LAPPEENRANNAN TEKNILLINEN YLIOPISTO
TIETOTEKNIIKAN OSASTO

Tietoturva käyttäjän kannalta langattomaan lähiverkkotekniikkaan perustuvassa kaupunkiverkossa

Diplomityön aihe on hyväksytty Lappeenrannan teknillisen yliopiston tietotekniikan osaston osastoneuvoston kokouksessa 11.9.2002.

Työn tarkastajina toimivat professori Jari Porras ja TkT Jouni Ikonen ja ohjaajana TkT Jouni Ikonen.

Lappeenrannassa 25.3.2003

Sami Seppänen
Punkkerikatu 1 A 2
53850 Lappeenranta

TIIVISTELMÄ

Tekijä: Seppänen, Sami

Nimi: **Tietoturva käyttäjän kannalta langattomaan lähiverkkotekniikkaan perustuvassa kaupunkiverkossa**

Osasto: Tietotekniikan osasto

Vuosi: 2003

Paikka: Lappeenranta

Diplomityö. Lappeenrannan teknillinen yliopisto.
77 sivua, 13 kuvaa ja 1 liite.

Tarkastajat: Professori Jari Porras ja TkT Jouni Ikonen

Hakusanat: tietoturva, wlan, langaton, verkko

Langattomien lähiverkkotekniikoiden käyttö on yleistynyt nopeasti viime vuosina. Varsinkin IEEE:n 802.11b-standardi on ollut suosittu. Tätä tekniikkaa on käytetty myös alueellisten access-verkkojen rakentamiseen. Tämä työ on tehty hankkeeseen, jossa tutkitaan langattoman lähiverkkotekniikan käyttöä operaattoririippumattoman kaupunkiverkon toteuttamiseen. Työssä tutkittiin langattoman lähiverkkotekniikan vaikutusta verkon käyttäjän tietoturvaan ja pyrittiin löytämään avoimeen kaupunkiverkkoon sopiva ratkaisu, joka parantaa käyttäjän tietoturvaa.

Työssä käsitellään aluksi tietoturvan teoriaa ja langattomuuden vaikutusta tietoturvaan. Hankkeessa käytetty langaton lähiverkkotekniikka IEEE 802.11b ja sen tietoturvaominaisuudet esitellään. Tutustutaan myös lyhyesti muutamiin julkisiin, 802.11b-tekniikkaa käyttäviin verkkoihin, sekä niiden tietoturvaratkaisuihin. Työssä esitellään tuote, jolla pyrittiin parantamaan käyttäjien tietoturvaa hankkeen verkossa. Lisäksi kuvaillaan tuotteen asennus testiverkkoon. Testiverkon käyttöperiaatteiden perusteella päädyttiin tulokseen olla ottamatta testattua tuotetta käyttöön, vaikka tuote sinällään oli teknisesti toimiva.

ABSTRACT

Author: Seppänen, Sami

Subject: **User security in a regional network based on wireless local area network technology**

Department: Information technology

Year: 2003

Place: Lappeenranta

Master's Thesis. Lappeenranta University of Technology.
77 pages, 13 figures and 1 appendix.

Supervisors: Professor Jari Porras and D.Sc. Jouni Ikonen

Keywords: security, wlan, wireless, network

The use of wireless local area network technologies has grown in popularity in the last few years. In particular the IEEE 802.11b standard has been popular. This technology has also been used to construct regional access networks. This thesis has been done to a project in which the use of wireless local area network technology to construct a city-wide multioperator network is studied. In this thesis the impact of wireless local area network technology to user security is studied. Also a solution to improve security is sought.

Firstly theory of security in computer systems is studied. The impact of wireless technologies to security of networking is then examined. The technology used in the project's network, IEEE 802.11b, is introduced and the security properties of 802.11b are closely analysed. Then we have a short look on some public networks utilising 802.11b and their security solutions. Lastly the product chosen to improve project network users' security is introduced. The product's installation to the test network is outlined also. Based on the usage policy of the project's network it was decided that the product would not be used in this project, even though the product was found to be technically working solution.

SISÄLLYSLUETTELO

LYHENTEET

ACL	Access Control List
AES	Advanced Encryption Standard
BSD	Berkeley Software Distribution
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CTS	Clear To Send
DCF	Distributed Coordination Function
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
ESS	Extended Service Set
ETSI	the European Telecommunications Standards Institute
FHSS	Frequency Hopping Spread Spectrum
GHz	Gigahertsi
HIPERLAN	High Performance Radio Local Area Network
HTTP	Hypertext Transfer Protocol
IBSS	Independent Basic Service Set
ICV	Integrity Check Value
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
ISM-kaista	Band for the Industrial, Scientific and Medical use
IV	Initialization Vector
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
LLC	Logical Link Control layer
MAC	(Lähiverkoissa) Media Access Control

MAC	(Kryptografiassa) Message Authentication Code
MAN	Metropolitan Area Network
Mb/s	Megabittiä sekunnissa
MHz	Megahertsi
MPN	Mobile Private Network
NAT	Network Address Translation
OSI	Open Systems Interconnection
PAT	Port Address Translation
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunneling Protocol
PRNG	Pseudo-Random Number Generator
RADIUS	Remote Authentication Dial-In User Service
RSN	Robust Security Network
RTS	Request To Send
SS	Spread Spectrum
SSH	Secure Shell
SSID	Service Set ID
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
XOR	eXclusive OR

1 JOHDANTO

Langattomat lähiverkot ovat yleistyneet viime vuosien aikana rajusti. Langattomien lähiverkkojen suosio alkoi nousta IEEE:n vuonna 1997 valmistuneen 802.11-standardin myötä. Varsinaiseen suursuosioon ne nousivat vuonna 1999 esitellyn standardin laajennuksen, 802.11b:n myötä. Siinä nostettiin langattoman lähiverkon tiedonsiirtonopeus sellaiselle tasolle, että se oli useimpiin käyttötarkoituksiin riittävä. Internet-operaattorit ovat huomanneet tekniikan tarjoamat mahdollisuudet ja rakentaneet langattomia verkkoja laajalti. Voidaan nähdä, että tietoverkoista on langattomuuden myötä tulossa kaikkialla läsnäolevia. Tietokoneen käyttötaito alkaa olemaan yksi yhteiskunnan perustaidoista ja verkottumisen myötä tietoverkkojen käyttötaito samoin. Useinkaan peruskäyttäjät eivät ole tietoisia tietokoneisiin ja tietoverkkoihin liittyvistä tietoturvakysymyksistä. Jotta tietoyhteiskunta toimisi, on tietoturvallisuuden hallitsemisesta tultava myös perustaito.

Tämän työn taustalla on vuonna 2001 Lappeenrannan teknillisen korkeakoulun (nyk. Lappeenrannan teknillinen yliopisto) tietoliikennetekniikan laitoksella käynnistynyt WLAN-hanke. WLAN-hankkeessa tutkitaan langattoman lähiverkkotekniikan käyttöä operaattoririippumattomana access-verkkona. Hanke edistää osaltaan tietoverkkojen leviämistä. Hankkeessa on toteutettu rajapinnat operaattoreille ja verkon palveluita varten. Operaattoreilla tarkoitetaan mitä tahansa tahoa, joka tarjoaa langattoman access-verkon, eli ns. sisäverkon käyttäjille mahdollisuuden päästä hallinnoimaansa verkkoon. Rajapintaa kutsutaan yhdysliikennepisteeksi. Siihen liittyneitä operaattoreita voi olla useita. Sisäverkon käyttäjät voivat olla asiakkaana yhdellä tai useammalla operaattorilla ja päästä sitä kautta ulos sisäverkosta, esimerkiksi Internetiin. Käyttäjän ei ole pakko olla asiakkaana yhdelläkään operaattorilla, jolloin hän pääsee käyttämään vain sisäverkossa olevia palveluita.

Tässä työssä keskityttiin tarkastelemaan verkon käyttäjän perustietoturvaa ja etenkin langattoman lähiverkkotekniikan vaikutusta käyttäjän tietoturvan kannalta. Työssä on paneuduttu ensin tietoturvan perusteoriaan, ja siitä tarkentaen tietokoneiden ja tietoverkkojen tietoturvaan. Nämä ovat aiheita, joista kaikkien tietoverkkoa käyttävien

olisi syytä olla tietoinen. Projektin verkossa käytettävän langattoman lähiverkkotekniikan (IEEE 802.11b) tietoturvaominaisuuksiin tutustuttiin tarkasti ja havaittiin niissä olevan heikkouksia. Työssä tarkasteltiin myös jo olemassa olevia julkisia langattomia lähiverkkoja ja niiden tietoturvaratkaisuja. Testiverkon käyttäjien tietoturvaa haluttiin parantaa ja tämän saavuttamiseksi päädyttiin testaamaan erästä tuotetta.

2 TIETOTURVA

Yhteiskunnan eri alojen toiminnot perustuvat keskeisesti tietoon, sen käsittelyyn ja siirtämiseen. Informaatiosta on muodostunut välttämätön kauppatavara ja kilpailuelementti. Koska informaatio, kulloisesta esiintymismuodostaan riippumatta, on ratkaisevan tärkeässä asemassa, tietoturvallisuus on strateginen ja jopa kohtalon kysymys. Tietoturvallisuuden voidaan lyhyesti määritellä olevan tietojen ja tiedonkäsittelyn turvallisuutta. [Ker99]

Tiedonkäsittely on muuttunut muutaman kymmenen vuoden aikana voimakkaasti. Aikaisemmin tieto oli lähes poikkeuksetta paperilla ja toimistoissa suuret arkistokaapit. Tietoturva oli perinteistä fyysistä turvaamista ja henkilöstöhallintoa. Sitten käyttöön tulivat tietokoneet sekä niitä yhdistävät verkot ja tieto muuttui sähköiseen muotoon. Tietojenkäsittely tehostui, mutta mukana tulivat myös tekniikkaan liittyvät tietoturvauhkat. Näitä uhkia torjumaan on kehitetty teknisiä tietoturvamenetelmiä. Nykyisin tekniikan muutostahti on hurja ja varsinkin verkottuminen aiheuttaa koko ajan uusia riskejä tietoturvallisuudelle. Kokonaisuutena puhutaan tietojärjestelmien tietoturvasta, jota tässä luvussa lähinnä käsitellään.

Tietojärjestelmät koostuvat useista tekijöistä (verkot, tietokoneet, palvelut, tiedot, sovellukset, käyttäjät), jotka itsessään ovat monimutkaisia kokonaisuuksia. Jotta tietojärjestelmien tietoturvallisuutta voidaan analysoida järkevästi ja implementoida toimivasti, on se jaoteltava selkeisiin ja toiminnallisesti itsenäisiin kokonaisuuksiin. Seuraavaksi esitellään tietoturvaan liittyvät peruskäsitteet ja jaottelut, jotka auttavat ymmärtämään tässä työssä käsiteltäviä asioita.

Käsitteitä tietoturvallisuus ja tietoturva on käytetty tässä työssä synonyymeina. Tietoturvallisuudella tarkoitetaan tilannetta, tavoitetilaa, missä tiedot, järjestelmät ja palvelut ovat asianmukaisesti suojattuja sekä normaali- että poikkeusoloissa hallinnollisten, teknisten ja muiden toimenpiteiden avulla.

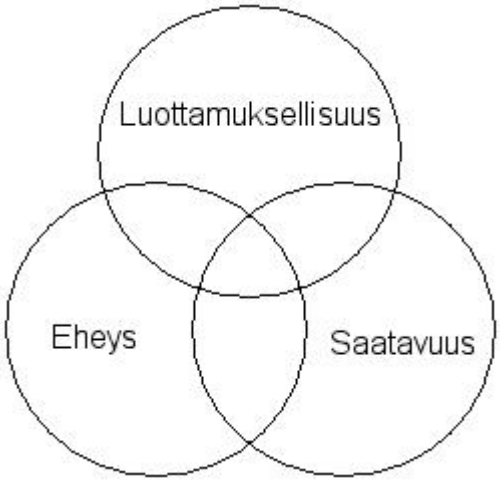
2.1 Tietoturvan perustavoitteet

Tietojärjestelmien tietoturvallisuus on sitä, että pyritään pitämään yllä tietojärjestelmän eri osien kolmea perusominaisuutta: luottamuksellisuutta, eheyttä ja saatavuutta.

- *Luottamuksellisuus* tarkoittaa sitä, että tietojärjestelmä, siinä oleva tieto ja muut ominaisuudet ovat vain niiden käyttöön oikeutettujen saatavilla. Tämä ominaisuus on lukutyyppistä: lukemista, katsomista, tulostamista tai vaikkapa vain tietämistä jonkun asian olemassaolosta. Luottamuksellisuudesta käytetään englannin kielessä termejä confidentiality, secrecy, privacy.
- *Eheys* tarkoittaa sitä, että tietojärjestelmää ja tietoja voi muuttaa vain siihen oikeutetut tahot. Eheyteen voi kuulua myös se, että saadaan tehdä vain sallitunlaisia muutoksia. Tässä yhteydessä muuttaminen pitää sisällään kirjoittamisen, vaihtamisen, tilan vaihtamisen (changing status), poistamisen ja luomisen.
- *Saatavuus* on sitä, että tietojärjestelmään kuuluvat osat ja tiedot ovat niihin oikeutettujen käytettävissä tarvittaessa. Nykyään tämä osuus aletaan käsittää niin, että saatavuuden tavoitteena on pitää tietojärjestelmä ja sen palvelut toiminnassa sekä sisäisesti että ulkoisesti. Tarkemmin määriteltyinä tavoitteita voisivat olla sopiva vasteaika (timely response), resurssien oikeudenmukainen jakaminen (fair allocation), viansietokyky, käytettävyys ja yhtäaikaisuuden hallinta (mahdollisuus yhtäaikaiseen pääsyyn ja poissulkeva pääsy, tarvittaessa).

