TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUS

OPINNÄYTETYÖRAPORTTI

WLAN –tekniikan heikkoudet ja niiden parantaminen
Weaknesses of WLAN –technique and repairing them

Aku Rautio

Tietojenkäsittelyn koulutusohjelma
huhtikuu 2007
Työn ohjaaja: Harri Hakonen

TAMPERE 2007

TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUS

Tekijä(t): Aku Rautio

Koulutusohjelma(t): Tietojenkäsittely/Tietoverkkopalvelut

Opinnäytetyön nimi: WLAN – tekniikan heikkoudet ja niiden parantaminen

Title in English: Weaknesses of WLAN – technique and repairing them

Työn valmistumis-kuukausi ja -vuosi: 04/2007

Työn ohjaaja: Harri Hakonen **Sivumäärä:** 31

TIIVISTELMÄ

Tässä tutkintotyössä käsitellään WLAN –tekniikan heikkouksia ja niiden estämistoimenpiteitä niin salausalgoritmien kuin itse langattoman median osalta. Näitä asioita käsitellään valmistaja- ja laitteistoriippumattomasti. Pyrkimyksenä on herätellä lukijaa ymmärtämään tietoturvan tärkeys WLAN – verkoissa.

Työssä esitellään yleiset käytössä olevat salausalgoritmit ja käsitellään niiden altistumista erilaisille hyökkäyksille yksitellen. Tekniikan osalta käydään läpi oleellisia seikkoja passiivisesta kuuntelusta aktiiviseen hyökkäykseen. Työn lopussa esittelen muutamia langattomia tukiasemia, jotka on valittu silmällä pitäen 1-20 työntekijän PK – yrityksien tarpeita. Käytössä on ollut suurimmaksi osaksi verkkoasiantuntijoiden kirjoittamia verkkojulkaisuja, koska varsinaisesta murtamisesta ja sen estämisestä ei ole kirjoitettu kunnollisia kirjoja. Osa tiedoista on tullut suoraan työni kautta yritä ja kokeile – menetelmällä.

Mikäli tietoturvapolitiikkaan ei kiinnitetä huomiota, eikä sitä päivitetä jatkuvasti, on vaarana, että ennen pitkää huolimattomasti suojattu verkko joutuu erilaisten hyökkäysten kohteeksi. Hyökkäykset voivat olla joko pelkkään verkkoon tunkeutumisia tai sitten yrityksen tietojen ja resurssien selvittämistä. Toisaalta tuskin kukaan haluaisi, että ulkopuoliset tahot käyttävät yrityksen WLAN – verkkoa edes harmittomaan surffailuun tai sitten kokeiluja päästä yrityksen tietoihin. Kaikkia hyökkäyksiä ei huomata ilman huomattavia taloudellisia panostuksia WLAN – tunkeutumisenestojärjestelmien hankkimiseen. Kannattaakin miettiä, onko langattoman lähiverkon rakentaminen sittenkään järkevää vai kannattaisiko sittenkin laajentaa vain langallista verkkoa.

Avainsanat: WLAN Tietoturva Murtaminen Salausalgoritmit Haittatoiminta

Sisällysluettelo

1 Johdanto

Tässä tutkintotyössä käsitellään WLAN -verkkojen turvattomuutta sekä turvattomuuden parantamiskeinoja. Ensimmäiseksi käsitellään verkkoliikenteen salaustekniikoita ja niiden toimintaa. Tämän jälkeen käydään läpi verkkoavainten salausalgoritmien toiminta, jonka jälkeen päästään itse asiaan eli salauksiin kohdistuviin hyökkäyksiin ja niiden ehkäisemiseen. Myös itse WLAN –signaalin häiritsemistapoja ja häirinnän estämistä käydään lävitse.

Tarkoituksena tässä työssä oli saada kattava paketti WLAN:n heikkouksista ja haittatoiminnan estämisestä yksiin kansiin. Verkkojen rakentamista käsitellään yritysten näkökulmasta ja kotikäyttöön tarkoitetut ratkaisut on tarkoituksella jätetty työn ulkopuolelle.

1.1 Aihe

Aihe on kiinnostanut jo pitemmän aikaa eikä opinnäytetyötäni aloittaessani minulla ollut tietoa työpaikasta saatikaan sitten tutkintotyönantajasta. Näin syntyi idea tehdä valmistaja- ja laitteistoriippumaton paketti WLAN –tekniikan heikkouksista.

1.2 Aineiston kerääminen

Aineiston keräämisen aloitin jo vuonna 2005. Samaan aikaan aloitin tutustumisen erilaisten valmistajien WLAN –ratkaisuihin saadakseni mahdollisimman kattavan yleissilmäyksen erilaisiin ratkaisuihin. Etsiessäni aiheeseen soveltuvaa kirjallisuutta havaitsin kuitenkin, että vaikka WLAN:sta ja sen tietoturvasta on kirjoitettu paljon, ne eivät ole kovin syvällisesti asiaan paneutuvia. Varsinkin salausalgoritmien toiminnasta ei kirjoissa ollut juurikaan mitään. Käydessäni läpi Internetin verkkoartikkeleita ja tietokantoja havaitsin, että niihin on algoritmien toiminnasta kirjoitettu paljon syvällisemmin ja yksityiskohtaisemmin kuin mihinkään kirjaan. Tästä johtuen suurin osa lähteistä on suoraan Internetistä. Tästä johtuen myös aineistoa piti käsitellä huomattavasti kriittisemmin ja selvittää kirjoittajien taustoja. Artikkeleiden kirjoittajilla olikin noin 10 – 15 vuoden kokemus algoritmien ja tekniikan saralta.

2 Käsitteitä

WEP	Ensimmäinen standardoitu WLAN -salaus josta myöhemmin löydetty lukuisia haavoittuvuuksia.
WPA	WEP -salauksen seuraaja
WPA2	Paremmalla tietoturvalla päivitetty WPA.
TKIP	Avaimienvaihtoprotokolla, joka alunperin kehitettiin vahvistamaan WEP-protokollan tietoturvattomuutta
DES	Erittäin vanha avaintenvaihtoalgoritmi, tänä päivänä murtuu alle vuorokaudessa
Triple DES	DES –algoritimin päivitysversio, salaa tiedon kolmella DES -avaimella
AES	Toistaiseksi murtumaton uuden sukupolven salausalgoritmi
RADIUS	Määrittely EAP -protokollan siitämisestä ethernet -paketin sisällä
DoS -hyökkäys	Palvelunestohyökkäys, laite tai palvelu saatettaan epävakaaseen tilaan esimerkiksi ”pommittamalla” yhteyspyyntöjä sitä vastaan
Man-in-the-middle –hyökkäys	Nimensä mukainen hyökkäys, hyökkääjä sijaitsee loogisesti työaseman ja palvelun välissä

3 Yleistä langattomasta lähiverkosta

Langattomia lähiverkkoja(WLAN, Wireless Local Area Network) rakennetaan kiihtyvässä tahdissa. Johtuen tekniikan langattomuudesta(tieto kulkee radioaaltoja pitkin) verkko on helppo pystyttää ja yksinkertaisimmillaan laitettavissa toimintakuntoon todella nopeasti. Langallisen verkon rakentamisessa puolestaan pitää huomioida verkkojohtojen vedot, rasiat, mittaukset ja päätelaitteet. Myös hankalissa paikoissa, missä johtoa ei välttämättä voi vetää on käytännöllistäkin tehdä verkon laajennus langattomasti.(Wireless LAN, Wikipedia 2005)

Toisaalta langattomien verkkojen perus pulma ovat radioaallot. Siinä missä verkkojohto pysyy rakennuksen sisällä, radioaalto ei näin tee. Tämän seikan takia WLAN on erittäin haavoittuva jo fyysiseltä ominaisuudeltaan. Tietoturva onkin tärkein seikka rakennettaessa WLAN:a ja siihen panostamatta jättämisellä saadaan hyvin tietoturvariskejä nostettua. Panostus vaatii kuitenkin aina peruspilarin eli rahaa, jota esimerkiksi PK -yrityksillä ei hirveästi ole.

Myös tiedottaminen ihmisille on tärkeää. Mikäli yrityksissä ei ymmäretä WLAN:n riskejä tai tiedetä tietoturva-aukoista, ei niihin voida edes suorittaa korjaavia toimenpiteitä. Internet on pullollaan ilmaisia ohjelmia joilla jo mitään asiasta tietämätönkin voi saada tuhoa aikaan. Ammattilaisen käsissä nämä ohjelmat ovat vielä vaarallisempia, koska kyseisillä ohjelmilla toimimista on erittäin hankala havaita.

Kytkentätapoja on kaksi;

- Ad-Hoc -tavassa langattomat laitteet keskustelevat suoraan toistensa kanssa peer-to-peer menetelmällä, joten tukiasemaa ei tässä tavassa käytetä. Tämä WLAN -käytäntö onkin kahden laitteen resurssien jakoon tarkoitettu tilapäinen verkko (Wireless LAN, Wikipedia 2005)

- Infrastruktuuri -tavassa käytetään tukiasemia(access point), joiden kautta langattomat laitteet keskustelevat keskenään ja käyttävät verkkoresursseja langallisen verkon(LAN) puolelta. Useasti tukiasemat ovat liitettynä langalliseen verkkoon, jolloin ne toimivat liityntäpisteinä langallisen ja langattoman verkon välillä. Infrastruktuuri -tapa on pysyvä ratkaisu, jota ei ns. pureta kun resurssien käyttö on lopetettu. (Wireless LAN, Wikipedia 2005)

4 Verkkoliikenteen salaustekniikat

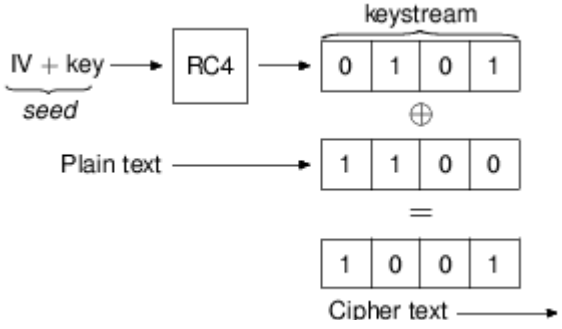
Monissa aktiivisissa WLAN:ssa on hälyttävän usein tehdasasetukset sisällä tai erittäin heikko salaus. Tehdasasetukset löytyvät lähes aina valmistajan kotisivuilta laitteiden ohjekirjoista, joten tietoturvattomuus kasvaa mitä enemmän verkkoja asennetaan ja mitä vähemmän niitä konfiguroidaan. Onko sinunkin yrityksesi verkkotunnus ”default”?

