyökkäys voidaan suorittaa myös langattomilla verkkokorteilla esimerkiksi muokkaamalla kortin ohjelmistoa ja pakottamalla se jatkuvaan lähetystilaan. Verkkokortin firmware-ohjelmiston muokkaaminen edellyttää, että hyökkääjä saa käsiinsä alkuperäisen lähdekoodin ja tuntee korttia ohjaavat käskyt halutun tilan saavuttamiseksi. On mahdollista, että korttien firmware-ohjelmistoissa on dokumentoimattomia

ominaisuuksia, joita käytetään laitteiden testaamiseen ja jotka mahdollistavat hyökkäyksen toteuttamisen.

ARP-myrkyttämistä voidaan käyttää myös DoS-hyökkäyksen suorittamiseen väärentämällä laitteen ARP-taulukko vaihtamalla sinne keksittyjä MAC-osoitteita oikeiden tilalle. Tämä johtaa pakettien hylkäämiseen ja estää käyttäjää lähettämästä liikennettä. ARP-myrkyttämiseen pohjautuvan hyökkäyksen toteuttaminen on helppoa valmiiden ohjelmien avulla. [49]

4.7.1 Ohjausliikenteeseen perustuvat hyökkäykset

IEEE 802.11 -standardin mukaista salaamatonta ohjausliikennettä voidaan käyttää palvelunestohyökkäyksien toteuttamiseen. Ohjausliikenteen eheyttä ei tarkisteta, joten väärennettyjen pakettien lähettäminen on mahdollista. Ohjausliikenteeseen perustuvien hyökkäyksien torjuminen on hankalaa, koska standardin mukaisesta toiminnasta poikkeaminen saattaa aiheuttaa yhteensopivuusongelmia.

Langaton media voidaan ruuhkauttaa lähettämällä sinne paljon liikennettä tai käyttämällä hyväksi kättelymenettelyn ominaisuuksia. Kättelyssä päätelaitteet pyytävät access pointilta lupaa lähettää RTS-viestillä ja access point antaa lähetysluvan CTS-viestillä. Muut verkon laitteet näkevät CTS-paketit ja eivät lähetä omaa liikennettään paketeissa määriteltynä aikana. Tekeytymällä verkon access pointiksi ja lähettämällä jatkuvasti CTS-paketteja keksityille osoitteille hyökkääjä estää muita verkon laitteita lähettämästä liikennettään. Yhdellä CTS-viestillä voidaan varata kanava 32 millisekunniksi (32767 μs) [5]. CTS-hyökkäyksen toteuttaminen edellyttää ohjausliikenteen hallittua lähettämistä. Ohjausliikenteen lähettämisestä huolehtii verkkokortin firmware-ohjelmisto, joten sitä pitää pystyä muokkaamaan halutunmuotoisten ohjauspakettien lähettämiseen soveltuvaksi. CTS-hyökkäyksen toteuttamista vaikeuttaa edelleen useiden laitevalmistajien tuotteiden toiminta kaistan varauksen suhteen IEEE 802.11 -standardista poikkeavalla tavalla [56].

Käyttäjäntunnistukseen liittyy monia DoS-hyökkäyksiä. Voimassa olevan todennuksen voi poistaa standardin mukaisella todennuksen purku -kehyksellä (deauthentication). Purkuilmoitus on ehdoton ja siihen ei voi reagoida muuten kuin siirtymällä todennustilakoneen ensimmäiseen todentamattomaan tilaan. Todentamattomassa tilassa oleva laite hylkää kaikki paitsi ensimmäiseen luokkaan kuuluvat kehykset ja datan lähettäminen on mahdollista vasta uuden todentamisprosessin loppuun suorittamisen jälkeen. Lähettämällä jatkuvasti yhteyden katkaisevia viestejä voidaan verkon päätelaitteita estää pääsemästä verkkoon. Hyökkäys voidaan suorittaa myös assosioinnin purku -viestillä (disassociation), mutta se aiheuttaa vain assosioinnin katoamisen ja hyökkäyksen kohteena oleva laite pääsee pienellä vaivalla takaisin verkkoon.

Myös kehittyneempää EAP-protokollan mukaista todentamista vastaan voidaan hyökätä vastaavalla tavalla lähettämällä väärennettyjä protokollan mukaisia viestejä vääriin aikoihin. Esimerkiksi EAP-succesfull- tai EAP-failure-viestien lähettäminen kesken todennusprosessin johtaa sen epäonnistumiseen.

IEEE 802.11 -standardin mukaista tehonsäästöominaisuutta voidaan myös hyödyntää palvelunestohyökkäyksen suorittamiseen. Akkukäyttöisten laitteiden toiminnan tehostamista varten standardissa on määriteltynä mahdollisuus laittaa verkkokortti välillä tehonsäästötilaan (power save), jolloin se ei voi vastaanottaa tai lähettää liikennettä. Access point puskuroi nukkuvalle laitteelle lähetettävää liikennettä kunnes laite on taas valmiina vastaanottamaan. Nukkuva laite herää tasaisin väliajoin tiedustelemaan access pointilta, onko sille tulossa liikennettä tehonsäästökyselypaketeilla (power save poll). Hyökkääjä voi lähettää kyselypaketteja uhrin nukkuessa, jolloin access point lähettää puskuroidun liikenteen. Vastaavasti hyökkääjä voi vastata uhrin kyselyyn access pointtina kertoen, että puskuroitua liikennettä ei ole, jolloin uhri palaa nukkumaan. Kolmantena vaihtoehtona hyökkäykselle on aiheuttaa tehonsäästötilassa olevan laitteen ajastuksen sotkeutuminen. Jos nukkuva laite ei ole synkronoituna access pointin kanssa, se ei osaa herätä oikeaan aikaan lähettämään kyselyitä ja vastaanottamaan liikennettä. [56]

Ohjausliikenteeseen liittyvien palvelunestohyökkäysten toteuttamista käsitellään tarkemmin J. Bellardon ja S. Savagen dokumentissa ”802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions” [56]. Ohjausliikenteeseen perustuvien hyökkäysten suorittaminen edellyttää hallittua ohjausliikenteen lähettämistä. Normaalissa tilassa verkkokortin firmware-ohjelmisto huolehtii ohjausliikenteen lähettämisestä ja käsittelystä ilman että käyttäjä pääsee käsiksi siihen. Hyökkääjän on muokattava kortin firmware-ohjelmistoa tai löydettävä jokin muu keino ohjauskehysten generointiin ilman että verkkokortti muuttaa niitä ennen lähetystä.

4.7.2 Hyökkäykset WPA-ratkaisuja vastaan

WPA-laitteita vastaan on olemassa ainakin yksi DoS-hyökkäys, joka perustuu WPA-ratkaisussa käytettyyn tunkeutumisilta suojaavaan ominaisuuteen. TKIP:n kanssa toimivaa MIC-eheydentarkistusta käytetään aktiivisten hyökkäysten torjunnassa. MIC-tarkistusta edeltää CRC-tarkistussumman ja alustusvektorien tarkistus, joten virhe MIC-tarkistuksessa johtuu yleensä aktiivisesta hyökkäyksestä. MIC-virheen sattuessa access point poistaa käytöstä senhetkiset salausavaimet. Jos virhe sattuu ryhmäavaimissa ne poistetaan ja vastaavasti virheen sattuessa pariavaimissa ne poistetaan käytöstä. Jos edellisestä virheestä on aikaa yli minuutti, lähettää access point uudet avaimet. Jos taas edellisestä virheestä on alle minuutti, odottaa access point minuutin jälkimmäisen virheen tapahtumisesta ja lähettää uudet avaimet vasta sitten. Hyökkääjän lähettäessä minuutin aikana kaksi MIC-tarkistuksessa kiinni jäävää pakettia verkkoon tulkitsee WPA sen yritykseksi päästä tunkeutumaan verkkoon. WPA suojautuu oletettua tunkeutumisyritystä vastaan katkaisemalla kaikki access pointissa olevat yhteydet minuutiksi. Hyökkääjä onnistuu näin aiheuttamaan kaikille kyseisen access pointin käyttäjille palvelunestohyökkäyksen. Hyökkäystä voidaan ylläpitää lähettämällä kaksi väärin salattua MIC-tarkistuksessa kiinni jäävää pakettia access pointille minuutin sisällä. Hyökkäyksen toteuttaminen vaatii pakettien, jotka menevät muista tarkistuksista paitsi MIC-tarkistuksesta läpi, lähettämistä ja on siten hankalaa, jollei hyökkääjällä ole pääsyä verkkoon. [57] [30]

4.7.3 DoS-hyökkäyksissä käytettävät ohjelmistot

DoS-hyökkäysten toteuttamiseen on olemassa valmiita ohjelmia, kuten edellisestä kappaleesta tutut Ettercap, AirJack ja Dsniff. Todentamiseen ja assosiointiin liittyvien hyökkäyksien toteuttamiseen on olemassa Void11 [58] ohjelma. DoS-hyökkäyksiä vastaan suojautuminen on hankalaa, koska suurin osa niistä perustuu protokollien normaaliin toimintaan. Osa hyökkäyksistä voidaan torjua ottamalla käyttöön kehittyneempiä todennusmenetelmiä ja staattisia verkkoasetuksia.

4.8 Hyökkäykset 802.1X-ratkaisuita vastaan

Heikoimpia EAP-toteutuksia vastaan on mahdollista suorittaa yhteyden kaappaus ja Man-in-the-Middle-hyökkäyksiä. Hyökkäyksien perustana on viestien aitouden tarkastamisen ja tilakoneiden synkronoimisen puute IEEE 802.1X ja IEEE 802.11 -standardeissa. EAP-MD5- ja EAP-TLS-versioita käytettäessä on mahdollista suorittaa MitM-hyökkäys tekeytymällä access pointiksi ja lähettämällä EAP-Success-paketti päätelaitteelle. Päätelaite siirtyy todennettuun tilaan alkuperäisestä tilastaan riippumatta ja lähettää kaiken liikenteensä suoraan hyökkääjälle. Yhteyden kaappaus voidaan suorittaa seuraavalla menetelmällä. Käyttäjä todentaa itsensä normaalisti, jonka jälkeen hyökkääjä lähettää hänelle MAC-disassociate-viestin. Käyttäjä menettää yhteytensä, mutta todennusjärjestelmä säilyy edelleen todennetussa tilassa. Hyökkääjä voi näin käyttää yhteyttä ottamalla itselleen käyttäjän MAC-osoitteen. Hyökkäyksien toimivuus edellyttää salausavaimen tuntemista tai salauksen puuttumista verkosta. [59]

Salauksen ja dynaamisten avainten käyttäminen ehkäisee edellä mainittuja hyökkäyksiä, mutta palvelunestomielessä hyökkäykset on edelleen mahdollista toteuttaa. Myös kehittyneempien EAP-versioiden käyttäminen auttaa.

4.9 Yhteenveto

Langatonta verkkoa on vaikea piilottaa avoimen siirtomediansa takia, joten lähes aina hyökkääjä onnistuu löytämään verkon. IEEE 802.11 -standardin mukaiset turvallisuuden perusratkaisut ovat selvästi riittämättömiä takaamaan luottamuksellista informaatiota kuljettavan verkon turvallisuutta. Käyttäjäntunnistuksen, WEP-salauksen ja lineaarisen tarkistussumman tarjoama turva riittää ainoastaan kotikäyttäjille. Lisäksi verkon ylläpidolliset ongelmat tulevat suurissa verkoissa ylitsepääsemättömiksi.