[Pfl97, Ker99]

Kuva 1 esittää tietoturvallisuuden kolmen perustavoitteen suhdetta toisiinsa. Nämä tavoitteet voivat olla päällekkäisiä ja ne voivat myös olla toisensa poissulkevia, mutta pääasiassa ne ovat itsenäisiä. Esimerkiksi vahva luottamuksellisuuteen panostaminen saattaa haitata pahasti saatavuutta. [Pfl97]



Kuva 1: Tietoturvan perustavoitteiden suhteet

2.2 Tietojärjestelmien tietoturvauhkat

Tietoturva on siis sitä, että varmistetaan tietojärjestelmän komponenttien luottamuksellisuus, eheys ja saatavuus. Tekniikan näkökulmasta katsottuna ja karkeasti jaoteltuna tietojärjestelmissä on kolme osa-aluetta, jotka ovat alttiita hyökkäyksille: laitteisto, ohjelmisto ja data. Nämä kolme osa-aluetta sekä niiden välinen kommunikointi ovat perustasolla ne paikat, joista tietojärjestelmien heikkoudet löytyvät. Tietojärjestelmien uhkat ovat tilanteita, jotka mahdollisesti aiheuttavat menetyksiä tai vahinkoa. Esimerkkejä uhkista ovat ihmisten tekemät hyökkäykset, luonnon katastrofit ja tahattomat virheet. Tietojärjestelmien perusuhkat ovat keskeytys, sieppaaminen, muuntaminen ja väärentäminen. [Pfl97]

Keskeytyksellä tarkoitetaan tilannetta, jossa tietojärjestelmän resurssi(t) rikotaan tai niitä ei voida käyttää. Esimerkkejä keskeytyksestä ovat laitteiston pahantahtoinen tuhoaminen, ohjelmiston/datan pyyhkiminen tai vaikkapa käyttöjärjestelmän häiriö, joka estää järjestelmän toiminnan tai aiheuttaa datan katoamisen.

Sieppaus on sitä, että luvaton osapuoli pääsee käsiksi järjestelmään ja pystyy anastamaan tietoja. Osapuoli voi olla henkilö, ohjelma tai tietokone. Sieppaus voi olla esimerkiksi datan kuuntelemista verkossa tai tiedostojen/ohjelmistojen laitonta kopiointia. Sieppausta voi olla hankalaa tai jopa mahdotonta huomata.

Jos luvaton osapuoli ei pelkästään pääse käsiksi vaan pystyy myös peukaloimaan järjestelmää, on kyseessä *muuntaminen*. Esimerkiksi joku voi muuttaa arvoja tietokannassa, muuntaa ohjelmistoa siten, että se toimii eri tavalla tai muuntaa lähetetyn sanoman sisältöä. Jopa laitteistoja on mahdollista muuntaa. Tästä esimerkkinä voisi olla älykortin peukaloiminen. Joissain tapauksissa muuntaminen on suhteellisen helppo huomata, mutta taitavasti tehdyt hienovaraiset muunnokset ovat erittäin vaikeita havaita.

Väärentäminen on kyseessä silloin, kun luvaton osapuoli pääsee syöttämään järjestelmään omia vastinetietoja. Hyökkääjä voi esimerkiksi syöttää väärennettyjä viestejä verkkoon tai lisätä tietueita tietokantaan. Taitavia väärennöksiä voi olla lähes mahdoton erottaa aidosta.
[Pfl97, Ker99]

2.2.1 Hyökkäykset

Ihmisten tekemät hyökkäykset ovat yleisin uhka tietojärjestelmille. Hyökkääminen on tietojärjestelmän jonkin heikkouden hyväksikäyttöä. Hyökkäämällä tavoitellaan aina jotain hyötyä: rahallista voittoa, julkisuutta, kostoa tai kenties vain hyökkäyksen onnistumisesta tulevaa omaa iloa. Käytännössä onnistuneessa hyökkäyksessä on viisi vaihetta:

1. Etsitään tietty kohde johon hyökätään ja kerätään tietoa kohteesta.
2. Analysoidaan kerätty tieto ja etsitään kohteesta heikkous, jonka avulla voidaan toteuttaa hyökkäyksen tavoitteet.
3. Hankitaan riittävän tasoinen pääsy kohteeseen.
4. Suoritetaan hyökkäys kohteeseen.
5. Viimeistellään hyökkäys – tämä voi pitää sisällään hyökkäyksestä jääneiden todisteiden tuhoamisen ja mahdollisten kostotoimien tai kiinnijäämisen välttämisen.

Hyökkäys jonkun yhtiön tietokoneille Internetin kautta voi tapahtua esimerkiksi niin, että vaiheessa 1 hyökkääjä valitsee kohteeksi tietyn yhtiön ja alkaa kerätä tietoa kohteesta. Tarvittavaa tietoa saa esimerkiksi kohteen web-sivuilta, ping-skannauksilla

(ping scan), porttiskannauksilla (port scan) ja muilla vastaavilla keinoilla. Näin voidaan saada selville mitä laitteistoja ja ohjelmistoja kohteella on käytössä.

Vaiheessa 2 pyritään löytämään heikkous. Hyökkääjä käy läpi keräämänsä tiedot ja saa kenties selville, että kohteessa on käytössä ohjelmisto tai palvelu, jossa on yleisesti tunnettu virhe jota voi käyttää hyväksi.

Vaiheessa 3 on saatava jonkinlainen pääsy tietokoneelle johon hyökätään. Internetissä tämä on triviaali toimenpide ellei konetta ole suojattu, koska kaikki verkossa olevat koneet ovat toistensa saavutettavissa.

Itse hyökkäys tapahtuu vaiheessa 4. Tämä voi olla hankalaa tai helppoa riippuen hyökkäyksen kohteena olevan järjestelmän ominaisuuksista ja ylläpidosta sekä hyökkääjän kyvyistä. Jotkut hyökkäykset saattavat vaatia hyökkäysprosessin toistamista. Saavuttaakseen pääkohteensa hyökkääjä voi suorittaa vaiheet 1-4 useampaan kertaan: jos itse pääkohteeseen ei ole suoraa pääsyä, voidaan murtautua ensin johonkin koneeseen jolta pääsee jatkamaan hyökkäystä kohti pääkohdetta.

Vaiheessa 5 viimeistellään hyökkäys. Jos hyökkääjä esimerkiksi etsii tiettyä tiedostoa, hän ottaa sen ja poistuu. Välttääkseen kiinnijäämistä hyökkääjä voi pyyhkiä lokitiedostot ja muutoinkin häivyttää jälkiään. Hyökkääjä saattaa myös jättää jälkeensä muokattuja systeemitiedostoja päästäkseen myöhemmin helpommin uudestaan järjestelmään. [Sch00]

Kaikki hyökkäykset eivät välttämättä käy läpi kaikkia edellä lueteltuja vaiheita. Läheskään kaikki hyökkäykset eivät ole niin suoraviivaisia kuin äskeisessä esimerkissä läpikäyty. Yleisesti tietoturvaa kuvataan ketjuna, ja järjestelmä on vain niin turvallinen kuin sen heikoin lenkki. Haavoittuvaisuudet (heikkoudet) ovat heikkoja lenkkejä. Mutta heikkouden löytäminen järjestelmän tietoturvasta on vasta ensimmäinen askel kohti tuon heikkouden hyväksikäyttöä. Onnistuneeseen hyökkäykseen tarvitaan pääsy sellaiseen asemaan, että pystyy käyttämään löydettyä heikkoutta hyväkseen, niin ikään pitää todella osata käyttää heikkoutta hyväkseen ja lopuksi vielä pitää poistua onnistuneesti. [Sch00]

2.2.2 Hyökkääjät

Ketkä sitten uhkaavat digitaalisen maailman tietoturvaa? Itse asiassa pahantekijät ovat samoja kuin tavallisessa fyysisessä maailmassamme, eli tavallisia rahallista hyötyä tavoittelevia rikollisia, teollisuusvakoojia etsimässä kilpailuetua, hakkereita kokeilemassa rajojaan salaisen tiedon haussa ja sotilaallista tiedustelua tekeviä tahoja. Ihmiset eivät ole muuttuneet – vain ympäristö, jossa he taitojaan käyttävät on muuttunut niin sanotuksi kyberavaruudeksi.

Tässä kutsutaan yleisesti minkä tahansa järjestelmän tietoturvaa vastaan hyökkääviä vastustajiksi. Vastustajat voidaan jaotella monella tapaa: päämäärän, pääsyoikeuksien, käytössään olevien resurssien, ammattitaidon ja riskienottokyvyn mukaan. Vastustajilla on monia päämääriä: pelkästään tuhojen tekeminen, taloudellinen hyöty, informaation saaminen, ja niin edelleen. Teollisuusvakoojan päämäärät eroavat järjestäytyneen rikollisjärjestön tavoitteista, ja näistä ensimmäistä vastaan suunnitellut vastatoimet eivät välttämättä tehoa ollenkaan jälkimmäiseen. On tärkeää ymmärtää mahdollisten hyökkääjien päämäärät, jotta voidaan suunnitella tehokkaat vastatoimet.

Vastustajilla on eritasoinen pääsy järjestelmiin. Esimerkiksi organisaation työntekijällä on paljon parempi pääsy organisaation järjestelmiin kuin organisaation ulkopuolisella henkilöllä. Vastustajilla on myös eri määrä resursseja: toisilla on paljon rahaa, toisilla taas ei juuri mitään (paitsi ehkä aikaa). Joillain on merkittävät tekniset taidot, toisilta taas osaaminen puuttuu kokonaan.

Erilaiset vastustajat ovat valmiita ottamaan eri tasoisia riskejä. Terroristit saattavat mielellään jopa kuolla asiansa puolesta. Rikolliset ehkä hyväksyvät mahdollisen vankilatuomion riskin, mutta eivät ole valmiita uhraamaan kaikkea. Julkisuuden tavoittelijat eivät halua vankilaan.

Mahdollisia ihmisiä ja organisaatioita, jotka yrittävät murtaa toisten tietoturvaa ovat siis lueteltuina: hakkerit, yksittäiset rikolliset, pahantahtoiset sisäpiiriläiset, teollisuusvakoojat, lehdistö (liian tutkiva journalismi?), järjestäytynyt rikollisuus,

erilaiset poliisivoimat, terroristit, kansalliset tiedusteluorganisaatiot ja informaatiosotilaat (infowarrior). [Sch00]

2.3 Suojautumismenetelmät ja suojautuminen

Suojautumismenetelmät tai vastatoimet ovat tietoturvallisuudesta puhuttaessa menetelmiä, jotka vähentävät tietojärjestelmien heikkouksia (vulnerabilities). Periaatteessa suojautumismenetelmät voidaan toteuttaa ehkäisemään mikä tahansa menestyksekkään hyökkäyksen viidestä askelesta. Ja tosiasia on, että minkä tahansa hyökkäyksen estämiseksi riittää kun estää yhden neljästä ensimmäisestä hyökkäysaskelesta toteutumasta. [Sch00]

Suojautumismenetelmät ovat:

- teknisiä, laitteistoihin ja ohjelmistoihin perustuvia tietoturvaratkaisuja
- fyysisiä tietoturvaratkaisuja
- hallinnollisia, eli toimintatapoihin perustuvia tietoturvaratkaisuja

[Ber98]

2.3.1 Tekniset tietoturvaratkaisut

Teknisillä tietoturvaratkaisuilla toteutetaan tietoturvapolitiikassa määriteltyjä tavoitteita. Teknisiä tietoturvaratkaisuja ovat mm.

- erilaiset tunnistamis- ja autentikointimenetelmät (identification & authentication)
- automaattiset virustarkistukset
- palomuurit
- kryptografiset menetelmät

Autentikointi tarkoittaa identiteetin todistamista, eli menetelmää, jolla alkuperäinen (aito) henkilö, tieto tai esimerkiksi kommunikaatio voidaan erottaa muista. Yleisesti ottaen autentikointi perustuu yhteen tai useampaan seuraavista kolmesta asiasta:

1. mitä henkilö on
2. mitä henkilö tietää
3. mitä henkilöllä on

Esimerkiksi ihmiset identifioivat heille tutut henkilöt fyysisistä ominaisuuksista (mitä henkilö on). Biometriset autentikointimenetelmät perustuvat myös tähän. Pankin maksupääte tunnistaa asiakkaan maksukortilla ja PIN-koodilla (mitä henkilöllä on ja mitä hän tietää).

Käyttäjätunnuksen ja salasanan yhdistelmä on nykyisin ylivoimaisesti suosituin tunnistamis- ja todentamismenetelmä tietojärjestelmissä. Käyttäjä tunnistetaan antamastaan käyttäjätunnuksesta ja antamalla salasanansa tämä todistaa identiteettinsä (eli todentaminen perustuu siihen mitä henkilö tietää). Tällä menetelmällä valvotaan tietojärjestelmiin pääsyä ja pyritään varmistamaan siellä olevan tiedon säilyminen luottamuksellisena ja eheänä. Käytännössä tämä tarkoittaa, että käyttäjätunnusten kautta määritellään mihin tietoihin kenelläkin on oikeus. Jos käyttäjällä on oikeus luoda uutta tietoa tai muuttaa olemassa olevaa, käyttäjätunnuksen avulla voidaan myös jäljittää tietolähde. Salasanojen käytössä autentikointiin on hyvänä puolena toteutuksen helppous. Valitettavasti salasanojen käyttö ei ole kovin vahva menetelmä tietoturvan kannalta, koska ihmiset usein valitsevat helposti muistettavia salasanoja, jotka on myöskin helppo arvata luvatonta pääsyä haluavien toimesta. Salasanojen murtamiseen tarkoitettuja ohjelmia on helposti saatavilla. Salasanat voidaan valita myöskin niin, että ne ovat vahvoja ja vaikeasti arvattavia. Huonona puolena tässä on, että vahvat salasanat ovat myöskin vaikeasti muistettavia. Tällöin ne saatetaan kirjoittaa ylös muistilapulle, josta ne voivat paljastua.

Automaattisilla virustarkistuksilla pyritään estämään virusten pääsy tietojärjestelmiin ja organisaation sisäisiin verkkoihin. Virukset ovat vahinko-ohjelmia, jotka tarttuvat muihin ohjelmiin ja pyrkivät leviämään. Virukset voidaan ohjelmoida tuhoamaan tietoja, välittämään niitä edelleen sekä häiritsemään tietojärjestelmien toimintaa. Viruksia voidaan käyttää myös pohjustamaan tulevaa hyökkäystä tietojärjestelmään.

Automaattiset virustarkistukset voidaan sijoittaa esimerkiksi yrityksen sisäisen ja julkisen verkon välissä olevalle palomuurille.