4.1 WEP (Wired Equivalent Privacy)

Ensimmäinen standardoitu WLAN -salaus, josta on myöhemmin löydetty lukuisia puutteita tietoturvan osalta. Tästä syystä sitä suositellaan käytettäväksi vain kotona käytettävissä WLAN:ssa. Tärkein seikka WEP -salauksessa on sen käyttö vain langattomassa verkossa. Mikäli tieto liikkuu jossain vaiheessa langallisessa verkossa ei se ole enää salattua.(WLAN Tietopankki WEP)

Käytössä on 64 tai 128 -bittinen salaus, joka koostuu 24 -bittisestä alustusvektorista(IV, Initialization Vector) ja 40 tai 104 -bittisestä salausavaimesta. Jokaisella työasemalla pitää olla sama avain kuin tukiasemalla, eikä keskitettyä avainten hallintaa ole. Avainten syöttäminen tapahtuu siis täysin manuaalisesti laite laitteelta. Tämä tekee WEP -salauksesta hankalasti ylläpidettävän.(Tom's Hardware WEP, 2002)

Salausprosessissa käytetään RC4 -algoritmia, joka on erittäin vanha algoritmi(kehitetty vuonna 1987). (Tom's Hardware WEP, 2002) Algoritmilla lisätään 24 –bittinen alustusvektori(IV, Initialization Vector) WEP –salausavaimeen. Tästä saadaan RC4 –avain, josta generoidaan RC4 –avainvuo. Jotta vastaanottaja pystyy käyttämään samaa avainta, IV lisätään WEP –kehykseen salaamattomana! Salaamattomasta datasta lasketaan kehyksen eheyttä turvaamaan ICV –tiiviste(Integrity Check Value), joka lisätään salatun datan perään. Tämän jälkeen avainvuo ja salaamaton datan pätkä(yhtä pitkät) lasketaan yhteen käyttäen XOR –funktiota(exclusive OR, matemaattinen funktio). (Puska, 2005:80) Kuvassa 1 näkyy periaatteellinen WEP –salauksen toiminta.



KUVA 1

4.2 WPA (Wi-Fi Protected Access)

Tietoturvaltaan huomattavasti paremman suojan kuin WEP –salaus antava WPA toimii monella eri tasolla, joten WPA:lla suojattuun verkkoon tunkeutuminen on hankalaa. WPA käyttää osia 802.1X -standardista sekä siihen kuuluvaa EAP -protokollaa(Extensible Authentication Protocol). Koska EAP toimii sekä langattomassa että langallisessa verkossa, salattu tieto ei liiku verkossa salaamattomana.(WPA: How It Works, 2004)

Työasema joka ottaa yhteyden tukiasemaan ei pääse käsiksi verkkoresursseihin ennenkuin se on täysin todenettu ja autentikoitu. Prosessin kulku menee seuraavaan malliin:

1.Työasema lähettää liittymispyynnön tukiasemalle
2.Tukiasema lähettää pyynnön edelleen palvelimelle
3.Palvelin käsittelee pyynnön ja lähettää identiteettikyselyn tukiaseman kautta työasemalle
4.Työasema muodostaa identiteettivastauksen ja lähettää sen tukiaseman kautta palvelimelle
5.Mikäli kaikki täsmää, päästetään työasema verkkoresursseihin käsiksi

Kyseistä mallia sanotaan nelinkertaiseksi kättelyksi ja sen tarkoituksena on estää mm. Man-in-the-middle -hyökkäykset. Tukiasemat siis toimivat vain pakettien välittäjinä ja varsinainen autentikointi suoritetaan päätelaitteilla(palvelin – työasema). (Geier 1, 2002)

4.3 WPA 2

Niinkuin nimikin sen jo sanoo, tämä on päivitetty versio WPA:sta. EAP -protokollan sijasta käytetään AES -salausta(Advanced Encyption Standard), joka vaatii enemmän prosessointitehoa tukiasemalta. Tästä johtuen vanhemmissa WLAN -laitteissa ei välttämättä riitä teho, mikäli WPA päivitetään. Uudemmissa laitteissa sen sijaan voidaan selvitä pelkällä ohjelmistopäivityksellä. (Wi-Fi Alliance WPA2, 2006)

4.4 WPA vs. WEP

WEP -salauksen heikkous on 24 -bittinen alustusvektori(IV). Vaikka jokaiselle salatulle datan palaselle on oma IV, samanlaisten alustusvektorien esiintyminen on suurta johtuen vektorin pienuudesta. Samanlaisten IV:den avulla hyökääjän on helppo laskea käytetty avain auki ja saada pääsy verkkoon. Palaamme tähän asiaan myöhemmin. WPA:ssa IV on tuplasti isompi, 48 -bittiä, joten samojen IV:den mää-

rä laskee dramaattisesti. Pakettien salaukseen käytettävien avaimien luontiin on myös tullut huomattavia parannuksia. (Open Extra, 2007)

WEP –salauksessa käytetään suoraan pääavainta datan salaamiseen, kun taas WPA:ssa TKIP –protokolla generoi aloitusavaimen(Temporal Key). Tämä aloitusavain yhdistetään puolestaan työaseman MAC –osoitteeseen sekä vuorossa olevan kehyksen järjestysnumeron neljään eniten merkitsevään bittiin, jolloin saadaan väliaikainen avain. Kehyskohtainen avain saadaan kun väliaikainen avain yhdistetään vielä vuorossa olevan kehyksen järjestysnumeron kahteen alimpaan bittiin. Myös jokaisen kehyksen aloitusvektorille suoritetaan salaus. Näin ollen jokaiselle kehykselle tulee varmasti erilainen avain ja MAC –osoitesidonnaisuus varmistaa, että jokaisella lähettävällä asemalla on erilainen salausavain käytössä. (Puska, 2005:82)

Kehysten eheyden tarkistus WEP –salauksessa on todettu erittäin heikoksi. WPA käyttää puolestaan MIC –tarkistusta(Message Integrity Check), joka paljastaa sanomien väärennysyritykset. Mikäli kehystä muutettaisiin, pitäisi muutoksen läpäistä ensin järjestysnumerotarkistus(TSC, TKIP Sequence Counter). Muutoksen tekijällä pitäisi olla myös kehyskohtainen salausavain tiedossaan. Vasta näiden jälkeen pitäisi vielä huijata MIC –tarkistusta. Käytännössä kehyksen muuttaminen on siis mahdotonta WPA:ta käytettäessä. (Open Extra, 2007)

5 Verkkoavainten salaustekniikat

5.1 TKIP

Temporal Key Intergrity Protocol suunniteltiin vahvistamaan WEP -salauksen heikkouksia. Alkuasetelma protokollaan oli, että sen pitää toimia laitealustasta riippumattomana, joten se ei voinut käyttää raakaa laitteiston prosessointitehoa tiedon salaamiseen. (TechFAQ, 2006)

Protokollaan kuuluu 128 -bittiset avaimet salaukseen ja 64 -bittiset avaimet autentikointiin. Toimintaan kuuluu myös oleellisena alustusvektoreiden salaaminen. Tällä toiminnallisuudella on pyritty pääsemään eroon heikoista IV:stä. Parannusta on siis uusi avainkäsittely sekä salausprosessin puhdistaminen WEP:n heikkouksista. TKIP ei ole WEP:n korvaaja vaan se toimii WEP:n ympärillä ja tuo vain omat parannuksensa tietoturvaan. (TechFAQ, 2006)

Jokaiselle paketille käytetään omaa salausavainta, joka koostuu aloitusavaimesta(luodaan aina kun työasema ottaa yhteyden tukiasemaan), lähettävän työaseman MAC –osoitteesta(Media Access Control) sekä jokaisen kehyksen järjestysnumerosta. Jälkimmäinen arvo on 48 -bittinen ja on siis eri jokaisessa paketissa. Sitä käytetään myös IV:ssä

joten jokainen alustusvektori on varmasti erilainen. WEP:n heikot IV:t ovat siis historiaa. Käytettäessä protokollaa yhdessä 802.1X:n kanssa, perusavain lähetetään salatussa muodossa autentikointipalvelimelle ja takaisin työasemalle. Mikäli käytetään PSK -avaimia, eli ennalta jaettuja avaimia, on perusavain aina sama eikä uniikki niinkuin 802.1X:n kanssa. (Networkworld, 2004)