Langaton liikenne on myös aina mahdollista kaapata ja useimmissa tapauksissa voidaan suorittaa verkkoa vastaan MitM-hyökkäys. Salaus on siis äärimmäisen kriittinen osa langattomassa verkossa siirrettävän informaation luottamuksellisuuden takaamista. Uusimmat dynaamisia avaimia hyödyntävät salausmenetelmät auttavat torjumaan perinteisiä WEP-hyökkäyksiä ja tehokkaiden eheydentarkastusmenetelmien kanssa verkko voidaan luottamuksellisuuden mielessä saada hyvinkin kestäväksi. Ulkoisten todentamispalveluiden käyttäminen ja tehokkaat käyttäjäntunnistusmenetelmät pystyvät lisäksi parantamaan todennuksen tehokkuutta huomattavasti. Yrityskäytössä WPA-

ratkaisun avulla voidaan yleensä taata riittävä turvallisuustaso. Myös VPN-sovellukset pystyvät antamaan langattomalle verkolle vastaavaa suojaa. WPA2-laitteiden saapumisen odotetaan edelleen nostavan langattomien verkkojen turvallisuuden uudelle tasolle.

Palvelun saatavuuden takaamiseen ei kuitenkaan ole vielä olemassa ratkaisua. Langattoman siirtomedian tukkiminen on aina mahdollista ja protokollan toimintaan perustuvien hyökkäyksien torjuntaan ei ole näköpiirissä keinoja standardin muutoksien avulla. Palvelun saatavuuden kannalta kriittisissä ympäristöissä palvelunestohyökkäyksien torjunta on suoritettava muilla tavoin, kuten estämällä hyökkääjän pääsy laitteiden kantaman sisäpuolelle.

5 Demonstraatio

Seuraavissa kappaleissa kuvaillaan erilaisia hyökkäysskenaarioita langattomia lähiverkkoja hyödyntäviä järjestelmiä vastaan sekä kokeillaan käytännössä erityyppisten hyökkäyksien toimivuutta. Hyökkäysskenaarioita kuvailtaessa käydään läpi eri vaihtoehtoja alkaen verkon laitteiden joutumisesta vihamielisten käyttäjien käsiin ja päätyen verkkoon kuulumattomien vihamielisten laitteiden aiheuttamiin uhkakuviin. Esitettäville hyökkäysvaihtoehdoille tarjotaan myös torjuntakeinoja olemassa olevien ratkaisuiden puitteissa. Hyökkäyksien kokeilu suoritetaan demonstraatioverkossa, jonka toiminta vastaa yksinkertaista langatonta lähiverkkoa.

5.1 Mahdollisia hyökkäysskenaarioita

Langattomia lähiverkkoja vastaan tapahtuvat hyökkäykset voidaan jakaa suoritustapansa mukaan karkeasti kahteen ryhmään hyökkäykseen käytettävien laitteiden mukaan. Hyökkäyksen lähtöpisteenä voi olla vihamielisen käyttäjän haltuun joutunut laite tai kokonaan verkon ulkopuolinen vihamielinen laite. Verkon normaalien laitteiden avulla suoritettavat hyökkäykset ovat verkon turvallisuuden kannalta ongelmallisia, koska luvattoman käytön erottaminen luvallisesta on hankalaa ja turvallisuuden parantaminen tapahtuu yleensä käyttäjäystävällisyyden kustannuksella. Seuraavassa käsitellään erilaisia uhkakuvia, esitellään tapausten mahdollistamia hyökkäyksiä ja tarjotaan vaihtoehtoja hyökkäysten torjuntaan.

5.1.1 Päätelaite vihamielisen käyttäjän hallussa

Päätelaitteen joutuminen vihamielisen käyttäjän haltuun aiheuttaa käytetyistä turvallisuusratkaisuista riippuen eriasteisen uhan. WEP-salauksen ja muiden perusratkaisuiden ollessa ainoat verkkoa suojaavat menetelmät päätelaitteen joutuminen vihamielisen käyttäjän haltuun johtaa verkon turvallisuuden huomattavaan heikkenemiseen. Salausavaimet on talletettuna päätelaitteeseen, joten hyökkääjä saa ne haltuunsa. Päätelaitteesta riippuen hyökkääjä voi jopa saada haltuunsa salausavaimet selkokielisenä ja siten käyttää niitä myös muissa laitteissaan. Todentaminen perustuu joko salausavaimiin tai päätelaitteen fyysisiin tunnistetietoihin. Kummassakin tapauksessa hyökkääjällä on kaikki tarpeellinen itsensä todentamista ja verkkoon pääsyä varten. Hyökkääjä voi hyödyntää verkon resursseja ja kaapata liikennettä. Salauksen

purkaminen onnistuu päätelaitteeseen talletettuja salausavaimia käyttäen. Tavoitteena hyökkääjällä voi olla salaisen tiedon kaappaaminen tai siirrettävän tiedon muokkaaminen.

Suurin ongelma hyökkäysten torjunnassa on niiden havaitseminen. Päätelaitteen joutumista vihamielisen käyttäjän haltuun ei välttämättä havaita nopeasti ja luvattoman toiminnan erottaminen luvallisesta on hankalaa. Turvallisuuden perusratkaisuita käytettäessä hyökkäysten torjuminen vaatii nopeaa reagoimista uhan tultua ilmi. Kaikkiin verkon laitteisiin on vaihdettava kaikki salausavaimet, sillä hyökkääjälle riittää että hän tietää yhden avaimen kunhan se on muilla samassa kohdassa salasanalistassa. Todennuksen perustuessa korttien fyysisiin tunnistetietoihin on access pointtien pääsylistoja muokattava vastaamaan muuttunutta tilannetta.

Kehittyneempien turvallisuusratkaisuiden ollessa käytössä päätelaitteen joutuminen hyökkääjän haltuun ei välttämättä johda yhtä suuriin ongelmiin kuin perusratkaisuiden ollessa kyseessä. EAP-protokollien mukaisessa todennuksessa voidaan käyttää useita eri todennusmetodeja. Laitesidonnaisen todennuksen sijaan voidaan käyttää käyttäjäsidonnaista todennusta tai niiden yhdistelmää. Käyttäjäsidonnaisen todennuksen ollessa käytössä hyökkääjälle ei riitä päätelaitteen saaminen haltuunsa, vaan hän tarvitsee luvallisen käyttäjän tunteman salasanan tai muun todennukseen käytettävän tunnisteen. Edelleen jos todennus tapahtuu vain laitteiston fyysisten tunnisteiden perusteella riittää hyökkääjälle päätelaitteen hankkiminen verkkoon pääsyn mahdollistamiseksi. Salauksen perustuessa TKIP- tai AES-menetelmien käyttöön ei salausavaimia tallenneta päätelaitteeseen vaan ne saadaan todennuksen päätteeksi todentamispalvelimelta. Lisäksi jokaiselle yhteydelle käytetään omia avaimiaan ja avaimia vaihdellaan säännöllisesti, joten yhden yhteyden avainten paljastuminen ei vaaranna koko verkon salausta.

Päätelaitetta voidaan käyttää myös palvelunestohyökkäyksien suorittamiseen verkon ulkopuolisen laitteen tavoin. Palvelunestohyökkäyksiä käsitellään verkon ulkopuolisista laitteista alkavien hyökkäysten yhteydessä.

5.1.2 Access Point vihamielisen käyttäjän hallussa

Access pointin joutuminen vihamielisen käyttäjän haltuun on vaarallisempaa kuin päätelaitteen tapauksessa. Access point on verkon kriittisin piste, sillä kaikki liikenne langattoman ja lankaverkon välillä kulkee sen kautta. Access pointtia hallitseva vihamielinen käyttäjä voi helposti suorittaa palvelunestohyökkäyksen. Asetusten muuttaminen tai yhteyden fyysinen katkaiseminen estää verkon normaalin käyttämisen. Hyökkääjä voi lisäksi muokata access pointin pääsylistoja ja sallia verkkoon pääsyn omille laitteilleen. Asetusten muokkaamista voidaan vaikeuttaa sallimalla se vain lankaverkon puolelta ja asettamalla vahva salasana suojaamaan access pointtia. Kehittyneempien todennusmenetelmien ja erillisten palvelimien käyttö estää hyökkääjää sallimasta verkkoon pääsyä uusille laitteille. Turvallisuuden perusratkaisuiden ollessa käytössä access pointista voidaan selvittää samat tiedot kuin päätelaitteistakin edellisessä kappaleessa.

Langattoman verkon salaus loppuu yleensä langattoman verkon reunalle ja yleensä tämä reunapiste on access point. Liikenteen kaappaaminen access pointin jälkeen mahdollistaa salaisen tiedon haltuun saannin ja muokkaamisen ilman salauksen purkua. Tiedon salaaminen langattoman verkon ulkopuolella voidaan hoitaa korkeamman tason sovellusten avulla tai esimerkiksi VPN-yhteyksiä käyttämällä.

5.1.3 Verkon ulkopuolinen vihamielinen laite

Verkon ulkopuolisen laitteen käyttäminen hyökkäykseen on helpompi havaita kuin verkon omien laitteiden suorittamat hyökkäykset. NIDS-ohjelmien käyttäminen luvattomien access pointtien ja päätelaitteiden havaitsemiseen mahdollistaa käynnissä olevien hyökkäysten tunnistamisen.

Access pointtia voidaan käyttää palvelunestohyökkäysten suorittamiseen, jos saadaan verkon käyttäjät assosioitumaan hyökkääjän asettamaan verkon ulkopuoliseen access pointtiin. Hyökkäystä varten käytetään suunta-antenneja voimakkaiden signaalien muodostamiseen, koska päätelaitteet yleensä assosioituvat voimakkaimman signaalin omaavaan access pointtiin. Väärään access pointtiin assosioituneet laitteet eivät pääse käsiksi verkon normaalisti tarjoamiin palveluihin. Assosioinnin jälkeen access pointtia voidaan hyödyntää myös MitM-hyökkäyksen suorittamiseen. Access pointtiin perustuvia hyökkäyksiä voidaan vaikeuttaa käyttämällä kaksisuuntaista todentamista ja siten estämällä väärät assosioitumiset.

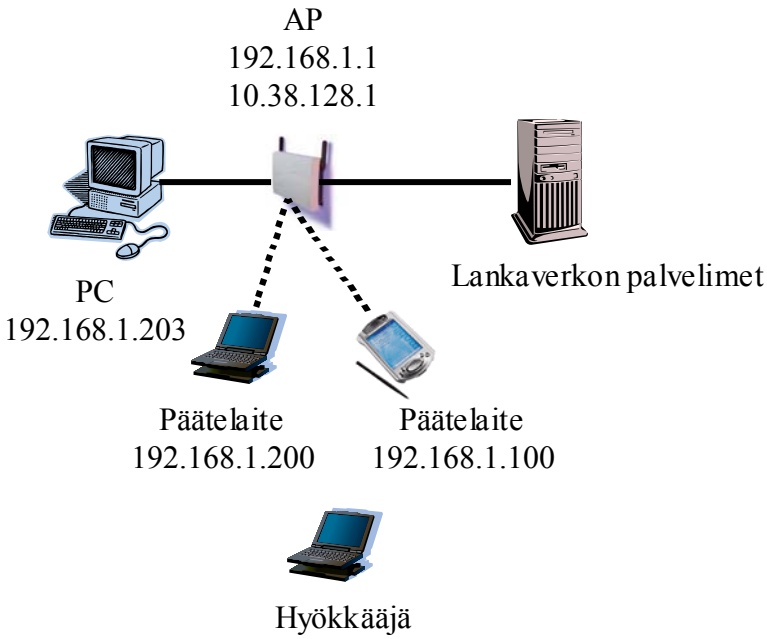
Päätelaitteita voidaan käyttää verkkoon liittymiseen, verkon salakuunteluun ja salauksen purkuun. Kehittyneiden todennus- ja salausmenetelmien käyttö vaikeuttaa verkkoon liittymistä sekä kaapatun liikenteen salauksen purkamista. Palvelunestohyökkäyksien estäminen on vaikeampaa. Kaistan tukkimiseen perustuvan hyökkäyksen lähde voidaan paikallistaa, mutta hyökkäyksen torjumisen ainoa vaihtoehto on vaihtaa kanavaa ja toivoa ettei uusi kanava ole tukossa. Käyttäjäntunnistukseen liittyviä hyökkäyksiä voitaisiin estää lisäämällä protokollan toimintaan viive ennen todennuksen purku -komennon toteuttamista. Normaalissa tapauksessa todennuksen purkuun johtavan pyynnön lähettäjä ei liikennöi verkkoon enää pyynnön jälkeen. Hyökkäyksen tapauksessa liikennöinti kuitenkin jatkuu ja pyynnön voitaisiin olettaa olevan palvelunestohyökkäyksen aikaansaama. Todennuksen purun keskeyttäminen liikennöinnin jatkuessa pyynnön lähettämisen jälkeen estäisi palvelunestohyökkäyksen toteuttamisen tällä menettelyllä.