Vahva tekninen tietoturva perustuu aina kryptografian käyttöön. Kryptografisilla menetelmillä voidaan varmistaa tiedon eheys, luottamuksellisuus, tietolähteen todennus (eli autentikointi) ja kiistämättömyys. Kryptografiaa voidaan käyttää myös pääsyn valvonnassa tarkistamaan käyttäjän henkilöllisyys tai oikeus järjestelmän käyttöön. Kryptografiaa tarkastellaan tärkeytensä vuoksi tarkemmin omassa osuudessaan.
[Ber98]

2.3.2 Fyysiset tietoturvaratkaisut

Tietojärjestelmien tietoturvaa suunniteltaessa fyysinen turvallisuus usein unohtuu, vaikka fyysiset tietoturvaratkaisut muodostavat tietoturvan perustan. Fyysisen turvallisuuden ongelmaa on yritetty ratkaista aikojen alusta saakka. Seinät, lukot ja aseistetut vartijat ovat kaikki fyysisen turvallisuuden työkaluja. Fyysisten tietoturvaratkaisujen tarkoitus on estää mahdollisen tunkeutujan pääsy fyysisesti järjestelmään käsiksi.

Fyysiseen tietoturvaan liittyviä toimia ovat mm.

- kulunvalvonta
- laitteiden ja verkon kaapeleiden sijoittaminen turvalliseen ja eristettyyn tilaan
- varmuuskopioiden ottaminen tarvittavista tiedoista ja ohjelmistoista
- tilojen suunnittelu niin, että (suur)onnettomuuksien riski on pieni

[Ber98, Pfl97]

Erilaiset organisaatiot ovat jo pitkän aikaa olleet tekemisissä fyysistä tietoturvaa koskevien kysymysten kanssa. Suurin osa niistä onkin jo oppinut käyttämään sen mukaisia fyysisiä tietoturvaratkaisuja kuin niitä kohtaan kohdistuvat uhkat edellyttävät. Esimerkkinä nykyajan fyysisen tietoturvan haasteista ovat uudet päätelaitteet: kannettavat tietokoneet, taskutietokoneet, älypuhelimet jne. Paljon arvokkaita tietoja on varastettu kannettavien tietokoneiden mukana, kun työntekijät ovat vieneet töitä mukaan matkoille tai kotiin. [Sch00]

2.3.3 Toimintatapoihin perustuvat tietoturvaratkaisut

Teknisillä ja fyysisillä tietoturvaratkaisuilla ei koskaan voida kokonaan taata tietoturvan toteutumista. Keskeisessä asemassa ovat ihmiset ja heidän toimintatapansa, olivat he sitten yksittäisiä kotikäyttäjiä tai yritysten tai laitosten henkilökuntaan kuuluvia. Ihmiset ja heidän vuorovaikutuksensa tietokonejärjestelmien kanssa ovat usein turvajärjestelmien heikoin lenkki.

Toimintatavat voidaan jakaa tietojärjestelmistä ja verkoista vastaavien henkilöiden toimintatapoihin ja käyttäjien toimintatapoihin. Tietojärjestelmistä ja verkoista vastaavat huolehtivat tietoturvan käytännön toteuttamisesta tietoturvapolitiikan mukaisesti eli teknisten ja fyysisten tietoturvaratkaisujen toteuttamisesta oikein, huolellisesti ja sovitun mukaisesti. Tämän jälkeen tärkein suojausmenetelmä on jatkuva järjestelmien ja verkkojen tarkkailu, poikkeaviin tilanteisiin reagointi ja tietoturvapolitiikan parantaminen kokemusten pohjalta. Tietojärjestelmistä ja verkoista vastaavilla on lisäksi salassapitovelvollisuus luottamuksellisten tietojen osalta. Heidän tulee myös tietää mitä tietoja käyttäjistä on luvallista järjestelmiin kerätä ja miten tietoja saa käyttää.

Käyttäjien toimintatavat liittyvät yrityksessä tai organisaatiossa sovittujen tietoturvamenetelmien käyttöön. Ihmiset eivät yleisesti ottaen tunne tietokoneita, joilla työskentelevät, kovinkaan hyvin ja ovat erittäin alttiita manipuloinnille (social engineering). Esimerkiksi salasanoja annetaan puhelimessa järjestelmän valvojaksi esittäytyvälle ja avataan rakkauskirjeiksi naamioitujen sähköpostien liitteitä, joissa on virus. Jo varsin yksinkertaisilla ja perustelluilla toimintatavoilla (eli käyttäjien tietoturvapolitiikalla), jotka selkeästi tuodaan käyttäjien tietoon, saavutetaan hyviä tuloksia. Keskeisiä kohtia ovat mm. salasanojen ja käyttäjätunnusten sekä kryptografiassa käytettävien salaisten avainten pitäminen salassa. Salaisia avaimia ja salasanoja ei tule luovuttaa muiden käyttöön. Käyttäjä ei myöskään saa ohittaa jotain sovittua tietoturvaratkaisua, esimerkiksi palomuuria ottamalla suoran yhteyden modeemilla omasta, verkkoon liitetystä koneesta. On myös syytä määritellä mitä tietoja saa luovuttaa mihinkin.

Yksittäisen kotikäyttäjän kohdalla toimintatavat liittyvät niin ikään huolellisuuteen salasanojen ja salaisten avainten säilytyksessä sekä kykyihin ja mahdollisuuksiin käyttää erilaisia tietoturvateknologioita. Hyvin tärkeää on myös tietämys eri teknologioista ja tietoisuus niihin liittyvistä uhkista, jotta niihin osataan varautua. [Ber98]

2.3.4 Syvyyspuolustus

Usein yksittäiset tekniset tietoturvaratkaisut nähdään ratkaisuina kaikkiin tietoturvaongelmiin. Mutta yksikään tekninen tietoturvaratkaisu ei itsenään ole yleislääke tietoturvan saavuttamiseksi. Tietoturva on yhtä vahva kuin sen heikoin lenkki - tällä yleensä viitataan yksittäisiin teknologioihin. Järkevässä ja hyvin suunnitellussa järjestelmässä tietoturvateknologioita voidaan käyttää kerrostaen siten, että puolustuksessa on syvyyttä, jolloin järjestelmän tietoturva onkin siinä olevien tietoturvalenkkien summa. Esimerkkinä tästä on Internetiin kytketyn tietokoneen suojaaminen sopivalla yhdistelmällä teknisiä tietoturvaratkaisuja: palomuurilla estetään ulkopuolisten pääsy järjestelmään, vahvalla autentikoinnilla varmistetaan että vain sallitut käyttäjät pääsevät kirjautumaan koneelle ja verkkoyhteyksissä käytetään salausta. [Sch00]

2.3.5 Tehokas puolustaminen

Järjestelmää vastaan hyökkääminen on monimutkaisempaa kuin pelkästään jonkun heikkouden löytäminen järjestelmästä. Samalla tavoin järjestelmän puolustaminen on monimutkaisempaa kuin pelkästään yksittäisten vastatoimien lisääminen järjestelmään ilman minkäänlaista suunnittelua. Tehokkaaseen puolustusjärjestelmään kuuluvat seuraavat osa-alueet:

- suojaaminen (protection)
- havaitseminen (detection)
- reagointi (reaction)

Fyysisen maailman tehokasta puolustusta havainnollistava tapaus on esimerkiksi jonkun yhtiön kassakaappiinsa tallettama salainen asiakirja, jota toisen yrityksen teollisuusvakooja, eli hyökkääjä, tavoittelee. Puolustavan yhtiön puolustus on tehokas ja siihen kuuluu kassakaapin lisäksi hälytysjärjestelmä ja kiertelevät vartiomiehet. Hyökkääjän olisi siis kassakaappiin murtautumisen lisäksi ohitettava hälytysjärjestelmä ja vartijat. Kassakaappi on suojaava vastatoimi, hälytysjärjestelmä puolestaan havaitsee hyökkäykset ja vartijat ovat reagoiva puolustusjärjestelmän osa.

Tällä periaatteella rakennetussa puolustuksessa on se hyvä puoli, että toimivan puolustuksen osien ei tarvitse olla täydellisiä. Äskeistä kassakaappiesimerkkiä käyttäen: jos vartijat kiertävät kassakaappihuoneen kautta puolen tunnin välein tarkastamassa tilanteen, ei kassakaapin tarvitse kestää kuin puoli tuntia yhtämittaista hyökkäystä.

Tietojärjestelmiin liittyvät puolustusmenetelmät ovat suurimmalta osin suojaavia: kryptografiaa, palomuureja ja salasanoja. Joitakin havaitsemiseen liittyviä menetelmiä on ja niitä kutsutaan nimellä tunkeutumisen havaitsemisjärjestelmä (Intrusion Detection System, IDS). Vielä harvinaisempia ovat reagointimenetelmät, esimerkiksi järjestelmään kirjautumismenetelmä (login system) joka lukittuu kolmen epäonnistuneen kirjautumisyrityksen jälkeen. On muistettava, että havaitsemisjärjestelmät ovat itsessään turhia, jos sellaisen antamaan hälytykseen ei reagoida mitenkään.

Digitaalisen maailman tietoturvassa luotetaan nykyisin lähes täysin pelkästään suojaaviin teknologioihin. Tämä on kuitenkin väärä lähestymistapa. Puolustautuminen pelkästään suojaavilla teknologioilla toimii vain mikäli käytetyt teknologiat ovat täydellisiä; täydellisesti suunniteltuja ja toteutettuja. Valitettavasti yksikään teknologia ei ole täydellinen, ja kaikissa tietokoneisiin liittyvissä tuotteissa on heikkouksia. Tämän vuoksi hyökkäyksien havaitseminen ja niihin reagointi ovat erittäin tärkeitä osatekijöitä kunnollisessa tietoturvallisuudessa. Kun kaikki tietoturvaan liittyvät ratkaisut toimivat yhdessä, ei yhdenkään yksittäisen ratkaisun tarvitse yksinään kantaa vastuuta hyökkääjän pysäyttämisestä.
[Sch00]

2.3.6 Järkevä suojautumismenetelmien käyttö

Erilaisia heikkouksia ja potentiaalisia hyökkäyksiä on valtava määrä. Järkevin puolustautuminen on sellaista, jossa pyritään tasaisesti kattamaan potentiaaliset uhkat. Pitää pyrkiä löytämään uhkat jotka aiheuttavat suurimmat riskit ja puolustautua niitä vastaan. Puolustusmenetelmiin sijoitettaessa kannattaa myöskin käyttää järkeä. Ei kannata sijoittaa huippukalliiseen yksittäiseen turvatuotteeseen, jos muutoin ei tietoturvaan panosteta ollenkaan. Samoin ei kannata puolustaa mitään kalliimmalla kuin mitä sen arvo on. Tässä tietysti ongelmaksi nousee se, että kaikki eivät arvosta samoja asioita samalla tavalla. Se on otettava jollain tavalla huomioon puolustusta suunniteltaessa. Usein parhaan ja kustannustehokkaimman tietoturvan takaa yksinkertaisten puolustusmenetelmien käyttö, kouluttaminen ja huolella mietitty tietoturvakäytäntö (policy). [Sch00]

2.4 Tietoturva tietoverkoissa

Nykyisin tietokonejärjestelmät verkotetaan lähes poikkeuksetta ainakin paikallisesti lähiverkolla. Varsin usein paikallisverkko yhdistetään myös muihin verkkoihin ja tämä tarkoittaa lähes aina sitä, että liitytään Internetiin. Internet yhdistää verkkoja globaalisti. Tietoverkkoon liitetyllä tietojärjestelmällä on kaikki samat haavoittuvaisuudet kuin verkottamattomalla tietojärjestelmällä (tietokoneella), mutta verkoilla on lisäksi myös omat erityiset haavoittuvaisuutensa.

2.4.1 Yleistä verkoista ja niiden uhkista

Yksinkertaisimmillaan verkko on sellainen, jossa kaksi tietokonetta (tai yleisesti vain laitetta) on yhdistetty jonkun median yli käyttämällä kommunikointiin jotain laitteistoa ja ohjelmistoa. Kommunikointiin voidaan käyttää erilaisia siirtoteitä, jotka ovat ilma, jossa siirto tapahtuu esimerkiksi radiotekniikalla, tai erilaiset fyysiset mediat, joita ovat esimerkiksi eri tyyppiset kaapelit. Kommunikointi tapahtuu käyttämällä jotain yhteyskäytäntöä, eli protokollaa. Tietokoneiden välisen kommunikoinnin yksityiskohtia piilotetaan eri tasoisilla protokollilla, ja näin saavutetaan korkeammilla protokollatasoilla riippumattomuus alla piilevästä laitteistosta. Eri tasoisista protokollista muodostuu protokollapino, joka on kerrostettu kommunikointimalli.

Protokollapino on siis ohjelmistojen ja laitteiden kokonaisuus, joka organisoi verkkokomponentit eritasoisiin, hyvin määriteltyihin kerroksiin. Suosittuja protokollapinoja ovat OSI-malli (Open Systems Interconnection) ja TCP/IP-arkkitehtuuri (Transmission Control Protocol / Internet Protocol). Kaikissa verkoissa käytetään jotain osoitejärjestelmää. Osoite on verkon pisteen ainutlaatuinen tunniste. Verkot luokitellaan yleensä maantieteellisen kattavuuden mukaan lähiverkkoihin (Local Area Network, LAN), kaupunkiverkkoihin (Metropolitan Area Network, MAN), laajan alueen verkkoihin (Wide Area Network, WAN) ja internet-verkkoihin. Internet-verkot yhdistävät verkkoja toisiinsa ja tämän hetken laajinta globaalia verkkoa kutsutaan yksinkertaisesti vain Internetiksi. Verkoilla on myös erilaisia topologioita. Kaikki mainitut verkon ominaisuudet vaikuttavat tietoturvaan.