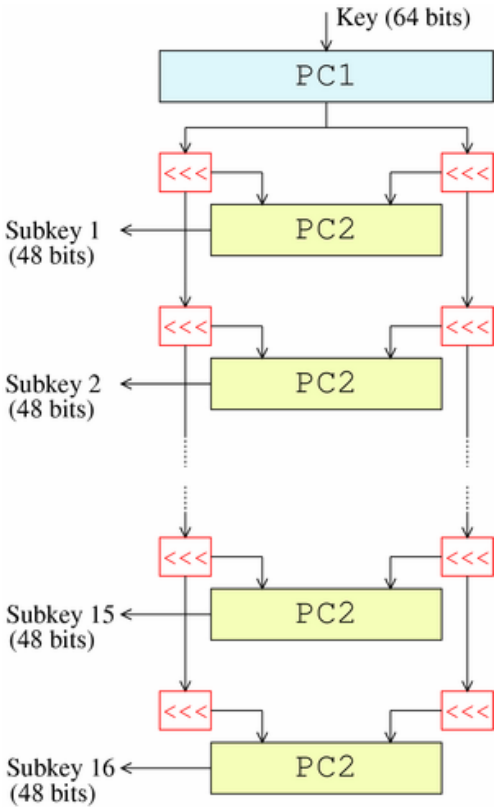
Ensimmäiset TKIP -sovelmat olivat pitkälti laitevalmistaja riippuvaisia, jolloin käyttäjät olivat kiinni yhden valmistajan laitteissa. Eri laitevalmistajien TKIP -ratkaisut eivät siis toimineet keskenään. Wi-Fi Group niminen organisaatio alkoikin kehittää standardoitua ratkaisua ja tarkoituksena oli luoda salausprotokolla joka käyttäisi TKIP:tä muutenkin paremmin. Tähän ratkaisuun päästiinkin ja salausprotokollan nimeksi muodostui WPA. (TechRepublic, 2003)

5.2 DES(Data Encryption Standard)

Salausalgoritmien dinosaurus syntyi jo vuonna 1976. Tosin vastoin sen alkuperäisiä suunnitelmia, sen tietoturvaa heikennettiin kenties poliittisista syistä. On myös monia vahvistamattomia huhuja, joiden mukaan kyseinen protokolla sisältäisi takaoven Yhdysvaltain turvallisuusorganisaatiolle NSA:lle(National Security Agency).(Data Encryption Standard, Wikipedia 2007)

Alkuperäinen avainkoko oli 64 -bittiä, jota pienennettiin 56 -bittiin NSA:n painostuksesta. Johtuen tästä pienennyksestä, onnistunut DES:n murtaminen kestää alle 24 tuntia. Varsinaiseen algoritmin ytimeen ei kuitenkaan ole onnistuttu hyökkäämään, johtuen koko prosessin monimutkaisuudesta. (Data Encryption Standard, Wikipedia 2007)

Toiminta jakautuu 16 eri vaiheeseen ja siinä käytetään 64 -bitin kokoisia raaka datan palasia(Kuva 2). Jokaiselle raaka datan palaselle luodaan 16 kappaletta 48 -bitin kokoisia vaiheavaimia, toisin sanoen yksi jokaiselle vaiheelle. Varsinainen tiedon salaus käsittää tiedon jakamisen kahteen 48 -bitin kokoiseen lohkoon, nimettäköön vaikkapa vasen ja oikea puoli. Toinen lohkoista jää kuitenkin vajaaksi varsinaisen tiedon osalta, joten siihen lisätään ns. täytebittejä jolloin saadaan kaksi yhtäsuurta lohkoa käsiteltäväksi. Tämän jälkeen kumpikin puolisko käytetään XOR –funktion(exclusive OR, matemaattinen funktio) läpi yhdessä vaiheavaimen kanssa. Seuraavassa vaiheessa täytebittejä lisätään toiselle puolelle, esim. mikäli ensin on lisätty oikealle puolelle niin toisessa vaiheessa lisätään vasemmalle puolelle näitä täytebittejä. Prosessi jatkuu samalla tavalla koko 16 -vaiheisen toiminnan aikana. Täytebittien ns. puolen vaihdolla on pyritty lisäämään algoritmin tietoturvaa.(Data Encryption Standard, Wikipedia 2007)



KUVA 2

5.3 Triple DES(Triple Data Encryption Strandard)

Kun DES:n puutteet ja turvattomuus huomattiin, alettiin hakemaan ja kehittämään lisäturvaa. Koska uuden algoritmin kehittäminen on hitaampaa kuin vanhan muokkaaminen, eikä uuden algoritmin heikkouksia tunneta, oli Triple DES:lle kysyntää. Yksinkertaisin ero DES:n verrattuna on se, että Triple DES salaa tiedon kolmeen kertaan DES:llä. Huomaa, että Triple DES ei tarkoita 3DES -salausta. 3DES on Triple DES:n epästandardimpi muoto. (Triple DES, 2007)

Salaustapoja Triple DES:ssä on kaksi. Tieto joko salataan kolmeen kertaan peräkkäin(EEE, Encryption Encryption Encryption) tai sitten ”keskellä” tieto muutetaan kerran salaamattomaksi(EDE, Encryption Decyption Encryption). Riippumatta siitä kumpaa menetelmää käytetään, ei ole merkitystä tietoturvaan. Koko salauksen suuruus on 168 -bittinen, joka koostuu siis kolmesta 56 -bittisestä avaimesta. Triple DES on poistumassa pikkuhiljaa laitevalmistajien siirtyessä tehokkaamman AES -salauksen pariin, mutta on kyllä käytössä WLAN:en ulkopuolella vielä pitkään. Esimerkiksi maksupäätejärjestelmien EMV -suojaus pohjaa itsensä juuri Triple DES:n.(Triple DES, 2007)

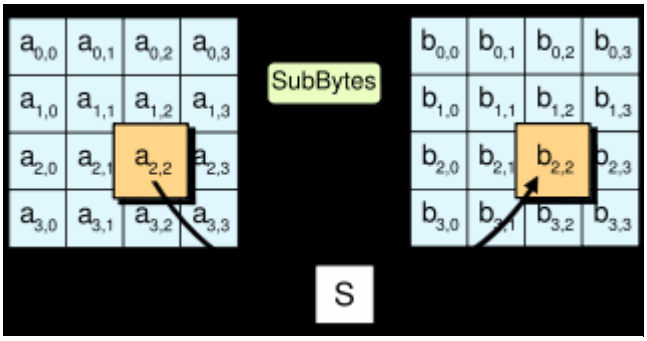
5.4 AES(Advanced Encryption Standard)

Rijandel -algoritmista kehitetty uuden sukupolven AES on 128 -bittinen ja se käyttää kolmea erikokoista avainta(128-, 192- tai 256 -bittiä). Vaikka useasti Rijandel -nimeä käytetään puhuttaessa AES:sta, ei tekniikka ole kuitenkaan sama. Siinä missä AES käyttää kolmea erikokoista avainta, voidaan Rijandel:ssa käyttää mitä tahansa kokoa 128 – 256 -bitin välillä. (Wi-Fi Planet, 2005)

Salaus toimii 4x4 bitin taulukossa(array), josta käytetään termiä tila(state). Jokaisessa salausvaiheessa(tarkkaa määrää ei ole määritetty) käydään läpi neljä alivaihetta. Ne ovat seuraavat:

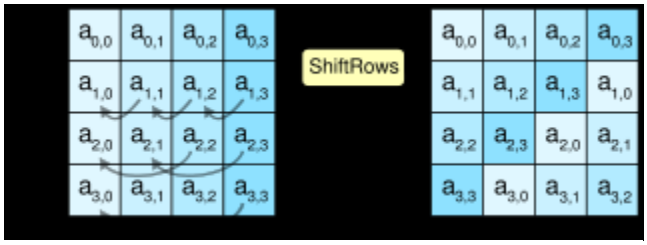
1. AddRoundKey – jokaiseen tilan tavuun yhdistetään vaiheavain, joka lasketaan varsinaisesta pääavaimesta

2. SubBytes – tässä epä-lineaarisessa alivaiheessa vaihdetaan tavu toiseen, käyttäen hyväksi erityistä seurantataulua(lookup table) (Kuva 3)



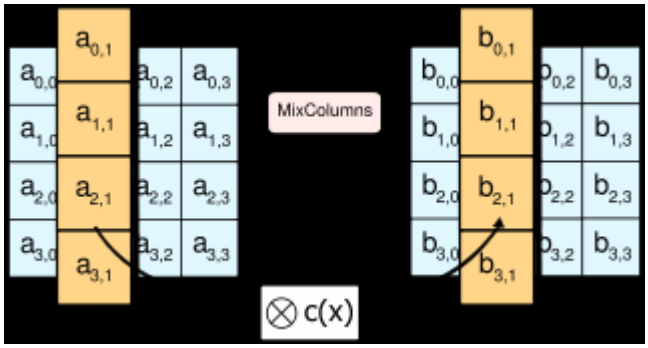
KUVA 3

3. ShiftRows – nimensä mukaisesti siirretään tavuja jokaisen rivin sisällä(Kuva 4)



KUVA 4

4. MixColumns – ottaa käsittelyyn neljä tavua ja jakaa ne tunnetulla polynomilla, käsittelyssä on siis aina yksi sarake. Tätä vaihetta ei suoriteta viimeisessä päävaiheessa.(Kuva 5)



KUVA 5

Vaikka AES on tänä päivänä erittäin hyvä suojaus, on sitä vastaan tehty jo onnistuneita hyökkäyksiä laboratorio-olosuhteissa sekä teoriassa. Mitään todisteita ei ole vielä onnistuneesta hyökkäyksestä AES:a vastaan käytännön ratkaisuissa. (AES, Wikipedia 2006)

6 Käyttäjän autentikointitekniikat

6.1 RADIUS(Remote Authentication Dial-In User Service)

802.11 -standardiin kuuluvan WEP -salauksen heikkoon tietoturvaan ja ennen kaikkea hankalaan salasanojen vaihtoon(jokaiselle laitteelle syötettävä erikseen), on olemassa vankemman tietoturvan ja helpomman käyttäjien ja salasanojen ylläpitämisen tarjoava 802.1X -standardi. Se on oma standardinsa eikä kuulunut WLAN -standardeihin ennen kuin 802.11i ratifioitiin. Tämä standardi ei kuitenkaan itsessään tarjoa käyttäjien autentikointia vaan käyttää siihen EAP -protokollaa. EAP taas puolestaan juontaa juurensa PPP –protokollan(Point-to-Point Protocol) käyttäjäautentikointiin. (Snyder, 2002)