5.2 Demonstraatiojärjestelmä

Demonstraatiossa käytettävä verkko koostuu yhdestä access pointista ja kahdesta päätelaitteesta. Hyökkäykset suoritetaan kolmatta päätelaitetta käyttämällä. Access pointtina käytetään Linksys BEFW11S4 langatonta access point -reititintä [60], johon on kytkettynä PC asetusten määrittelyä varten ja josta on yhteys lankaverkkoon. Lankaverkossa on tarvittavat palvelimet liikenteen luomista ja verkon toimintaa varten.

Päätelaitteina toimivat Dell Inspiron 4100 [61] kannettava tietokone Microsoft Windows 2000 [34] -käyttöjärjestelmällä ja Linksys WPC11 versio3 [60] langattomalla verkkokortilla sekä Compaq iPaq [62] kämmentietokone D-Link Air DCF-660W [63] langattomalla verkkokortilla ja Opie versio 0.9.1 [64] -käyttöjärjestelmällä varustettuina.

Verkon osoitteet on jaettu kuvan Kuva 5-1 mukaisella tavalla. Eri hyökkäyksien aikana osoitteiden jakaminen toteutetaan joko manuaalisesti tai access pointissa toimivan DHCP-palvelimen avulla. Verkon SSID on latenet ja käytettävä kanava on 1. Käytettävät salaus- ja todennusmenetelmät määritellään tapauskohtaisesti. Verkon liikenne luodaan siirtämällä tiedostoja päätelaitteiden ja lankaverkossa olevan http-palvelimen välillä sekä lähettämällä PING-kyselyjä päätelaitteiden ja access pointin välillä.



Kuva 5-1 Demonstraatioverkon kokoonpano

Hyökkääjänä käytetään Dell Inspiron 4150 [61] kannettavaa tietokonetta Microsoft Windows XP [34] ja Red Hat Linux 9 [65] -käyttöjärjestelmillä ja Orinoco 11b PC Card Gold [66] langatonta verkkokorttia. Hyökkäyksiin käytettäviä ohjelmia käsitellään erikseen kunkin hyökkäyksen yhteydessä.

5.3 Toteutettuja hyökkäyksiä

5.3.1 Verkon löytäminen ja verkkoon liittyminen

Verkon löytämistä ja verkkoon liittymistä tutkitaan kolmella eri tapauksella. Tapauskohtaisesti määritellyt asetukset on kuvattuna kunkin tapauksen yhteydessä. Eri tapauksissa verkon havaitsemiseen käytetään kulloinkin siihen soveltuvaa ohjelmaa ja verkkoon liitytään riittävien tietojen selvittyä.

5.3.1.1 Tapaus 1: NetStumbler

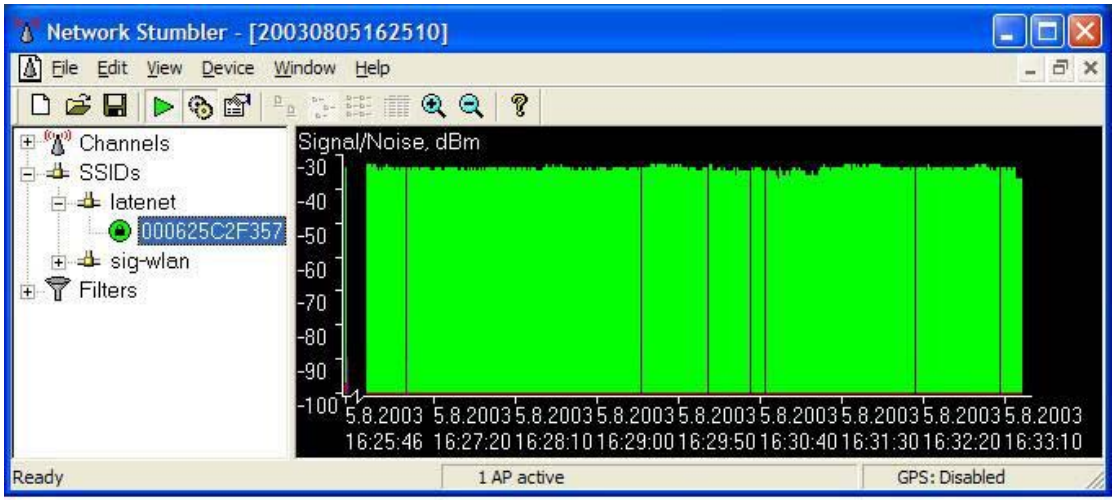
Ensimmäisessä tapauksessa verkon löytämiseen käytetään NetSumbler-ohjelmaa. Verkkoasetukset tässä tapauksessa ovat taulukon Taulukko 5-1 mukaiset. Majakkapalvelua pidetään päällä, jotta voidaan demonstroida NetStumblerin toimintaa. Muilla asetuksilla ei ole verkon löytymisen kannalta merkitystä.

Taulukko 5-1 Tapaus 1 verkkoasetukset

Tapaus	Majakka	Todennus	Salaus	DHCP
1	päällä	avoin	40 bittinen	päällä

NetStumbler havaitsee alueelta kaksi langatonta verkkoa kuvan Kuva 5-2 mukaisesti. Testiverkkomme osalta saamme selville SSID:n, access pointin MAC-osoitteen, käytetyn kanavan, salauksen sekä paljon muuta hyödyllistä tietoa access pointista ja signaalin laadusta. Signaalin laatua voi tarkastella myös graafisesti, kuten kuvassa Kuva 5-3 näkyy testiverkon access pointin signaalikohinasuhde ajan funktiona.

Kuva 5-2 NetStumbler havaitsemassa verkkoja



Kuva 5-3 NetStumbler signaalikohinasuhde

Verkkoon liittymistä varten tarvitsisimme salausavaimen, jonka selvittämiseen palataan myöhemmin.

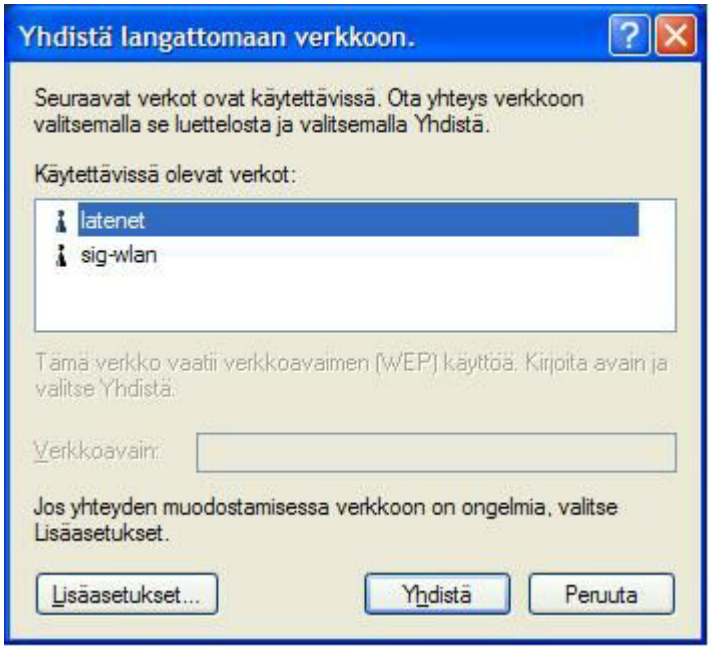
5.3.1.2 Tapaus 2: Windows XP

Toisessa tapauksessa käytetään hyväksi Windows XP:n tarjoamia ominaisuuksia. Verkon asetukset löytyvät taulukosta Taulukko 5-2. Asetukset ovat muuten samat kuin ensimmäisessä tapauksessa mutta salaus on kytketty pois verkkoon liittymisen demonstrointia varten.

Taulukko 5-2 Tapaus 2 verkkoasetukset

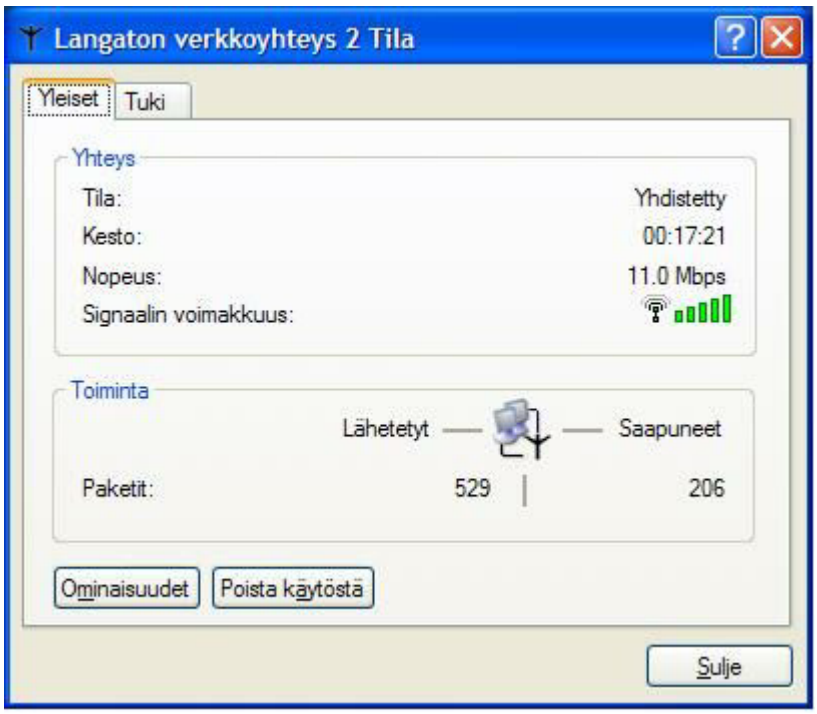
Tapaus	Majakka	Todennus	Salaus	DHCP
2	päällä	avoin	pois	päällä

Windows XP havaitsee alueella toimivat verkot kuvan Kuva 5-4 mukaisesti. Havaitseminen perustuu samoihin menetelmiin kuin NetStumblerilla. Verkkoon liittyminen onnistuu nappia painamalla ja tarvittavat osoiteasetukset saadaan aktiiviselta DHCP-palvelimelta.

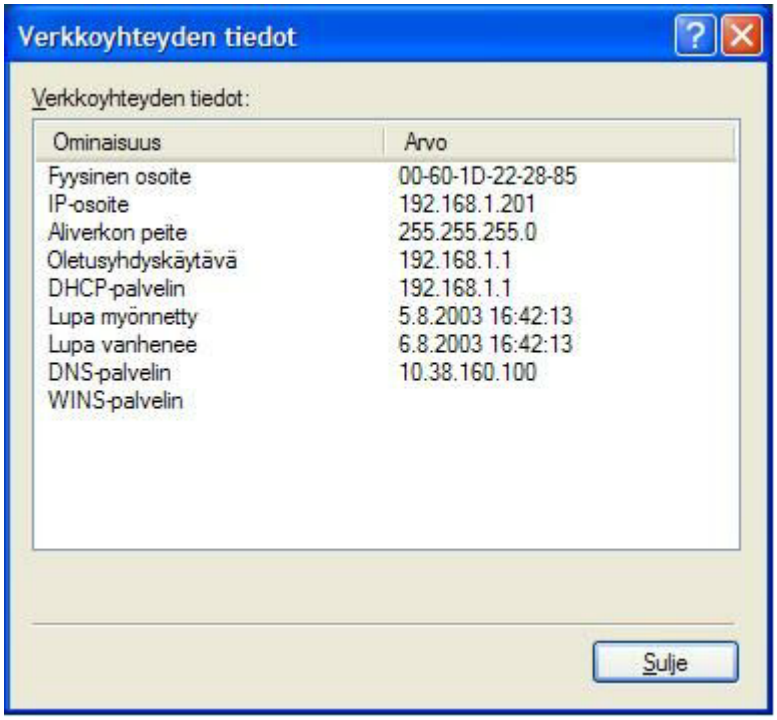


Kuva 5-4 Windows XP havaitsemassa verkkoja

Liittymisen jälkeen verkosta saadaan huomattavasti enemmän informaatiota. Kuvassa Kuva 5-5 nähdään yleisiä tietoja muodostetusta yhteydestä, kuten yhteyden nopeus ja vastaanotetun signaalin voimakkuus. Tarkempia tietoja verkosta saadaan valitsemalla TCP/IP-yhteyden tiedot. Kuvassa Kuva 5-6 näkyy käytettyjen palvelinten osoitteet sekä muuta tietoa verkon osoitteista.