Verkosta voidaan siis erottaa yleisesti seuraavat osat: (1) Yksittäiset tietokoneet, jotka on liitetty (2) kommunikointilinkeillä (3) lähiverkkoon. Tietokoneissa on paikallisia (4) datavarastoja, (5) prosesseja ja (6) laitteita. Lähiverkossa on myös (7) yhdyskäytävä, joka liittää sen (8) verkkojen välisillä kommunikointilinkeillä (9) reitittimiin ja sitä kautta (10) muissa verkoissa oleviin resursseihin. Kaikkien näiden osien luottamuksellisuutta, eheyttä ja saatavuutta vastaan voidaan hyökätä. [Pfl97]

Yleisesti ottaen verkoille mahdollisia uhkia ovat:

- salakuuntelu
- toisena esiintyminen
- viestien luottamuksellisuuden rikkominen
- viestien eheyden rikkominen
- hakkerointi (tai krakkerointi)
- ohjelmien eheyden rikkominen
- palvelunesto

Salakuuntelu voidaan tehdä niin, ettei lähettäjä ja vastaanottaja huomaa mitään. Passiivinen salakuuntelu on vain verkkoliikenteen kuuntelua. Aktiivisessa salakuuntelussa lisätään jotain liikenteeseen. Salakuuntelussa on yleensä päästävä fyysisesti varsin lähelle kaapelointia tai verkkolaitteita. Radiotekniikkaan perustuvien kommunikointilinkkien salakuuntelu on siinä mielessä helpompaa ja riskittömämpää,

että fyysistä läheisyyttä ei tarvita. Voidaan kuitenkin olettaa, että kaikki kommunikointilinkit kahden verkon pisteen välillä ovat salakuunneltavissa. Varsinkin avoimissa verkoissa on suositeltavaa käyttää salausta datan luottamuksellisuuden turvaamiseksi.

Toisena esiintyessään hyökkääjä käyttää yleensä jotain seuraavista vaihtoehdoista:

- arvaa kohteen identiteetti- ja todentamistiedot, eli esimerkiksi käyttäjätunnus-salasana -yhdistelmän
- poimii identiteetti- ja todentamistiedot jostain aikaisemmasta kommunikoinnista, vaikkapa salakuuntelemalla
- kiertää tai tekee toimimattomaksi todentamismekanismin kohdekoneessa (yleensä käyttäen hyväksi jotain vikaa tai heikkoutta käyttöjärjestelmässä tai ohjelmistossa)
- käyttää kohdetta, jota ei todenneta (esimerkiksi joissain järjestelmässä olevat ”guest” ja ”anonymous” –käyttäjät, tai käyttää hyväksi järjestelmien välillä olevia luottamussuhteita)
- käyttää kohdetta, jonka todentamistiedot ovat tiedossa (esimerkiksi joissain laitteissa olevat tehtaan esiasettamat käyttäjätunnus-salasana –yhdistelmät)

Jo käsitellyt salakuuntelu ja toisena esiintyminen voivat johtaa *viestien luottamuksellisuuden rikkoutumiseen*. Myös eräät muut haavoittuvaisuudet voivat vaikuttaa luottamuksellisuuteen. Tällaisia ovat esimerkiksi väärinjakelu tai datan paljastuminen väliaikaisista puskureista, kun data matkaa verkon pisteiden välillä. Liikenneanalyysi on myös hyökkäys viestien luottamuksellisuutta vastaan.

Edeltävät kohdat ovat käsitelleet lähes pelkästään tietoliikenteen luottamuksellisuutta. Luottamuksellisuus on tietenkin erittäin tärkeää, mutta monissa tapauksissa *kommunikoinnin eheys* ja oikeellisuus on vähintään yhtä tärkeää. Hyökkääjä voi:

- muuttaa viestin sisällön (osittain tai kokonaan)
- korvata viestin kokonaan toisella
- käyttää uudelleen vanhaa viestiä
- muuttaa viestin näennäisen lähteen
- ohjata viestin väärään paikkaan

- tuhota viestin

Tällaisten hyökkäysten lähteitä voivat olla aktiivinen salakuuntelu, troijalaiset, toisena esiintyminen ja vallattu tietokonejärjestelmä.

Hakkeroijat voivat käyttää mitä tahansa hyökkäysten yhdistelmää päästäkseen tavoitteeseensa. Olennaista hakkeroinnissa on, että hyökkääjä voi kehittää automaattisia työkaluja, joilla voi nopeasti ja laajasti etsiä heikkouksia ja käyttää niitä hyväksi.

Vahingot ajettaville ohjelmistoille ovat vakava uhka verkkoympäristössä, koska kaikenlaiset vahinko-ohjelmat leviävät siellä erittäin tehokkaasti. Pahaa aavistamattomat käyttäjät saattavat ladata verkosta ohjelmia, jotka sisältävät vahinko-ohjelman joka taas muuttaa, korvaa tai tuhoaa muita ohjelmia. Erityisen nopeasti vahinko-ohjelmat leviävät sähköpostin liitetiedostoina. Joskus ohjelmien lataaminen verkosta tapahtuu ilman käyttäjän tietoa tai hyväksymistä.

Ihmiset tulevat koko ajan riippuvaisemmiksi toimivista tietoliikenneyhteyksistä. Näin ollen myös *palvelunestohyökkäysten* vaikutukset kasvavat. Palveluneston voi aiheuttaa verkkolaitteiden vikaantuminen, reititysongelmat, verkon tahallinen tukkiminen pakettitulvalla ja ohjelmistoissa olevien vikojen hyväksikäyttö.

2.4.2 Tietoturvamenetelmät verkoissa

Edellä käytiin läpi pitkä lista verkkoihin ja tietoliikenteeseen liittyviä uhkia ja hyökkäyksiä. Onneksi myös turvamenetelmiä on olemassa. Kenties tehokkaimpia niistä ovat salausmenetelmät. Monet perinteiset keinot kuten pääsynhallinta sekä käyttäjien ja järjestelmien todentaminen ovat välttämättömiä myös verkkoympäristössä.

Salausmenetelmät käsitellään myöhemmässä kappaleessa tarkemmin, mutta ne ovat ehkäpä tehokkain tekninen tietoturvamenetelmä. Salausmenetelmillä voidaan varmistaa datan luottamuksellisuus, autenttisuus ja eheys. Koska verkoissa uhkat ovat moninaisemmat, käytetään useasti tiedon salausta muiden menetelmien lisäksi. Verkkoympäristössä salausta voidaan käyttää periaatteessa millä tahansa

tietoliikenneprotokollan kerroksella. Useimmiten salausta kuitenkin käytetään joko kahden laitteen välillä tai kahden sovelluksen välillä (eli OSI-mallissa linkki- tai sovelluskerroksella). Myös verkkokerroksen salaus on suosittua (IPSec, Internet Protocol Security). Salausmenetelmiin liittyvä perinteinen ongelma on avainten jakelu luotettavasti.

Pääsynhallinta on erittäin tärkeää verkkoon liitetyssä koneessa, koska ei voida olla varmoja ketä kaikkia verkkoon on liittyneenä. Pääsyä voidaan rajoittaa esimerkiksi verkko-osoitteen perusteella. Yksittäiselle verkottomalle koneelle pääsyä voidaan rajoittaa fyysisesti. [Pfl97]

Verkkoresurssien etäkäytössä tarvitaan käyttäjän tai prosessin todentamista. Todentamisen on oltava sellainen, että toisena esiintyminen ei onnistu. Todentamiseen käytettävistä viesteistä ei saa paljastua salaisuus, johon todentaminen perustuu, ja todentamisen pitää olla sellainen ettei sitä voida myöhemmin toistaa. Todentaminen voidaan suorittaa luotettavasti kryptografian keinoilla. [Pfl97]

Datan eheys riippuu sen virheettömästä luomisesta sekä muuttumattomana varastoinnista ja siirtämisestä. Eheys siirron aikana voidaan varmistaa kryptografisella tarkistussummalla ja digitaalisella allekirjoituksella. [Pfl97]

Eräs käytetyimmistä verkkojen tietoturvamenetelmistä on palomuuri. Palomuurilla tarkoitetaan ohjelmia ja laitteita, joilla tarkkaillaan ja rajoitetaan kahden verkon välistä liikennettä. Palomuurilla yleensä suojellaan yksityisen verkon resursseja ulkopuolisten verkkojen käyttäjiltä, mutta sillä on myös mahdollista valvoa ja rajoittaa omien käyttäjien liikennettä verkon ulkopuolelle. Palomuuri tutkii jokaisen verkkoon tulevan ja sieltä lähtevän paketin, ja annettujen sääntöjen perusteella päättää saako paketti jatkaa matkaansa. [Shi00]

Virtuaalinen yksityisverkko (Virtual Private Network, VPN) on menetelmä, jolla voidaan yhdistää kaksi yksityistä verkkoa (tai käyttäjää) turvattoman verkon yli turvallisesti ja läpinäkyvästi. Yhdistäminen tapahtuu tunneloimalla liikenne kahden VPN-yhdyskäytävän välillä. Tunneloinnissa lähettävän pään yhdyskäytävä salaa

alkuperäisen paketin kokonaisuudessaan ja paketoi sen uuteen pakettiin. Paketti lähetetään vastaanottavan pään yhdyskäytävälle joka taas purkaa paketoinnin ja salauksen. Tämän jälkeen alkuperäinen paketti pääsee jatkamaan matkaansa vastaanottajalle. Erilaisia VPN-protokollia ovat mm. IPSec, PPTP (Point-to-Point Tunneling Protocol) ja L2TP (Layer Two Tunneling Protocol). [Shi00]

2.4.3 Internetin tietoturva

Internet on valtavan laaja erilaisista verkoista koostuva verkko, joka yhdistää kymmeniä miljoonia tietokoneita. Yhteys Internetiin on helposti kenen tahansa saatavilla ja Internetiin kytketty kone on saavutettavissa mistä tahansa verkon pisteestä riippumatta mistään kansallisista tai maantieteellisistä rajoista. Tämä on tiedon liikuteltavuuden kannalta erittäin kätevää ja mukavaa, mutta verkkoliittymän myötä tulee myös uhkia. Verkkoon liitettyyn koneeseen voidaan murtautua verkon yli ja verkossa liikkuvaa dataa voidaan kuunnella tai muunnella. Ja hyökkääjiä, joita käsiteltiin kappaleessa 2.2.3, riittää Internetin kymmenien miljoonien käyttäjien joukossa.

Internetiin kytketty kotitietokone on suosittu hyökkäyskohde. Tunkeutujat yrittävät löytää kotikoneilta rahanarvoista tietoa tai käyttää koneen resursseja hyödykseen (levytilaa, nopeaa Internet-yhteyttä). Varsin usein vallatun koneen resursseja käytetään hyökätessä muihin Internetin koneisiin. Näin hyökkääjä voi peittää jälkensä. Kotikoneille tunkeutuminen on usein varsin helppoa, koska keskivertokäyttäjällä ei yleensä ole tiedossa, että hänen tietoturvallisuutensa on verkottumisen takia uhattuna ja että hänen pitäisi jotenkin kiinnittää huomiota tietokoneensa turvallisuuteen.

Tunkeutujat murtautuvat koneelle käyttäen mm. seuraavia menetelmiä:

- Hyökkääjä lähettää sähköpostin, jonka liitteenä on ohjelma joka suoritetaan jos liite avataan. Ohjelma avaa tunkeutujalle järjestelmään tien, jonka kautta voi hallita konetta verkon yli. Toisin sanoen sähköpostin liitteenä lähetetään troijalainen, eli vahinko-ohjelma joka avaa koneelle ns. takaportin.
- Hyökkääjä käyttää hyväksi tietokoneen ohjelmistoissa olevia vikoja ja heikkouksia pääsyn saamiseksi.

- Hyökkääjä huijaa väärennetyllä sähköpostilla käyttäjän paljastamaan käyttäjätunnuksia ja salasanoja.
- Käyttäjä lataa verkosta ohjelman, joka ajettaessa asentaa takaportin tai tekee muuta vahinkoa.
- Käyttäjä käyttää helposti arvattavia salasanoja ja hyökkääjä saa pääsyn koneelle arvaamalla salasanan.

Muita Internetin käyttöön liittyviä tietoturvan kannalta huomion arvoisia asioita ovat esimerkiksi että sähköpostin turvallisuus on postikortin luokkaa – sen voi lukea monet ihmiset helposti ja sellainen on helppo väärentää. Verkon käytön yksityisyys on myös uhattuna, sillä esimerkiksi web-sivujen selailutottumuksia voidaan seurata erilaisilla menetelmillä. Varsinkin Internetin mainosfirmat tekevät tätä. [Gra02]

Käyttäjällä on myös onneksi keinoja puolustautua varsin tehokkaasti yleisimpiä uhkia vastaan:

- Asenna ja käytä virustentorjuntaohjelmistoa. Pidä virusmäärittelytiedostot ajan tasalla, jos ohjelma ei niitä automaattisesti päivitä. Tarkasta kaikki sähköpostien liitetiedostot ennen niiden avaamista/ajamista. Tarkasta kaikki verkosta ladatut ohjelmat ennen niiden suorittamista. Tarkasta kaikki koneen tiedostot säännöllisin väliajoin.
- Pidä käyttöjärjestelmä ja käyttämäsi ohjelmistot ajan tasalla päivittämällä ne valmistajan tarjoamilla päivityksillä. Päivityksillä korjataan usein vikoja ja heikkouksia, joita tunkeutujat käyttävät saadakseen pääsyn järjestelmään.
- Ole varovainen sähköpostin liitteiden kanssa. Sähköpostin liitetiedostoina on viime aikoina levinnyt paljon erilaisia haittaohjelmia. Sähköpostiohjelmassa ei missään nimessä kannata olla sellaista optiota päällä, että se avaa liitetiedoston automaattisesti. Ei edes liitteen esikatselua.
- Asenna ja käytä palomuuria. Palomuurilla voidaan tehokkaasti rajoittaa verkkopääsyä koneelle. Palomuurin sääntöjen kohdalleen saaminen vaatii työtä ja jonkun verran tietoa tekniikasta, mutta on oikein asennettuna hyvä suoja.
- Tee varmuuskopiot ainakin kaikista tärkeistä ja korvaamattomista tiedostoistasi. Paras vaihtoehto on tietysti varmuuskopio koko järjestelmästä, mutta se saattaa vaatia jo kohtuullisia sijoituksia. Varmuuskopiot kannattaa säilyttää niin ettei

niihin kuka tahansa pääse käsiksi ja mielellään fyysisesti eri tilassa kuin missä itse järjestelmä on.

- Käytä aina vahvoja salasanoja. Käytä aina riittävän pitkiä salasanoja, joissa on isoja ja pieniä kirjaimia ja erikoismerkkejä. Salasanoja ei saisi kirjoittaa muistiin, eikä samaa salasanaa pitäisi käyttää useassa paikassa.
- Ole varovainen, kun lataat ja asennat ohjelmistoja. Ohjelmistoista kannattaa ottaa selville mahdollisimman paljon ennen sen asentamista ja ajamista. Ohjelmiston vaikutus järjestelmään, ohjelmiston toiminta ja muiden käyttökokemukset ovat hyviä tietää.
- Käytä salausta, kun talletettavan/siirrettävän tiedon arvo sitä edellyttää.