Toiminta perustuu samantyyliseen malliin kuin TKIP, joka myös käyttää EAP -protokollaa käyttäjien todentamiseen. Työasemaa joka ei ole autentikoitunut, ei siis pääse verkkoresursseihin käsiksi ennenkuin autentikointipalvelin on kyseisen työaseman ja käyttäjän todentanut oikeaksi. Koska kyseessä on client-server tyyppinen ratkaisu, ei tukiasemien tarvitse muutakuin välittää RADIUS -pyyntöjä työaseman ja palvelimen välillä. Tosin joillakin laitevalmistajilla on omia pieniä RADIUS -palvelimia jo tukiasemiin implementoituina, mutta niiden toimintaan ei tässä perehdytä. Koska käyttäjien autentikointi hoidetaan palvelimella ja tieto salataan työasemalla ja palvelimella, on käyttäjien ja salasanojen hallinnointi helpompaa, kun jokaiseen tukiasemaan ei tarvitse konfiguroida käyttäjätietoja erikseen. (Snyder, 2002)

Miksi sitten puhutaan RADIUS -salauksesta jos 802.1X -standardi ei ota kantaa varsinaiseen autentikointiin? Kyseinen standardiin kuuluu vain määritykset siitä, miten EAP -protokollaa kuljetetaan ethernet -pakettien sisällä. Se sopii siis niin langalliseen(LAN, Local Area Network) kuin langattomaankin(WLAN) verkkoon, pitäen näin ollen tiedon salattuna koko ajan. (Roshan, 2001)

6.2 EAP(Extensible Authentication Protocol)

Vaikka EAP – protokollaa käytetään yleensä WLAN – verkoissa, voidaan sitä käyttää myös langallisessa verkossa. EAP on Internet Engineering Task Force, IETF, yhtymän standardisoima protokolla, joka määrittelyn mukaan tarjoaa käyttäjien autentikoinnin lähiverkon yli. Varsinaisesti EAP itsessään ei ole autentikointimekanismi, vaan standardisointi siitä, miten käyttäjät pitäisi autentikoida verkon yli. EAP – autentikointimekanismeja puolestaan sanotaan EAP – metodeiksi ja niitä onkin noin 40 erilaista metodia. Yleisimmät EAP – metodit, joita käytetään langattomissa lähiverkoissa ovat:

- EAP-TLS(EAP Transport Layer Security)
- EAP-SIM(EAP for GSM Subscriber Identity)
- EAP-AKA(EAP for UMTS Authentication and Key Agreement)
- PEAP(Protected EAP)
- LEAP(Lightweight EAP)
- EAP-TTLS(Tunneled Transport Layer Security)

EAP toimii siis työasema-palvelin periaatteella, niin kuin luvussa 4.2 on kerrottu.(Extensible Authentication Protocol, 2007)

7 Haittatoiminta ja sen estäminen

Haittatoimintaa on monenlaista, aina verkon käyttämiseen liittyvistä DoS –hyökkäyksistä(Denial of Service), verkon käyttäjätietojen selvittämiseen. Käydään seuraavaksi läpi tärkeimmät huomionarvoiset seikat.

7.1 Kuuntelu

Kuuntelusta käytetään nimitystä War Driving, suomeksi parkkipaikkahyökkäys. Nimitys kuvaa hyvin osuvasti kuuntelun luonnetta. Siinä hyökkääjä kuuntelee ulos säteilevää WLAN -signaalia ja kaappaa passiivisesti verkkoliikennettä, vaikka yrityksen parkkipaikalla autossa istuen. Kuuntelu on täysin passiivista toimintaa ja sitä on käytännössä mahdotonta havaita. Siitä ei jää jälkiä verkkolaitteiden logi -tiedostoihin eikä mihinkään muualle. (Stuart, Scambray, Kurtz, 2002 :500-502)

Miten sitten kuuntelusta voi päästä eroon? Periaatteessa ei mitenkään, ellei sitten poista koko WLAN -verkkoa pois käytöstä. Tämä onkin radikaali toimenpide, joten parempi on rajoittaa signaalin säteilyä sijoittamalla tukiasemat siten, että mahdollisimman vähän signaalia säteilee toimiston ulkopuolelle.

7.2 WEP salauksen heikkous

WEP:n suurin heikkous on salatun paketin alkuinitialisointivektori(IV). Vaikka jokaisen paketin kohdalla IV muuttuu, niin ennenpitkää liikenteessä kuitenkin tulee esiintymään samanlainen IV, joita hyökkääjä tarvitsee kaksi kappaletta, jotta salauksen purkaminen on mahdollista.(Tom's Hardware WEP, 2002)

Sama vektori toistuu noin joka 17. miljoonas kerta ja jos oletetaan WLAN -verkon liikenteen määrän olevan 30Mbit/s, liikkuu tällöin joka sekunti 15 000 kehystä, kun kehyksen keskimääräinen koko on 250 tavua. Mikäli kuuntelemme liikennettä noin 19 minuuttia, on mahdollista saada yli 17 miljoonaa kehystä, joista löytyy nuo kaksi samanlaista alkuinitialisointivektoria.(Puska, 2005:81)

Maaliskuussa vuonna 2005 julkisuuteen tuli FBI:n(Federal Bureau of Investigation) keksimä WEP -hakkerointimetodi, joka kutistaa hakkerointiajan noin kolmeen minuuttiin. Liikenteen kaappaamiseen käytettiin yleisesti saatavia open source -ohjelmistoja, jotka löytyvät Internetistä pienellä hakemisella. Ryhmä käytti niinsanotusti aktiivista hyökkäystä jossa työasemalle lähetettiin koko ajan verkosta pois liittymispaketteja, jolloin kyseinen asema liittyi uudelleen verkkoon. Kun toinen hyökkääjä teki tätä työaseman ”tiputusta” verkosta, toinen samaan aikaan keräsi dataa haitallisen työaseman ja oikean työaseman välillä. Näin ollen liikenteen määrä oli suurempi mitä normaalisti, jolloin aika pieneni huomattavasti.(CompliancePipeLine, 2005) Pitää kuitenkin ottaa huomioon, että kovin piilossa tapahtuva hyökkäys tämä ei ole ja valaistunut käyttäjä voi hyvinkin nopeasti tajuta, että jokin on vinossa.

Miten sitten suojautua hyökkäyksiltä jos käytössä on vain WEP? Yleensäkään pelkän salauksen käyttäminen ei tuo tarpeeksi turvaa. Mikäli käytössä on vain WEP -salaus eikä mitään muuta mahdollisuutta ole, on turvallisin vaihtoehto käyttää VPN:ää(Virtual Private Network) yhdessä WEP:n kanssa. Näin itse verkko on suojattu vain WEP:llä, mutta verkkoresursseihin pääsee vain VPN:n kautta. Mikäli verkkoon päästään kiinni, ei hyökkääjä saa paljoa lähtödataa seuraavaan hyökkäykseen.(Stuart, Scambray, Kurtz, 2002 :500-502) Verkkoliikenne kun kulkee VPN -”putken” sisällä eikä WEP -salattuna ilmassa.

7.3 WPA:n heikkoudet

WPA:n heikkous on oikeastaan ylläpitäjän puolelta tapahtunut virhe. Mikäli verkon salasana on heikko, esim. kissa, voidaan WPA:ta vastaan käyttää sanakirja -hyökkäyksiä. Mikäli käytössä on vaikea ja monimutkainen salasana on WPA käytännössä erittäin turvallinen. Koska WPA toimii eri tavalla kuin esim. WEP, ei hyökkääjän tarvitse kaapata kuin muutama paketti ja suorittaa itse murtaminen vaikka kotonaan. Näin ollen passiivista kuuntelua hyväksi käyttäen, ei tunkeutumisesta jää jälkiä.(WNN WPA crack, 2004)

Jättämällä siis yksinkertaiset ja heikot salasanat käyttämättä olet verrattain turvassa WPA:ta vastaan tehdyistä hyökkäyksistä.

7.4 RADIUS heikkoudet

Mikäli RADIUS -palvelu sijaitsee tukiasemassa eikä keskitetyssä palvelimessa, voidaan RADIUS:ta vastaan tehdä hyökkäys. Ensiksi hyökkääjän pitää asentaa yrityksen verkkoon oma tukiasemansa. Sen jälkeen suoritetaan ARP –myrkytys(ARP poisoning) koko verkolle. (Nobel, 2004) ARP –myrkytyksessä hyökkääjä lähettää verkkolaitteille muunnetun paketin, joka sisältää muunnetun MAC –osoitteen tai muunnetun IP -osoitteen. Näin ollen esimerkiksi työasema luulisi keskustelevansa suoraan tukiaseman kanssa, vaikka liikenne oikeasti kulkisi hyökkääjän koneen kautta.(ARP cahce poisoning, 2005)

Tämän jälkeen lähetetään työasemalle uloskirjautumis -paketti, jolloin se liittyy uudelleen verkkoon ja keskustelee normaalisti palvelimen kanssa autentikointiproseduurin. Tässä kohdassa kun tukiasema lähettää avaimet työasemalle, saa hyökkääjä samat avaimet käyttöönsä. Viimeisenä vaiheena RADIUS -palvelulle kohdistetaan brute force tai sanakirja -hyökkäys, jotta saadaan varsinainen pääavain. (Nobel, 2004)

7.5 DES -salauksen murtaminen

DES käyttää 56 -bitin kokoisia avaimia, joten erilaisia avaimia on 256. Yksi tapa murtautua DES -salauksen sisään on ns. brute force -hyökkäys missä kaikkia avainkombinaatioita kokeillaan yksitellen. Tämä on aikaa vievää puuhaa, koska erilaisia vaiheita DES:n salausprosessissa on 16 kappaletta ja jokaisessa vaiheessa käytetään eri avaimia. Erilaisia laillisia kilpailuja on myös järjestetty DES:n murtamiseen. Näiden kilpailujen tarkoituksena on ollut selvittää, kuinka kauan DES:n murtamiseen menee ja on murtaminen mahdollista lainkaan. Viimeinen isku DES:ä vastaan tuli vuonna 1998, jolloin EFF(Electronic Frontier Foudation) rakensi neljännesmiljoonan maksaneen mikrosirun joka pystyi brute force -hyökkäyksellä selvittämään kaikki DES:n 16 vaihetta 56 tunnissa. Puoli vuotta myöhemmin tuo aika tippui 22 tuntiin ja 15 minuuttiin.(EFF DES cracker, Wikipedia 2007) Myös muita hyökkäyksiä on suunniteltu, mutta niiden toteuttaminen on jäänyt teoreettiselle tasolle eikä niiden käytännön toteutuksia ole tietoa.