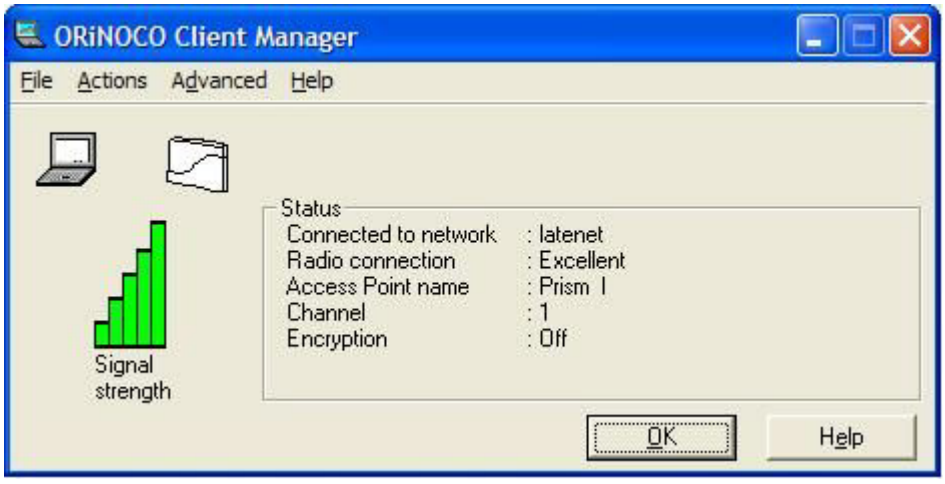


Kuva 5-5 Windows XP verkkoyhteyden tila

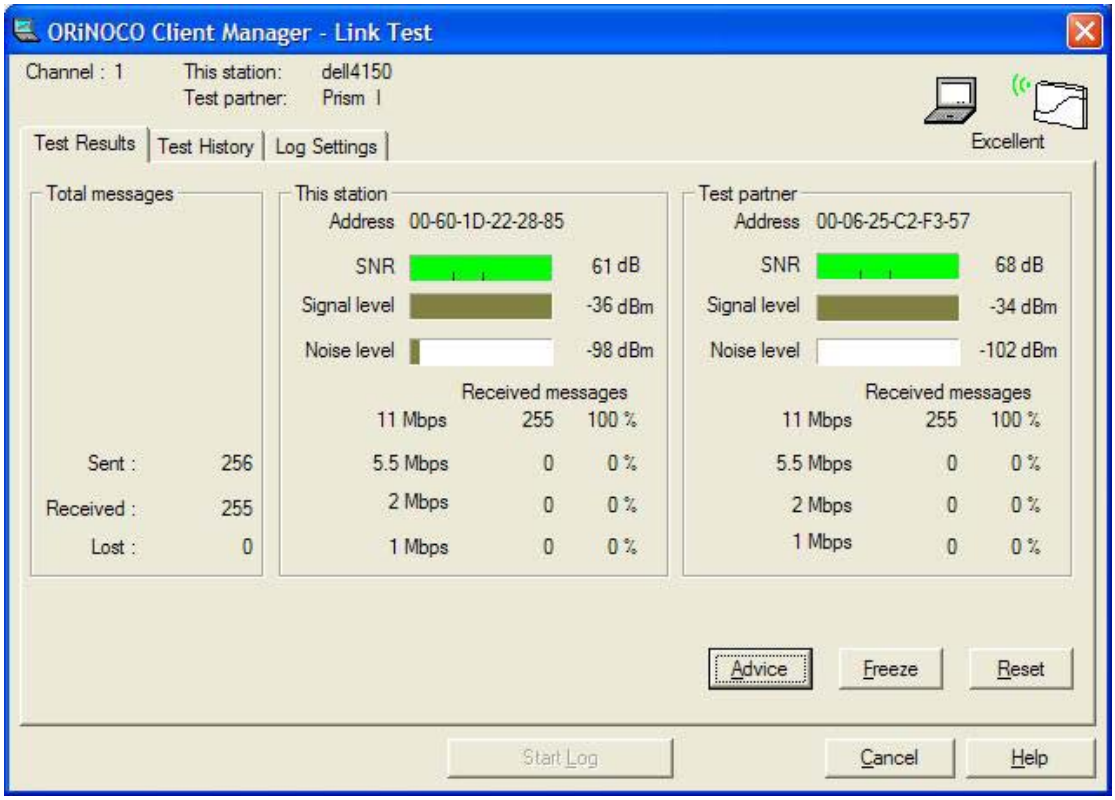


Kuva 5-6 Windows XP verkkoyhteyden tiedot

Verkkoyhteyden tilan tarkkailuun voidaan käyttää myös verkkokortin valmistajan tarjoamia ohjelmia. Kuvissa Kuva 5-7 ja Kuva 5-8 käytetään Orinocon Client Manager -ohjelmaa, jolla saadaan muutettua kortin asetuksia ja tarkkailtua langattomien yhteyksien ominaisuuksia. Ohjelma tarjoaa työkalut yhteyden laadun testaamista ja seurantaa varten.



Kuva 5-7 Orinoco verkkoyhteyden tila



Kuva 5-8 Orinoco langattoman yhteyden testaus

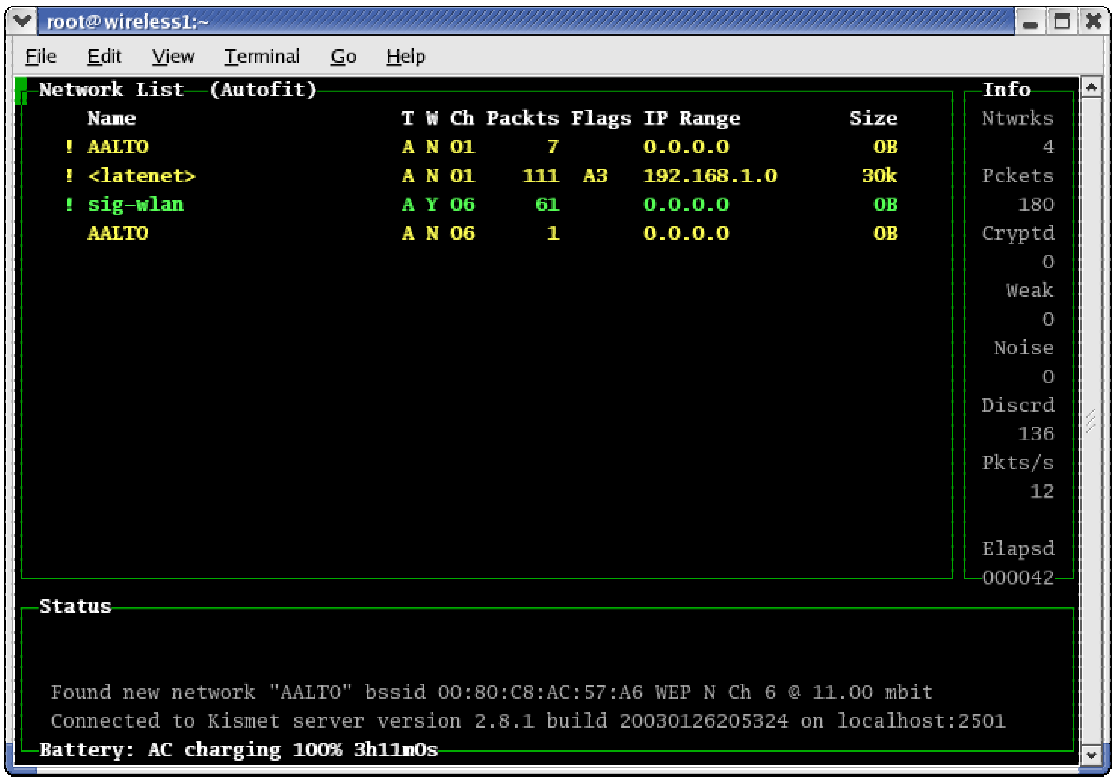
5.3.1.3 Tapaus 3: Kismet

Kolmannessa tapauksessa verkosta on kytketty majakka- ja DHCP-palvelut pois päältä. Tapauksen verkkoasetukset on esitettynä taulukossa Taulukko 5-3.

Taulukko 5-3 Tapaus 3 verkkoasetukset

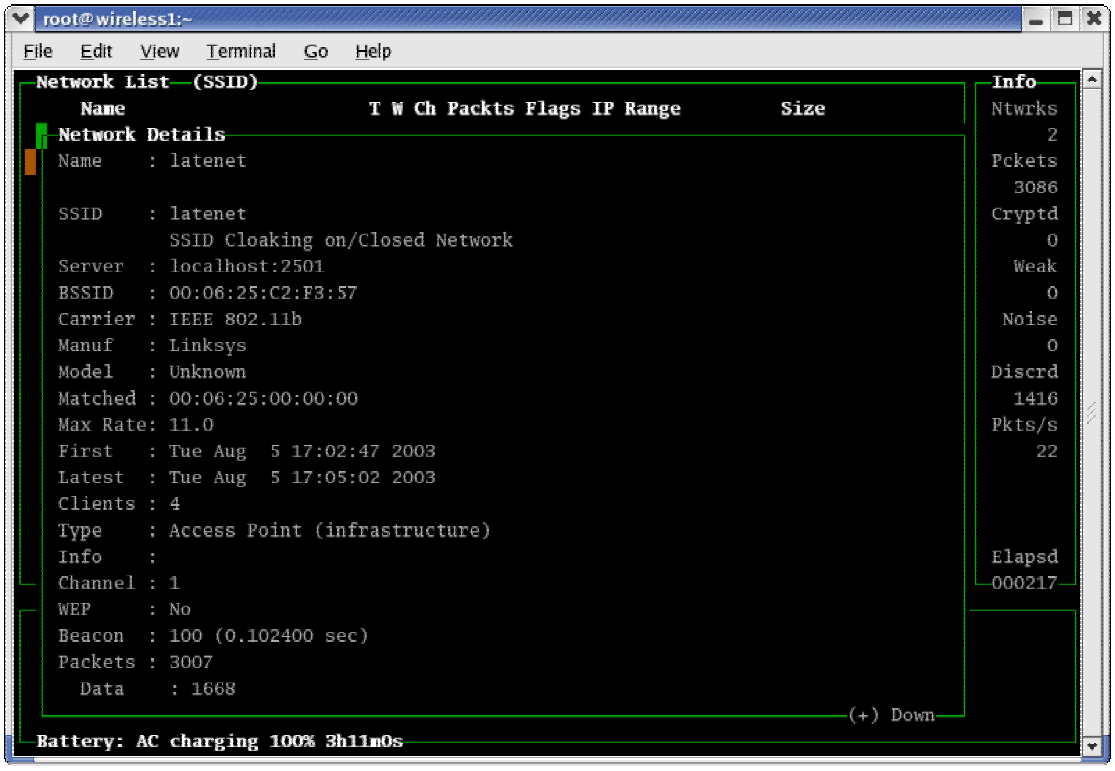
Tapaus	Majakka	Todennus	Salaus	DHCP
3	pois	avoin	pois	pois

Majakkapalvelun poiskytkeminen estää NetStumbler- ja Windows XP -ohjelmia havaitsemasta verkkoa. Havaitsemiseen käytetään Kismet-haistelijaohjelmaa. Kismet osaa etsiä verkkoja hyppimällä kanavalta toiselle, joten koko taajuusalue saadaan kerralla tutkittua. Kismet havaitsee alueelta kuvan Kuva 5-9 mukaiset verkot ja testiverkon havaitaan toimivan ensimmäisellä kanavalla. Taajuushyppely voidaan lopettaa ja siirtyä kaappaamaan liikennettä ensimmäiseltä kanavalta. Verkkoon liittymistä varten nyt on selvitettynä SSID ja kanava, mutta DHCP-palvelun ollessa pois päältä ei liittyminen onnistu ennen sopivan osoitteen löytämistä. Jatkamalla haistelua halutulla kanavalla ja halutussa verkossa saadaan osoiteavaruus selville.



