TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto

Toni Tuominen

WLAN TIETOTURVA

Tutkintotyö, joka on jätetty opinnäytteenä tarkastettavaksi insinöörintutkintoa varten
Tampereella 13.10.2005

Työn valvoja: Ari Rantala
Työn ohjaaja: Saara Lyyski, Auto-Kivitila Oy

Tekijä: Toni Tuominen
Työn nimi: WLAN tietoturva

Päivämäärä: 13.10.2005
Sivumäärä: 42 sivua ja 1 liitesivu
Hakusanat: WLAN, tietoturva, WEP, WPA
Koulutusohjelma: Tietotekniikka
Suuntautumisvaihtoehto: Tietoliikennetekniikka

Työn valvoja: lehtori Ari Rantala

Työn ohjaaja: Saara Lyyski
Auto-Kivitila Oy

Tietoturva on olennainen osa nykyaikaista tietoliikennetekniikkaa. Työssä on tutkittu WLAN-standardiin sisällytettyjä tietoturvaratkaisuja. Lisäksi työssä on käsitelty vaihtoehtoiseksi suojaukseksi tai suojauksen lisäämiseksi tarjottuja ratkaisuja. Työn tarkoituksena on tutkia WLAN-tekniikkaa pääpiirteissään ja keskittyä langattoman verkon tietoturvaan. Työssä on myös tarkoituksena tutkia langattoman verkon soveltuvuutta tietoturvan kannalta yrityksen kaapeloidun sisäverkon jatkeeksi.

802.11-standardin ensimmäinen salausmenetelmä oli WEP, joka oli valinnaisesti joko 64- tai 128-bittinen. Kyseinen salausmenetelmä todettiin nopeasti heikoksi ja tästä johtuen alettiin kehittämään uusia tietoturvaa nostavia ratkaisuja, joista suurimman edistysaskeleen sai aikaan WPA-salausmenetelmä. WPA käyttää TKIP-salausta, joka käyttää pakettikohtaisia salausavaimia ja täten parantaa huomattavasti langattoman verkon tietoturvan tasoa. Yksinkertaisempana vaihtoehtoja menetelmässä on tarjolla jaetun avaimen menetelmä, joka itsessään soveltuu vain pienien toimisto- ja kotiverkkojen käyttöön. Suurin heikkous WPA-salauksessa on menetelmän tapa suojautua DDoS-hyökkäykseltä. Kyseisen hyökkäyksen sattuessa koko verkko suljetaan kaikilta, myös sallituilta, käyttäjiltä minuutin ajaksi.

Tulevaisuuden langattomien tietoturvaratkaisujen pohjana tullaan käyttämään 802.11i-lisästandardin mukaisia ratkaisuja. Tässä ratkaisussa salausmekanismina toimii DES salausmekanismin korvaava AES lohkosalausmekanismi.

Author:	Toni Tuominen
Name of the thesis:	WLAN information security
Date:	13.10.2005
Number of pages:	42 pages, 1 appendice
Keywords:	WLAN, information security, WEP, WPA
Degree programme:	Computer Systems Engineering
Specialisation:	Telecommunication Engineering

Supervisor:	lecturer Ari Rantala
Instructor:	Saara Lyyski Auto-Kivitila Oy

Information security is one of the most essential part of today's telecommunications technique. This thesis handles information security solutions which are included in the WLAN standard. In addition it handles alternative security solutions. The purpose of this work is to study the basics of the WLAN technique and to concentrate on information security of wireless networks. Additional intention is to study how well wireless network can be used as an extension of company's wired network from information security aspect.

The first encryption method in the 802.11 standard was WEP which uses 64- or 128-bit encryption. The method was rapidly discovered very weak and as a consequence, development of new methods was started. The biggest improvement was achieved with WPA encryption method. WPA uses TKIP encryption, which uses encryption keys dynamically and therefore considerably improves information security of wireless network. The biggest weakness in WPA is method's habit to protect itself from DDoS attacks. When DDoS attack is noticed, the whole network is shut down and all – allowed users included – will be blocked from thenetwork for a minute.

Future's information security methods will be based on the 802.11i extension standard. In this solution the encryption method will be AES, which replaces the DES encryption mechanism.

ALKUSANAT

Työn aihetta työstettiin keväästä puoleen väliin kesää, eli aikana jolloin suoritin harjoittelua Auto-Kivitila Oy:ssä. Vaihtoehtona oli muutamia muita aiheita, mutta kuitenkin päädyimme tähän aiheeseen sen parhaan hyödyn kannalta. Varsinaisen työn tekeminen alkoi heinäkuussa ja työtä on tehty aina kun vapaa-aikaa on ollut. Kiitoksen työn tekemisen mahdollistamisesta kuuluvat Auto-Kivitilalle, työn valvojalle ja ohjaajalle.

Tampereella 13.10.2005

KÄYTETYT LYHENTEET

AES	Advanced Encryption Standard, lohkosalausmekanismi ja DES-standardin korvaaja
AH	Authentication Header
ADSL	Asymmetric Digital Subscriber Line
AP	Access Point, pääsykohta
ASCII	American Standard for Information Interchange, tietokoneissa käytössä oleva merkistö, sisältää aakkoset, numerot, välimerkkejä ja joitakin ohjauskoodeja.
BSOD	Blue Screen Of Death, windowsin virheilmoitusruutu
BSS	Basic Service Set, peruspalvelujoukko
CCA	Clear Channel Assessment Signal, signaali joka tarkkailee onko siirtotie vapaana
CDMA/CA	Code Division Multiple Access with Collosion Avoidance, välttää törmäyksiä
CDMA/CD	Code Division Multiple Access with Collision Detection, tunnistaa törmäykset
CRC	Cyclic Redundary Check, tarkistussumma
DBPSK	Differential Binary Phase Shift Keying, differentiaalinen binäärivaihemodulaatio
DDoS	Distributed Denial of Service, hajautettu palvelunestohyökkäys
DLC	Data Link Control, siirtoyhteyskerros. OSI-mallin 2. kerros
DNS	Domain Name Service, nimipalvelujärjestelmä
DNSSEC	DNS Security Extensions, nimipalvelujärjestelmän turvallisuus lisäykset
DoS	Denial of Service, palvelunestohyökkäys
DQPSK	Differential Quadrature Phase Shift Keying, differentiaalinen kulmavaihemodulaatio
DS	Distribution System, jakelujärjestelmä joka yleensä on runkoverkko
DSSS	Direct Sequence Spread Spectrum, suorasekvenointi hajaspektri
EAP	Extensible Authentication Protocol, käyttäjien tunnistusprotokolla

EIRP	Equivalent Isotropically Radiated Power, lähetystehon ja ´ antennivahvistuksen summan
ESP	Encapsulating Security Payload, pakettivirtojen turvaamisessa käytetty protokolla
ESS	Extended Service Set, laajennettu peruspalvelujoukko
ETSI	European Telecommunications Standards Institute
FHSS	Frequency Hopping Spread Spectrum, taajuushyppely hajaspektri
GFSK	Gaussian shaped FSK (Frequency Shift Keying), taajuudesta riippuvainen modulaatiomenetelmä
GPS	Global Positioning System, satelliittipaikannusjärjestelmä
GRE	Generic Routing Encapsulation, Ciscon kehittämä IP-tunnelointiprotokolla
HIPERLAN	HIgh PErformance Radio Local Area Network, eurooppalainen langattoman verkon standardi
IBSS	Independent Basic Service Set, itsenäinen peruspalvelujoukko, infrastuktuuriton verkko
ICMP	Internet Control Message Protocol, TCP/IP-pinon kontrolliprotokolla
ICV	Intergrity Check Value, eheystarkiste
IDS	Intrusion Detection System, tunkeutumisen havainnointi järjestelmä
IEEE	Institute of Electrical and Electronic Engineering
IFTF	Internet Engineering Task Force
IPSec	Internet Protocol Security, IP:n suojausprotokolla
IPv4	IP version 4, 32-bittinnen osoiteavaruus joka on esimerkiksi muodossa: 192.168.100.196
IPv6	IP version 6, 128-bittinen osoiteavaruus joka on esimerkiksi muodossa: 2001:708:310:4952:4320:436c:6965:6e74
IR	Infrared, infrapuna
ISM	band for Industrial, Scientific and Medical use, vapaassa käytössä oleva taajuusalue
IV	Initialization Vector, alustusvektori
L2F	Layer 2 Forwarding, tunnelointiprotokolla

L2TP	Layer 2 Tunneling Protocol, uusin tunnelointiprotokolla
LLC	Logical Link Control, looginen linkki kontrolli, toimii OSI-mallin 2. kerroksella
MAC	Media Access Control, siirtotielle pääsykerros
MIB	Management Information Base, hallintatietojen tietokanta
MIC	Message Integrity Control, varmistaa että paketteja ei ole muuteltu
MITM	Man-in-the-middle, hyökkäystapa
NSA	National Security Agency
OFDM	Orthogonal Frequency Division Multiplexing, ortogonaalinen taajuusjakoinen kanavointi
OSI	Open Systems Interconnection
OTSS	One Touch Secure Setup, buffalon kehittämä tietoturvan asetus tekniikka
PHY	Physical Layer, fyysinen kerros. OSI-mallin 1. kerros
PLCP	Physical Layer Convergence Protocol, fyysisen kerroksen konvergenssiprotokolla
PMD	Physical Medium Dependent, fyysisestä tiestä riippuvainen alikerros
PMK	Pair-wise Master Key, asiakaskoneen ja palvelimen luoma avainpari
PPTP	Point-to-Point Tunneling Protocol, tunnelointiprotokolla
PRNG	Pseudo-Random Number Generator, näennäislukugeneraattori
RADIUS	Remote Authentication Dial-In User Services, ohjelmisto jonka avulla voidaan antaa käyttäjälle käyttöoikeudet
RC4	Ron’s Code 4, Rivest Cipher 4, salausalgoritmi
SATAN	Security Analysis Tool for Auditing Networks, verkkoturvallisuusohjelmisto
SSID	Server Side IDentifier, langattoman verkon muutettavissa oleva tunnus
TCP	Transmission Control Protocol, yhteydellinen tietoliikenneprotokolla
TKIP	Temporal Key Integrity Protocol, tietoturvaprotokolla joka huolehtii yhteyksien salauksesta

UDP	User Datagram Protocol, yhteydetön tietoliikenneprotokolla
VoIP	Voice over IP, protokolla jonka avulla voidaan soittaa internetin kautta
VPN	Virtual Private Network, virtuaalinen yksityisverkko
WEP	Wired Equilevant Privacy, ensimmäinen salausmenetelmä langattomiin verkkoihin
WiLDing	Wireless Lan Driving, tunnetaan myös war-drivingina
WLAN	Wireless Local Area Network, langaton verkko
WPA	Wi-Fi Protected Access, kehittyneempi langattomien verkkojen salausmenetelmä
WPA-PSK	WPA – Pre-Shared Key, jaettu avain

SISÄLLYSLUETTELO

1 JOHDANTO

Tässä työssä on tutkittu langatonta lähiverkkotekniikkaa ja siihen läheisesti liittyvää tietoturvaa. Työssä on pyritty ottamaan huomioon erilaiset näkökulmat ja lähestymistavat käsiteltäviin asioihin. Työssä on käsitelty myös laitevalmistajien tietoturvaratkaisuja. Työssä esitellään myös langattomien verkkojen perustekniikoita.

1.1 Työn tavoite

Työssä on tavoitteena tutkia WLAN-tekniikan tietoturvallisuutta ja langattomuudesta syntyviä uhkia ja toteuttaa lähitulevaisuudessa työn pohjalta tietoturvallinen langaton verkko työn teettävään Auto-Kivitila Oy:hyn.