7.6 Triple DES -salauksen murtaminen

Mitään käytännöllistä hyökkäystä Triple DES:ä vastaan ei ole. Teoreettisia malleja kyllä löytyy, mutta yhdenkin mallin käyttäminen maksaisi miljardeja ja veisi useita vuosia kehittää. (Triple DES, Wikipedia 2007) Sopiikin miettiä onko järkevää edes rikkaiden hallitusten käyttää varojaan ja resurssejaan moiseen.

7.7 WLAN signaalin häirintä

WLAN toimii 2,4GHz:n taajuusalueella ja sisältää 13 kappaletta eri kanavia. Näistä kanavista vain kanavat 1, 6, 11 ja 13 eivät toimi toistensa päällä. Niimpä esimerkiksi kaupunkien keskustoissa sijaitsevat eri WLAN -verkot voivat häiritä toisiaan, ilman että se olisi tahallista. Mitä useampia tukiasemia toimii samalla kanavalla suhteellisen lähellä toisiaan ne huonontavat liikennettä huomattavasti. Signaalia ei myöskään lähetetä kovin tehokkaasti, koska signaalin sieppaaminen olisi vielä helpompaa. (ManageEngine, 2007)

Yksinkertaisella verkkoskannerilla saadaan skannattua kantoalueella olevat verkot varsin vaivattomasti ja verkkojen perustiedot saadaan selville passiivisella kuuntelulla. Niinpä signaalin häirintä on erittäin helppoa. Ei tarvita kuin oma tukiasema, kenties suunta-antenni ja häirintä voi alkaa. Ensiksi pitää tietenkin häiriölähteeseen konfiguroida oikea kanava jolle haluamme tehdä kiusaa. Tämä esiintyy käyttäjille

käytännössä heikompana signaalina ja nopeuden laskuna. Myös mitään jälkiä varsinaisen verkon lokitiedostoihin ei jää. Varsinkin kaupunkialueella on mahdotonta havaita mistä häirintä mahdollisesti tulee. Toisaalta hieman paremmalla laitteistolla olisi mahdollista luoda valkoista kohinaa, eli radiosignaalia missä ei varsinaisesti ole dataa, 2,4GHz:n alueelle suuremmalla teholla kuin millä varsinaiset tukiasemat toimivat, jolloin kokonaisen WLAN –verkon käyttäminen olisi mahdotonta.(ManageEngine, 2007)

Mitä sitten pitäisi tehdä, jotta tällainen toiminta ei haittaisi jokapäiväistä toimintaa? Tukiasemien fyysinen sijoittelu rakennukseen lienee se ainoa mahdollinen ratkaisu. Asennetaan tukiasemat siten, että toimitilojen ulkopuolelle säteilevä signaali ei kuulu kovin kauas. On myös tarjolla ohjelmistoja, jotka valvovat langattomien verkkojen toimintaa ja niihin on mahdollista luoda omia hälytystasoja. Ylläpito voisi esimerkiksi tehdä hälytyksen, joka hälyttää kun tietty signaalitaso on alitettu. Tosin mitään halpaa lystiä tällaisen ohjelmiston käyttö ei ole.

7.8 Tukiaseman poistaminen käytöstä

Kun tukiasemat ovat huonosti konfiguroituja eikä tietoturvaan ole kiinnitetty tarpeeksi huomiota voi hyökkääjä suorittaa onnistuneen ns. Man-in-the-middle -hyökkäyksen. Siinä joko hyökkääjän työasema tai tukiasema on konfiguroitu samalla tavalla kuin verkko johon ollaan tekemässä kiusaa. Lähettämällä hieman parempaa signaalia, on näin mahdollista saada pahaa aavistamaton käyttäjä liittymään hyökkääjän laitteistoon. Mikäli viaton työasema ei heti ota yhteyttä, voidaan se pakottaa uudelleenliittymisprosessiin lähettämällä verkosta poistumis -paketti työasemalle. WLAN:n luonteesta johtuen työasema liittyy automaattisesti uudelleen, tällä kertaa ehkä jopa hyökkääjän tukiasemaan. (ManageEngine, 2007 2)

Riippuen haluaako hyökkääjä tehdä kiusaa vai kaapata verkossa liikkuvaa liikennettä tai tunnuksia voi hyökkääjä esimerkiksi reitittää liikenteen takaisin oikeaan verkkoon. Näin ollen liikenne työaseman ja verkon välillä kulkisi hyökkääjän laitteiston kautta. Tämän kaltainen tietojen kerääminen on vaikea havaita ilman minkäänlaisia langattoman verkon seuranta ohjelmistoja.(ManageEngine, 2007 2)

Ei siis kannata jättää tietoturvaa huomiotta. Kunnollisella käyttäjien autentikointipalveluilla tämänkaltaiset hyökkäykset saadaan kitkettyä erittäin tehokkaasti. Myös langattoman verkon seuranta- ja hallinta -ohjelmiston käyttäminen on suotavaa.

7.9 Haitallisten tukiasemien ja työasemien havaitseminen

Kuuntelu on passiivista, man-in-the-middle -hyökkäyksen havaitseminen hankalaa ja muunkinlaiset uhat vaanivat koko ajan langattomia verkkoja vastaan. Miten sitten havaitsisimme ei-toivotun tukiaseman tai työaseman?

Yksi toimintatapa on hankkia automaattisesti langattoman verkon toimintaa seuraava järjestelmä, johon konfiguroidaan erilaisia hälytyksiä, käyttäjien autentikointi tietoja ja muita verkkoon liittyviä asetuksia. Järjestelmään voitaisiin sitten lisätä vaikkapa omien tukiasemien MAC -osoitteet ja asettaa hälytys sitä varten, jos vieraalla MAC -osoitteella varustettu tukiasema liikennöi lähellä. Tosin sitä emme voi tietää onko esimerkiksi naapuriin muuttanut toinen yritys joka asentaa omaa langatonta verkkoaan.(ManageEngine, 2007 2)

Radiosignaalisensoreilla varustettuna tällainen järjestelmä on varmasti todella hyvä, mutta hyväkään järjestelmä ei suojaa verkkoa, mikäli siihen ei ole laitettu kunnollisia salaus- ja autentikointijärjestelmiä. (ManageEngine, 2007 2)

Ei-toivotun työaseman havaitsemiseen on myös omia oireita joita tutkimalla selviää onko oma verkko hyökkäyksen kohteena. WLAN:n toimintaan kuuluu oleellisena turvamekanismi, joka ei anna kahden työaseman tai tukiaseman lähettää samanaikaisesti. Tämä siksi, ettei tapahtuisi liikenteen törmäyksiä, jolloin tieto korruptoituu. Lähetys tapahtuu siis vuoron perään ja näitä vuoroja ohjataan odotusajalla, mikä ilmoitetaan jokaisessa paketissa mikä lähetetään. Tätä toiminnallisuutta voidaan siis ohjata ja käyttää myös haittatoimintaan. (ManageEngine, 2007 2)

Mikäli havaitaan verkossa työasema, joka lähettää pidennetyn odotusajan sisältäviä paketteja, on kyseessä todennäköisesti ei-toivottu työasema eli hyökkääjä, joka yrittää haistella tietoja verkosta. Lähettämällä tarpeeksi pitkän odotusajan sisältäviä paketteja, on mahdollista pistää kokonainen langaton verkko pois toiminnasta. (ManageEngine, 2007 2)

Toinen oire ei-toivotusta työasemasta on verkkoon liittymätön työasema, joka kuitenkin lähettää verkkoon paketteja koko ajan. Tämä voi johtua hyökääjästä, joka yrittää selvittää verkon toimintaa, siihen kuuluvia salausprotokollia sekä koko verkon yleistä infrastruktuuria. (ManageEngine, 2007 2)

Näiden tapauksien havaitsemiseen tarvitaan myös käytännössä havaintojärjestelmä. Järjestelmään voisi esimerkiksi konfiguroida sallitut MAC -osoitteet, jotka saavat liikennöidä verkkoon. Tämä on kuitenkin työläs toimenpide, koska MAC -osoite on jokaisen verkkolaitteen oma

yksilöllinen osoite. Mitä sitten jos laite vaihtuu? MAC -osoitteisto pitää päivittää ja suurissa ympäristöissä tällainen ylläpito on erittäin työlästä ja aikaa vievää. (ManageEngine, 2007 2)

Toisaalta voisi käyttää järjestelmässä sallittua laitetoimittajaa ja muut laitetoimittajan laitteet estettäisiin automaattisesti. Ongelmana tässä on taas vierailijat, joilla on aivan varmasti eri laitetoimittajan laitteisto kuin omassa verkossa. Toisaalta laitetoimittajan selvittäminen on äärimmäisen helppoa. Hyökkääjä voisi esimerkiks kuunnella passiivisesti hetken liikennettä ja päätellä MAC -osoitteista oikean laitetoimittajan. Se tieto kun kuuluu MAC -osoitteeseen. (ManageEngine, 2007 2)