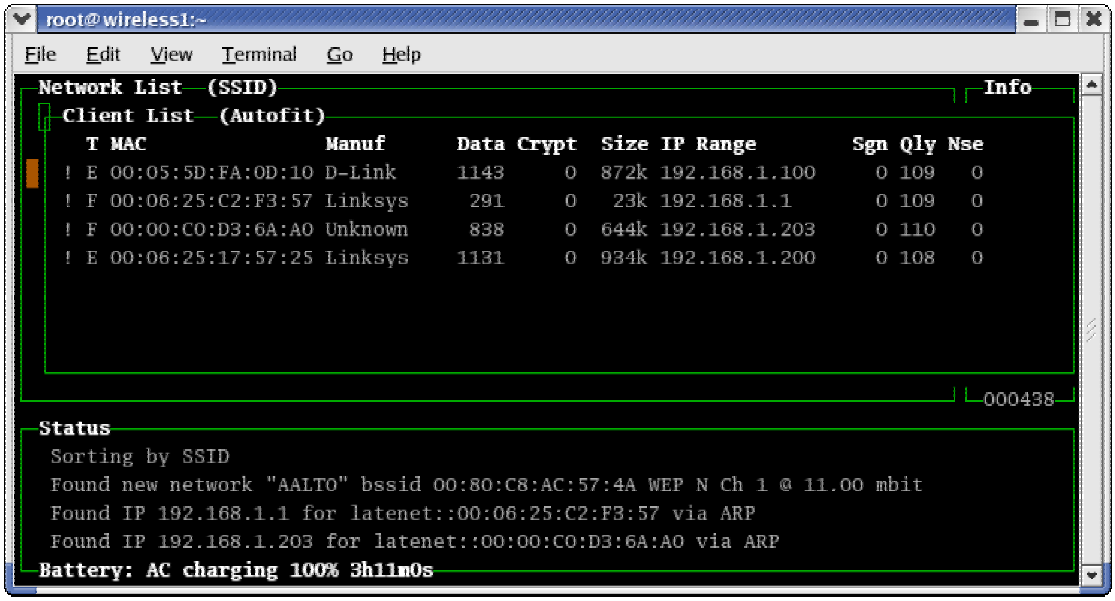
Kuva 5-9 Kismet havaitsemassa verkkoja

Kismetin avulla voidaan saada paljon tietoja verkon laitteista. Kuvassa Kuva 5-10 on esitettynä testiverkon informaatiota, josta käy ilmi esimerkiksi verkon asetuksia, access pointin ominaisuuksia ja päätelaitteiden lukumäärä.

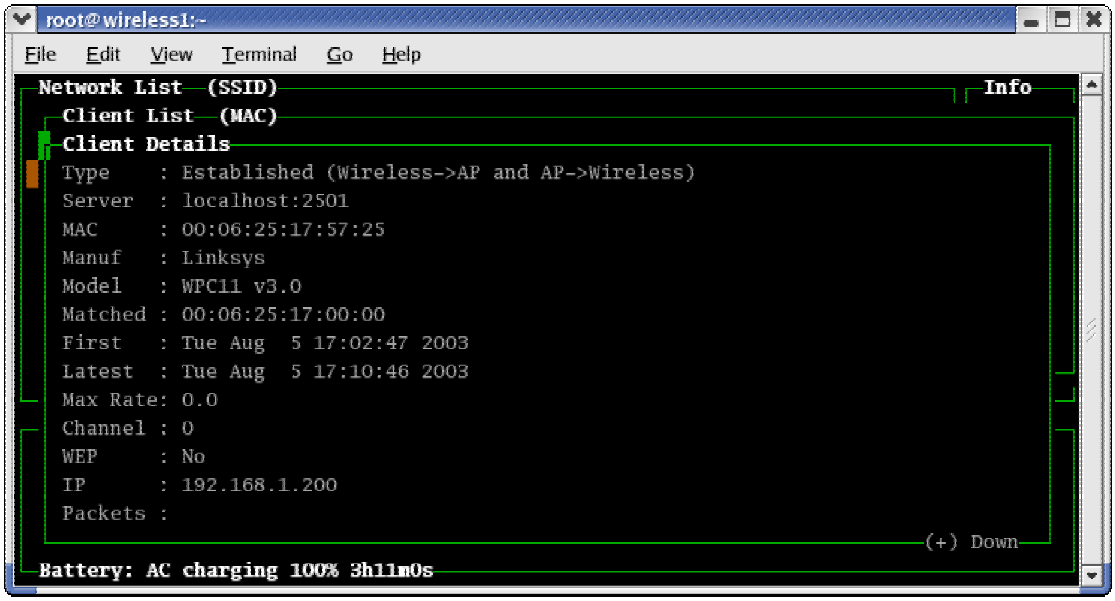


Kuva 5-10 Verkon tietoja Kismetin esittämänä

Kismet muodostaa listan verkon laitteista kuvan Kuva 5-11 mukaisesti. Listasta käyvät ilmi laitteiden MAC- ja IP-osoitteet sekä valmistajat. Tarvittaessa listasta voidaan valita verkon hyväksymä MAC-osoite, jos MAC-suodatus on päällä. Lista auttaa myös sopivan IP-osoitteen valinnassa. Yksittäisen laitteen tietoja voidaan tutkia tarkemmin kuvan Kuva 5-12 mukaisesti.



Kuva 5-11 Verkon laitteet Kismetin listaamana



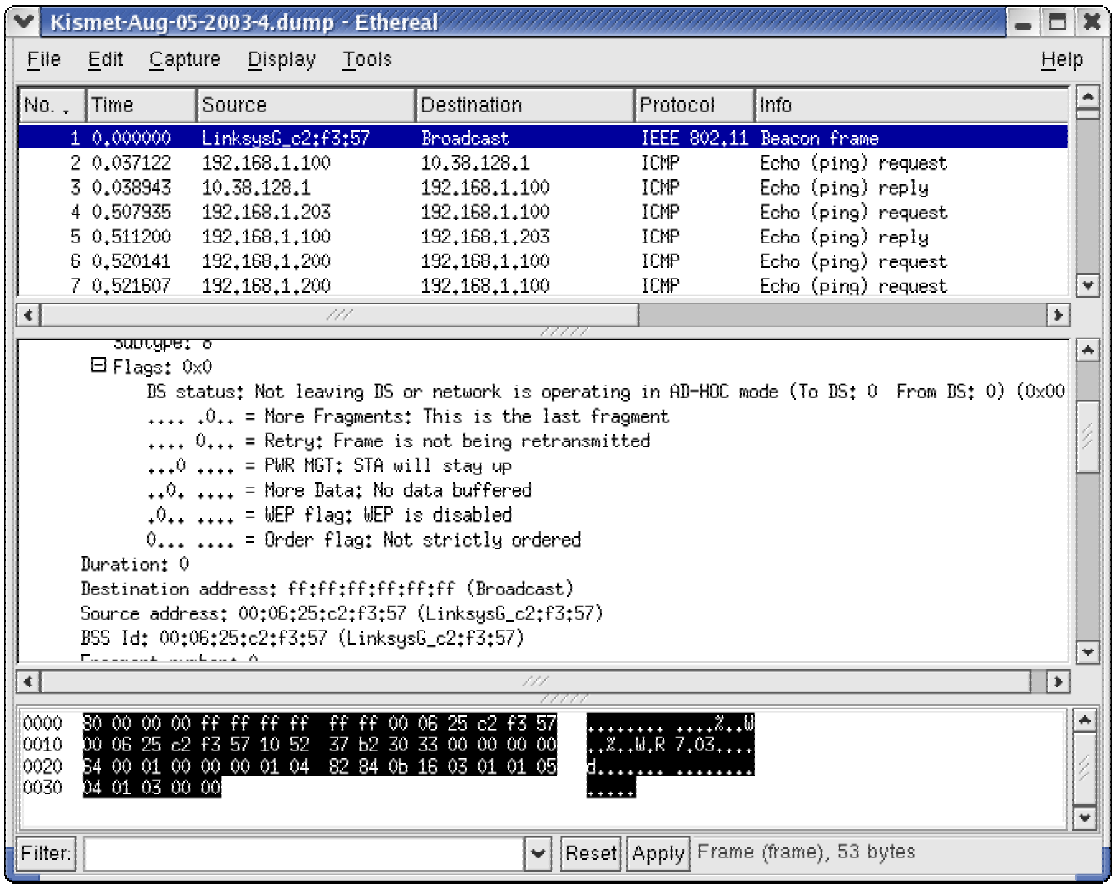
Kuva 5-12 Päätelaitteen tietoja Kismetin esittämänä

Verkkoon liittymistä varten on nyt kaikki tarvittava informaatio. Hyökkääjän IP-osoitteeksi valitaan vapaa osoite verkon osoiteavaruudesta, esimerkiksi 192.168.1.50. MAC-osoitetta ei tarvitse vaihtaa, mutta tarvittaessa sopiva MAC-osoite saataisiin tutkimalla verkon laitelistaa pidemmällä aikavälillä ja valitsemalla sallittu osoite, joka ei

kyseisenä hetkenä ole verkossa. Oletusyhteyskäytäväksi asetetaan access pontin osoite ja todennusmenetelmäksi avoin todennus, koska WEP-salausta ei ollut päällä. Verkkoon liittyminen on valmis.