Näillä keinoilla päästään varsin hyvälle tietoturvallisuuden tasolle kotioloissa. Jo pelkästään tietämys tekniikasta ja tietoturvan tarpeesta kannustaa panostamaan siihen. Tunkeutujat käyttävät yleensä automatisoituja hyökkäystyökaluja, eivätkä vaivaudu käyttämään aikaa hyvin puolustettua konetta vastaan hyökkäämiseen kun kohteita on runsaasti muutenkin. Suurin osa tunkeilijoista on vieläpä sellaisia, jotka eivät itse hallitse tekniikkaa syvällisesti vaan käyttävät verkosta saamiaan valmiita työkaluja. Tällaisilla hyökkääjillä ei edes ole tarvittavaa tietotaitoa monimutkaisten hyökkäysten toteuttamiseen.
[CERT01, CERT02]

2.5 Kryptologia

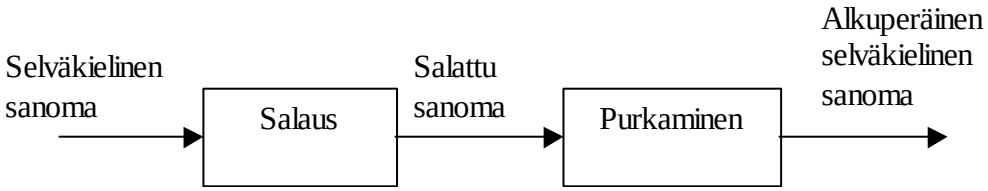
Kryptologia, eli ahtaasti tulkittuna salakirjoitustiede, pitää sisällään kaksi alihaaraa: kryptografian ja kryptoanalyysin. Kryptografiassa tutkitaan salaamiseen tarvittavia algoritmeja ja menetelmiä. Kryptoanalyysi puolestaan pyrkii murtamaan salauksia ja salausalgoritmeja. [Sch96]

Viime aikoina kryptologia on ymmärretty laajemmin käsittämään tietoturvatieteen kokonaisuudessaan, jolloin salakirjoitus on vain osa sitä. Muita tietoturvan elementtejä ovat autenttisuus, laillisuus, yksimielisyys, samanaikaisuus jne. [Ker99]

2.5.1 Kryptografia

Kryptografia ja siihen perustuvat menetelmät ovat paras tekninen keino toteuttaa tietoturvaa monissa tilanteissa, kuten avointen tietoverkkojen tietoturvaongelmien ratkaisussa. Kryptografiaa käytetään toteuttamaan tiedon luottamuksellisuutta, eheyttä, autentikointia ja kiistämättömyyttä (nonrepudiation). Kryptografian perustyökaluja ovat salausalgoritmit, tiivistefunktiot ja todistusmenetelmät.

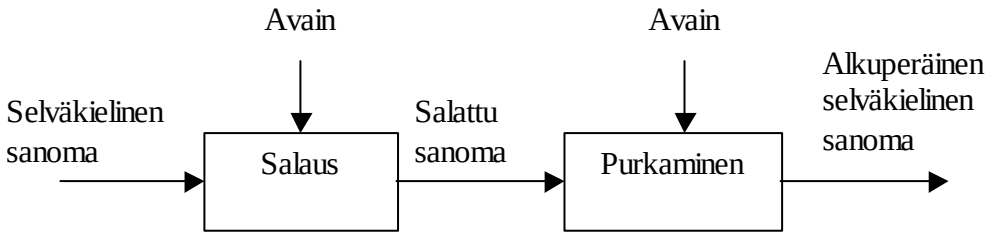
Salaaminen on matemaattinen menetelmä, jolla selväkielinen sanoma (plaintext) muutetaan (encryption) ulkopuoliselle käsittämättömään muotoon (ciphertext). Salaukseen kuuluu myös käänteinen menetelmä, jolla salakirjoitus puretaan eli tulkitaan (decryption). Kuva 2 esittää salaamisen ja purkamisen periaatteen.



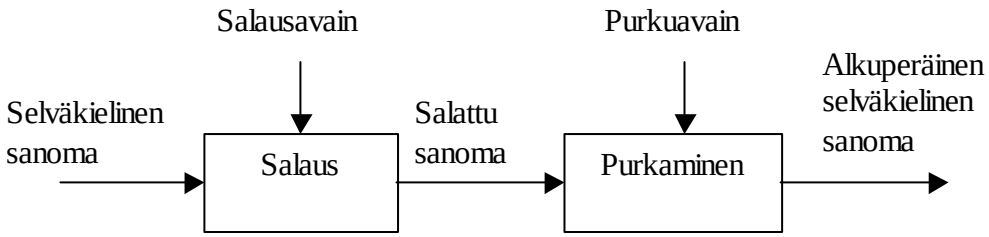
Kuva 2: Salaaminen ja purkaminen

[Ber98, Sch96]

Hyvän salausjärjestelmän tulee toteuttaa Kerckhoffin periaate, jonka mukaan järjestelmä on varma, vaikka sen salaus- ja purkuprosessien yksityiskohdat julkistetaan lukuun ottamatta salaista avainta. Eli kaikki turvallisuus algoritmeissa perustuu käytettyyn avaimeen (tai avaimiin). [Sch96] Joissakin algoritmeissa käytetään samaa avainta sekä salaamiseen että purkamiseen, ja tietyissä algoritmeissa salaamiseen käytetään eri avainta kuin purkamiseen. Kuva 3 ja kuva 4 esittävät näiden tapausten periaatteet.



Kuva 3: Salaaminen ja purkaminen samalla avaimella



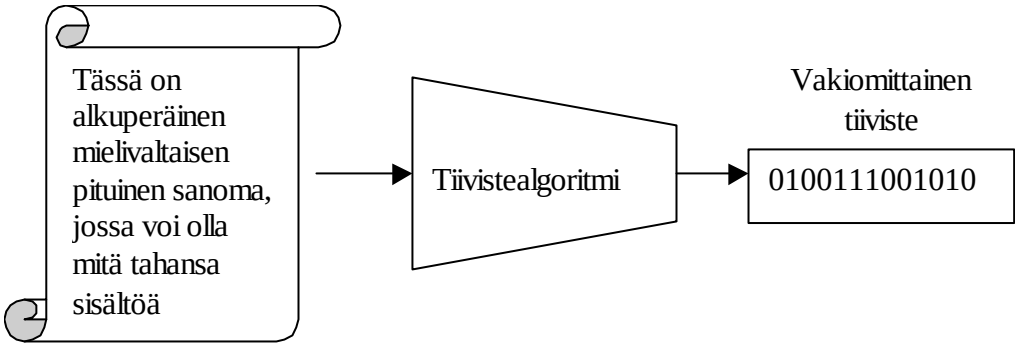
Kuva 4: Salaaminen ja purkaminen eri avaimilla

Salausalgoritmit ovat yleisellä tasolla jaoteltuna salaisen avaimen algoritmeja, eli symmetrisiä tai julkisen avaimen algoritmeja, eli asymmetrisiä. Symmetrisissä salausalgoritmeissa käytetään samaa avainta salaamiseen ja purkamiseen. Tämä tarkoittaa sitä, että kommunikoivien osapuolien, lähettäjän ja vastaanottajan, täytyy sopia käytettävästä avaimesta jollain luotettavalla tavalla ennen kuin voivat käyttää symmetristä salausmenetelmää viestiensä salaamiseen. Symmetrisen salauksen turvallisuus riippuu avaimesta ja sen salaisena pysymisestä. Symmetriset salausalgoritmit voidaan jakaa edelleen kahteen ryhmään: jonosalaajiin (stream cipher) ja lohkosalaajiin (block cipher). Jonosalaaja muuntaa selkotekstin salamuotoon bitti kerrallaan (joissain tapauksissa tavu tai merkki kerrallaan). Lohkosalaajissa selväkielinen teksti syötetään salausalgoritmin läpi lohko kerrallaan, eli useampi bitti tai merkki kerrallaan (tyypillinen lohkon koko on 64 bittiä). [Sch96]

Julkisen avaimen salausmenetelmässä käytetään salaamiseen ja purkamiseen eri avaimia, jotka ovat matemaattisesti toisistaan riippuvia siten, että tieto, joka on salattu toisella avaimella voidaan purkaa vain toista käyttäen. Näitä avaimia ei voi johtaa toisistaan (ainakaan missään järkevässä ajassa). Nimitys julkisen avaimen menetelmä tulee siitä, että toinen avaimista voidaan julkaista yleisesti ja halukkaat voivat käyttää

tuota avainta viestien salaamiseen, mutta vain vastaavan purkuavaimen haltija voi avata viestin. Purkuavain on pidettävä salaisena (yksityisenä). [Dif76]

Tiivistefunktiot (käytetään myös nimiä yksisuuntainen hash-funktio, sormenjälki ja kryptografinen tarkistussumma) ovat keskeisessä asemassa digitaalisissa allekirjoituksissa ja datan eheyden tarkistamisessa. Tiivistefunktio on funktio (kuva 5), joka ottaa syötteenä mielivaltaisen pituisen datan ja antaa tuloksena vakiomittaisen tiivisteen (tyypillinen tiivisteen pituus on 128 tai 160 bittiä). Sanoman tiivistämiseen hash-funktiolla ei tarvita erillistä avainta. Alkuperäistä sanomaa ei voida johtaa tiivisteestä. Hyvä tiivistefunktio on törmäysvapaa, eli on oltava erittäin hankalaa (tai mahdotonta) löytää kaksi erilaista dataa, joista tuotettu tiiviste on samanlainen. Tiivistearvo on siis tavallaan datan sormenjälki. Tiivistearvoja käytetään varmistamaan, että tiedon eheys on säilynyt siirron aikana. Näin voidaan myös varmistaa, että jollakin on tietty sama tiedosto kuin itsellä, mutta ei haluta lähettää tiedostoa verkon yli. Tiivistefunktioista on myös avaimellisia versioita (ns. avainnettu hash-funktio tai MAC-koodi, Message Authentication Code), joissa tiivisteen luontiin käytetään salaista avainta kuten symmetrisessä salauksessa. Teoria on muuten sama kuin tiivistefunktioissa, mutta tässä tapauksessa tiivistearvon voivat varmistaa vain ne, jotka tietävät avaimen. [Sch96]



Kuva 5: Yksisuuntaisen tiivistefunktion käyttö tiivisteen muodostamisessa

Digitaalinen allekirjoitus on tietoturvan yksi keskeisimpiä palveluja ja tietoturvaprotokollien rakennuspalikoita. Digitaalista allekirjoitusta voidaan käyttää henkilöiden ja ohjelmien todentamiseen, aineiston eheyden tarkistamiseen ja kiistämättömyyden (non-repudiation) toteuttamiseen. Digitaalinen allekirjoitus on

julkisen avaimen kryptografian sovellus (digitaalinen allekirjoitus voidaan toteuttaa myös pelkästään symmetristä salausta ja luotettua kolmatta osapuolta käyttäen, mutta se ei ole käytännössä toimiva ratkaisu). Käytännössä digitaalisen allekirjoituksen protokolla yleisellä tasolla toimii seuraavasti:

1. Allekirjoittava osapuoli (lähettäjä) laskee allekirjoitettavasta aineistosta yksisuuntaisen tiivisteen.
2. Allekirjoittava osapuoli salaa tiivisteen käyttäen yksityistä avaintaan, jota kukaan muu ei tunne, täten allekirjoittaen dokumentin.
3. Allekirjoittaja lähettää aineiston ja siitä tuotetun allekirjoitetun tiivisteen vastaanottajalle.
4. Vastaanottaja muodostaa saamastaan aineistosta tiivisteen. Seuraavaksi hän purkaa allekirjoitetun tiivisteen lähettäjän julkisella avaimella. Jos allekirjoitettu tiiviste vastaa generoitua tiivistettä, allekirjoitus on validi. Vain vastaavan salaisen avaimen haltija on voinut tehdä allekirjoituksen (kiistämättömyys).

Allekirjoitukseen voidaan sisällyttää halutessa aikaleima ja yksilöllinen sarjanumero, joilla estetään allekirjoituksen uudelleenkäyttö. [Sch96]

Edellä esitellyillä julkisen avaimen menetelmillä ei vielä pelkästään voida taata, että varmasti keskustelee haluamansa osapuolen kanssa (esim. pankin palvelimen kanssa). Joku voi esiintyä pankkina ja antaa oman julkisen avaimensa. Samoin pankki ei voi olla varma kenen kanssa on tekemisissä. Tämä ongelma voidaan ratkaista varmenteilla ja PKI:llä (Public Key Infrastructure). Varmenne on luotetun kolmannen osapuolen allekirjoittama tietorakenne, jolla julkinen avain sidotaan johonkin yksilölliseen tietoon (yksilöllinen nimi, henkilötiedot, sarjanumero tms.). Vaihtamalla varmenteita ja tarkistamalla luotetun osapuolen allekirjoitukset, keskustelevat osapuolet voivat varmistua olevansa tekemisissä sen kanssa kuin oli tarkoituskin.

2.5.2 Kryptoanalyysi

Kryptoanalyysissä pyritään löytämään salatun viestin selkoteksti ilman pääsyä salaamisessa käytettyyn avaimeen. Onnistunut kryptoanalyysi voi paljastaa pelkän

selkotekstin tai avaimen (ja sitä kautta selkotekstin). Voidaan myös löytää heikkous kryptosysteemistä (kryptosysteemi käsittää salausalgoritmin, kaikki mahdolliset selkotekstit, salatut tekstit ja avaimet), mikä johtaa näihin tuloksiin. Kryptoanalyysin yrittämistä kutsutaan hyökkäykseksi. Hyökkäykset (tai murrot) jaetaan neljään päätyyppiin. Kerckhoffin periaatteen mukaan kaikissa näissä oletetaan, että murtajalla on täydelliset tiedot käytetystä salausalgoritmista.