7.10 Ei-toivottujen tukiasemien ja työasemien eristäminen

Ei-toivottu tukiasema kun havaitaan, on pari tapaa jolla kyseisen laitteen saa pois käytöstä. Ensimmäinen tapa on käyttää samoja metodeja kuin hyökkääjä eli esimerkiksi DoS -hyökkäyksen suorittaminen kyseistä tukiasemaa vastaan. Toisessa tavassa oletuksena on, että haitallinen tukiasema on jotenkin saatu hyökkääjän toimesta kytkettyä omaan verkkoon. Tällöin mahdollisuutena on seurata kyseisen laitteen MAC -osoitetta niin kauan kunnes saavutaan kytkimelle jonka kautta kyseinen asema liikennöi verkkoon. Yksinkertaisesti sulkemalla kyseinen kytkimen portti manuaalisesti saamme tukiaseman pois pelistä.(ManageEngine, 2007 2)

Työaseman tapauksessa DoS -hyökkäys tulisi kyseeseen, mutta ohjelmallinen tapa on selvittää haitallisen työaseman MAC -osoite ja laittaa joko langattoman verkon havaintojärjestelmään tai tukiasemien pääsylistoihin, että tällä MAC -osoitteella varustettu työasema ei saa enää liikennöidä tähän verkkoon. Haittapuolena tällä vastaiskulla on MAC -osoitteen ohjelmallinen väärentäminen ja mikäli hyökkääjä tietää mitä tekee, on hän jo näin tehnyt. (ManageEngine, 2007 2)

8 Laitevalmistajien tarjonta

Tähän asti olemme käsitelleet salausalgoritmeja yleisellä tasolla. Seuraavaksi käymme läpi muutamien laitevalmistajien(D-Link, Zyxel, Hewlett-Packard, Cisco Systems) tarjontaa PK –yrityksen näkökulmasta. Laitteiden valinnassa on huomioitu mahdollisimmat monipuoliset ominaisuudet niin salauksen kuin muiden turvaominaisuuksien osalta. Esitellyt laitteet soveltuvat 1 – 20 työntekijän yrityksiin.

8.1 D-Link DI-784

Laitteen konfigurointiin on tarjolla vain selainpohjainen käyttöliittymä. Ensimmäistä kertaa laitetta konfiguroitaessa käytössä on asennusvelho, joka opastaa erilaiset konfigurointimahdollisuudet läpi. Kyseinen laite tuntuukin peruskäyttäjälle tehdyltä johon ei ole lisätty mitään ylimääräistä.

Salausalgoritmeista löytyy WEP –salaus, joko 64-, 128-, tai 152 –bittisenä versiona. Mikäli salausta halutaan käyttää 802.11b/g verkoissa ovat edellä mainitut kolme salausta mahdollisia. 802.11a –standardin verkkoihin on tarjolla 152 –bittinen salaus, jossa on mahdollisuus konfiguroida D-Link spesifisiä ominaisuuksia. Tuntuukin, että laite on tehty toimimaan pelkästään D-Link tuotteiden kanssa. (DI-784 manuaali 2007:13)

Myös WPA –salaus on tuettuna niin RADIUS –palvelimen kanssa tai ennaltajaetun avaimen(PSK) kanssa. Jälkimmäinen ei vaadi verkkoon liitettyä RADIUS –palvelinta. Tukiasemassa itsessään ei ole sisäänrakennettua RADIUS –palvelua. (DI-784 manuaali 2007:13)

8.2 Zyxel NWA-3500

Myös Zyxel tarjoaa vain selainpohjaisen käyttöliittymän. Laitteessa on kaksi antennia ja ne voivat toimia joko samassa tai useammassa verkossa. Mahdollisuutena on konfiguroida esimerkiksi omat verkot niin työntekijöille kuin vieraillekkin. Eri verkoille voidaan myös konfiguroida erilaisia verkkoresursseja. Esimerkiksi vieraille varattuun verkkoon voidaan asettaa pääsy vain Internettiin ja yhdelle verkkotulostimelle. (NWA-3500 manuaali, 2007:54-55)

NWA-3500 mallista löytyvät niin WEP-, WPA- sekä WPA2 -tuki. Kaksi jälkimmäiseksi mainittua toimivat myös RADIUS -palvelimen kanssa mikäli sellainen löytyy. Mikäli ko. palvelinta ei löydy niin vaihtoehtona on vielä WPA(2)-PSK, joka on siis WPA -salattu ennaltajaettu avain. Mikäli verkkokortit eivät ole WPA -yhteensopivia, on mahdollista käyttää myös WEP -salausta(64- ,128-, 152 -bittiset versiot). (NWA-3500 manuaali, 2007:103)

RADIUS –palvelimen kanssa käytettävistä autentikointiprotokollista ovat tuettuna seuraavat EAP -protokollan versiot:

- EAP-TLS(EAP Transport Layer Security)
- EAP-TTLS(EAP Tunneled Transport Layer Security)
- EAP-MD5(EAP Message Digest 5)
- PEAP(Protected EAP)

(NWA-3500 manuaali, 2007:104)

RADIUS -tuki löytyy niin ulkoiselle palvelimelle kuin laitteen sisäiselle palvelimelle.(NWA-3500 manuaali, 2007:116) Sisäisen RADIUS –palvelimen turvallisuus on kuitenkin heikompi kuin ulkoisen, kuten luvussa 7.4 on kerrottu. Laitteen omaan RADIUS -palvelimeen tarvitsee konfiguroida yleisten asetusten lisäksi *"luotetut tukiasemat"* sekä *"käyttäjätilit"*. Sisäisen autentikointipalvelimen tuetut käyttäjän tunnistusprotokollat rajoittuvat PEAP -protokollaan sekä MD5 -salausalgoritmiin.(NWA-3500 manuaali, 2007:157) Sisäinen RADIUS -palvelin toiminto ei kuitenkaan tue toimialuetilejä.
(NWA-3500 manuaali, 2007:158)

Zyxel on panostanut myös laajan salauksen lisäksi automaattiseen(tai ylläpitäjän halutessa myös manuaaliseen) ei-toivotun tukiaseman havaitsemiseen. Se pystyy havainnoimaan standardien 802.11a ja 802.11b/g tukiasemat. Mikäli verkko koostuu useammasta tukiasemasta tai naapuriyrityksen verkosta emme halua ilmoituksia, laitteelle pitää konfiguroida myös ystävällisten tukiasemien lista(friendly AP list). Listaan merkitään kunkin ystävällisen tukiaseman MAC -osoite. Kun ei-toivottu tukiasema havaitaan, lähettää oma NWA-3500 sähköpostiviestin verkon ylläpitäjille.(NWA-3500 manuaali, 2007:143-145)

8.3 Hewlett-Packard ProCurve 420

HP:n puolelta tarkastelussa on HP ProCurve 420 tukiasema, jossa on Ciscon tavoin niin WEB -pohjainen hallintaliittymä kuin myös komentokehoitteeseen nojautuva hallintaliittymä(Command-Line Interface, CLI).

Procurve 420 tarjoaa sekä perus WEP -salauksen, että dynaamisen WEP -salauksen joka toimii yhdessä RADIUS -autentikoinnin kanssa. Jälkimmäiseen tarvitaan siis RADIUS -palvelin. WEP -avainten pituuksia löytyy 64- ,128- ,tai 152 -bittiä. (Procurve 420 manuaali, 2005 :184)

Tukiasemasta löytyy muutama eri WPA -kombinaatio erilaisiin verkkoihin. 802.1X + EAP tarjoaa perusraamit käyttäjien autentikoimiseen ja dynaamiseen avainten jakamiseen. EAP -tyypeistä mainitaan EAP-TLS, EAP-TTLS tai PEAP. PEAP on näistä eri versioista turvallisin vaihtoehto. Myös TKIP vaihtoehto löytyy ja sitä suositellaan käytettäväksi WEP:n sijasta. Mikäli yrityksestä ei löydy resursseja RADIUS -palvelimen hankintaan tai käyttämiseen, löytyy WPA -salauksesta myös PSK muoto joka toimii yhdessä TKIP:n kanssa. Mikäli yrityksessä on monenlaisia WLAN -kortteja eikä niiden yhtenäistäminen käy, voidaan ProCurve 420 konfiguroida myös yhteinen WPA ja WEP -tuki. Kun verkkokortti ilmoittaa tukiasemalle, että se on WPA -

yhteensopiva lähettää tukiasema verkkokortille avaimen TKIP:tä hyväksikäyttäen. Mikäli työasema ilmoittaa olevansa vain WEP -yhteensopiva, käytetään avaimien lähettämiseen WEP unicast paketteja. Koska molemmille salauksille tarkoitettujen avaimien pitää olla samat, varsinainen verkkoliikenteen salaus toimii vain WEP -salauksella.(Procurve 420 manuaali, 2005:172-173)

Koska WPA2 on taaksepäin yhteensopiva, sopii sen käyttämiseen niin PSK kuin RADIUS, TKIP tuella. Eroavaisuutena on kuitenkin AES -algoritmi, josta on Ciscon tapaan käytössä AES Counter-Mode encyption with Cipher Block Chaining Message Authentication Code, AES-CCMP. Kyseinen AES -malli on standardi ominaisuus WPA2 -algoritmin käyttämiseen. Koska kyseessä on algoritmi jossa tarvitaan paljon laskentatehoa, pitää myös laitteiston tukea WPA2:sta. Näin ollen myös työasemien verkkokortit pitää päivittää WPA2 -tukeviksi. Tällä tavalla rakennettu verkko on erittäin turvallinen, sillä verkkoliikenteen salaaminen toimii 128 -bittisten avaimien avulla. (Procurve 420 manuaali, 2005:173-174)