1.2 Auto-Kivitila Oy

Auto-Kivitila Oy on vuonna 1973 perustettu perheyritys, jonka toimitusjohtaja on Riitta Kivitila. Yli kolmen vuosikymmenen aikana Auto-Kivitilasta on kasvanut Suomen markkina-alueen suurin yksityinen Ford-piirimyyjä. Yrityksen liikevaihto vuonna 2004 oli 39,4 miljoonaa euroa. Työntekijöitä Auto-Kivitilan palveluksessa on tällä hetkellä noin 90.

Tyytyväiset asiakkaat ja henkilöstön hyvinvointi ovat Auto-Kivitilalle erittäin tärkeitä. Yrityksen menestyksen perustana voidaan pitää asiakasläheisyyttä, yrittäjähenkisyyttä ja luovuutta. Jokaisen yksilön työpanosta, terveyttä ja työturvallisuutta pidetään erittäin tärkeänä. Yrityksessä on käynnissä alati jatkuvana prosessina palveluiden ja osaamisen tason kehitys. Erinomaisesta ja nykyaikaisesta sisäisestä kehityksestä hyvänä esimerkkinä on Kivitilassa käyttöön otettu Suomen ensimmäinen reaaliaikainen Internet-pohjainen huollon ajanvarausjärjestelmä. Kivitilassa kannetaan huolta myös ympäristöstä ja Kivitilassa onkin noudatettu jo useiden vuosien ajan Autoalan Keskusliiton ympäristöohjelmaa.

Auto-Kivitila saavutti ensimmäisenä autoliikkeenä pohjoismaissa autokaupan ISO 9002-sertifikaatin. Tämän lisäksi Auto-Kivitilalle myönnettiin vuonna 2002 autoalan keskusliiton mallin mukainen laatujärjestelmä.

2 WLAN-TEKNIIKAN PERUSTEITA

Tietotekniikan jatkuvien kehitysaskeleiden ja suhteessa halventuneiden hintojen myötä ovat kannettavat tietokoneet yleistyneet huimaa vauhtia työ- ja kotikäytössä. Kannettavien yleistyessä alettiin myös kehittämään langatonta verkkotekniikkaa, jossa mobiiliasemat voisivat liittyä helposti verkkoon ja jonka alueella kyseisiä asemia voisi liikutella ilman että täytyy ajatella kaapeleiden rajallista liikkuvuutta tai niiden hankalaa vetämistä. Langaton lähiverkko voidaan kuitenkin toteuttaa monella eri teknologialla. Tällöin langattomat ratkaisut olivat häiriöalttiita ja kalliita.

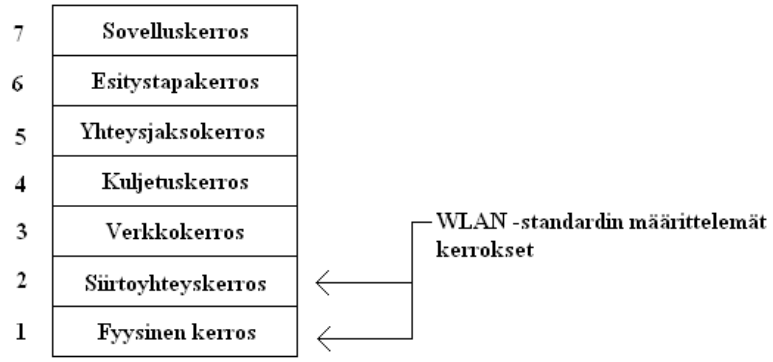
Vuonna 1990 IEEE (*Insititute of Electrical and Electronic Engineering*) aloitti projektin jonka päämääränä oli langattomien verkkojen standardointi. Nykyään käytössä olevat langattomat lähiverkot toteutukset käyttävät lähes poikkeuksetta IEEE:n 802.11-standardeja. WLAN (*Wireless Local Area Network*) on Amerikassa kehitetty standardi ja vastaava eurooppalainen standardi on HIPERLAN (*HIgh PErformance Radio Local Access Network*) tämä tekniikka on ETSIn (*European Telecommunications Standards Institute*) kehittämä langaton lähiverkkoratkaisu. HIPERLAN-tekniikasta ei ole ainakaan vielä ollut edes haastamaan WLAN-tekniikkaa.

WLAN-verkoissa informaatio liikkuu sähkömagneettisina aaltoina laitteiden välillä eli fyysistä siirtotietä, kaapelia, ei enää tarvita. Nämä sähkömagneettiset aallot eli radioaallot toimivat kantoaaltoina, joihin varsinainen informaatio lisätään moduloimalla kyseiset signaalit.

Langaton verkko on organisaation kaapeloidun lähiverkon jatkeena hyvä ja käytännöllinen. Langaton toteutus tuo myös suuria etuja työkäyttöön, esimerkiksi lääkäreiden kärryihin voidaan asentaa kannettava tietokone, jolla lääkäri voi olla reaaliaikaisesti yhteydessä sairaalan sisäverkkoon ja täten käyttää potilastietokantoja apuna kierroksillaan. Nettikahvilassa ja hotellissa asiakas voi käyttää omalla kannettavalla tietokoneella, jossa on WLAN-kortti, langatonta verkkoa ja tätä kautta Internetiä ja olla yhteydessä esimerkiksi oman yrityksensä lähiverkkoon.

Vuosituhannen alussa eräs suurimmista ongelmista langattomissa lähiverkoissa oli hitaat tiedonsiirtonopeudet. Teknologian kehittymisen myötä tämä ongelma ratkesi ja tiedonsiirtonopeudet ovat kasvaneet huomattavasti alkuaikojen 1-2 Mbps:n siirtonopeuksista. Myös langattomien verkkotuotteiden korkea hinta ja saatavuus aiheutti ongelmia vielä vuosituhannen vaihteessa. Nykypäivän suurimpana kompastuskivenä langattomissa verkoissa on puutteellinen tietoturva. Langattomien sovellutusten yleistymisen esteenä yrityskäytössä on aina ollut heikot salaukset. Tietoturva on kuitenkin kehittynyt huomattavasti siitä mitä se alkuun WEP-salauksen kanssa oli. Koska WLAN-tekniikka toimii yleisellä 2.4GHz:n taajuusalueella muodostuu ongelmaksi mm. mikroaaltouunien, bluetooth-laitteiden, aiheuttamat häiriöt. Häiriöalttius edellä mainituille tekijöille on kuitenkin yritetty minimoida, yleensä häiriötekijät eivät kuitenkaan ole vakava ongelma.

WLAN-standardi määrittelee OSI-mallin fyysisen ja siirtoyhteyskerroksen toimintatavat, kuten alla olevassa kuvassa 1 näkyy.



KUVA 1. WLAN –standardin määrittelemät kerrokset.

Työaseman liittäminen WLAN-verkkoon on erittäin yksinkertaista ja se vaatii vain WLAN-verkkokortin ja tarkoitukseen sopivat ajurit. Itse langattoman verkon yhdistäminen lankaverkkoon tapahtuu tukiaseman avulla.

Liikenne langattomassa verkossa työasemien ja/tai tukiasemien välillä on vuorosuuntaista (*half duplex*). Liikennöinnistä saadaan kuitenkin kaksisuuntaista (*full duplex*) jos molemmissa päissä on kaksi korttia.
/ 1 / / 2 / / 3 / / 4 /

PROTOKOLLAT

Infrapuna

Edellä mainituista kolmesta tekniikasta ainoastaan infrapunalla tapahtuva liikennöinti on helposti rajoitettavissa, sillä infrapunavalo ei läpäise seiniä samalla lailla kuin sähkömagneettiset radioaallot. Infrapunatekniikka on siis kohtuullisen tietoturvallista muihin verrattuna, mutta liikennöintinopeus jää vain yhden ja kahden Mbps:n luokkaan. Infrapunavalon aallonpituus on 850 - 950nm, eli lähes näkyvää valoa. Standardi ei edellytä näköyhteyttä lähettäjän ja vastaanottajan välille, mutta maksimietäisyys vastaanottajan ja lähettäjän välillä on noin 10 metriä, ellei lähettäjän ja vastaanottajan välissä ole ulkoisia häiriöitä kuten auringon valoa tai muita kuumia säteilylähteitä.

Tällä tekniikalla rakennettu verkko toimii käytännössä katsoen kunnolla vain silloin, kun ei edellytetä nopeaa yhteyttä ja alue, jolla verkon on tarkoitus toimia on kooltaan erittäin pieni, kuten esimerkiksi luokkahuone tai neuvotteluhuone. Infrapunateknologian suurin etu on sen yksinkertaiset ja erittäin halvat lähettimet ja vastaanottimet. Yksi huomattava lisäetu on se, ettei infrapunavalo häiritse sähkölaitteita, kuten radioaallot häiritsevät. Lähettiminä voi toimia ledi tai laserdiodi ja vastaanottimena toimii fotodiodi. Jos tiedonsiirrossa käytetään LED-valojen (*Light Emitting Diode*) sijasta laseria, niin tarvitsee ottaa huomioon myös turvallisuusrajoitukset.

DSSS-tekniikka

DSSS-tekniikassa (*Direct Sequence Spread Spectrum, suorasekvenointi*) on käytössä 22MHz:n taajuusalue. Tällaisessa hajaspektrijärjestelmässä informaatio hajotetaan käyttämällä niin kutsuttua Barker-koodia, eli 11 mikrobitin sekvenssiä (+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1) ja lähetetään koko taajuusalueella yhtenä signaalina, hajaspektristä johtuen asiaa tuntematon tarkkailija luulee lähetystä kohinaksi. Tämä menetelmän hyviä puolia ovat sen sietokyky häiriöille ja vastustuskyky monitie-etenemisen vaikutuksiin. Tämä toteutus muistuttaa CDMA -tekniikan toteutuksia. Ikävä kyllä DSSS-tekniikalla toteutettu langaton verkko on kallein, mutta kuitenkin suurin osa nykyisistä langattomista on toteutettu tällä tekniikalla

FHSS –tekniikka

FHSS-tekniikka (*Frequency Hopping Spread Spectrum, taajuushyppely*) on toinen WLAN-tekniikassa käytetty hajaspektritekniikka, joka mahdollistaa monta eri verkkoa samanaikaisesti samalla taajuusalueella. Taajuushyppelyssä lähettäjä vaihtaa lähetystaajuuttaan tietyn algoritmin mukaisesti ja käytetään yhtä taajuutta 79:sta standardissa määritellystä hyppelykanavasta kerrallaan, mutta esimerkiksi Japanissa on määritelty vain 23 hyppelykanavaa. Algoritmi jonka mukaan taajuus vaihtuu voi olla täysin satunnainen, mutta joka tapauksessa algoritmin on oltava sellainen että lähettäjä ja vastaanottaja tietävät satunnaisuuden tai että se on etukäteen sovittu. Kuuntelija joka ei tunne tai tiedä taajuuksien vaihtomallia, ei voi seurata liikennettä. Yleensä taajuutta vaihdetaan vähintään 400 millisekunnin välein ja tämän lisäksi taajuudessa täytyy olla vähintään 6 megahertsin hyppy. Lisäksi ETS 300-328-dokumentissa on määritelty maksimilähetysteho, joka on Euroopassa suuruudeltaan 100mW EIRP (*Equivalent Isotropically Radiated Power*) ja Amerikassa (*FCC 15.247-dokumentti*) 1W EIRP. EIRP lasketaan lähetystehon, siirtolinjahäviöiden ja antennivahvistuksen avulla. EIRP lasketaan seuraavan kaavan mukaisesti:

EIRP = (lähetysteho – siirtolinjahäviö) + (antennivahvistus)

Vaikka maksimilähetysteho on standardissa ilmoitettu watteina, lasketaan laskutoimitukset yleensä desibelien avulla.