1. Tunnetun salasanoman murto (ciphertext-only attack) – murtautujalla on käytettävissään useita algoritmilla salattuja salasanomia. Hänellä ei ole käytössään selkokielisanomia eikä salaamiseen käytettyjä salaisia avaimia. Tehtävänä on löytää selväkieliset sanomat tai mieluummin avaimet.
2. Tunnetun selkokielisanoman murto (known-plaintext attack) – murtautujalla on käytössään salasanomia ja niitä vastaavat selkotekstit. Tehtävänä on löytää salaamiseen käytetty avain tai löytää algoritmi, jolla voidaan purkaa uudet salasanomat joiden salaamiseen on käytetty samaa avainta.
3. Valitun selkokielisanoman murto (chosen-plaintext attack) – murtautujalla on käytössään salasanomia ja niitä vastaavat selkokielisanomat, ja lisäksi hän pääsee valitsemaan salattavat selkotekstit. Tämä on tehokkaampi kuin tunnetun selkokielisanoman murto, koska murtautuja voi valita sellaiset salattavat selkokielitekstit, jotka saattavat antaa lisätietoa avaimesta. Tavoite on sama kuin edellisessä hyökkäyksessä.
4. Adaptiivinen valitun selkokielisanoman murto (adaptive-chosen-plaintext attack) – tämä on erikoistapaus valitun selkokielisanoman murrosta. Sen lisäksi, että murtautuja voi valita salattavan selkotekstin, hän voi myös muuttaa valintaansa edellisen salauksen tuloksien perusteella. Valitun selkokielisanoman murrossa murtautuja saattaa saada vain yhden suuren valitun selkotekstin salattua. Adaptiivisessa murrossa murtautuja voi valita pienemmän selkotekstin ja sen jälkeen toisen, ja niin edelleen.

Kaikki mainitut murtotyypit ovat mahdollisia ja niistä kaksi ensimmäistä yleisimpiä. Suoraviivaisin tapa yrittää murtaa salaus on käydä läpi kaikki avainvaihtoehdot (brute-force attack). Tämä on tunnettu selkokielisanomamurto ja edellyttää vain pientä salasanoman ja sitä vastaavan selkokielisanoman tuntemista. Salasanomaa yritetään

purkaa systemaattisesti avain kerrallaan niin kauan kunnes purettu sanoma on sama kuin tunnettu selväkielisanoma. Kun näin tapahtuu, algoritmin salainen avain on löytynyt.

Usein kuitenkin tehokkain tapa hyökätä salausalgoritmia vastaan on niiden kanssa tekemisissä olevien ihmisten kautta. Murtautuja/hyökkääjä huijaa, uhkailee, kiristää, kiduttaa tai lahjoo saadakseen avaimen haltuunsa.
[Sch96, Ker99]

3 LANGATTOMAT LÄHIVERKOT JA IEEE 802.11

Tässä luvussa käydään läpi langattomaan lähiverkkoon liittyviä perusasioita. Käsitellään langattomia lähiverkkoja yleisesti, niihin liittyviä tekniikoita, protokollia ja standardeja sekä erityisesti langattomuuteen liittyviä tietoturvaongelmia. Tarkemman tarkastelun saa IEEE 802.11b-standardi tietoturvaratkaisuineen.

3.1 Langattoman lähiverkon perusteet

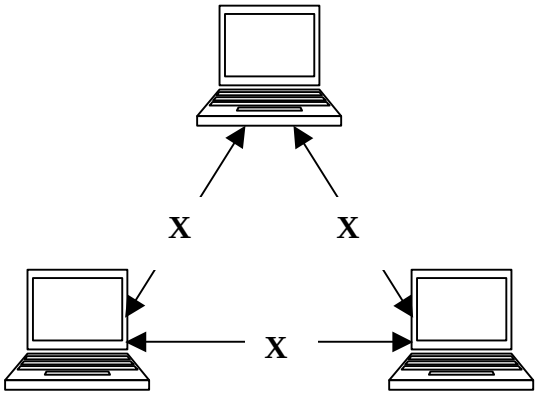
Lähiverkko (Local Area Network, LAN) yhdistää tietokonelaitteita ja mahdollistaa niiden välisen kommunikoinnin. Yleensä lähiverkko toimii pienellä maantieteellisellä alueella ja kattaa yhden rakennuksen tai organisaation. Lähiverkko ja siihen yhdistetyt laitteet ovat usein yhden organisaation omistuksessa. Lähiverkkojen sisäiset siirtonopeudet ovat yleensä huomattavasti suurempia kuin laajemmalla alueella toimivien verkkojen. Ylivoimaisesti suosituin lähiverkkotyyppi on Ethernet. [Sta97b]

Perinteisessä lähiverkossa laitteiden yhdistäminen tapahtuu kaapeloinnilla. Langattomassa lähiverkossa (Wireless LAN, WLAN), kuten nimikin jo kertoo, kaapelointi on korvattu langattomilla yhteyksillä. Joustavuuden ja liikkuvuuden ansiosta langattomat lähiverkot ovat houkuttelevia vaihtoehtoja langalliselle verkolle. Niitä voidaan käyttää laajentamaan perinteisiä verkkoja ja niillä on helppo kattaa paikkoja, joiden kaapeloiminen on hankalaa (esim. aukeat tehdashallit). Langattomien lähiverkkojen suosio on viime vuosina kasvanut rajusti sen ansiosta, että markkinoille on saatu standardoituja laitteita, joiden tiedonsiirtonopeus alkaa olemaan kilpailukykyinen langallisten verkkojen kanssa. Langaton lähiverkko tarjoaa kaiken langallisten verkkojen toiminnallisuuden ilman johtojen aiheuttamia fyysisiä rajoituksia. [Sta97a]

3.1.1 Ad hoc –verkko

Yksinkertaisimmillaan langaton lähiverkko on sellainen, jossa kaksi tai useampi langattomalla sovittimella (verkkokortilla) varustettua laitetta kommunikoivat suoraan

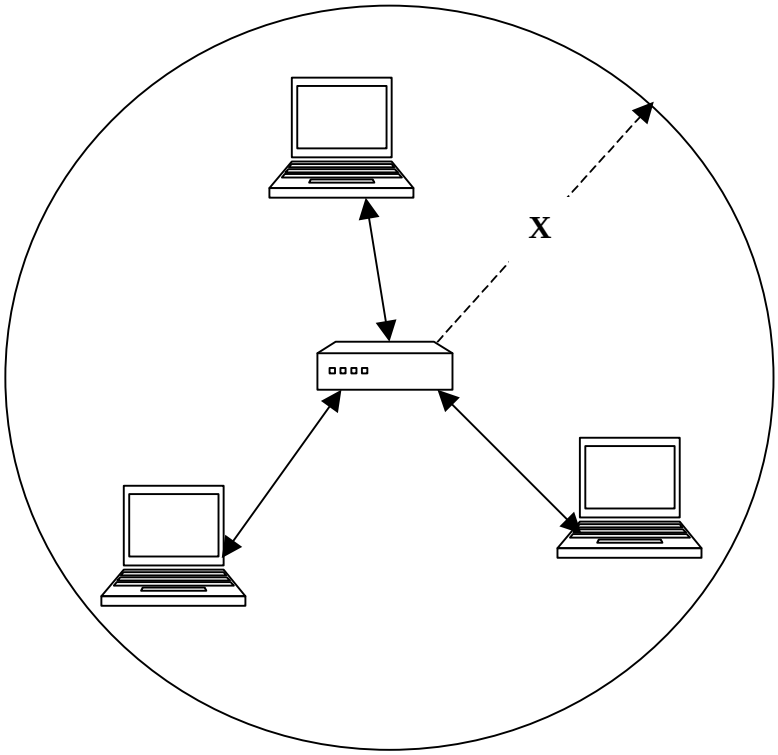
keskenään (ks. kuva 6). Tällaista itsenäistä verkkoa kutsutaan ad hoc –verkoksi (tai peer-to-peer, eli vertaisverkoksi). Voidaan puhua myös ns. yhden solun verkosta. Ad hoc –verkon etuihin kuuluu, että sellainen voidaan järjestää vaivatta tarpeen vaatiessa. Mitään etukäteiskonfigurointia tai erillistä verkonhallintaa ei yleensä tarvita. [Gei99]



Kuva 6: Ad hoc -verkko

3.1.2 Infrastruktuuriverkko

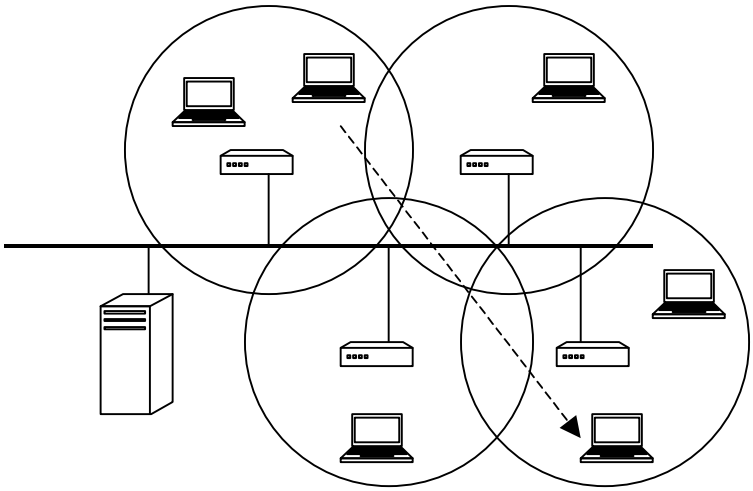
Kun verkkoon lisätään tukiasema, puhutaan infrastruktuuriverkosta. Kuva 7 esittää yksinkertaisinta infrastruktuuriverkkojärjestelyä. Tukiasema toimii toistimena, jonka kautta kaikki langattomien asiakaskoneiden toisilleen lähettämä liikenne kulkee. Tukiasema kasvattaa verkon kantaman jopa kaksinkertaiseksi ad hoc –verkkoon nähden. Tukiasemana voi toimia tavallinen langattomalla verkkokortilla varustettu tietokone tai erillinen tukiasemalaite. [WLANA]



Kuva 7: Yksinkertainen infrastruktuuriverkko

Kun halutaan koota laajempi langaton lähiverkko ja siihen lisätään useampia tukiasemia, on ne liitettävä toisiinsa jollakin tavalla, jotta eri tukiasemien alueilla olevat asiakaskoneet voivat liikennöidä keskenään. Usein tukiasemia yhdistävä siirtoverkko on perinteinen langallinen verkko. Tällöin tukiasemat toimivat siltoina langallisen ja langattoman verkon välillä. Myös tukiasemien liittäminen toisiinsa langattomasti on mahdollista.

Langaton lähiverkko voidaan rakentaa siten, että tukiasemien peittoalueet ovat osittain päällekkäisiä. Tällöin käyttäjän on mahdollista liikkua peittoalueelta toiselle ilman yhteyden katkeamista. Yhteys verkkoon säilyy, vaikka käytettävä tukiasema vaihtuu käyttäjän sijainnin mukaan. Vaihdokset samaan langattomaan lähiverkkoon kuuluvien tukiasemien välillä ovat käyttäjälle näkymättömiä. Tekniikkaa kutsutaan nimellä roaming. Kuva 8 esittää infrastruktuuriverkkoa ja roamingin periaatetta siinä.



Kuva 8: Infrastruktuuriverkko ja roaming

3.1.3 Langattomat yhteydet

Ylivoimaisesti suosituin siirtotekniikka, eli fyysisen kerroksen ratkaisu, langattomissa lähiverkoissa on radioaallot. Muita langattomiin yhteyksiin käytettyjä tekniikoita ovat esimerkiksi infrapuna ja laser. Radioaaltojen hyvänä puolena on, että yhteyden saamiseksi ei tarvitse olla näköyhteyttä lähettimen ja vastaanottimen välillä. Radioaallot pystyvät läpäisemään jonkun verran esteitä, kuten seiniä, ja mahdollistavat kunnollisen liikkuvuuden lähiverkon käyttäjille.

Radioaaltojen huonona puolena on, että ne ovat alttiita häiriöille. Jos langattoman lähiverkon käyttöalueella on laitteita, jotka käyttävät samoja taajuusalueita, saattaa syntyä interferenssiä, joka laskee verkon suorituskykyä tai estää sen toiminnan kokonaan (tämä pätee varsinkin perinteisille kapeakaistalähetyksille). Laajalle ympäristöön leviävät radioaallot aiheuttavat myös tietoturvariskin. Luvattomat tahot voivat kuuluvuusalueella salakuunnella verkossa lähetettävää dataa.