Toisena eroavaisuutena pelkkään WPA -algoritmiin on WPA2 Mixed Mode, joka antaa sekä WPA -työasemien että WPA2 -työasemien ottaa yhteyttä samaan verkkoon. Unicast –pakettien salaus neuvotellaan erikseen jokaiselle työasemalle, riippuen tukevatko ne TKIP -protokollaa vai AES-CCMP:tä. Broadcast -paketeille käytettävä salaus toimii ainoastaan TKIP:llä, kun käytössä on mixed moodi. WEP -salaus on kielletty kokonaan. (Procurve 420 manuaali, 2005:173-174)

Useamman tukiaseman verkoissa, on kiinnitetty huomiota työaseman mahdolliselle liikkumiselle eri tukiasemien välillä. Koska WPA2 -salaus ja käyttäjien tunnistaminen on hidas prosessi, saattavat erilaiset verkko-ohjelmat lakata toimimasta. Tämä johtuu siitä, että jokaiselle tukiasemalle pitäisi suorittaa WPA2 -prosessi uudelleen. Tätä helpottamaan on kehitetty ennalta-autentikointi(Preauthentication) sekä avainten tallentaminen erityiseen välimuistiin tukiasemassa(Key caching). Key caching -toiminnolla WPA2 -työasema saa ensimmäisellä autentikoitumiskerralla pääavaimen jota se käyttää muita liikennöintiavaimia luodessaan. Kun tukiasema pitää työaseman ja pääavaimen tietoja välimuistissaan, uudelleen autentikoitumista ei tarvita. Preauthentication -toiminnolla tukiasema puolestaan lähettää toiselle tukiasemalle valmiiksi alkuautentikointi tiedot, jonka alueelle työasema on menossa. Kun työasema liittyy uuteen tukiasemaan ja lähettää autentikointipyynnön uudelle tukiasemalle, on se jo autentikoitu(edellisen tukiaseman puolesta), jolloin se voi siirtyä suoraan avainten ja resurssitietojen vaihtoon. Tämä nopeuttaa huomattavasti työaseman liikkumista suuressa langattomassa verkossa. (Procurve 420 manuaali, 2005:173-174)

8.4 Cisco Systems

Cisco Systems käyttää Aironet tukiasemissaan yhteneväistä käyttöjärjestelmää IOS:a, joten jokaiselle mallille ei tarvitse tehdä omaa manuaaliaan. Tosin eri malleissa saattaa olla joitain erovaisuuksia niin salauksen kuin laitteiden ominaisuuksien kanssa.

Niinkuin muissakin laitteissa, myös Ciscon laitteissa on tuki WEP -salaukselle. Hewlett-Packardin tapaan on mahdollisuus myös dynaamiselle WEP -salaukselle, joka käyttää EAP -autentikointialgoritmia. Tämä auttaa estämään WEP -avaimien passiivista kuuntelua, koska avaimet vaihtuvat tietyn väliajan päästä. (Cisco Wireless IOS manuaali, 2006:210)

WPA kuuluu myös tuettuihin algoritmeihin ja mikäli halutaan käyttää WPA:ta tai Ciscon omaan keskitettyä avainten hallintaa, Cisco Centralized Key Management, CCKM, tarvitsee algoritmiperheen(chipher suite) laittaa erikseen päälle. Aironet 1130AG ja 1230AG mallit tukevat WPA2:sta. Aironet 1100, 1200 ja 1300 mallit tukevat WPA2:sta mikäli IOS päivitetään versioon 12.3(2)JA tai parempaan. WPA –salauksissa on mahdollista käyttää niin TKIP –protokollaa kuin AES-CCMP –algoritmiakin. (Cisco Wireless IOS manuaali, 2006:218-223)

Ensimmäinen huomion arvoinen seikka RADIUS -palvelun konfiguroinnissa Ciscon laitteelle on, että se pitää hoitaa laitteen komentokehoitteesta(CLI). RADIUS -palvelimet tunnistetaan joko niiden laitenimillä tai IP -osoitteella ja UDP -porttinumerolla. Näiden kahden elementin summasta saadaan palvelimelle uniikki tunnus, jolla mahdollistetaan usean eri portin käyttäminen. Mikäli kaksi RADIUS -tunnusta on luotu samalle resurssille, käytetään toista tunnusta varatunnuksena ensimmäiselle tunnukselle. Tunnukset voidaan joko liittää tiettyyn palvelimeen tai sitten koko verkon RADIUS -palvelimille. (Cisco Wireless IOS manuaali, 2006:272-275)

Cisco:lla on myös laitteissaan aktiivisia turvamekanismeja. Niinkuin Zyxelin ei-toivottujen tukiasemien havainnointi palvelussa, on Cisco:lla tunkeilijan esto palvelu(Wireless Intrusion Detection Service, WIDS) tukiasemissaan. Paras käyttöaste tavoitetaan kun WIDS:ä käytetään CiscoWorks Wireless LAN Solution Enginen(WLSE) kanssa. Tällöin tukiasemat havaitsevat tunkeutumisyritykset ja ottavat osaa haitallisen tukiaseman havaitsemiseen. Havaitsemisjärjestelmään kuuluvat seuraavat osa-alueet:

- Kytkimen portin jäljittäminen ja ei-toivotun tukiaseman toiminnan lakkauttaminen(Switch port tracing and rogue suppression)

  - Kun tukiasema havaitsee mahdollisen ei-toivotun tukiaseman, se ilmoittaa siitä WLSE -palvelulle joka alkaa etsiä havaitun tukiaseman MAC -osoitteen perusteella siinä kiinni olevaa kytkintä. Mikäli tämä osoite löytyy, WLSE pistää kyseisen kytkimen portin kiinni.

- Hallintapakettien määräkohtainen tarkistus(Excessive management frame detection)

  - Mikäli suhteellisen suuri määrä verkon hallinnointipaketteja havaitaan, se voi olla hyökkäys langatonta verkkoasi kohtaan. Käynnissä voi olla esim. DoS -hyökkäys. Kun tukiasemat on konfiguroitu havainnoimaan tällaista toimintaa ne ilmoittavat siitä WLSE:lle.

- Epäonnistuneiden kirjautumispyyntöjen havainnointi (Authentication/protection failure detection)

  - Tämä osa-alue tarkistaa verkkoliikennettä hyökkääjien varalta jotka yrittävät ohittaa kirjautumisprosessia tai yrittävät toimia tukiaseman ja työaseman välissä(man-in-the-middle). Näissä hyökkäyksissä käytetään joko Extensible Authentication Protocol Over LAN, EAPOL floodausta(hyökkääjä lähettää verkkoon esim. RADIUS –autentikoitumispyyntöjä niin että RADIUS –palvelin ei niitä kaikkia ehdi käsitellä, täten jumittaen palvelimen), pakettien tarkistussummien muuttamista, salausalgoritmien manipulointia tai MAC -osoitteiden väärentämistä.

- Kehysten kaappaaminen(Frame capture mode)

  - Ne tukiasemat, jotka ovat konfiguroitu osallistumaan tähän toimintoon, keräävät langatonta verkkoliikennettä ja lähettävät ne edelleen WIDS –palvelulle.

- Hallinnointikehysten turvaaminen(Management Frame Protection)

  - Kun työasema liittyy tai poistuu verkosta, käytetään kyseisiin toimintoihin hallinnointikehyk-

siä. Johtuen kehyksien käyttötarkoituksesta niitä ei voi salata. Tämä lisätoiminto turvaa hallinnointikehysten oikeellisuutta ja tarvitsee WLSE:n toimiakseen. Tämä lisätoiminto on saatavilla vain 32Mb muistia sisältäville laitteille(1130AG ja 1240AG sekä 1300 sarjalaiset tukiasemamoodissa). (Cisco Wireless IOS manuaali, 2006:239-245)

8.5 Vertailu

Laitteita ja laitevalmistajia on moneen lähtöön. Joillakin valmistajilla on omia sovelmiaan yleisistä standardeista, jotka eivät toimi muiden laitevalmistajien tuotteiden kanssa. Kannattaakin olla tarkkana mitä eri ominaisuuksia laitteista löytyy ja miten ne toimivat muiden laitteiden kanssa.

WEP –salaus on vielä hyvin tuettuna tässä työssä esitellyissä tukiasemissa ja jokaisessa vieläpä 152 –bittisenä versiona. Tosin kaikkien muiden paitsi D-Link:n manuaalissa mainittiin, ettei WEP –salausta kannata enää käyttää, johtuen sen heikosta tietoturvasta.

WPA ja WPA2 –salausalgoritmit löytyvät puolestaan Zyxelin, Hewlett-Packard:n sekä Cisco Systems:n tuotteista. AES –algoritmi puolestaan löytyy vain Hewlett-Packard:lta sekä Cisco Systems:n laitteista. Ilmeisesti Zyxel:n laitteisto ei ole niin tehokas laskentateholtaan kuin edellä mainitut kaksi isoa valmistajaa. Kuitenkin TKIP –protokolla antaa hyvän suojan sekin kun käytetään joko WPA –salausta tai WPA2 –salausta.

Sisäinen RADIUS –palvelin löytyy vain Zyxel NWA-3500 tukiasemasta, joka on hyvä lisä kyseiseen tuotteeseen. Vaikka onkin mahdollisuus, että hyökkääjä voi hyökätä sisäistä RADIUS –palvelinta vastaan, on sen toteuttaminen kuitenkin erittäin vaikeaa. NWA-3500 malli antaakin mahdollisuuden RADIUS –autentikointiin niille yrityksille, joilla erilliseen ulkoiseen RADIUS –palvelimeen ei ole resursseja. Ulkoisen palvelimen tuki löytyykin sitten kaikista muista paitsi DI-784 tukiasemasta.