5.3.2 Salakuuntelu

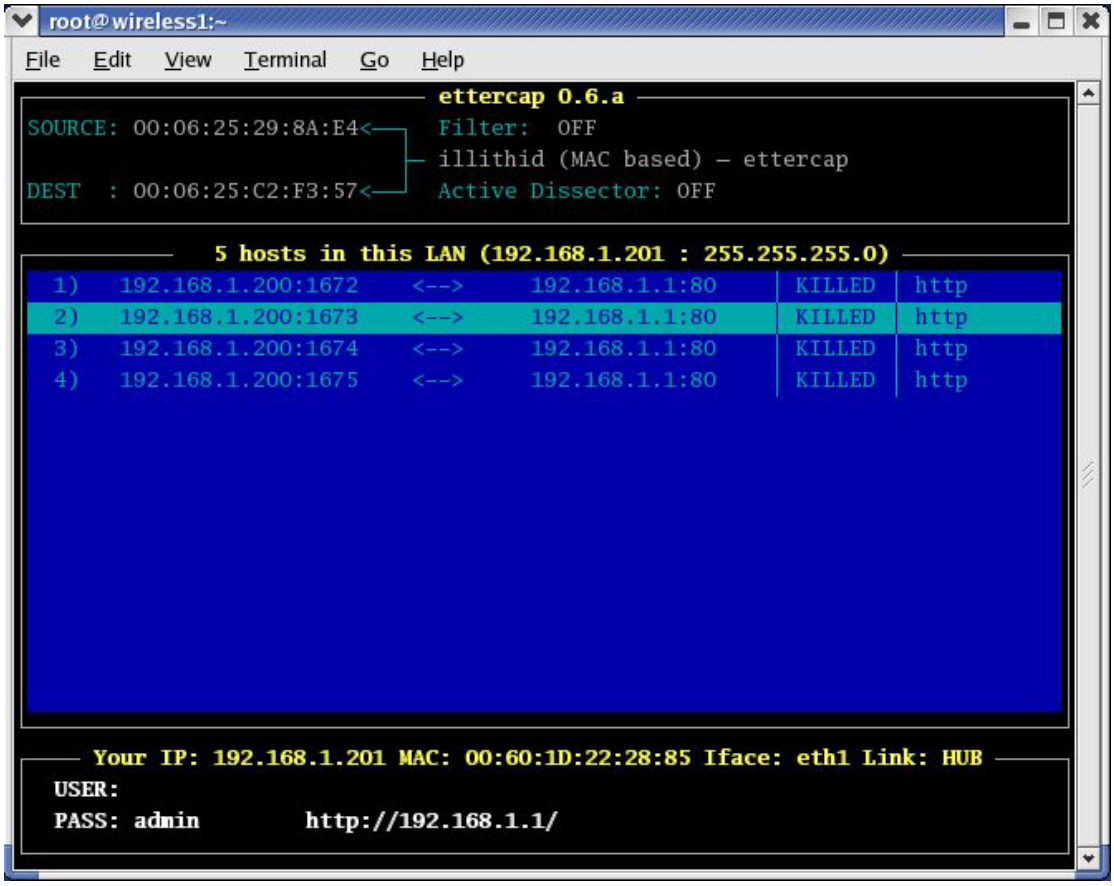
Salakuunteluhyökkäyksessä käytetään liikenteen kaappaamiseen edellisestä kohdasta tuttua Kismet-haistelijaohjelmaa ja kaapatun liikenteen analysointiin Ethereal-ohjelmaa. Verkossa liikkuvien salasanojen kaappaamiseen käytetään Ettercap-ohjelmaa. Hyökkäyksen aikana verkossa ei käytetty salausta hyökkäyksen demonstroinnin yksinkertaistamiseksi. Salauksen ollessa päällä joudutaan käytetty salausavain ensin selvittämään liikenteen analysoinnin mahdollistamiseksi. Pakettien otsikkotiedot ovat salatussakin liikenteessä luettavissa ilman salausavaimen tuntemista. Kuvassa Kuva 5-13 on esitettynä osa majakkapakettia Etherealilla analysoituna. Paketista nähdään access pointin tietoja sekä verkon asetuksia. Esimerkiksi kuvassa nähdään access pointin merkki ja osoitteet sekä WEP-salauksen tila.



Kuva 5-13 Beacon paketti Etherealin esittämänä

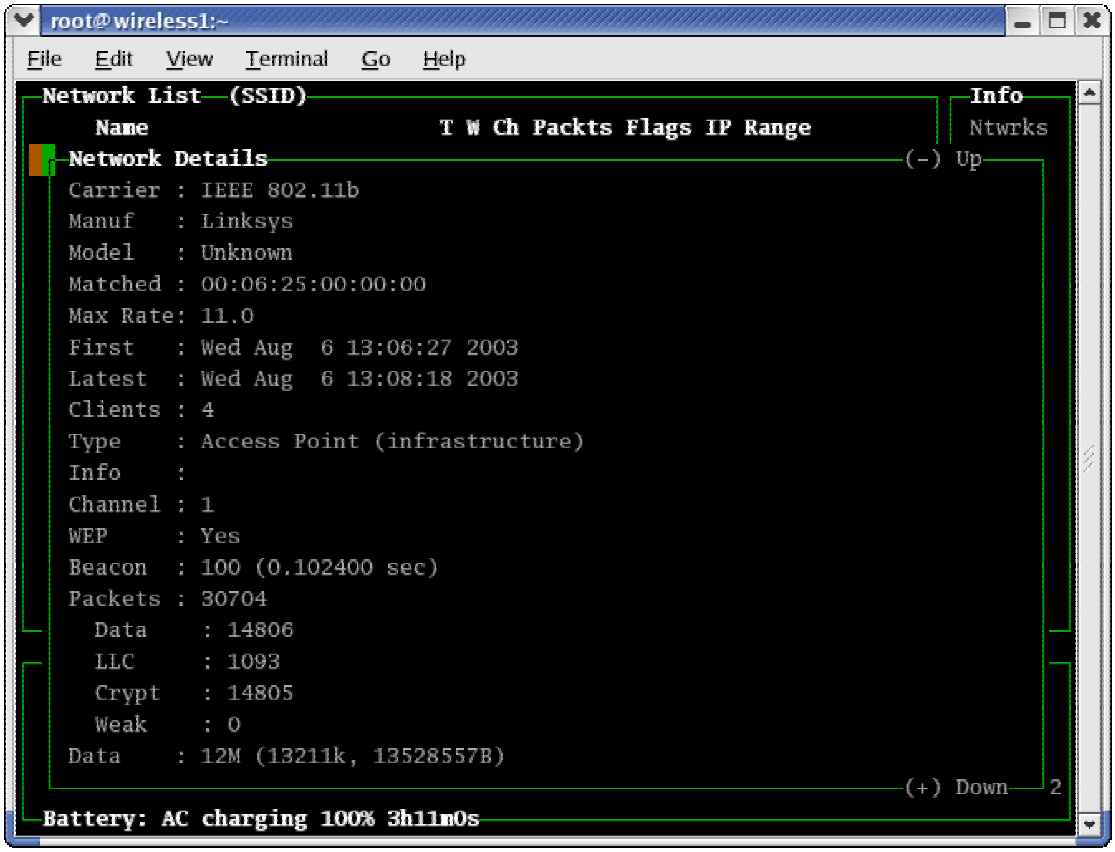
Access pointin asetusten muuttamista varten siihen on ensin kirjauduttava sisään. Sisään kirjautuminen edellyttää voimassaolevan käyttäjätunnuksen ja salasanan tietämistä. Ettercap-ohjelma osaa liikennettä kaappaamalla selvittää verkossa liikkuvia salasanoja.

Kuvassa Kuva 5-14 Ettercap kaappaa access pointin ja päätelaitteen välistä liikennettä kun päätelaitteen käyttäjä kirjautuu access pointtiin muuttaakseen sen asetuksia. Ettercap poimii käyttäjätunnuksen sekä salasanan ja hyökkääjä voi myöhemmin suorittaa esimerkiksi palvelunestohyökkäyksen muuttamalla access pointin käyttämiä salasanoja tai verkkoasetuksia. Selvitetty salasana on ”admin” ja sitä käytetään http yhteyden kanssa osoitteessa 192.168.1.1, joka on access pointin osoite.

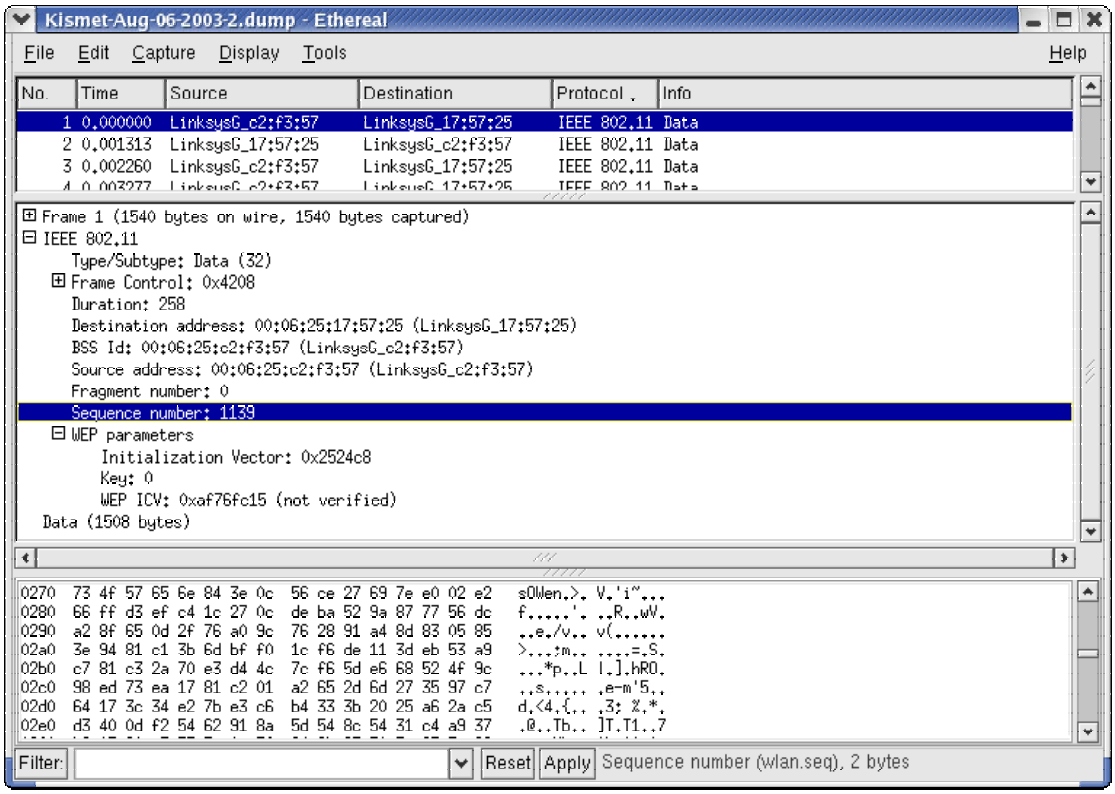


Kuva 5-14 Salasanan kaappaaminen Ettercap-ohjelmalla

WEP-salauksen purkamista varten tarvitaan suuri määrä kaapattua liikennettä. Salatun liikenteen kaappaamiseen voidaan käyttää edelleen Kismet-ohjelmaa. Kuvassa Kuva 5-15 kaapataan salattua liikennettä Kismet-ohjelmalla. Kismet laskee heikkojen alustusvektoreiden määrän suoraan kaapatessaan liikennettä. Salattu paketti on Etherealilla avattuna kuvassa Kuva 5-16, josta nähdään esimerkiksi käytetyn salausavaimen indeksi ja alustusvektori. Salauksen purkamista käsitellään seuraavassa kappaleessa.



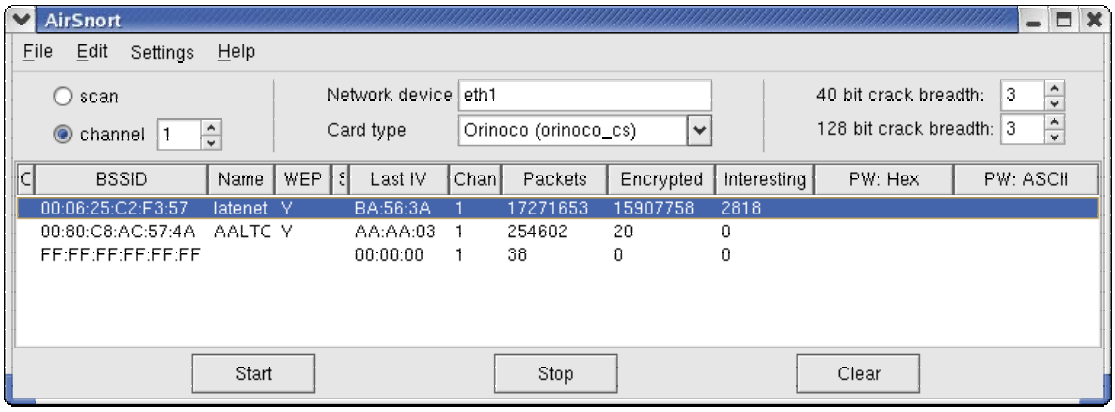
Kuva 5-15 WEP-salatun liikenteen kaappaamista Kismetillä