FHSS on toteutukseltaan huomattavasti yksinkertaisempi ja halvempi kuin DSSS mutta haittapuolena ovat kohtuullisen hitaat yhteydet, jotka eivät tue kuin yhden ja kahden megabitin nopeuksia. Hitautensa lisäksi FHSS:llä on huonompi virheensietokyky kuin DSSS:llä.

Infrapuna-, DSSS- ja FHSS-ominaisuudet koskevat vain fyysisen kerroksen toimintaa. Standardi koskee myös osaa siirtoyhteyskerroksesta, joka jaetaan kahteen eri alikerrokseen LLC (*Logical Link Control Layer*) ja MAC (*Media Access Control Layer*). Erona näillä alikerroksilla on se että LLC määrittää

rajapinnan verkkokerrokseen ja MAC taasen määrittelee pääsyn fyysiseen kerrokseen.

Ethernetissä toimivan CSMA/CD-tekniikan (*Carrier Sense Multiple Access with Collision Detection, törmäyksen havainnointi*) käyttö ei ole toimiva langattomassa verkossa. Langattomissa verkoissa käytetään törmäyksen havaitsemisen sijaan tekniikkaa, jossa asemat pyrkivät välttämään törmäyksien syntyä kuuntelemalla siirtotietä ennen varsinaisen datakehyksen lähettämistä eetteriin. Edellä kuvailtua tekniikkaa kutsutaan CSMA/CA:ksi (*Carrier Sense Multiple Access with Collision Avoidance, törmäysten välttäminen*).
/ 3 / / 8 /

Modulaatio

Sekoituksessa lähetin yhdistää kaksi signaalia, joista toinen on satunnaislukugeneraattorin tuottamaa kohinaa (suurinopeuksista bittivirtaa) ja toinen on digitaalisesti moduloitu informaatiosignaali (pieninopeuksinen). Kun nämä signaalit ovat yhdistetty, niin saadaan signaali joka on nopean signaalin mukainen mutta sisältää myös informaation. Vastaanottavapää kykenee erottelemaan signaalit toisistaan, koska sillä on satunnaisen bittivirran sekvenssi tiedossa. Tämän tekniikan avulla signaalit voidaan tulkita oikein vaikka informaatiosignaali olisi jopa 35dB pienempi kuin kohinan voimakkuus.

Moduloinnin tarkoituksena on muokata lähetettävää viestiä lähetyksen ja siirron kannalta edullisempaan muotoon. Modulaatiossa kantoaallon muunnetaan järjestelmällisesti moduloivan signaalin tahdissa. Kaikilla siirtoteillä signaalit käyttäytyvät erilailla, käyttäytymiseen vaikuttaa pulssin taajuus ja tästä johtuen informaatio on lähetettävä tietylle taajuudelle (kantoaalto) moduloituna, tai sen välittömään läheisyyteen, jotta informaatio saapuisi vääristymättömänä perille. WLAN-tekniikassa fyysisen kerroksen PMD-alikerros käsittelee signaalien modulaation ja koodauksen ja dekoodauksen.

Standardissa IEEE 802.11 on määritelty FHSS:lle modulaatiomenetelmäksi GFSK (*Gaussian shaped FSK (Frequency Shift Keying*). 1 Mbit/s nopeudelle käytetään kaksitasoista GFSK:ta, jossa yksi bitti liitetään yhteen taajuuteen. 2

Mbit/s nopeudelle käytetään nelitasoista GFSK:ta, jossa kaksi bittiä liitetään yhteen taajuuteen.

DSSS:ssä käyttää lähettämiseen DBPSK:ta (*Differential Binary Phase Shift Keying, differentiaalista binäärivaihemodulaatiota*) kun nopeus on 1Mbit/s ja DQPSK:ta (*Differential Quadrature Phase Shift Keying, differentiaalinen kulmavaihemodulaatio*) kun nopeus on 2Mbit/s.
/ 8 / / 10 / / 11 /

Taajuudet

Standardi käyttää 2.4 - 2.483 GHz:n taajuusaluetta, joka tunnetaan paremmin ISM-kaistana (*band for Industrial, Scientific and Medical use*). Tällä kyseisellä 2.4GHz:n taajuusalueella toimivat langattomien verkkojen lisäksi muun muassa mikroaaltouunit, langattomat puhelimet, bluetooth-laitteet ja radio-ohjattavat laitteet.

2.4GHz:n taajuusalue on niin sanottu yhteistaajuusalue johon kaikilla taajuusalueen käyttäjillä on yhtä suuret oikeudet. Tästä johtuen yhteistaajuusalueella toimivalle radiolaitteelle ei tarvitse hankkia erillistä radioliikennöintilupaa. Koska taajuusalueelle ei tarvita radiolupaa, niin taajuusalueella toimiville radiolaitteille ei ole yksilöllisiä taajuuksia. Tämä puolestaan tarkoittaa sitä, ettei taajuusaluetta käyttäville radiolaitteille voida taata häiriötöntä toimintaa. Itse laitteiden tekniset spesifikaatiot Eurooppaan ovat määritelty ETSI:n standardissa ETS 300 328.

Langattomien verkkojen tiedonsiirtokaistojen toimintataajuuksiksi on määritelty, ETS 300-328-dokumentissa, Eurooppaan seuraavat taajuudet, poikkeuksena Euroopan alueella ovat Ranska ja Espanja, joilla omat erikseen ilmoitetut alueet alla olevassa taulukossa 1:

Alue	Taajuuden alaraja	Taajuuden yläraja
Eurooppa	2.402 GHz	2.480 GHz
Ranska	2.448 GHz	2.482 GHz
Espanja	2.447 GHz	2.473 GHz

Taulukko 1. IEEE 802.11-standardissa määritellyt taajuudet.

Tämän lisäksi IEEE 802.11a-standardille on määritelty 5-725 – 5,825 GHz:n taajuusalue. Tällä taajuusalueella on vähemmän käytössä olevia sovellutuksia, ja täten se on myös häiriöttömämpi taajuusalue kuin 2.4 GHz:n taajuusalue. Korkea taajuus läpäisee huonommin rakennusmateriaaleja ja tämän lisäksi vaimenee nopeammin kuin matalataajuisempi signaali. Näistä tekijöistä johtuen kuuluvuusalue pienenee huomattavasti verrattuna matalataajuisempaan langattomaan verkkoon.
/ 12 / / 8 /

2.1 Langattomien verkkojen nykyinen käyttö

Langattomat verkot ovat tällä hetkellä suosituimpia kotitalouksien käytössä, mutta myös julkishallinnon ja yritysten kiinnostus langattomia verkkoja kohtaan on ollut suuressa nousussa. Langattomien verkkojen pystytys esimerkiksi omakotitaloon on vaivatonta ja täten suurin yksityisten henkilöiden mielenkiintoa langattomia verkkoja kohtaan nostanut tekijä. Lähes puolet kotitalouksien langattomista verkoista on täysin suojaamattomia, ja täten esimerkiksi naapuri voi hyödyntää tätä käyttämällä toisen nettikaistaa ilmaiseksi.

Yksi suurimmista yritysten kiinnostusta langattomia verkkoja kohtaan kasvattanut tekijä on ollut langattomien verkkojen parantunut tietoturva. Vierailijaverkkojen yleistyessä jokainen yritys haluaa tarjota asiakkailleen mahdollisuuden käyttää internetiä mahdollisimman helposti – kuitenkin siten että vierailijat ovat rajattu oman sisäverkon palomuurin ulkopuolelle. Vähitellen kun tekniikka yleistyy, kehittyy ja vakinaistaa paikkansa yritysmaailman käytössä, siitä tulee vähitellen itsestäänselvyys, että yrityksen verkon kautta pääsee esimerkiksi neuvotteluhuoneessa tai yrityksen kahviossa käyttämään Internetiä tai oman yrityksen intranetiä omalla kannettavallaan tai kämmenmikrollaan.

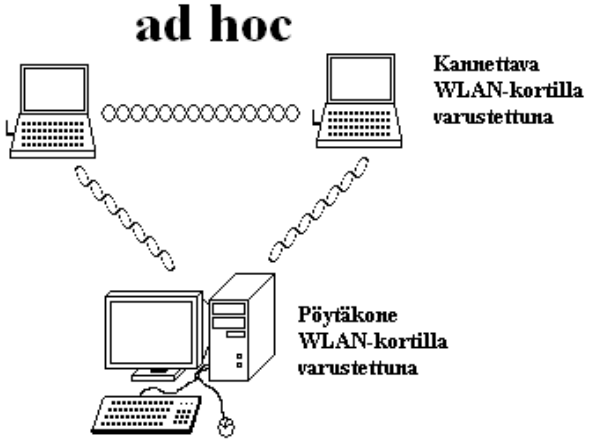
Julkishallinnon kiinnostuksesta langattomia verkkoja kohtaan kertoo myös se, että Tampereen kaupunki harkitsee tällä hetkellä julkisen langattoman verkon rakentamista. Sekä se että Suomessa on jo kolmessa kaupungissa langaton verkko, joista Lahti ja Oulu tarjoavat langatonta verkkoaan ilmaiseksi ja Turku maksua vastaan.
/ 7 /

2.2 Langattoman verkon arkkitehtuuri

Langattomissa verkoissa on kaksi perustekijää, joista toinen on langattomat päätteet ja toinen on tukiasema. Tukiasemat ovat usein esimerkiksi kotitalouksissa kytketty ADSL-modeemiin (*Asymmetric Digital Subscriber Line*), tai lähiverkon kytkimeen, reitittimeen tai hubiin, ja jakavat internet yhteyttä talouden kaikille koneille.

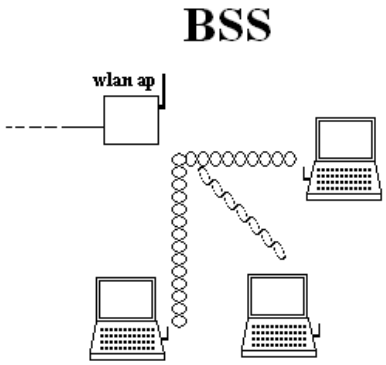
WLAN-verkko voidaan toteuttaa ilman tukiasemaa tai sen kanssa, jos langaton verkko on toteutettu vain langattomilla päätelaitteilla, kuten seuraavan sivun kuvassa 3, niin silloin verkon topologia on ad hoc (*tilapäis/vertais-verkko*). Tällaista langatonta verkkoa voidaan kutsua myös infrastruktuurittomaksi verkoksi tai siitä voidaan käyttää nimitystä IBSS (*Independent Basic Service Set, itsenäinen peruspalvelujoukko*). Kun ad hoc-topologiaan pohjautuvan verkon päätelaitteiden välinen etäisyys kasvaa liian suureksi, yhteys päätelaitteiden välillä katkeaa ja kun yhteys taas pienenee tarpeeksi, niin yhteys muodostuu automaattisesti uudestaan.

Langattomat verkot tarjoavat erittäin hyvää joustavuutta johon langalliset verkot eivät pysty esimerkiksi katastrofitilanteessa, jossa langalliset yhteydet ovat täysin tuhoutuneet. Tällaisessa tilanteessa voitaisiin esimerkiksi soittaa puheluita VoIP-protokollan (*Voice over IP*) avulla. Esimerkiksi matkapuhelinverkot ovat suuripinta-alaisia infrastruktuuripohjaisia verkkoja.