Aktiivisia langattoman verkon tunkeutumisen estojärjestelmiä on sekä NWA-3500 tukiasemassa että myös Cisco Systems:n tukiasemissa. NWA-3500:n järjestelmä on mielestäni vielä parempi, koska se ei tarvitse erillisiä havainnointipalveluja toimiakseen täysin. Koko toiminnallisuus on rakennettu pelkästään tukiaseman sisään. Mikäli esimerkiksi Cisco Systems:n tukiasemien estojärjestelmistä haluttaisiin ottaa kaikki hyöty irti, tarvittaisiin siihen hankkia lisäjärjestelmiä, jotka täten syövät PK –yritysten resursseja lisää. Hewlett-Packard ei ole sisäl-

lyttänyt varsinaisesti tukiasemiinsa havainnointi ja estojärjestelmiä vaan tarjoavat erillistä ohjelmistopakettia lisänä langattomaan verkkoon.

Mikäli yrityksellä on resursseja hankkia niin sanotusti viimeisen päälle langaton verkko ja siihen tunkeutumisen estojärjestelmä, niin manuaalien perusteella olisi helppo suositella laitevalmistajista joko Hewlett-Packard:a tai Cisco Systems:ä. Mikäli yrityksen resurssit ovat kovin rajalliset, eikä varsinaista IT –henkilöstöä ole, tulee kysymykseen Zyxel NWA-3500 tukiasema jossa on kuitenkin kehittynyt liikenteen salaus sekä käyttäjien autentikointijärjestelmä. Jos taas pitäisi hankkia langaton verkko erittäin pienelle yritykselle(1-2 henkilöä), voisin suositella kyllä D-Link DI-784 tukiasemaa. Se on kuitenkin peruskäyttöön erittäin hyvä, vaikka siitä puuttuu WPA2 –salaus.

	DI-784	NWA-3500	ProCurve 420	Cisco Systems
WEP	x	x	x	x
WPA	x	x	x	x
WPA2	-	x	x	x
RADIUS	x	x	x	x
Muu turva	-	x	lisäohjelmisto	lisäohjelmisto

TAULUKKO 1

9 Loppusanat

Langatonta verkkoa rakennettaessa kaikkein tärkein asia on tietoturvapolitiikka. Sitä pitää pitää peruspilarina ja mikäli se on retuperällä ei sen päälle kannata rakentaa mitään. Oikea oppiseen tietoturvapolitiikkaan kuuluvat sanat rakenna, testaa, korjaa ja rakenna.

Pitää myös muistaa, että liikenteen salaaminen ei ole yksinään turvallinen ratkaisu. Käyttäjien autentikointipalvelut sekä virtuaaliset yksityisverkot(VPN) tulisi ottaa käyttöön joko yksinään tai yhdessä. Käyttäjien kannalta monimutkainen kirjautuminen on tietenkin hankalaa ja valituksia varmasti tulee mikäli jokaiseen palveluun tulee kirjautua yksitellen. Tähän on ratkaisuna ainakin RADIUS -autentikointi, jonka ominaisuus intergoitua Active Directoryyn on Windows serverien ylläpitäjille varmasti helpotus. Avaintenvaihtoalgoritmeista vain AES on vielä murtamatta käytännön tasolla, mutta teoreettiset mallit ovat jo valmiina.

Laitteiden fyysinen sijoittelu tulisi myös harkita tarkkaan. Mikäli WLAN -signaali säteilee kovinkin kauas rakennuksesta, on hyökkäykset sekä hyökkäysyritykset pikemmin kasvu- kuin laskusuunnassa. Passiiviseen kuunteluun tulisi suhtautua äärimmäisellä vakavuudella. WLAN -verkon eristäminen langallisesta verkosta(LAN) palomuurein on myös varteenotettava vaihtoehto. Kannattaa myös miettiä onko WLAN -verkon rakentaminen järkevää vai tulisiko sittenkin langallinen verkko halvemmaksi.

Haasteena tässä työssä oli materiaalin ja lähteiden saatavuus. WLAN -verkkojen rakentamisesta löytyy kyllä kirjallisuutta, mutta salaustekniikasta sekä murtautumistavoista ei juurikaan. Lähteet painottuvatkin Internet -artikkeleihin. Mielestäni onnistuin kuitenkin hyvin tavoitteessani, saada yksiin kansiin kattava silmäys erilaisista haittatoiminnan tavoista sekä haittatoiminnan estämisestä.

10 Lähteet

AES, Wikipedia 2006. Advanced Encryption Standard
[online] [viitattu 14.8.2006]
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

ARP cahce poisoning, 2005. GRC – ARP cache poisoning
[online] [viitattu 1.4.2007]
http://www.grc.com/nat/arp.htm

Cisco Wireless IOS manuaali, 2006. Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA
[online] [viitattu 26.4.2007]
http://cisco.com/application/pdf/en/us/guest/products/ps4076/c2001/ccmigration_09186a00807d1cda.pdf

CompliancePipeLine, 2005. FBI Teaches Lesson In How To Break Into Wi-Fi Networks.
[online] [viitattu 12.12.2005]
http://www.compliancepipeline.com/showArticle.jhtml?articleId=160502612&pgno=2

Data Encryption Standard, Wikipedia 2007. Data Encryption Standard
[online] [viitattu 1.2.2007]
http://en.wikipedia.org/wiki/Data_Encryption_Standard

DI-784 manuaali 2007. D-Link Air Premier AG DI-784 11a/11g Dualband Wireless 108Mbps Router Manual
[online] [viitattu 26.4.2007]
ftp://ftp.dlink.se/Products/di-products/di-784/Documentation/di784_manual_100.pdf

Extensible Authentication Protocol, 2007. Extensible Authentication Protocol
[online] [viitattu 28.4.2007]
http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

EFF DES cracker, Wikipedia 2007. EFF DES cracker
[online] [viitattu 15.3.2007]
http://en.wikipedia.org/wiki/EFF_DES_cracker

Geier 1, 2002. 802.1X Offers Authentication and Key Management
[online] [viitattu 8.12.2005]
http://www.wi-fiplanet.com/tutorials/article.php/1041171

Networkworld, 2004. Explaining TKIP
[online] [viitattu 16.10.2006]
http://www.networkworld.com/reviews/2004/1004wirelesstkip.html

Nobel, 2004. WLANs Exposed by Hack
[online] [viitattu 15.3.2007]
http://www.eweek.com/article2/0,1759,1627206,00.asp

ManageEngine, 2007. RF Jamming Attack
[online] [viitattu 14.3.2007]
http://manageengine.adventnet.com/products/wifi-manager/rfjamming-attack.html

ManageEngine, 2007 2. Rogue Detection and Blocking – Whitepaper.
[online] [viitattu 13.3.2007]
http://manageengine.adventnet.com/products/wifi-manager/rogue-detection-and-blocking-whitepaper.html

NWA-3500 manuaali, 2007. NWA-3500 802.11a/b/g Wireless Access Point User's Guide
[online] [viitattu 26.4.2007]
ftp://ftp.zyxel.fi/NWA-3500/user_guide/NWA-3500_3.60.pdf

Open Extra, 2007. WPA vs WEP: How your Choice Affects your Wireless Network Security
[online] [viitattu 1.2.2007]
http://www.openxtra.co.uk/articles/wpa-vs-wep.php

Procurve 420 manuaali, 2005. ProCurve Wireless Access Point 420 Management and Configuration Guide
[online] [viitattu 26.4.2007]
ftp://ftp.hp.com/pub/networking/software/59906006-0505.pdf

Puska, 2005. Langattomat lähiverkot. Jyväskylä:Talentum

Roshan, 2001. 802.1X authenticates 802.11 wireless
[online] [viitattu 15.8.2006]
http://www.networkworld.com/news/tech/2001/0924tech.html

Snyder, 2002. What is 802.1x?
[online] [viitattu 15.8.2006]
http://www.networkworld.com/research/2002/0506whatisit.html

Stuart, Scambray, Kurtz, 2002. Hakkeroinnin torjunta – uusimmat salaisuudet ja ratkaisut. Helsinki:Satku

TechFAQ, 2006. What is TKIP (Temporal Key Integrity Protocol)?
[online] [viitattu 16.10.2006]
http://www.tech-faq.com/tkip-temporal-key-integrity-protocol.shtml

TechRepublic, 2003. What the TKIP protocol is all about
[online] [viitattu 16.10.2006]
http://articles.techrepublic.com.com/5100-6350-5071789.html?tag=search

Tom's Harware 2002. WEP secure or not
[online] [viitattu 8.12.2005]
http://www.tomsnetworking.com/network/20020719/

Triple DES, 2007. Triple DES
[online] [viitattu 1.2.2007]
http://en.wikipedia.org/wiki/Triple_DES

WEP, Wikipedia 2007
[online] [viitattu 1.4.2007]
http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

Wi-Fi Alliance WPA2, 2006. WPA2 (Wi-Fi Protected Access 2)
[online] [viitattu 14.8.2006]
http://www.wi-fi.org/opensection/knowledge_center/wpa2/

Wi-Fi Planet, 2005. AES
[online] [viitattu 14.8.2006]
http://wi-fiplanet.webopedia.com/TERM/A/AES.html

Wireless LAN, Wikipedia 2005. Wireless LAN
[online] [viitattu 29.11.2005]
http://en.wikipedia.org/wiki/Wireless_LAN

WNN WPA crack, 2004. WPA Cracking Proof of Concept Available
[online] [viitattu 14.12.2005]
http://wifinetnews.com/archives/004428.html
WLAN Tietopankki 2005. WEP – Wired Equivalence Privacy
[online] [viitattu 8.12.2005]
http://wlan.dacco.fi/sanasto.htm#wep

WPA: How It Works, 2004. WPA: How It Works
[online] [viitattu 8.12.2005]
http://www.compactpci-systems.com/PDFs/Meetinghouse.Apr04.pdf