Kuva 5-16 WEP-salattu paketti Etherealilla katsottuna

5.3.3 WEPin purkaminen

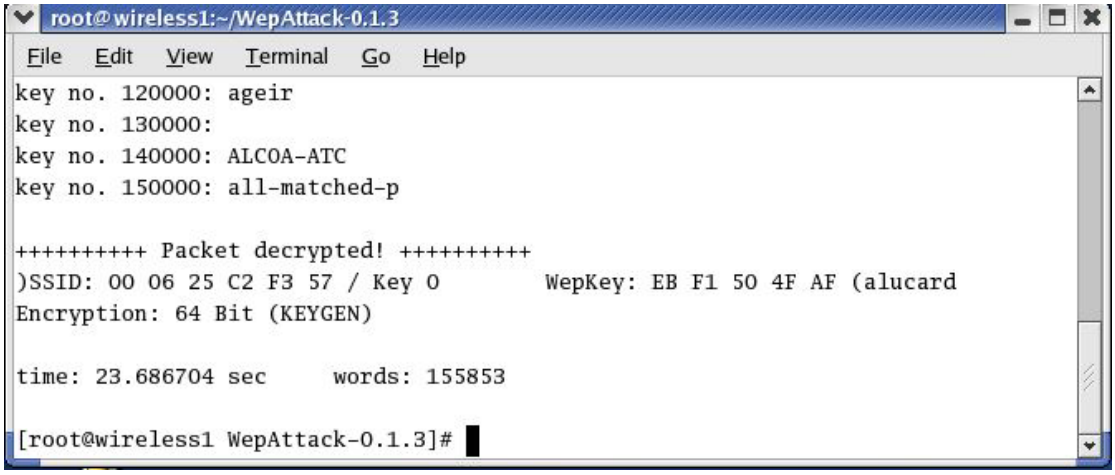
WEP-salauksen purkamiseen käytetään AirSnort- ja WepAttack-ohjelmia. AirSnort-ohjelma voi suorittaa itse myös liikenteen kaappaamisen ja purkaa salausta kaappauksen ohella. AirSnort voi hyökätä useampia verkkoja vastaan samanaikaisesti vaikka ne olisivat eri kanavilla. Kuvassa Kuva 5-17 on esitettynä AirSnort toiminnassa. Kuvasta voidaan nähdä kaapattujen salattujen pakettien määrä ja kiinnostavien heikkojen alustusvektoreiden määrä sekä viimeisin käytetty alustusvektori. Salauksen purkua voidaan nopeuttaa lisäämällä arvausten määrää mutta samalla kasvatetaan väärien arvausten todennäköisyyttä.



Kuva 5-17 AirSnort purkamassa WEP-salausta

Testiverkon salauksen purkaminen järkevässä ajassa ei onnistunut AirSnort-ohjelmalla. AirSnort kaappasi onnistuneesti liikennettä ja sai lopulta kasaan yli 5000 kiinnostavaa alustusvektoria. Aikaa kiinnostavien vektoreiden keräämiseen meni kaksi viikkoa ja kaikkiaan ohjelma kaappasi yli 50 GB salattua liikennettä. Suurin osa liikenteestä oli access pointin ja Linksys-päätelaitteen aiheuttamaa. Kaapatun liikenteen analyysi osoitti, että Linksys-laitteet eivät käytä kaikkein heikoimpia alustusvektoreita ollenkaan. Laitteen IV-laskurit hyppäävät vektoreiden, joiden keskimmäiset tavut ovat 0xFF, yli. AirSnort hyödyntää paljon muitakin vektoreita kuin pelkästään kaikkein heikoimpia. Muiden vektoreiden todennäköisyys paljastaa osa salasanaa on kuitenkin huomattavasti pienempi kuin 5 % ja testiverkon tapauksessa salasanan paljastaminen ei onnistunut.

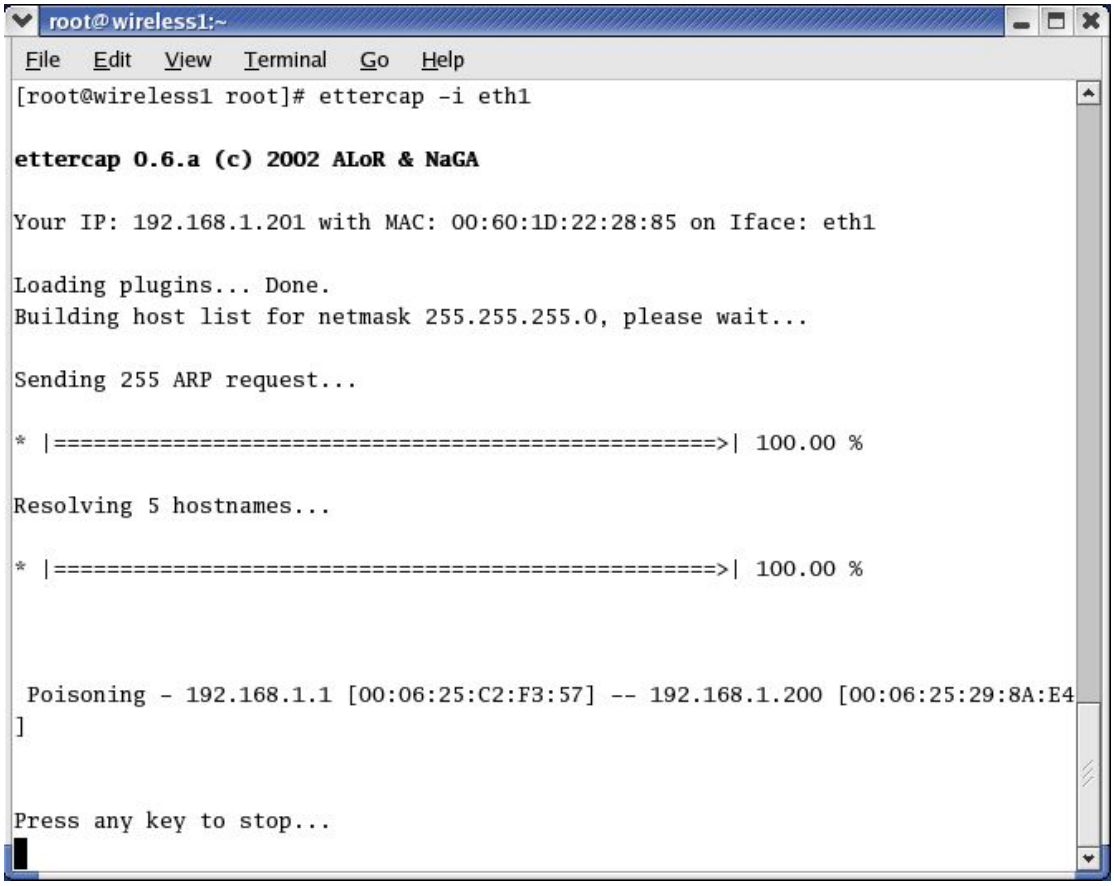
WepAttack-ohjelman toiminta perustuu sanakirjahyökkäykseen. Sanalistassa olevista sanoista muodostetaan salausavaimia, kuten verkkokortit ja access pointit muodostavat salausavaimia käyttäjän määrittelemistä fraaseista. Hyökkäystä varten määriteltiin verkolle access pointilla salausavain fraasilla, jonka tiedettiin olevan sanalistassa. Kismet-ohjelmalla kerätään 100 MB salattua liikennettä ja suoritetaan hyökkäys. WepAttack purkaa onnistuneesti salauksen ja paljastaa käytetyn avaimen kuten kuvassa Kuva 5-18 näkyy. WepAttackin sanakirjahyökkäys ei onnistu, jos salausavaimen muodostava fraasi ei ole sanalistassa tai joku listan fraaseista ei sattumalta muodosta salausavainta.



Kuva 5-18 Salausavaimen purkaminen WepAttack-ohjelmalla

5.3.4 DoS-hyökkäys

Palvelunestohyökkäyksen toteuttamiseen käytetään Ettercap-ohjelmaa. Ohjelman suorittama hyökkäys perustuu ARP-myrkyttämiseen. ARP-myrkyttäminen on tyypillinen kytketyille verkoille suoritettu hyökkäys ja on mahdollista suorittaa sekä lanka- että langattomissa verkoissa. Hyökkäyksen alkaessa hyökkääjä lähettää väärennetyt ARP-reply-paketit kohteille ja ohjaa niiden liikenteen kulkemaan itsensä kautta. Samalla on mahdollista suorittaa Man-in-the-Middle-hyökkäys välittämällä edelleen liikenne oikeaan määränpäähänsä. Demonstraation tapauksessa liikennettä ei ohjata uudelleen ja keskitytään verkon normaalin toiminnan häiritsemiseen. ARP-taulukkojen myrkytyttyä katkeaa liikenne kohteiden välillä. Liikenteen katkeaminen havaitaan käynnissä olevan tiedonsiirron katkeamisena ja PING-kyselyiden epäonnistumisena. Hyökkäyksen toteuttaminen näkyy kuvassa Kuva 5-19, josta havaitaan hyökkäyksen kohdistuvan access pointin ja yhden päätelaitteen väliseen liikenteeseen. Hyökkäyksen lopettamisen jälkeen Ettercap lähettää ARP-taulukot korjaavat paketit kohteille, joten MitM-hyökkäyksen tapauksessa hyökkäys on mahdollista toteuttaa ja lopettaa uhrien sitä havaitsematta.



Kuva 5-19 DoS-hyökkäys Ettercap-ohjelmalla

6 Johtopäätökset

Tämän diplomityön tavoitteena oli tutkia langattomien lähiverkkojen eri turvallisuusratkaisuiden toimivuutta. Kirjallisuuslähteiden, spesifikaatioiden ja kokeiden avulla oli tarkoitus kartoittaa eri ratkaisuiden riittävyyttä tarjoamaan langattomalle verkolle turvallisuuspalveluita. Turvallisuusratkaisuiden esittelyn lisäksi työssä kuvattiin mahdollisia hyökkäyksiä eri ratkaisuja vastaan sekä esitettiin keinoja hyökkäysten havaitsemiseen ja estämiseen. Demonstraatioverkossa esiteltiin muutamia hyökkäyksiä toiminnassa.

IEEE 802.11 -standardia valmisteltaessa tavoitteena oli tarjota lankaverkkoa vastaava turvallisuustaso langattomassa ympäristössä, mutta on osoittautunut että standardin tarjoamat turvallisuuskomponentit ovat riittämättömiä tarjoamaan verkolle tehokasta suojaa hyökkäyksiä vastaan. Käyttäjäntunnistuksessa ja salauksessa on useita heikkoja kohtia, jotka altistavat verkon hyökkäyksille ja heikentävät verkon turvallisuutta.

Standardin mukaisten turvallisuusratkaisuiden osoittauduttua riittämättömiksi useat laitevalmistajat alkoivat kehittämään omia parannuksiaan niihin. Osa näistä parannuksista on nykyään yleisesti käytössä kaikkien valmistajien laitteissa ja niiden avulla voidaan hieman parantaa langattoman verkon turvallisuutta. Turvallisuuden parantamisen perusratkaisut auttavat kuitenkin ainoastaan satunnaisia hyökkäyksiä vastaan. Nimenomaan tiettyä verkkoa vastaan suunnattujen tarkkojen hyökkäysten torjuntaan tarvitaan kehittyneempiä turvallisuusratkaisuita. Luottamuksellista liikennettä kuljettavien verkkojen turvallisuuden varmistamiseen tulisi aina käyttää kehittyneempiä turvallisuusratkaisuja.

Kehittyneemmät turvallisuusratkaisut parantavat paitsi verkon turvallisuutta myös verkon hallittavuutta. Ulkoisten todentamispalvelimien käytön mahdollistaminen ja salausavainten dynaaminen jakaminen nostavat verkon turvallisuuden uudelle tasolle. IEEE 802.1X -standardi ja EAP-protokollat huolehtivat kehittyneemmissä ratkaisuissa käyttäjän todentamisesta sekä salausavainten jakamisesta. WPA-ratkaisu parantaa lisäksi salauksen tehokkuutta ottamalla käyttöön TKIP-salauksen ja pakettikohtaiset avaimet. WPA-sertifikaatilla varustettujen laitteiden pitäisi olla keskenään yhteensopivia.