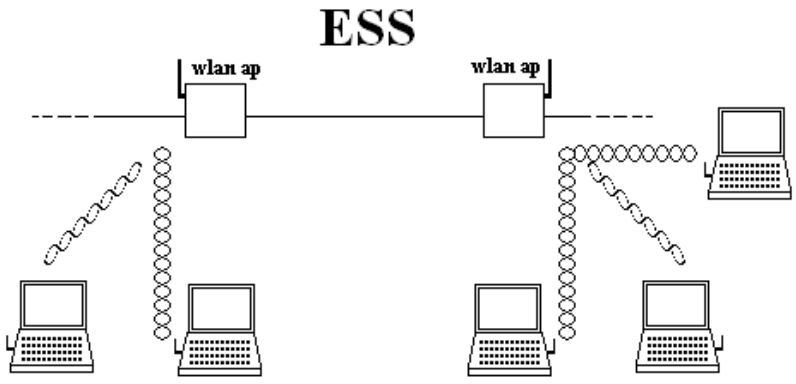
KUVA 3. Infrastruktuurittoman verkon esimerkkikuva

Jos langattoman verkon toteutuksessa on käytetty yhtä tai useampaa tukiasemaa langattomien päätelaitteiden lisäksi, niin verkon topologiaa kutsutaan infrastruktuuriseksi verkoksi. Yhden tukiaseman langattomasta verkosta, alla oleva kuva 4, käytetään nimitystä BSS (*Basic Service Set, peruspalvelujoukko*). Usein AP (*Access Point, pääsykohta*) toimii siltana toisiin langallisiin tai langattomiin verkkoihin.



KUVA 4. Yhden tukiaseman langaton verkko esimerkkikuva

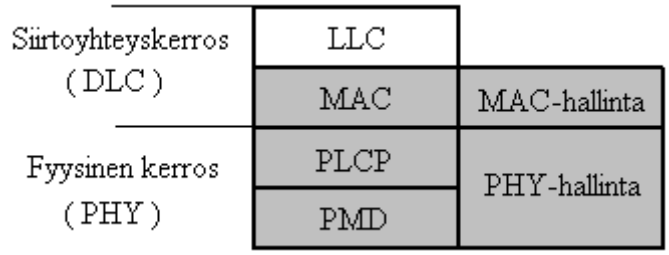
Kahden tai useamman tukiaseman muodostamasta langattomasta verkosta, kuvan 5 mukainen, käytetään nimitystä ESS (*Extended Service Set, laajennettu palvelujoukko*). Tässä tapauksessa tukiasemille joudutaan määrittelemään taajuusalueet, kanavat, joilla ne toimivat, jottei toisten tukiasemien liikenne häiritsisi toisten tukiaseman liikennöintiä. Yleensä tukiasemat ovat kytkettynä samaan runkoverkkoon DS (*Distribution System*). Runkoverkon kautta tukiasemat voivat kommunikoida keskenään sekä saavat yhteyden langalliseen lähiverkkoon. Asemat voivat valita AP:n johon on paras yhteys ja käyttää sitä. AP:t itsessään tukevat kyseistä vaihtoa, joka tunnetaan paremmin termillä roaming.
/ 8 / / 9 /



KUVA 5. Kahden tai useamman tukiaseman langattoman verkon esimerkkikuva

2.3 Protokolla-arkkitehtuuri

IEEE 802.11-standardi on määrittelee vain fyysisen kerroksen (*PHY, Physical Layer*) ja siirtotielle pääsykerroksen (*MAC, Media Access Control*), kuten muutkin 802.X-standardit. Fyysinen kerros on jaettu kahteen eri osaan PLCP-kerrokseen (*Physical Layer Convergence Protocol, fyysisen kerroksen konvergenssiprotokolla*) ja PMD-kerrokseen (*Physical Medium Dependent, fyysisestä tiestä riippuvainen alikerros*). Seuraavalla sivulla olevalla kuvalla 6 on selvennetty kerroksien jakautumista. PMD-kerroksen toiminnot riippuvat siirtotavasta ja PLCP-kerroksen toiminnot ovat samanlaiset kaikissa toteutustavoissa. Salaus, siirtotielle pääsy ja käyttäjädatan pilkkominen yhdessä muodostavat MAC-kerroksen perustehtävät.



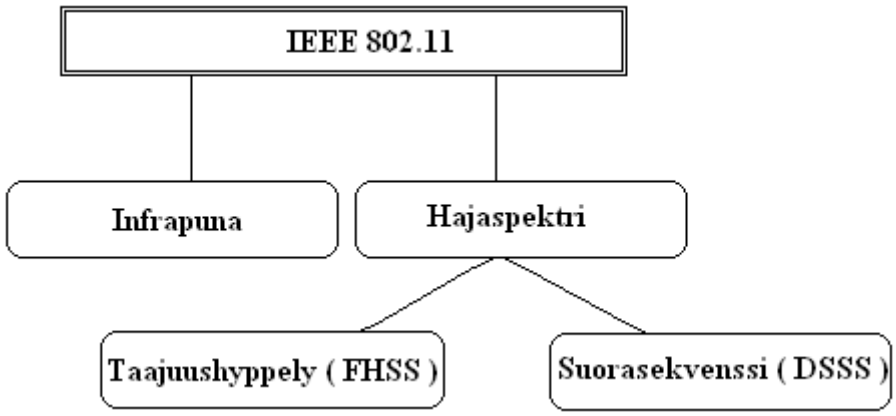
Kuva 6. Standardin kattamat osat

Standardissa on tuettuna kolme erilaista fyysisen kerroksen toteutustapaa, FHSS, DSSS ja infrapuna. Kaikkiin toteutustapoihin kuuluu CCA-signaalin (*Clear Channel Assessment Signal, vapaan kanavan arviointi*) käyttö. Kyseisen signaali tuotetaan PLCP-alikerroksessa ja sen avulla pystytään tarkistamaan onko siirtotie sillä hetkellä vapaana.

MAC-hallinta tukee aseman liittymistä ja irtaantumista pääsykohdista, myös roaming-piirre eri pääsykohtien välillä on MAC-hallinnan tukema. Tämän lisäksi se hallitsee todennusmekanismeja, salausta, aseman synkronointia pääsykohdan kanssa, sekä mahdollista tehonhallintaa. Tämän lisäksi MAC-hallinta ylläpitää MAC:in hallintatietojen tietokantaa MIB:iä (*Management Information Base*). Vastaavasti PHY-hallinnan päätehtäviin kuuluu kanavanviritys ja fyysisen kerroksen MIB:stä vastaaminen.

3 IEEE 802.11-STANDARDIN KEHITYS

802.11-standardin kehitys sai alkunsa vuonna 1990 ja valmistui seitsemän vuoden kehitystyön tuloksena vuonna 1997 IEEE:n toimesta. Standardille on määritelty kolme edellä mainittua siirtotapaa DSSS, FHSS ja infrapuna. 802.11-standardin rakenne näkyy alla olevassa kuvassa 2.



KUVA 2. 802.11-standardin mukaiset perustekniikat

802.11-standardin tukemat 1 Mbps ja 2 Mbps siirtonopeudet todettiin nopeasti liian hitaiksi ja tästä johtuen alettiin kehittämään uutta standardia. Suurin kehitysharppaus otettiin vuonna 1999, jolloin 802.11b-standardi valmistui. 802.11b-standardilla kyettiin saavuttamaan jopa 11 Mbps:n liikennöintinopeus. Jotta 802.11b-standardilla kyettiin saavuttamaan 11Mbps:n liikennöintinopeus, piti taajuushyppely (*FHSS*) jättää pois ja siirtyä käyttämään pelkästään suorasekvenointi-tekniikkaa (*DSSS*). 802.11b-standardissa on määritelty myös 1, 2 ja 5.5 Mbps:än siirtonopeudet. Olemassa on myös 802.11b+-standardi joka eroaa vain nopeuden osalta 802.11b-standardista. 802.11b+ mahdollistaa 22 Mbps:n siirtonopeuden, mutta on tästä huolimatta jäänyt sisarstandardinsa jalkoihin.

Uudempi 802.11a-standardi ei koskaan lyönyt itseään lävitse suurille markkinoille yhtä hyvin kuin 802.11b-standardi. Suurin syy tähän on 802.11a-laitteiden kallis hinta ja suhteessa erittäin huono kuuluvuusalue. 802.11a-standardin käytössä ovat taajuudet: 5.15 – 5.25 GHz ja USA:ssa 5.25 – 5.35 GHz. Standardi perustuu myös OFDM-kanavajakotekniikkaan (*Orthogonal Frequency Division Multiplexing*), joka tarkoittaa ortogonaalista taajuusjakoista kanavointia. Tarkemmin selitettynä

tämä tarkoittaa että kantoaallossa yhden taajuuden ollessa keskikohdassaan muiden taajuuksien amplitudit ovat nollassa, jolloin taajuudet eivät häiritse toisiaan. Teoriassa tällä kyseisellä standardilla voidaan saavuttaa 54 Mbps:n siirtonopeus suorasekvenointi (*DSSS*) tekniikan avulla.

IEEE:n markkinoilla uudehko standardi 802.11g käyttää 2.4GHz:n taajuusaluetta ja kykenee myös 802.11a-standardin 54 Mbps:n siirtonopeuteen. 802.11g-standardin laitteet ovat yhteensopivia 802.11b-standardin mukaisten laitteiden kanssa. 802.11g-standardin laitteet tarjoavat yhtä suuren nopeuden lisäksi halvemman hinnan ja suuremman kantoalueen kuin 802.11a-standardi.

Edellä mainittujen tuttujen standardien lisäksi on myös olemassa vähemmän tunnettuja lisäominaisuuksien standardeja. 802.11e-standardilla on yritetty parantaa langattoman verkon soveltuvuutta multimediapalveluihin, jotka ovat tekniikan kehittymisen myötä alkaneet lyödä itseään paremmin läpi.

802.11f-standardilla on pyritty parantamaan eri valmistajien laitteiden välillä ilmenneitä yhteensopivuusongelmia. Jotka pahimmillaan ovat heikentäneet tietoturvaa oleellisesti

802.11h-standardilla on pyritty parantamaan 802.11a-standardissa havaittuja ja oleelliseksi koettuja puutteita, kuten esimerkiksi automaattinen tehonsäätö ja dynaaminen kanavanvaihto.

802.11d-standardi on vahvasti liitoksissa h-standardiin, sillä se mahdollistaa laitteiden dynaamisuuden käytettävän taajuuskaistan suhteen. Käytännössä tämä tarkoittaa sitä, että WLAN-kortti pystyisi virittymään kunkin maan taajuuksille, siten että kortti saa taajuus tiedot tukiasemalta johon se kiinnittyy. Tämä parantaa paljon liikkuvien työntekijöiden koneiden WLAN-korttien toimivuutta maissa, joissa on käytössä eri taajuusalueet kuin työntekijän kotimaassa.

802.11i-standardilla on keskitytty parantamaan tietoturvaa. 802.11s-standardin tarkoituksena on mahdollistaa suurten silmukkaverkkojen muodostaminen.
/ 5 / / 6 / / 8 /

4 TIETOTURVA

Langattoman verkon paras ominaisuus on samalla sen heikoin ominaisuus, koska langattomassa verkossa informaatio lähetetään radioaaltoina ilmassa ja kaikki, joilla on asianmukaiset laitteet radiosignaalin kantaman alueella, voivat liittyä samaiseen verkkoon ja alkaa kuunnella liikennettä vapaasti. WLAN-verkon kuuluvuusalue on usein suurempi kuin verkkoa suunniteltaessa on ajateltu. Käytännössä tämä tarkoittaa sitä, että yrityksen sisäinen langaton verkko saattaa olla kuunneltavissa ja pahimmillaan käytettävissä jopa satojen metrien säteellä, paikoissa, joista mahdollinen verkkoon tunkeutuminen tai verkon tarkkailu on helppo toteuttaa. Toisaalta tarkkailu ja mahdollinen tunkeutuminen voidaan myös tehdä esimerkiksi lähelle pysäköidystä pakettiautosta. Langattomien verkkojen salakuuntelu voidaan toteuttaa muun muassa Internetistä löytyvien niin sanottujen nuuskintaohjelmistojen avulla.