Suosituin radiotekniikka langattomissa lähiverkoissa on hajaspektritekniikka (Spread Spectrum, SS), joka on alun perin sotilaskäyttöön kehitetty laajakaistatekniikka. Hajaspektritekniikalla lähetettäessä alkuperäinen signaali hajautetaan laajalle taajuusalueelle, ja vastaanotettaessa kasataan alkuperäiseen muotoonsa. Hajautuksen ansiosta lähetystehon tiheys (mitattuna tehoyksikköä/hertsi) on paljon pienempi kuin

samalla kokonaisteholla lähettävän kapeakaistaradion. Tämä mahdollistaa sen, että kapeakaista- ja hajaspektrilähetykset voivat jakaa saman taajuusalueen aiheuttamatta toisilleen juurikaan häiriöitä. Satunnaiselle vastaanottimelle hajaspektrisignaali näyttää taustakohinalta, jos tiedossa ei ole hajaspektrisignaalin muodostamiseen käytettyjä parametreja. Muut radiolähetykset ja elektroninen kohina, jotka ovat tyypillisesti luonteeltaan kapeakaistaisia, häiritsevät vain pientä osaa hajaspektrisignaalista. Hajaspektritekniikka uhraa tehokkuutta kaistanleveyden käytön suhteen, jotta saavutetaan luotettavat, eheät ja turvalliset tiedonsiirtoyhteydet. Kaksi tärkeintä hajaspektritekniikkaa ovat suorasekvenssihajaspektri (Direct Sequence Spread Spectrum, DSSS) ja taajuushyppelyhajaspektri (Frequency Hopping Spread Spectrum, FHSS). [WLANA, Gei99]

Taajuushyppelyhajaspektrissä käytetään kapeakaistaista kantoaaltoa, jonka taajuutta vaihdetaan tietyn kaavan mukaan lyhyin väliajoin. Eli signaali hyppii taajuudelta toiselle ajan funktiona ja yhdellä taajuudella viivytään kerrallaan vain lyhyt aika. Mikäli jollain taajuudella häiriö estää lähetyksen, tehdään uudelleenlähetys kun hypätään seuraavalle taajuudelle. [Sch90, Dea97]

Suorasekvenssihajaspektritekniikkaan perustuvissa lähetyksissä alkuperäinen signaali (eli lähetettävä tieto / informaatiokaista) moduloidaan sitä paljon laajakaistaisemmalla digitaalisella signaalilla. Käytännössä siis alkuperäisen datan bitit muunnetaan ennen lähetystä esitettäväksi useammalla bitillä. Digitaalista signaalia, jonka mukaan tämä muunnos tehdään, sanotaan hajautuskoodiksi. Vastaanottajan on tiedettävä myös tämä koodi, jotta alkuperäisen datan kokoaminen on mahdollista. Suorasekvenssilähetyksen redundanttisuuden ansiosta on mahdollista selvittää alkuperäinen signaali, vaikka osa lähetyksestä kärsisikin häiriöistä. Suorasekvenssitekniikalla päästään huomattavasti suurempiin tiedonsiirtonopeuksiin kuin taajuushyppelytekniikalla. [Sch90, Dea97]

3.1.4 Langattomien lähiverkkojen standardointi

Tietokoneverkot ja radiotekniikka yhdistettiin ensimmäisen kerran jo vuonna 1971 ALOHANET-projektissa Havaijin yliopistossa. Radiotekniikkaan perustuvien lähiverkkokomponenttien kaupallisen kehittämisen mahdollisti Pohjois- ja Etelä-

Amerikassa 1980-luvun puolivälissä tehty päätös vapauttaa niin sanotut ISM-kaistat (Industrial, Scientific and Medical bands) julkiseen käyttöön. Nämä taajuuskaistat ovat 902-928 MHz, 2.40-2.4835 GHz ja 5.725-5.850 GHz, eikä niitä käyttäville laitteille tarvitse hakea erillistä lupaa. Euroopassa ja Aasiassa 2.4 GHz ISM-kaista hyväksyttiin 1995 ja tämä kaista onkin lähes maailmanlaajuisesti lisenssivapaa. Valmistajakohtaisia ratkaisuja alkoikin ilmestyä pian 1980-luvun päätöksen jälkeen (lähinnä Yhdysvalloissa ja 902 MHz kaistalle), mutta markkinoiden kiinnostus langattomia lähiverkkoja kohtaan pysyi vähäisenä vuoden 1997 loppuun saakka, jolloin ilmestyi ensimmäinen virallinen ja kansainvälisesti hyväksytty standardi langattomille lähiverkoille. Kyseessä oli IEEE:n (Institute for Electrical and Electronic Engineers) standardi 802.11, jota käsitellään kappaleessa 3.3 tarkemmin. [Gei99]

Eurooppalainen ETSI (the European Telecommunications Standards Institute) on myös kehittänyt oman langattomien lähiverkkojen standardin nimeltään HIPERLAN (High Performance Radio Local Area Network). Nykyään on meneillään toisen sukupolven HIPERLANin kehitystyö (HIPERLAN/2), jonka ensimmäinen versio julkaistiin vuonna 2000. HIPERLAN/2 käyttää 5GHz:n taajuuskaistaa. HIPERLAN on jäänyt häviölle suosiossa IEEE:n 802.11 standardille.

Standardoinnista on monia hyötyjä: Eri valmistajien tietyn standardin mukaiset laitteet ovat (ainakin periaatteessa) keskenään yhteensopivia. Valmistajien tuotekehitys nopeutuu ja siihen kuluu vähemmän resursseja. Mikäli standardoitu tuote osoittautuu suosituksi, markkinoille tulee useampia valmistajia, mistä seuraa hintakilpailua. Kuluttajille standardi näkyy siis paremman yhteensopivuuden lisäksi hintojen laskemisena. [Gei99]

Edes saman standardin mukaiset langattoman lähiverkon laitteet eivät välttämättä ole yhteensopivia keskenään. Tähän on käytännössä kolme syytä. Ensinnäkin standardissa voi olla määriteltynä useampi protokolla jonkun asian toteuttamiseen, ja eri protokollat eivät toimi yhdessä. Esimerkiksi 802.11 standardissa on fyysisen kerroksen radioprotokollavaihtoehtoina suorasekvenssi- ja hajaspektritekniikat, jotka ovat toteutustavoiltaan erilaisia. Toiseksi eri taajuuskaistaa käyttävät ratkaisut eivät toimi keskenään vaikka käyttäisivätkin samaa tekniikkaa ja protokollia. Kolmanneksi eri

valmistajien laitteet eivät välttämättä toimi keskenään vaikka käyttäisivätkin samaa tekniikkaa ja taajuuskaistaa. Eri valmistajien toteutustavoissa voi olla eroavaisuuksia, jotka estävät yhteentoimivuuden. [Sep00]

3.2 Langattoman lähiverkon tietoturvaongelmia

Radiotekniikkaan perustuvat langattomat lähiverkot (samoin kuin kaikki langattomat verkot) ovat luonnostaan turvattomampia kuin langalliset lähiverkot. Langaton lähiverkko ja siinä liikkuva data on altis kaikille samoille hyökkäyksille kuin perinteinen langallinen verkko, mutta langattoman verkon turvattomuutta lisää se, että radioaallot läpäisevät fyysisiä esteitä ja leviävät joka puolelle lähettimen ympäristöön.

Lähetetty, ja mahdollisesti luottamuksellinen data voidaan siis kuulla vaikkapa toimiston seinien ulkopuolelta, mikäli kuuntelijalla on käytettävissään sopiva vastaanotin. Langattoman verkon, jota ei ole suojattu millään keinoin, asentaminen merkitsee langallisen verkon termeillä kuvattuna tilannetta, jossa verkkoon pääsyyn tarvittavia pistokkeita asennetaan kaikkialle ympäristöön. Näin hyökkääjälle avautuu pääsy organisaation verkon sisäisiin osiin vaikkapa toimiston läheiseltä parkkipaikalta. [Cis01] Toisin sanoen langattomaan verkkoon hyökkääminen ei tarvitse mitään fyysisiä erikoisjärjestelyjä. Perinteisessä langallisessa verkossa turvallisuus saavutetaan fyysisesti rajoittamalla pääsyä verkon komponentteihin. Hyvin turvatuissa tiloissa voidaan olla suhteellisen varmoja siitä, ettei verkkoon ole liitetty mitään ylimääräisiä tai luvattomia laitteita. Kun fyysinen turvaaminen ei ole mahdollista, paras ratkaisu verkon yhteyksien suojaamiseen on käyttää kryptografisia menetelmiä. [Aso95]

Mahdollisia langattomiin lähiverkkoihin kohdistuvia hyökkäyksiä ovat esimerkiksi salakuuntelu, palvelunesto, verkon resurssien luvaton käyttö, liikenneanalyysi ja liikenteen toisto sekä väärentäminen. Myös siirtyvän luottamuksen hyväksikäyttö voi olla mahdollista. Näitä käsitellään tarkemmin seuraavissa kappaleissa.

3.2.1 Salakuuntelu

Salakuuntelu on hyökkäys verkossa liikkuvan datan luottamuksellisuutta vastaan ja luultavasti yleisin uhka langattomille lähiverkoille. Radioliikennettä voidaan ottaa vastaan täysin passiivisesti, joten salakuuntelua ei pystytä havaitsemaan. Kuuntelemalla verkkoliikennettä voidaan saada selville käyttäjätunnuksia, niihin liittyviä salasanoja ja muuta tärkeää dataa. Salasanojen avulla voidaan saada edelleen parempi pääsy verkkoresursseihin ja dataan. Ratkaisu tähän on käyttää salausta ainakin silloin kun dataa siirretään radiotiellä.

Hajaspektritekniikkaan perustuvien langattomien lähiverkkojen on sanottu olevan turvallisia, koska hajaspektrilähetyksiä on vaikea havaita ja ottaa vastaan, jos hajautuksessa käytettävät parametrit eivät ole tiedossa. Tämä pitääkin paikkaansa tietyssä määrin, kun on kyse valmistajakohtaisista laitteista, joita ei ole yleisesti saatavilla, eikä myöskään tietoa niiden määrityksistä. Tosin riittävillä resursseilla ja taidoilla varustettu henkilö pystyy saamaan selville mitkä tahansa hajaspektritekniikkaan perustuvat lähetykset. [Sch90]

Kun on kyse yleiseen standardiin perustuvasta tekniikasta, ei voida missään tapauksessa luottaa hajaspektritekniikan tuovan yksityisyyttä langattoman verkon yli tehtäviin yhteyksiin. Jotta tietyn standardin mukaiset laitteet toimisivat keskenään yhteensopivasti, on standardissa kerrottava miten hajaspektritekniikkaa käytetään. Tämä mahdollistaa sopivan vastaanottimen rakentamisen. Yleensä on myös mahdollista modifioida langatonta verkkosovitinta siten, että sillä voi ottaa kaiken liikenteen vastaan. Edelleen erinäisistä rajoituksista johtuen kaupallisissa tuotteissa ei yleensä voida hajauttaa yhteyttä erityisen laajalle taajuuskaistalle, mikä helpottaa havaitsemista.

Salakuunteluun liittyy liikenneanalyysi. Koska radioliikenne on helppoa kuunnella, voidaan tehdä liikenneanalyysi, vaikka verkossa liikkuvan pakettimuotoisen datan hyötykuorma olisikin salattu vahvasti.

3.2.2 Palvelunesto

Vakava uhka langattomille lähiverkoille on myös mahdollinen palvelunestohyökkäys. Radiotekniikkaan perustuvan lähiverkon liikennöinti voidaan estää lähettämällä riittävästi häiriötä radiotielle. Hajaspektritekniikka auttaa selviämään suhteellisen pahoistakin häiriöistä niin, että verkko toimii vaikkakin tiedonsiirtonopeudet laskevat. Mutta verkon toiminnan kokonaan estävän laajakaistaisen häirintälaitteen rakentaminen on mahdollista ja onnistuu jopa kohtuullisen pienillä resursseilla. Radiotien häirinnästä on erittäin vaikeaa saada syyllistä kiinni ja vastuuseen teostaan. [Rus01]

3.2.3 Luvaton pääsy

Jos langattomassa lähiverkossa ei ole mitään menetelmiä, joilla tunnistetaan ja todennetaan verkkoon liittyvät laitteet, ei myöskään ole mahdollista rajoittaa pääsyä verkkorajapintaan. Jos pääsynhallintaa ei ole järjestetty, on luvattomien tahojen mahdollista päästä käsiksi verkon resursseihin pitkänkin matkan päästä, koska radioverkko ei välttämättä rajoitu fyysisiin esteisiin. Langattomassa lähiverkkotekniikassa tulisikin olla tehokas keino, jolla verkkoon kuuluvat laitteet voivat todentaa itsensä. Luvaton pääsy voi johtaa laajempaankin murtoon, esimerkiksi verkossa oleville palvelimille. Luvaton pääsy verkkoresursseihin voi olla myös esimerkiksi Internet-yhteyden luvatonta käyttöä.

3.2.4 Siirtyvä luottamus

Langallisessa verkossa on aina mahdollista jäljittää päätelaitteelta lähtevä verkkokaapeli seuraavaan verkkosolmuun, jolloin tiedämme ainakin jossain määrin kenen kanssa olemme tekemisissä. Langattomassa ympäristössä tämä ei ole niin suoraviivaisesti mahdollista. Langattomassa lähiverkossa on tietoturvan kannalta oleellista, että keskustelevat laitteet voivat todentaa toisensa.

Mikäli keskinäistä todentamista ei langattomassa lähiverkkotekniikassa ole, on siirtyvän luottamuksen hyökkäys mahdollinen. Siinä pyritään saamaan langattomat päätelaitteet luottamaan hyökkääjän omaan tukiasemaan. Yleensä, kun langaton päätelaite kytketään päälle, se pyrkii kirjautumaan verkkoon, jonka signaali on vahvin. Mikäli hyökkääjä saa

asennettua sopivaan paikkaan tukiaseman, jossa on voimakas lähetysteho, saattavat päätelaitteet kirjautua ensin tähän kyseiseen verkkoon. Hyökkääjä voi yrittää naamioida oman verkkonsa muistuttamaan yrityksen verkkoa, ja tallentaa syntyvän liikenteen saaden näin salasanoja ja muuta tärkeää tietoa. Hyökkääjä voi myös vain yksinkertaisesti tallentaa päätelaitteiden kirjautumisyrityksistä syntyvän liikenteen ja yrittää löytää siitä hyödyllistä tietoa.