IEEE 802.11i -standardi tulee parantamaan langattomien lähiverkkojen turvallisuutta esittelemällä kokonaan uuden salausmenetelmän. AES-salauksen oletetaan parantavan oleellisesti salauksen kestävyyttä, mutta sen tehokkuus on vielä käytännössä testaamatta. Muuten IEEE 802.11i -standardin ratifioiminen yhdistää monet jo käytössä olevat turvallisuusratkaisut yhteen pakettiin ja määrittelee niiden toteutustavat

mahdollistaen paremmin eri laitevalmistajien tuotteiden yhteensopivuuden. Nykyään eri valmistajien toteuttamat kehittyneemmät turvallisuusratkaisut eivät välttämättä ole yhteensopivia keskenään.

VPN-ratkaisujen käyttö langattomassa ympäristössä on myös mahdollista. Lankaverkosta tutut VPN-sovellukset toimivat WLAN-kerrosten päällä ja tarjoavat vaihtoehdon turvallisuuden varmistamiseen yhteyden päästä päähän. VPN-ratkaisut on kuitenkin suunniteltu lankaverkon tarpeita ja ominaisuuksia silmälläpitäen. Langattomassa verkossa niiden heikkoutena on verkon suorituskyvyn lasku ja langattomalle verkolle ominaisten palveluiden, kuten liikkuvuus, vaikeutuminen.

Langattomassa ympäristössä liikenteen kaappaaminen on yksinkertaista. Kaikki signaalin kantaman sisäpuolella olevat voivat halutessaan salakuunnella siirrettävää tietoa. Salauksen merkitys on siis huomattavasti suurempi kuin perinteisessä lähiverkossa. Langattomuus helpottaa myös MitM-hyökkäyksien suorittamista ja siirrettävän tiedon muokkaamista salauksen murtumisen jälkeen. Avoin siirtomedia ja ohjausliikenteen salaamattomuus mahdollistavat lukuisien DoS-hyökkäysten toteuttamisen ja siten verkon normaalin toiminnan estämisen.

Demonstraatioverkossa suoritetut hyökkäykset osoittivat perusratkaisuiden riittämättömyyden verkon suojaajina. Vaikka salauksen purkaminen tilastollisella analyysillä ei onnistunutkaan tällä kertaa, kehittyvät myös hyökkäyksiin käytettävät ohjelmistot ja niiden algoritmit jatkuvasti. Laitteistojen pitäminen päivitettyinä auttaa mutta turvallisuuden kannalta kriittisissä verkoissa on syytä käyttää kehittyneempiä turvallisuusvaihtoehtoja kuten WPA tai odottaa IEEE 802.11i -standardin kanssa yhteensopivien laitteiden saapumista markkinoille.

Tässä työssä tutustuttiin nykyisiin langattomalle lähiverkolle tarjolla oleviin turvallisuusratkaisuihin ja esiteltiin tulevaisuuden ratkaisuita lyhyesti. IEEE 802.11i -standardin kypsyttyä ja sen mukaisten laitteiden tultua markkinoille on tarpeen analysoida tarkemmin uuden turvallisuusratkaisun tehokkuutta ja mahdollisten heikkouksien tultua esiin tutustua jälleen uuden sukupolven ratkaisuihin.

Lähdeluettelo

[1] Institute of Electrical and Electronics Engineers, http://www.ieee.org [21.08.2003].

[2] European Telecommunications Standards Institute, http://www.etsi.org [21.08.2003].

[3] HomeRF, http://www.homerf.org [21.08.2003].

[4] Bluetooth, http://www.bluetooth.com [21.08.2003].

[5] IEEE Std 802.11, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, 1999.

[6] IEEE Std 802.11a-1999, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 1: High-speed Physical Layer in the 5 GHz band*, 1999.

[7] IEEE Std 802.11b-1999, *Supplement to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Higher-Speed Physical Layer Extension in the 2.4 GHz Band*, 1999.

[8] RSA Data Security, http://www.rsasecurity.com [21.08.2003].

[9] Dr. Cyrus Peikari & Seth Fogie, *Wireless Maximum Security*, 2002.

[10] Trey Dismukes, *Wireless Security Blackpaper*, 18.07.2002, http://www.arstechnica.com/paedia/w/wireless/security-1.html, [21.08.2003].

[11] *Proxim Wireless Network Security White Paper v2.2*, 2003, http://www.proxim.com/learn/library/whitepapers/wireless_security.pdf [21.08.2003].

[12] IEEE Std 802.1X-2001, *Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control*, 2001.

[13] L. Blunk & J. Vollbrecht, RFC 2284, *PPP Extensible Authentication Protocol (EAP)*, Maaliskuu 1998, http://www.ietf.org/rfc/rfc2284.txt [21.08.2003].

[14] C. Rigney, S. Willens, A. Rubens & W. Simpson, RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*, Kesäkuu 2000, http://www.ietf.org/rfc/rfc2865.txt [21.08.2003].

[15] C. Rigney, W. Willats & P. Calhoun, RFC 2869, *Radius Extensions*, Kesäkuu 2000, http://www.ietf.org/rfc/rfc2869.txt [21.08.2003].

[16] R. Rivest, RFC 1321, *The MD5 Message-Digest Algorithm*, Huhtikuu 1992, http://www.ietf.org/rfc/rfc1321.txt [21.08.2003].

[17] H. Haverinen & J. Salowey, *Internet-Draft, EAP SIM Authentication*, Helmikuu 2003, http://www.globecom.net/ietf/draft/draft-haverinen-pppext-eap-sim-03.html [21.08.2003].

[18] J. Arkko & H. Haverinen, *Internet-Draft, EAP AKA Authentication*, Helmikuu 2003, http://www.globecom.net/ietf/draft/draft-arkko-pppext-eap-aka-03.html [21.08.2003].
[19] B. Aboba & D. Simon, RFC 2716, *PPP EAP TLS Athentication Protocol*, Lokakuu 1999, http://www.ietf.org/rfc/rfc2716.txt [21.08.2003].
[20] T. Dierks & C. Allen, RFC 2246, *The TLS Protocol Version 1.0*, Tammikuu 1999, http://www.ietf.org/rfc/rfc2246.txt [21.08.2003].
[21] Paul Funk, Internet-Draft, *EAP Tunneled TLS Authentication Protocol (EAP-TTLS)*, Marraskuu 2002, http://www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-02.txt [21.8.2003].
[22] A. Palekar, D. Simon, G. Zorn & S. Josefsson, Internet-Draft, *Protected EAP (PEAP) Protocol*, Maaliskuu 2003, http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-06.txt [21.8.2003].
[23] A. Erkkilä, *IEEE 802.1X Authentication In Operator's WLAN*, 2003.
[24] Sami Iivarinen, *Onko sinun langaton lähiverkkosi tietoturvariski*, 2003, http://cisco.evolvis.net/ivision/pdfs/Sami_Iivarinen_Ivision_langattomat_lahiverkot.pdf [21.08.2003].
[25] S. Convery, D. Miller & S. Sundaralingam, *Cisco SAFE: Wireless LAN Security in Depth*, 2003, http://www.cisco.com/application/pdf/en/us/guest/netsol/ns314/c654/ccmigration_09186a008009c8b3.pdf [21.08.2003].
[26] J. Bhola, *Wireless LANs Demystified*, 2002.
[27] Wireless-Fidelity, http://www.wi-fi.org/OpenSection/index.asp [21.08.2003].
[28] Wi-Fi Alliance, *Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks*, Huhtikuu 2003, http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf [21.08.2003].
[29] B. Bing, *Wireless Local Area Networks: The New Wireless Revolution*, 2002.
[30] IEEE Std 802.11i/D3.0, *Draft Supplement to Standard for Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Specification for Enhanced Security*, Marraskuu 2002.
[31] M. Disabato, *Wi-Fi Protected Access Web Cast*, June 2003, http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_ProtectedAccessWebcast_2003.pdf [21.08.2003].
[32] National Institute of Standards and Technology, http://www.nist.gov [21.08.2003].
[33] B. Carter & R. Shumway, *Wireless Security End to End*, 2002.
[34] Microsoft, http://www.microsoft.com [21.08.2003].
[35] NetStumbler, http://www.netstumbler.com/ [21.08.2003].
[36] J. Wright, *Detecting wireless LAN MAC Address Spoofing*, 21.01.2003, http://www.astalavista.com/library/wlan/wlan-mac-spoof.pdf [21.08.2003].

[37] Kismet, http://www.kismetwireless.net/download.shtml [21.08.2003].
[38] Ethereal, http://www.ethereal.com/ [21.08.2003].
[39] WildPackets, http://www.wildpackets.com/ [21.08.2003].
[40] A. Stubblefield, J. Ioannidis & A. D. Rubin, *Using the Fluhrer, Mantin and Shamir Attack to Break WEP*, 06.08.2001, http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf [21.08.2003].
[41] S. Whalen, *Analysis of WEP and RC4 Algorithms*, Maaliskuu 2002, http://www.rootsecure.net/content/downloads/pdf_downloads/wep_analysis.pdf [21.08.2003].
[42] T. Newsham, *Cracking WEP Keys*, 2001, http://www.blackhat.com/presentations/bh-usa-01/TimNewsham/bh-usa-01-Tim-Newsham.ppt [21.08.2003].
[43] S. Fluhrer, I. Mantin & A. Shamir, *Weaknesses in the Key Scheduling Algorithm of RC4*, Elokuu 2001, http://downloads.securityfocus.com/library/rc4_ksaproc.pdf [21.08.2003].
[44] WEPAttack, http://wepattack.sourceforge.net/ [21.08.2003].
[45] WEPCrack, http://wepcrack.sourceforge.net/ [21.08.2003].
[46] AirSnort, http://airsnort.shmoo.com/ [21.08.2003].
[47] J. Walker, *Unsafe at any key size: An analysis of the WEP encapsulation*, Lokakuu 2000, http://www.dis.org/wl/pdf/unsafe.pdf [21.08.2003].
[48] AirMagnet, http://www.airmagnet.com/ [21.08.2003].
[49] S. Whalen, *An Introduction to ARP Spoofing*, Huhtikuu 2001, http://www.rootsecure.net/content/downloads/pdf_downloads/arp_spoofing_intro.pdf [21.08.2003].
[50] B. Fleck & J. Dimov, *Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network*, 2001, http://www.cigitallabs.com/resources/papers/download/arppoison.pdf [21.08.2003].
[51] Dsniff, http://www.monkey.org/~dugsong/dsniff/ [21.08.2003].
[52] Ettercap, http://ettercap.sourceforge.net/ [21.08.2003].
[53] Airjack, http://802.11ninja.net/airjack/ [21.08.2003].
[54] ARPWatch, http://www.securityfocus.com/tools/142 [21.08.2003].
[55] B. Potter & B. Fleck, *802.11 Security*, 2002.
[56] J. Bellardo & S. Savage, *802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions*, Kesäkuu 2003, http://ramp.ucsd.edu/~bellardo/pubs/usenix-sec03-80211dos-color.pdf [25.08.2003].

[57] J. Geier, *WPA Security Enhancements*, 2003, http://www.wi-fiplanet.com/tutorials/article.php/2148721 [21.08.2003].
[58] Void11, http://www.wlsec.net/void11/ [25.08.2003].
[59] A. Mishra & W. A. Arbaugh, *An Initial Security Analysis of the IEEE 802.11X Standard*, 06.02.2002, http://www.cs.umd.edu/~waa/1x.pdf [21.08.2003].
[60] Linksys, http://www.linksys.com [21.08.2003].
[61] Dell, http://www.euro.dell.com/countries/fi/fin/gen/default.htm [21.08.2003].
[62] Compaq, http://h18000.www1.hp.com/ [21.08.2003].
[63] D-Link, http://www.dlink.com/ [21.08.2003].
[64] Opie, http://opie.handhelds.org/ [21.08.2003].
[65] Red Hat, http://www.redhat.com/ [21.08.2003].
[66] Orinoco, http://www.orinocowireless.com/ [21.08.2003].