Kuuluvuusalueen huomioiminen ja rajaus verkon suunnittelu- ja rakennusvaiheessa parantavatkin langattoman verkon turvallisuutta, mutta silti on oletettava, että kuka tahansa saattaa kuunnella tai liittyä verkkoon. Toisaalta taas esimerkiksi julkisissa tiloissa tarjottua kuuluvuusaluetta ei ole tarkoituksenmukaista rajoittaa, koska yleensä on tarkoitus tarjota mahdollisimman hyvä ja toimiva palvelu.

Yrityksissä väärin toteutetut vierailijaverkot tai huonosti toteutettu sisäinen langaton verkko muodostavat riskin, joka saattaa altistaa yrityssalaisuudet kolmannen osapuolen luettavaksi tai muunneltavaksi. Suurimman riskitekijän tietoturvan kannalta muuten oikein toteutetussa langattomassa verkossa aiheuttavat tietämättömyyttään tai piittaamattomuuttaan yrityksen työntekijät. Haavoittuvuus syntyy, kun työntekijät pystyttävät itse oman AP:n, josta verkon ylläpitäjä ei ole tietoinen, helpottamaan omaa työskentelyään. Nämä AP:t asennetaan yleensä ilman suojauksia ja palomuurin taakse. Tällainen tapaus mahdollistaa periaatteessa esteettömän yhteyden yrityksen verkkoon. Langattoman verkon puuttuminen yrityksessä lisää sitä todennäköisyyttä, että työntekijät pystyttävät itse itselleen jonkinlaisen langattoman verkon, joka yleensä

ikävä kyllä on lähes suojaamaton tai erittäin kevyesti suojattu ja kaiken lisäksi yhteydessä yrityksen omaan sisäverkkoon.

WLAN-verkkojen tietoturvaa voi tutkia kahdesta eri näkökulmasta, joista toinen perustuu datan salaukseen ja toinen verkkoon pääsyn rajoittamiseen (*autentikointi*). Murtautuminen voi tapahtua verkkokerroksella joko access pointin (*AP*) tai yksittäisen työaseman kautta, joka on liitetty verkkoon tai toimii ad hoc-moodissa ja viestii peer-to-peer-tavalla. Pääsylistojen avulla voidaan estää ulkopuolisten verkon käyttäjien pääsy verkkoon MAC-osoitteiden perusteella. Kyseistä pääsylistaa ylläpidetään Access Pointissa (*AP*). Tämän avulla voidaan kohentaa tietoturvaa, mutta tämä on erittäin työläs verkon ylläpitäjille, sillä MAC-osoitteet pitää syöttää jokainen yksitellen käsin. MAC-osoitteet kulkevat kuitenkin selväkielisinä paketteina vaikka data onkin salattua. Mahdollisen hyökkääjän on siis helppo selvittää verkossa pääsylistalla oleva MAC-osoite ja kloonata kyseinen osoite ohjelmallisesti oman verkkokorttinsa käyttöön.
/ 13 / / 14 / / 15 / / 3 /

4.1 Langattomien verkkojen suunnittelu

Langattomien verkkojen fyysisen toteutuksen hyvällä suunnittelullakin on erittäin suuri merkitys kyseisten verkkojen tietoturvan tasoon. Suunnittelussa on tärkeää ottaa huomioon antennien ja tukiasemien sijainti, lähetystehot, suuntaus, seinät ja ikkunat. Ottamalla edellä mainitut asiat huomioon suunnittelussa voidaan langattoman verkon kuuluvuusalue minimoida alueelta, jolla langattoman verkon ei ole tarkoitus edes toimia. Vaikka yllä mainitut asiat olisikin huolellisesti huomioitu suunnittelussa, olisi silti syytä erottaa langaton verkko palomuurin avulla yrityksen varsinaisesta sisäverkosta. Tällaisessa tapauksessa yhteys voidaan toteuttaa käyttämällä esimerkiksi IPSec-tekniikkaa (*Internet Protocol Security*) tai VPN-tekniikkaa (*Virtual Private Network*).

SSID – Server Side IDentifier

Yksi turvallisuudentunnetta kasvattava tekninen ominaisuus on SSID (*Server Side IDentifier*), mutta tekniikalla ei hienosta lyhenteestään huolimatta ole käytännössä mitään tekemistä turvallisuuden kanssa. SSID on tarkoitettu erottamaan

langattomat verkot toisistaan, eikä suinkaan tarjoamaan turvallisuutta. Vaikka joistain tukiasemista saa SSID:n lähetyksen kytkettyä pois, verkon tunnus on silti erittäin helposti selvitettävissä siihen tarkoitetuilla ilmaisohjelmilla.
/ 16 /

4.2 Valmistajien ratkaisumallit

Myös valmistajat ovat havahtuneet tuotteidensa loppukäyttäjien mielenkiinnon puutteesta salausten konfiguroinnissa. Kyseessä on erittäin yleinen ilmiö, jossa suurin osa käyttäjistä perustelee kantaansa sillä, että jos jotakuta kiinnostaa tulla koneelleni tai käyttää verkkoani, niin ihan vapaasti. Kyseinen ilmiö onkin synnyttänyt lieveilmiöt, jotka tunnetaan paremmin nimillä war-driving ja war-chalking, joista kerron tarkemmin myöhemmin. Valmistajista ainakin Buffalo on kehittänyt AirStation AOSS-tekniikan (*Airstation One-touch Secure System*). Tämän tekniikan avulla pystytään eliminoimaan heikkojen avainten mahdollisuus ja käyttämään vahvoja avaimia vain yhden napinpainalluksen avulla. Kyseisen tekniikan varsinaisiin tietoturvaominaisuuksiin en ota kantaa, mutta heikko suojaus on parempi kuin ei mitään. Buffalon eräissä tukiasemamalleissa on myös Intrusion Detection-palomuuriominaisuus. Tämän ominaisuuden avulla hyökkäys torjutaan ja siitä ilmoitetaan käyttäjälle.

Hewlett Packard on kehittänyt uuden innovatiivisen tavan hidastaa nopeasti leviäviä matoja ja viruksia. Tämä uusi tekniikka tunnetaan nimellä Virus Throttling. Kun palvelin tai kytkin, jossa kyseinen ohjelmisto on, havaitsee huomattavan liikennöinnin lisääntymisen eri IP-osoitteisiin, reagoi se tilanteeseen kuristamalla kyseisen laitteen käytössä olevaa kaistaa ja tarvittaessa katkaisee liikennöinnin kokonaan. Tämän tekniikan avulla saadaan lisäaikaa perinteisten virustutkien päivityksille erittäin nopeasti leviäviä matoja ja viruksia vastaan. Esimerkiksi Sql Slammer-mato saastutti noin 80,000 työasemaa noin puolessa tunnissa. Virus Throttling -tekniikka ei siis varsinaisesti tunnista matoa tai virusta vaan tunnistaa niiden perinteiset toimintatavat, joilla ne yrittävät levitä mahdollisimman tehokkaasti, ja estää niiden toiminnan poistamalla niiltä yhteyden toisiin koneisiin.
/ 17 / / 18 / / 19 / / 36 / / 38 /

5 SALAUSMENETELMÄT

Tässä osiossa käsitellään WLAN-tekniikkan spesifikaatioihin sisällytettyjä salausmenetelmiä, joita ovat WEP, WPA ja 802.11i, joka tunnetaan myös WPA2:sena.

5.1 WEP – Wired Equilevant Privacy

WLAN-verkkoja varten ensimmäinen standardoitu salausjärjestelmä oli WEP-salaus. WEP-salaus tarjoaa suojaa peruskäyttäjälle, mutta on kuitenkin suurten heikkouksiensa takia kohtuullisen helposti murrettavissa. Tehokkainta WEP-salausta käytettäessä 16.752 miljoonasta lähetetystä paketista noin 9000 pakettia sisältää ohjausvektoritietoa. Suurin osa salausavaimista pystytään murtamaan noin 2000 heikon paketin perusteella. Aika, jona salaus pystytään murtamaan, riippuu täysin liikenteen määrästä, eli jos verkossa on muutama kone ja liikennettä erittäin vähän, niin murtaminen saattaa kestää jonkin aikaa.

Vaikka WEP-salaus onkin puutteellinen, niin monesti se riittää kotikäyttäjälle, sillä langattoman verkon salaaminen kertoo siitä, että verkko ei ole avoin verkko, joten WEP-salauksella suojattu verkko on haavoittuvainen vain harkituille väärinkäytöksille. Edellä mainittu salauksella suojattu verkko on verrattavissa esimerkiksi kaupan oveen, josta saa kulkea silloin, kun se on auki, mutta jos ovi on lukossa, niin ovesta ei saa kulkea – jos kuljetaan, niin rikotaan lakia.

WEP on siirtoyhteyskerroksen salausmekanismi, joka ei ole pakollinen WLAN -verkossa. WEP on pyritty suunnittelemaan sellaiseksi, että sillä voitaisiin estää verkkoon pääsy ulkopuolisilta ilman salasanaa (*WEP-salausavainta*) ja suojata data salaamalla se WEP-avaimella sekä estää datan korruptoituminen CRC-32-tarkistussummalla (*Cyclic Redundary Check*), jonka tarkastamisella paketin purkava osapuoli voi varmistua tiedon aitoudesta. Tällä tarkistuksella ei kuitenkaan pystytä takaamaan sitä, että kryptotekstiin ei ole tehty muutoksia.

WEP-salauksessa on sovellettu RC4-suojausalgoritmia, jota käytetään myös suojaamaan verkossa tapahtuvaa kaupankäyntiä. RC4 (*Ron's Code 4, Rivest Cipher 4*) on Ronald Rivestin 1987 suunnittelema salausalgoritmi. Syyskuun 9.

vuonna 1994 RC4:n lähdekoodi julkaistiin Internetissä tuntemattoman ihmisen toimesta. Algoritmia pidetään yleisesti ottaen turvallisena, mutta WEP:n tapa soveltaa 24-bittistä alustusvektoria heikentää salauksen tasoa.

RC4 on symmetrinen jonosalaaja ja se salaa tiedon yksi tavu kerrallaan. Symmetrisyys tarkoittaa sitä, että sitä käytetään sekä salaamiseen että purkamiseen. Algoritmin toiminta on nopeaa ja se perustuu vaihtelevan mittaiseen salaiseen avaimeen. Käytännössä RC4 on satunnaislukugeneraattori (*PRNG, Pseudo-Random Number Generator*). Sillä luodaan siis isoja satunnaislukuja annettujen avainten perusteella. Satunnaisluvun ja salattavan tekstin yhdistämisellä XOR-operaatiolla saadaan salattu teksti.

Alkuun RC4-avaimen pituus oli rajoitettu 40 bittiin USA:n vientirajoitusten vuoksi. Vuonna 2000 Suomi kuitenkin liittyi Wassenaarin sopimuksen piiriin, mikä mahdollisti salaustuotteiden maahantuonnin USA:sta Suomeen. Nimellisesti salausavain on nykyään siis joko 64 tai 128 bittiä pitkä, jotka muodostuvat salaisesta avaimesta (*40- tai 104- bittiä*) ja alustusvektorista (*24-bittiä*). Alustusvektorin ja salaisen avaimen yhdistäminen tehdään jokaisen salattavan paketin yhteydessä, jotta jokaisesta paketista saataisiin loppujen lopuksi erilainen RC4-avain.

Alustusvektorilla alustetaan suuria näennäislukuja tuottava RC4-salausalgoritmi. 24 bitin pituudella on mahdollista käyttää 2^{24} (16,777,216) erilaista bittijonoa. Kohtuullisen suuren vektoriparien määrän vuoksi murtautuminen ei onnistu käden käänteessä, mutta kuitenkin tarpeeksi kauan liikennettä seurattaessa löytyy oikea vektoripari ja tämän jälkeen murtautuminen onnistuu. Internetistä löytyy nykyään erilaisia ohjelmia (*esim. Airsnort, Aircrack, WEPCrack jne.*), joilla pystyy seuraamalla liikennettä laskemaan salausavaimen.

Kaikilla WEP-salauksen omaavassa verkossa olevilla työasemilla tulee olla sama tunnistusavain kuin tukiasemalla jotta ne voivat liittyä verkkoon ja alkaa kommunikoida keskenään.
/ 15 / / 20 / / 21 / / 22 / / 3 / / 39 /

5.2 WPA – Wi-Fi Protected Access

Koska WEP-salaus todettiin nopeasti liian heikoksi, alettiin kehitellä toista salausta, WPA-salausta (*Wi-Fi Protected Access – Wireless Fidelity*). WPA:han on sisällytetty 802.11i-tietoturvastandardin mukaisia ominaisuuksia. Tämän lisäksi se on nykyisten ja tulevien laitteiden kanssa yhteensopiva, koska sitä on kehitelty yhteistyössä 802.11i-standardin kehittäjien kanssa. WPA:n loi Wi-Fi-allianssi, joka omistaa oikeudet Wi-Fi-tavaramerkkiin. WPA:ta käytettäessä riittävät pelkät ohjelmistopäivitykset tukiasemiin, verkkokortteihin ja joissain tapauksissa käyttöjärjestelmiin. Myös autentikointipalvelimen lisääminen yritysverkkoon on tarpeellista.

TKIP – Temporal Key Integrity Protocol

Myös WEP-salauksessa käytössä olleet ja heikoksi todetut alustusvektorit (*IV*) ovat korjattu WPA-salauksessa ja tämän lisäksi salausavainta vaihdetaan automaattisesti 10 000 paketin välein. Yksi huomattavammista kehityksistä WEP:hen nähden oli TKIP (*Temporal Key Integrity Protocol*), joka huolehtii yhteyksien salaamisesta. TKIP parantaa oleellisesti langattomien verkkojen tietoturvallisuutta ottamalla käyttöön pakettikohtaiset salausavaimet. Liikenne on salattu TKIP:ssä aiemmin esitellyllä RC4-salausmenetelmällä, mutta salausavaimen pituus on 128 bittiä ja alustusvektorin (*IV, Initialization Vector*) pituus on 48 bittiä. Suurena erona WEP:n ja WPA:n välillä on myös se, että WEP jättää headerit suojaamatta, WPA salaa kaiken, jopa MAC-tiedon headerit. WPA-salaukseen on sisällytetty MIC-toiminto (*Message Integrity Control*), jonka avulla pystytään kontrolloimaan jokaista pakettia ja tarkistamaan, ettei mahdollinen murtautuja pysty nappaamaan paketteja ja muuttamaan niiden tietoja. Tämä toiminto tapahtuu erittäin vahvan matemaattisen funktion avulla, jossa molemmat osapuolet, sekä vastaanottaja että lähettäjä, laskevat paketille tarkistesummat, joita verrataan keskenään, jotta voidaan todeta paketin eheys.

Kun käyttäjä on tunnistettu verkkoon käyttäjänä, luo kirjautumispalvelin (*RADIUS*) tai tukiasema (*AP*) käyttäjälle uniikin PMK:n (*Pair-wise Master Key, pääavainpari*), jota käyttäjä käyttää kyseisen istunnon ajan. TKIP-protokolla

antaa käyttäjälle avaimen ja luo avainhierarkian ja dynaamisten avainten hallintajärjestelmän. Kyseisen avaimen mukaan TKIP luo dynaamisesti pakettikohtaiset avaimet, joilla jokainen verkkoon toimitettu paketti salataan.

WPA:n huonona puolena pidetään sen tapaa suojautua DDoS-hyökkäyksiltä (*Distributed Denial of Service, hajautettu palvelunestohyökkäys*). Kun palvelunestohyökkäys havaitaan, WPA sulkee koko verkon minuutiksi. Tällöin kaikki, myös verkon lailliset käyttäjät jäävät ilman verkkoa. Myös WPA:sta on löydetty vakava tietoturva-aukko, jota hyökkäystyökalu WPA Cracker käyttää hyväkseen. Tämä tietoturva-aukko muodostuu, kun langattomat tukiasemat lähettävät salausavaimeen liittyviä tietoja. Tietoturva-aukko ei uhkaa yritysratkaisuja, joissa on käytössä 802.1X-standardin mukainen autentikointi. WPA-salausmenetelmässä pitäisi pyrkiä käyttämään yli 20-merkkisiä salasanoja.

WPA on suunniteltu käytettäväksi 802.1X-todennuspalvelimen kanssa, joka jakaa jokaiselle käyttäjälle erilaiset avaimet. Joka tapauksessa WPA-salausta voidaan käyttää vähemmän turvallisella tavalla, kun verkossa on käytössä jaetun avaimen autentikointi (*WPA-PSK tai PSK, Pre-Shared Key*).

WPA-PSK – Pre-shared key

Jaetun avaimen autentikointitekniikka on suunniteltu kotiverkoille ja pienille toimistoverkoille, joilla ei ole varaa 802.1X-autentikointipalvelimen ylläpitoon ja monimutkaisuuteen. Jokaisen käyttäjän pitää esittää tunnuslause voidakseen liittyä verkkoon. Tunnuslause voi muodostua 8 – 64 ASCII-merkistä (*American Standard Code for Information Interchange*) tai 8 – 64 heksadesimaalinumerosta.

Heikko kohta kuitenkin muodostuu siitä, että käyttäjät luovat heikkoja tunnuslauseita. Suositeltua on käyttää tunnuslausetta, jossa on 14 täysin satunnaista kirjainta. Jotta saavutettaisiin maksimaalinen suoja, on kuitenkin käytettävä 22:ta täysin satunnaista kirjainta. Tunnuslauseita pitäisi vaihtaa aina, kun joku verkon käyttäjistä menettää oikeutensa verkon käyttöön. Myös siinä tapauksessa tunnuslause tulisi vaihtaa, kun esimerkiksi kannettava, johon tunnuslause on laitettu, varastetaan tai hukataan.

/ 23 / / 24 / / 25 /

5.3 802.11i / WPA2

802.11i on tietoturvastandardi, joka tunnetaan myös WPA2:sena, jolla on pyritty ratkaisemaan tunnetut tietoturvaongelmat. Kyseisessä standardissa on määritelty 802.1X-standardin mukaiset todennus- ja dynaamiset avainten hallinnan käytännöt. Sen lisäksi salausmenetelmiä on parannettu. Vanhojen WPA-standardin mukaisten ratkaisujen lisäksi on tarjolla uudentyyppinen AES-lohkosalausmekanismi (*Advanced Encryption Standard*). AES tunnetaan myös belgialaisten kehittäjiensä John Daemen ja Vincent Rijmen mukaan nimellä Rijndael. AES-salausmekanismi on myös amerikkalaisen NSA:n (*National Security Agency*) taholta todettu tarpeeksi turvalliseksi, jotta USA:n hallitus voi käyttää sitä luokittelemattoman materiaalin salaamisessa.

Salausalgoritmina AES eroaa hyvinkin paljon WPA:n käyttämästä RC4-algoritmista, ja se vaatii hieman enemmän prosessointitehoa. Se pystyy käyttämään erimittaisia avaimia ja vaihtoehtoina ovat 128-, 192-, ja 256-bittiset avainpituudet.
/ 15 / / 37 / / 38 /

802.1X-standardi

802.1X-standardi on porttipohjainen standardi, joka tarjoaa tunnistuksen laitteille, jotka ovat liitettyinä LAN-porttiin. Jos tunnistus läpäistään, luodaan point-to-point-yhteys tai jos ei läpäistä, niin yhteys kyseisestä portista estetään. Tämä tapa on usein käytössä AP:ssä ja se perustuu EAP:hen (*Extensible Authentication Protocol*). Vaikka kyseessä on langattomissa ja kaapeloiduissa verkoissa toimiva protokolla, niin kyseinen protokolla on huomattavasti yleisempi langattomissa verkoissa. WPA- ja WPA2-standardeille on virallisesti hyväksytty 5 EAP-tyyppistä tunnistamismekanismia. Vaikka 802.1X-standardi käyttää WEP-salausta, niin molemminpuolinen tunnistus ja dynaaminen avainten hallinta lisää huomattavasti WLAN-verkon turvallisuutta perus WEP-suojaukseen nähden. Dynaaminen avainten hallinta vähentää avainhyökkäyksille altistumista ja molemminpuolinen tunnistus auttaa varmistamaan sen, että työasemat kommunikoivat tunnettujen verkkojen kanssa, esimerkki alla olevassa kuvassa 7.
/ 29 /

6 SALAAVAT TUNNELOINTIMENETELMÄT

Langattomien verkkojen omien salausmenetelmien heikoista tietoturvaominaisuuksista johtuen langattomien verkkosovellusten kanssa on otettu salaavia tunnelointimenetelmiä, joiden avulla yrityksissä voidaan käyttää huomattavasti tietoturvallisemmin langatonta verkkoa. Tällöin langattomien verkkojen tukiasemat ovat sijoitettu yrityksen sisäverkon palomuurin ulkopuolelle.

Käytännössä käyttäjälle konfiguroidaan käyttöoikeudet, joilla mahdollisuus muodostaa esimerkiksi VPN-tunneli oman koneen ja yrityksen palomuurin välille, jolloin liikenne tapahtuu muodostetun tunnelin sisällä. Itse liikennöinti VPN-tunnellissa salataan käyttämällä esimerkiksi IPSec-protokollaa, joka hoitaa tunnelin sisällä liikkuvien pakettien salaamisen.

6.1 IPSec – IP Security Architecture

IPSec-protokollaa voidaan käyttää WLAN-verkossa WLAN:ien omien suojauksien sijasta tai lisänä. IPSec on todistetusti kohtuullisen turvalliseksi osoittautunut protokolla, minkä lisäksi hyvä ohjelmistotuki on antanut sille jalansijan muihinkin käyttötarkoituksiin, esimerkiksi VPN:ääm.

IPSec on IFTF:n (*Internet Engineering Task Force*) standardiehdotus, jolla on pyritty parantamaan IP-protokollan turvallisuutta. IPv6-versioon IPSec on jo sisällytetty, mutta se voidaan ottaa käyttöön myös nykyisessä IPv4-versiossa. IPSec on verkkokerroksen tietoturvamekanismi, eli se toimii TCP-protokollan (*Transmission Control Protocol*) ja UDP-protokollan (*User Datagram Protocol*) alla.

Verkkokerroksen kryptografialla ja erityisesti IPSec:llä on etuna joustavuus jota ei ole alemmalla tasolla tapahtuvalla salaamisella tai ylemmän tason sovellusten välillä tapahtuvalla salauksella. Vaikka myös IPSec on saanut hieman kritiikkiä osakseen, esimerkiksi monimutkaisuudestaan, on se silti kriitikoidenkin mielestä parasta, mitä IP:n suojaamiseksi on tarjolla.

IPSec:n normaali toimintaperiaate on yksinkertainen. Internet-protokolla saa ylemmän tason protokollalta (*TCP, UDP tai ICMP*) toimitettavakseen paketin ja lisää siihen omat otsikkokentät (*lähettäjän ja vastaanottajan IP-osoitteet*). IPSec muokkaa edelleen tätä pakettia lisäämällä omia otsikoita, joihin on sisällytetty tunnisteita, joista vastaanottajan päässä voidaan tulkita tehdyt operaatiot. IPSec mahdollisesti lisää otsikkokenttään paketista lasketun hash-arvon (*tiivistearvon*), jonka perusteella voidaan todeta paketin autenttisuus, tämän matemaattisen operaation tekee IPSec:n AH-protokolla (*Authentication Header, RFC 2402*).

IPSec voi myös salata ylempää tulleen datan ESP -protokollan (*Encapsulating Security Payload, RFC 2406*) avulla. Jos kuljetuksen sijasta halutaan käyttää tunnelointimenetelmää, niin salaus- ja/tai autentikointioperaatio koskee koko IP-pakettia ja tuloksen eteen asetetaan kokonaan uusi IP-otsikko. Jos käytetään tunnelointia, niin koko alkuperäinen IP-paketti salataan osoitteineen kaikkineen.
/ 15 / / 33 / / 31 / / 32 /

6.2 VPN – Virtual Private Networks

Virtuaaliset yksityiset verkot ovat yrityksien suosima tapa yhdistää maantieteellisesti kaukana toisistaan sijaitsevat sisäverkot, joita on kaksi tai useampi, toisiinsa. Yhdistäminen tapahtuu julkisen verkon ylitse, mutta kuitenkin saadaan näennäisesti yksityiseen verkkoon verrattavissa oleva yhteys. Nykyään määritelmä on laajennettu koskemaan myös yksittäisen työaseman yhdistämistä yrityksen verkkoon.

VPN-tekniikat perustuvat yleisesti saatavilla oleviin menetelmiin, joilla yrityksen etäpisteet yhdistetään tietoturvallisesti toisiinsa. VPN-verkoilla pyritään samaan verkon ja palvelujen saatavuus-, tehokkuus-, ja tietoturvatasoon kuin kaapeleilla, kuitenkin entistä pienemmillä kustannuksilla ja paremmalla skaalattavuudella ja hallittavuudella.

VPN-arkkitehtuurit

VPN-arkkitehtuurit voidaan jakaa kolmeen osaan: access-VPN, intranet-VPN ja ekstranet-VPN. Jokainen edellä mainitusta VPN-tyypistä soveltuu erilaisiin liike-

elämän sovellutuksiin, kuten yhteyden muodostamiseen joko liikkuviin työntekijöihin, etätoimistoihin, yhteistyökumppaneihin tai asiakkaisiin.

Access-VPN-palvelut on tarkoitettu lähinnä suuressa kasvussa oleville liikkuvan työvoiman markkinoille. Työntekijät voivat olla yhteydessä yrityksensä intranet- tai ekstranet-verkkoihin milloin ja mistä tahansa. Intranet- ja ekstranet-VPN-palveluilla voidaan yhdistää yrityksen etäpisteet, asiakkaat ja tavarantoimittajat käyttämällä internetiä tai operaattorin tarjoamaa verkkopalvelua (*IP-backbone*).

VPN-tekniikka

VPN-tekniikka sinällään perustuu hyvinkin yksinkertaiseen tekniikkaan. Monilla yrityksillä on jo VPN-yhteyksien muodostamiseen tarvittavat laitteet. Tärkeimpiä tunnelointitapoja ovat IETF:n IPSec-standardiin perustuvat IP-tunnelit tai yleiseen reititysstandardiin (*GRE, Generic Routing Encapsulation*) perustuvat tunnelit. Molempien edellä mainittujen tapojen avulla voidaan toteuttaa turvallisia VPN-yhteyksiä yleisen verkon päälle.

Tunnelointi tapahtuu OSI-mallin kerroksella 2, joka on linkkikerros. Luotavalle tunnelille pitää määritellä alku- ja loppupää. Tunnelointiprotokollista kaksi tärkeintä ovat vanhemmat protokollat PPTP (*Point-to-point Tunneling Protocol*) ja sen kilpailija L2F (*Layer 2 Forwarding*). Näihin kahteen pohjautuvana on kehitetty uudempi L2TP (*Layer 2 Tunneling Protocol*).

Tunnelointi yksin ei toimi salaavana yhteytenä. Salaukseen tarvitaan lisäksi muita tietoturvatoimia. Salaukseen voidaan käyttää esimerkiksi OSI-mallin kerroksen 3 IPSec-protokollaa, ja sillä salataan IP-paketit ennen kuin ne lähetetään VPN-yhteydelle. Etäkäyttäjien tunnistamiseen voidaan käyttää RADIUS-ohjelmistoa (*Remote Authentication Dial-In User Services*), jonka avulla voidaan käyttäjälle antaa käyttöoikeudet.
/ 15 / / 33 / / 34 / / 35 / / 36 /

7 HYÖKKÄYSTAPOJA

Sun Tzu kirjoitti kirjassaan Sodankäynnin taito: ”Tunne vihollisesi”. Tämä lause pätee myös nykyaikaiseen ”ohjelmistosodankäyntiin”. Tehokkaimmat ja onnistuneimmat hyökkäykset voidaan tehdä vain, jos kohde tunnetaan tarpeeksi hyvin.

Verkkoturvallisuusohjelmistoilla, kuten esimerkiksi SATAN (*Security Analysis Tool for Auditing Networks*), tutkitaan verkossa olevan koneen ominaisuudet ja mahdolliset tietoturva-aukot. Kaksi kyseisen ohjelmiston tärkeintä käyttäjäryhmää ohjelmistolle ovat verkon turvallisuudesta vastaavat henkilöt sekä mahdolliset murtautujat. Muita verkkoturvallisuusohjelmia ovat muun muassa NetSonar ja PingWare.

Hyökkäyksellisiä keinoja on huomattava määrä, joista mainitsen muutaman mielestäni erityisen tärkeän:

Yhtenä ovat ohjelmointivirheet. Nykyaikaisia ohjelmistoja koodattaessa syntyy huomattavan suuria määriä koodia, johon jää aina lähes poikkeuksetta virheitä. Yleensä näistä virheistä toimintoja estävät tai vääriä toimintoja aiheuttavat korjataan lähes aina. Taustalle saattaa silti jäädä virheitä, joita ei huomata ja näitä virheitä, jotka eivät aina välttämättä näy ohjelman toiminnassa, pystytään joissain tapauksissa hyödyntämään murtautumisessa.

Toisena merkittävänä keinona ovat Troijan hevoset. Kuten historiallinen esi-isänsä myös nykyaikainen troijalainen esittää olevansa jotain muuta, kuin käyttäjä olettaa. Tavallisesti troijalaiset tekevät käyttäjän haluaman toiminnon, mutta tekevät siinä sivussa jotain muuta. Ne voivat esimerkiksi aktivoida madon tai viruksen, mutta ne voivat myös tuhota tiedostoja tai tehdä vähemmän harmitonta tiedonhakua jälkiä jättämättä. Syyskuun 7. päivänä vuonna 2005 Tietokonelehden julkaisemassa nettiartikkelissa kirjoitettiin uudesta Yusufali-A-troijalaisesta, joka tarkkailee Internet-selaimen osoitekentässä olevia sanoja, ja jos jokin yhdeksästä kielletystä sanasta esiintyy osoitekentässä, troijalainen minimoi ikkunan ja näyttää otteen Koraanista. Jos tämän jälkeen nettiselainta ei suljeta, kone jumiutuu.

Kolmantena keinona voidaan mainita social engineering (*sosiaalinen tiedustelu*). Tässä metodissa kräkkeri ottaa yhteyttä esimerkiksi puhelimella kohteeseensa ja esittää olevansa joku toinen, jolla on jotain tekemistä yrityksen tietojärjestelmien kanssa. Tällä tavalla yritetään huijata ihmisiä paljastamaan arkaluonteista tietoa, eli siis yritetään saada ihmiset toimimaan normaaleja käytäntöjä vastaan vetoamalla kahdenkeskiseen luottamukseen ja katteettomiin lupauksiin. Yleisesti on jo tunnustettu, että käyttäjät ovat tietoturvan heikoin lenkki. Joidenkin tutkimusten mukaan jopa 80% toimistotyöntekijöistä antoi salasanansa järjestelmänvalvojaa esittäneelle henkilölle. Lähihistoriasta tuttu hakkeri, Kevin Mitnick on sosiaalisen hakkerointitavan yksi tunnetuimmista käyttäjistä.

7.1 DoS & DDoS

Palvelunestohyökkäyksien päämääränä on kohteen verkkopalveluiden lamauttaminen siten, etteivät palvelut ole käytössä. Tämä päämäärä on siis helposti saavutettavissa WPA-tekniikan kanssa, joka sulkee automaattisesti verkon, kun DoS-hyökkäys havaitaan. Kyseisen hyökkäyksen tavoitteena ei ole kuitenkaan tunkeutua järjestelmään, vaan estää sen normaali toiminta. Jos hyökkäys tapahtuu monesta eri kohteesta samanaikaisesti, niin sitä kutsutaan DDoS-hyökkäykseksi (*Distributed Denial of Service, hajautettu palvelunestohyökkäys*). DDoS on yleisempi hyökkäysmuoto kuin DoS, joka on kovin tehoton. Palvelunestohyökkäyksen perustoteutustavat ovat:

1. Rajallisten resurssien kuluttaminen. Tämä on yleisin DDoS-hyökkäysten muoto, jossa hyökkääjä esimerkiksi saastuttaa jonkin kohdekoneen jonka kautta hän lähettää tuhansia sähköposteja ja tätä kautta kohdeyrityksen sähköpostipalvelimelle. Toinen tehokkaimpana tapana tunnettu hyökkäys on niin kutsuttu smurffi-hyökkäys, joka perustuu kohdekoneen hukuttamiseen ICMP-paketteihin. Hyökkäys tapahtuu kolmannen osapuolen verkon kautta, josta lähetetään directed broadcast, suunnattuja levitysviestejä, joissa lähettäjäksi on väärennetty hyökättävä kone. Jos esimerkiksi yksityisverkko-osoitteeksi määriteltyyn osoitteeseen 192.168.0.255 / 24 lähetetään ICMP echo request-pyyntö, vastaa jokainen verkossa oleva kone omalla IP-osoitteellaan pyyntöön. Suurissa verkoissa tämä aiheuttaa suuren määrän verkkoliikennöintiä.

2. Ohjaustietojen muuttaminen. Tässä tavassa ”myrkytetään” eli syötetään väärää tietoa DNS:n cache-tietoihin. Yksi pahimmista ongelmista kyseisessä hyökkäyksessä on joidenkin DNS-palvelinohjelmien oletustapa hyväksyä nimipalvelimien sille lähettämät tiedot. Eli murtautumalla DNS-palvelimeen tai tekeytyminen DNS-palvelimeksi ja tämän jälkeen väärien tietojen toteuttaa tämän skenaarion. Tämän ongelman takia voidaan ohjautua eri sivulle www.jotain.fi kuin mikä kyseisen sivun 111.222.333.444 muotoinen osoite on.

Edellä mainittuun ongelmaan on kehitetty ratkaisuksi DNSSEC (*Domain Name System Security Extensions, RFC 2535*), jonka avulla saadaan eheyttä DNS-päivityksiin ja autenttisuutta allekirjoituksilla. Lisäksi olemassa on DOC-niminen ohjelma joka etsii virheellisesti toimivia verkkoja lähettämällä asianmukaisille nimipalvelimille ja suorittaa saamien tietojen perusteella joukon erinäisiä analyysejä. Toinen torjuntatekniikka on käänteistarkistusjärjestely. Tässä järjestelyssä palvelu sovittaa yhteen normaalia ja käänteistä nimihakua, mutta tästä ei ole paljoa hyötyä jos kräkkeri on muuttanut normaalit ja käänteiset taulukot.

3. Vääränlaisen lähetteen syöttäminen palvelimelle. Tämän alan pioneeriohjelma oli WinNuke joka saa kohteena olevan koneen käyttöjärjestelmän kaatumaan. Vanhempien Windows-käyttöjärjestelmän sisältävien koneiden kohdalla tämä tarkoitti käytännössä BSOD:ta (*Blue Screen of Death*), eli Windows joutuu tilaan josta sitä ei voi nostaa muuta kuin uudelleen käynnistämällä se.

DDoS-työkalut kuten esimerkiksi Stacheldraht ja TFN2k ovat suunniteltu lähinnä vain tarkoitukseen jonka tarkoituksena on kaataa palvelimia. Kyseisten ohjelmien olemassa olo voidaan kuitenkin havaita esimerkiksi heuristisella skannauksella tai muutosten havaitsemisella. Virustorjunta ohjelmistot tunnistavat yleensä DDoS-työkalut.

7.2 War-driving & War-chalking

Vaikka war-driving tai war-chalking ei liity varsinaisesti hyökkäykseen niin kirjoitan siitä hyökkäystapojen alle. WLAN:ien yleistyessä on myös suojaamattomien verkkojen määrä noussut huimasti. Esimerkiksi lokakuussa

vuonna 2002 Tietokone-lehti teki kierroksen Helsingissä ja kyseisen war-driving -kierroksen aikana löytyi 152 tukiasemaa. Marraskuussa vuonna 2004 Tietokone-lehti teki uudestaan war-driving-kierroksen ja tällä kierroksella tukiasemia löytyi 1117, ja näistä tukiasemista alle puolet eli 589 ei käyttänyt mitään näkyvää salausta, ja 108 näistä salaamattomista tukiasemista oli tehdasasetuksilla. Ihmisten piittaamattomuus ja osaamattomuus ovat aiheuttaneet siis war-driving-lieveilmiön jota voisi verrata lintujen bongaamiseen. War-driving on wardialingin jatke, wardialing oli modeemiaikainen tapa etsiä sattumanvaraisilla soitoilla modeemeja. War-driving on siis lähinnä harmiton aktiviteetti jolla pyritään etsimään avoimia verkkoja esimerkiksi lähtemällä autolla ajelemaan tietylle alueelle ja kytketään kannettava tietokone etsimään langattomia verkkoja. War-driving tunnetaan myös joissain piireissä nimellä ”WiLDing” (*Wireless Lan Driving*). Kun harrastajat löytävät avoimen verkon merkitään se GPS-järjestelmän (*Global Positioning System*) avulla halutuille verkkosivuille. War-drivingissa käytettävät ohjelmistot ovat vapaasti internetistä imuroitavissa, esimerkiksi Windowsilla NetStumbler.

War-chalking on samanhenkinen kuin kulkureiden tapa merkitä ystävällismieliset talot, paitsi että avoimet verkot tuskin ovat avoimia omistajien ystävällismielisyydestä johtuen. War-chalking-merkit kehitti ryhmä ystäviä vuonna 2002 ja merkit julkaisi Matt Jones. Kun war-drivingin aikana löytyy avoin verkko, piirretään lähellä olevaan lyhtypylvääseen, seinään tai muuhun vastaavaan merkki, jonka avulla merkit tunteva henkilö pystyy heti sanomaan minkälainen langaton verkko kyseisellä paikalla. War-chalkingissa käytetyistä merkeistä liitteenä kuva – LIITE 1.
/ 26 / / 27 / / 37 /

7.3 Man-in-the-Middle / Middle-person

Tässä man in the middle (*MITM*) hyökkäystavassa hyökkääjä pystyy lukemaan, liittämään ja muokkaamaan kahden osapuolen välillä liikkuvia viestejä, ilman että kumpikaan osapuoli huomaa tätä. Hyökkääjän tarvitsee pystyä osapuolten välisten viestien tarkkailuun ja sieppaamiseen. Esimerkiksi tilanteessa jossa kolmas persoona Seppo sieppaa Irman julkisen luvun X mutta ei lähetä tätä eteenpäin vaan lähettää oman julkisen luvun X_2 Pertille. Kun Pertti lähettää oman

julkisen lukunsa X_3, korvaa Seppo tämän luvun omalla ja lähettää luvun Irmalle. Lyhyesti sanottuna Seppo ja Irma sopivat omasta salaisesta avaimestaan ja samoin tekevät Seppo ja Pertti. Tämän jälkeen Seppo voi avata, lukea ja muokata Irman ja Pertin välillä kulkevia viestejä mielensä mukaan. Man in the middle-hyökkäys soveltuu hyvin kyseiseen tilanteeseen, jossa käytössä on Diffie-Hellman avaimensopimisprotokolla, Diffie-Hellman-protokolla ei sellaisenaan pysty takaamaan osapuolten autenttisuutta. Tästä johtuen se on haavoittuvainen kyseiselle hyökkäystyypille. Ongelma on kuitenkin helposti ratkaistavissa digitaalisella allekirjoituksella tai muilla protokollavaihtoehdoilla.

7.4 Salasanan murtaminen

Salasanan murtoprosessi kuulostaa pelkästään haitalliselta, mutta on sillä hyödyllinenkin käyttötarkoitus järjestelmäylläpidolle. Salasanan murtajien avulla pystytään etsimään verkon heikot salasanat. Esimerkiksi John The Ripper-ohjelman kaltaiset salasanojen murtajat pystyvät murtamaan Windows NT ja UNIX-pohjaisia salasanatiedostoja.

Salasanojen murtaminen kuormittaa tietokoneen prosessoria ja muistia ja murtaminen voi kestää päiviä, viikkoja, kuukausia tai jopa vuosia riippuen salasanan vahvuudesta ja salauksessa käytetyistä algoritmeista. Salasanojen murtaminen on suoraan verrannollinen laitteiden tehokkuuteen, eli mitä tehokkaampi kone sitä nopeammin salasanat murtuvat.

Esimerkiksi Windows NT säilyttää salasanatiivistettä salasanoista rekisterin suojatussa osassa SAM. Nämä salasanatiivisteet voidaan ottaa koneelta talteen esimerkiksi ottamalla varmuuskopio SAMista rdisk-komennolla ja siirtää luotu varmuuskopiotiedosto salasanan murtavaan tietokoneeseen. Rdisk /s komennolla luodaan pakatun SAM-tiedoston %systemroot%:in repair-hakemistoon joka yleensä on c:\winnt\repair. Toinen tapa hankkia salasanat on nuuskia ne suoraan verkkokaapelista. Kyseinen temppu voidaan toteuttaa esimerkiksi L0phtCrack-ohjelmaan integroitujen ominaisuuksien avulla. L0phtCrack-ohjelman julkistaminen herätti aikoinaan keskustelua jossa todettiin että Microsoftin salasana-algoritmi oli hyvin puutteellinen.

8 LOPPUSANAT

Vasta työtä tehdessäni tajusin kuinka vähän varsinaisesti olen oikeastaan tiennyt tietoturvasta. Työtä tehdessäni opin huomattavan paljon tietoturvasta ja tietoturvattomuudesta. Tietoturvaan liittyvistä asioista on julkaistu kovin heikosti materiaalia ja julkaistut materiaalit ovat pirstaleisia, eli isot kokonaisuudet on hajotettu pieniksi osiksi ja tietoja joutuu kaivamaan ja yhdistämään ja pahimmillaan tietoja joutuu vertailemaan monen eri lähteen kesken ja tutkimaan mahdollisten eroavaisuuksien syitä ja tiedon paikkaansa pitävyyttä.

Olen myös erittäin vahvasti sitä mieltä että tietotekniikan koulutusohjelmaan olisi sisällytettävä tietoverkkojen tietoturvaa käsitteleviä pakollisia opintoja. Sillä tietoturvan merkitys nykyajan tietokoneiden alati kehittyvässä maailmassa on koko ajan kasvanut ja kasvanut. Tästä johtuen tietotekniikan alan insinöörillä pitää myös olla tietämystä kyseisen alan perusasioista.

9 LÄHTEET

/ 1 / http://www.lbagroup.com/associates/wlanfaq.php

/ 2 / http://users.tkk.fi/~mjsyrjal/wlan.html

/ 3 / http://www.tol.oulu.fi/~avesanen/Langaton_TT/luennot/wlan/Wlan.html

/ 4 / Lähiverkot – ethernet, Hannu Jaakohuhta

/ 5 / http://www.javvin.com/protocolWLAN.html

/ 6 / http://www.palowireless.com/i802_11/

/ 7 / Aamulehti 5.9.2005

/ 8 / Mobiili tietoliikenne, Jochen Schiller

/ 9 / http://www.finclockers.com/artikkeli.asp?id=81

/ 10 / http://en.wikipedia.org/wiki/Modulation

/ 11 / Tietoliikennetekniikka ja tiedonsiirto, Ari Rantala

/ 12 / http://www.palowireless.com/i802_11/

/ 13 / http://www.ficora.fi/suomi/tietoturva/ohjeet/ohje-2002-07.htm

/ 14 / Tietoverkkojen tietoturva, Esa Kerttula

/ 15 / http://www.wi-fi.org/OpenSection/secure.asp?TID=2

/ 16 / http://www.tech-faq.com/ssid.shtml

/ 17 / http://www.buffalo-technology.com/products/aoss.php

/ 18 / http://www.tietokone.fi/uutta/uutinen.asp?news_id=22444&tyyppi=1

/ 19 / http://wlan.dacco.fi/sanasto.htm#intrusion_detection

/ 20 / http://fi.wikipedia.org/wiki/RC4

/ 21 / http://en.wikipedia.org/wiki/Rc4

/ 22 / http://www.cs.helsinki.fi/group/turvasem/papers/niemi_wlan.pdf

/ 23 / http://www.tietokone.fi/uutta/uutinen.asp?news_id=22235&tyyppi=1

/ 24 / http://fi.wikipedia.org/wiki/WPA

/ 25 / http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

/ 26 / http://en.wikipedia.org/wiki/War_driving

/ 27 / http://www.warchalking.us/

/ 28 / http://www.drizzle.com/~aboba/IEEE/

/ 29 / http://www.ieee802.org/1/pages/802.1x.html

/ 30 / http://fi.wikipedia.org/wiki/Ipsec

/ 31 / http://en.wikipedia.org/wiki/Ipsec

/ 32 / http://www.cs.tut.fi/kurssit/8306000/TTP/print/ttp-a-2004.pdf

/ 33 / http://computer.howstuffworks.com/vpn.htm

/ 34 / http://fi.wikipedia.org/wiki/VPN

/ 35 / http://en.wikipedia.org/wiki/Vpn

/ 36 / http://www.cs.tut.fi/kurssit/8306000/TTP/print/ttj-ab.pdf

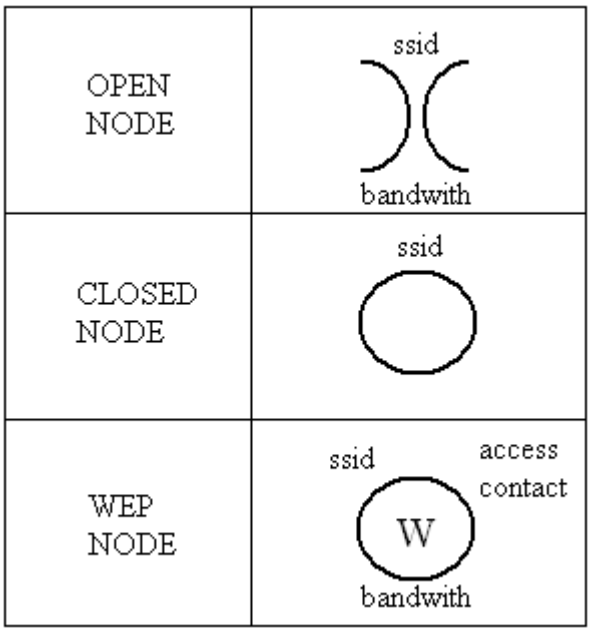
/ 37 / http://www.tietokone.fi/uutta/uutinen.asp?news_id=24631&
tyyppi=1

/ 38 / http://www.cs.tut.fi/kurssit/8306000/TTP/print/ttp-ab-2004.pdf

/ 39 / http://airsnort.shmoo.com/faq.html

10 LIITTEET

/ 1 / War-chalkingissa käytössä olevat symbolit



LIITE 1. War-chalkingissa käytetyt piirrosmerkit