Toinen tapa siirtyvän luottamuksen hyökkäykseen on yrittää saada verkko luottamaan hyökkääjän langattomaan päätelaitteeseen. Tällaiset ja monet muutkin hyökkäykset voidaan estää vahvalla keskustelevien laitteiden keskinäisellä todentamisella. Todentaminen on suoritettava niin, ettei todentamiseen tarvittavia salaisuuksia lähetetä verkon yli. Todentaminen ja siihen liittyvä pääsynhallinta on hyvä toteuttaa langattomassa verkossa linkkitasolla.
[Usk97]

3.2.5 Muut hyökkäykset

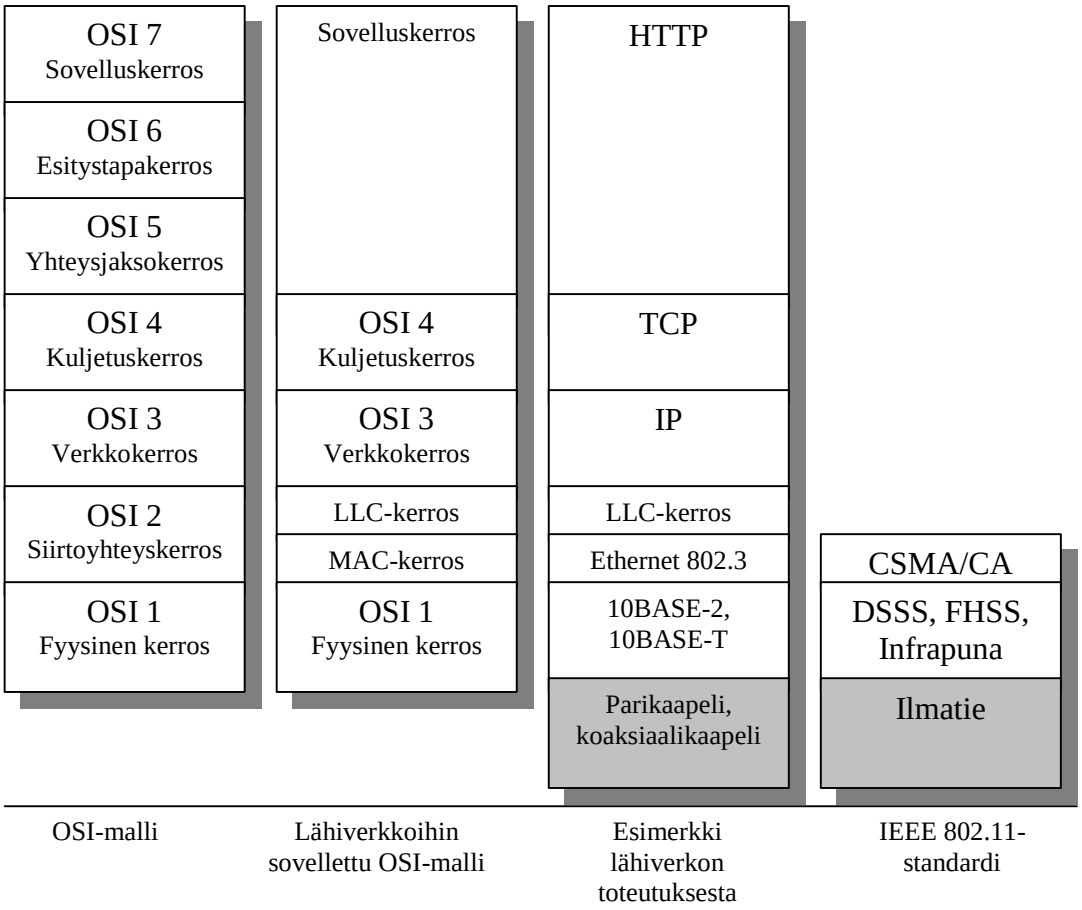
Toisto ja väärentäminen voivat olla mahdollisia riippuen langattoman lähiverkkotekniikan ominaisuuksista. Nämä ovat monimutkaisempia hyökkäyksiä, joita saatetaan käyttää osana muita hyökkäyksiä tai itsenäisinä. Mikäli tietoturvaa ei ole otettu riittävässä määrin huomioon tekniikkaa määritellessä, voi verkko olla käytännössä turvaton kaikkia edellä esiteltyjä hyökkäyksiä vastaan. Sama kyllä pätee tekniikan osalta myös langallisiin verkkoihin, mutta siellä pääsyä voidaan rajoittaa fyysisillä turvajärjestelyillä, kuten aiemmin jo todettiin.

3.3 IEEE 802.11

IEEE sai ensimmäisenä tahona aikaan kansainvälisesti hyväksytyn standardin langattomille lähiverkoille vuonna 1997. Korjattu versio standardista valmistui vuonna 1999. Standardi määrittelee MAC-kerroksen (Media Access Control) ja kolme erilaista fyysistä kerrosta (DSSS, FHSS ja infrapuna). Nämä protokollakerrokset sijoittuvat OSI-mallissa kahdelle alimmalle tasolle. OSI-mallissa kommunikointijärjestelmä esitetään

seitsemänä kerroksena, joilla jokaisella on erilainen toiminnallisuus. Kuvassa 9 esitetään 802.11-standardin suhtautuminen OSI-malliin. [ISO94, IEEE97, IEEE99a]

802.11-standardi tukee kahta erilaista verkkotopologiaa, joista käytetään standardissa nimitystä IBSS (Independent Basic Service Set) ja ESS (Extended Service Set). IBSS on ad hoc –verkko, jossa on vain keskenään keskustelevia langattomia liikkuvia asemia, eikä yhteyttä langalliseen verkkoon. ESS on infrastruktuuriverkko, johon kuuluu tukiasemia ja niitä yhdistävä siirtojärjestelmä (distribution system, joka usein on perinteinen langallinen verkko). Mikäli verkossa on mukana tukiasema, kaikki eri asemien välinen liikenne kulkee tukiaseman kautta. Liikkuva asema assosioituu yhteen tukiasemaan kerrallaan ja kaikki liikenne kulkee sen tukiaseman kautta johon asema on assosioitunut. Roaming ESS:n sisällä on myös määritelty. [Oha99] 802.11:n toiminnallisuus sijaitsee fyysisesti langattomassa verkkokortissa, verkkokortin ajurissa ja tukiasemassa [Tou00].



Kuva 9: Erilaisten protokollapinojen suhtautuminen OSI-malliin [Sep00]

3.3.1 Fyysinen kerros

Fyysinen kerros on se osa, joka on tekemisissä siirtomedian kanssa. Radiotekniikkaan perustuvassa langattomassa lähiverkossa siirtomediana toimii ilma ja fyysistä kerrosta voidaan kutsua myös nimellä radiomodeemi. Radiomodeemin pääominaisuuksia ovat sen käyttämä taajuuskaista, signalointinopeus, modulaatiotekniikka ja lähettimen teho. [Tou00]

802.11-standardi määrittelee kolme erilaista vaihtoehtoa fyysiselle kerrokselle. Nämä ovat DSSS, FHSS ja infrapuna. Infrapunaa käyttäviä toteutuksia ei ole markkinoilla juurikaan, joten sitä ei käsitellä tässä tarkemmin. Alkuperäisen, vuoden 1997, määrittelyn mukaan DSSS ja FHSS toimivat 2.4 GHz ISM-kaistalla ja niiden kummankin tiedonsiirtonopeuksiksi määriteltiin 1 Mb/s ja 2 Mb/s (signalointinopeus,

hyötykuorman osalta käyttäjän saama läpäisy jää yleensä noin puoleen signalointinopeudesta 802.11-tuotteissa). FHSS 2 Mb/s nopeuden toteuttaminen on vapaaehtoista. [IEEE97]

Vuonna 1999 valmistui standardin laajennus 802.11b. Siinä määriteltiin nopeampi 2.4 GHz kaistaa käyttävä fyysinen kerros. DSSS laajennettiin tukemaan 5.5 sekä 11 Mb/s nopeuksia [IEEE99c]. 802.11b-standardin mukaiset tuotteet ovat osoittautuneet erittäin suosituiksi tarjoamansa riittävän suuren tiedonsiirtonopeuden ansiosta.

802.11 standardin fyysisen kerroksen kehittämistä on jatkettu erinäisissä työryhmissä. Meneillään oleva työryhmä 802.11g kehittää laajennusta 802.11b standardiin, jolla voidaan päästä teoriassa 54 Mb/s nopeuteen. Työryhmä g on saanut standardin luonnoksen valmiiksi (tilanne 03/2003). Työryhmä a kehitti 5GHz:n taajuusalueella toimivan fyysisen kerroksen, jolla on mahdollista saavuttaa 54 Mb/s nopeus. 802.11a standardi julkaistiin vuonna 1999. [IEEE99b, IEEE03]

3.3.2 MAC

MAC-kerroksen tehtävänä on ohjata siirtomedian käyttöä. Tämä tapahtuu kanavapääsymekanismin (channel access mechanism) avulla. Se jakaa pääresurssin, eli tässä tapauksessa radiotien, verkon osapuolten kesken. Kanavapääsymekanismi on MAC-kerroksen ydin ja se kertoo jokaiselle verkon liikennöitsijälle koska voi lähettää dataa ja koska pitää kuunnella verkkoa. [Tou00] MAC-kerros sisältää myös standardin määrittelemät tietoturvapalvelut, jotka ovat luottamuksellisuus, autentikointi ja pääsynvalvonta. Standardin puitteissa nämä tietoturvaominaisuudet ovat rajatut koskemaan vain langattomasti tapahtuvaa kahden aseman välistä liikennettä. [IEEE97] Tietoturvallisuuteen liittyvät 802.11:n ominaisuudet käsitellään myöhemmin omassa kappaleessaan.

802.11:ssä määritellään kaksi median koordinointifunktiota (kanavapääsymekanismia), hajautettu (Distributed Coordination Function, DCF) ja keskitetty (Point Coordination Function, PCF). 802.11:n peruskanavapääsymekanismi on hajautettu koordinointifunktio, joka tunnetaan nimellä CSMA/CA (Carrier Sense Multiple

Access/Collision Avoidance). Sen pääperiaatteina on kuunnella ennen kuin lähettää ja kilpavaraus (contention). [IEEE97] Ennen lähettämistä kuunnellaan onko media varattu (carrier sense). Jos media on vapaa, voidaan lähettää, mutta jos media on varattu, odotetaan meneillään olevan siirron loppuun ja aloitetaan kilpavaraus. Kilpavarauksessa kaikki odottavat satunnaisen ajan ja se jolle tulee lyhin aika voittaa, eli pääsee lähettämään. Koska radiotekniikalla ei voida havaita suoraan tapahtuuko törmäys (eli kaksi asemaa lähettää yhtä aikaa, jolloin kummankin siirto luultavasti epäonnistuu) ja koska radio tarvitsee aikaa siirtyäkseen lähetys- ja vastaanottotilojen välillä, törmäykset aiheuttavat huomattavasti suurempia viiveitä kuin langallisissa verkoissa. Tämän takia niitä pyritään välttämään. [Tou00]

Törmäysten minimoimiseksi CSMA/CA:ta käytettäessä voidaan käyttää menetelmää, jossa lähetetään lyhyitä kontrollipaketteja RTS (Request To Send) ja CTS (Clear To Send) ennen varsinaista lähetystä. [IEEE97] RTS/CTS auttaa selviytymään niin sanotusta piilevän aseman ongelmasta (hidden node problem). Ongelma tulee esille esimerkiksi tilanteessa, jossa kaksi asemaa eivät kuule toisiaan suoraan radiolähetysten vaimenemisen vuoksi ja yrittävät lähettää samaan aikaan tukiasemalle, jonka kummatkin asemat kuulevat. Tukiasemalla tästä seuraa törmäys. Ratkaisu tähän ongelmaan on se, että lähettäjä lähettää vastaanottajalle (eli tässä tapauksessa tukiasemalle) lähetyspyynnön RTS ja vastaanottaja vastaa CTS-paketilla. Jokainen vastaanottajan kuuluvuusalueella kuulee CTS:n vaikka ei välttämättä RTS:ää kuulekaan. Asemat, jotka kuulevat CTS:n ovat potentiaalisia törmäyksen aiheuttajia, jotka nyt CTS-paketin tietojen mukaan osaavat olla lähettämättä riittävän ajan. [Tou00]

Keskitetty koordinointifunktio, PCF, kuuluu 802.11:een vapaaehtoisena toteutettavana. Sitä voidaan käyttää vain infrastruktuuriverkossa, jossa tukiasema toimii koordinoijana. Koordinoija tarkkailee liikennettä ja päättää minkä aseman vuoro on lähettää. PCF mahdollistaa sen, että verkon asemien ei tarvitse käyttää kilpavarausta ja DCF:ssä kilpavaraukseen kuluva aika voidaan käyttää hyödyksi. On myös mahdollista käyttää PCF- ja DCF-toimintoja yhtä aikaa samassa verkossa. [IEEE97]

Langatonta tiedonsiirtoa tehostamaan on MAC-protokollaan sisällytetty lisätekniikat MAC-tason uudelleenlähetys ja fragmentointi. MAC-tason uudelleenlähetyksen periaate

on yksinkertainen. Joka kerta kun asema ottaa vastaan paketin, se lähettää lyhyen vastauksen lähettäjälle ilmoittaakseen onnistuneesta siirrosta. Jos lähettäjä ei saa vastausta, paketti on kadonnut ja tehdään lähetys uudelleen. Radiotiellä tapahtuu enemmän virheitä kuin langallisessa verkossa ja tämä tekniikka auttaa korkeamman tason protokollia (kuten TCP:tä), joille on vahingollista menettää osia suuremmista paketeistaan alimmalla protokollatasolla, jolloin joudutaan tekemään uudelleenlähetys korkeammalla tasolla. Näin lisätään oleellisesti verkon suorituskykyä korkeammilla protokollatasoilla. Radiotien suuremmista virhemääristä selviytymiseen auttaa myös pakettien hajauttaminen pienempiin osiin (fragmentointi). Pienempi paketti pääsee todennäköisemmin virheittä perille kuin suuri paketti. [Tou00]

3.3.3 802.11-standardin tietoturvaominaisuudet

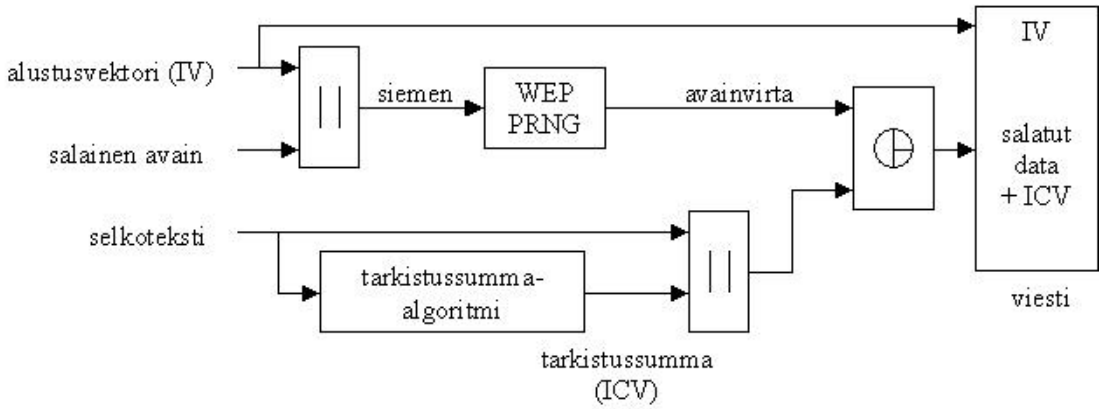
802.11-standardi tarjoaa MAC-kerroksella tietoturvapalvelut, joilla pyritään saavuttamaan ainakin samantasoinen tietoturvallisuus kuin langallisessa verkossa. Nämä palvelut ovat WEP (Wired Equivalent Privacy), eli datan luottamuksellisuuden takaava salaus, sekä autentikointi ja siihen liittyvä pääsynhallinta. WEP ei ole standardin mukaan pakollinen toteutettava. Laitteistojen valmistajat ovat kuitenkin perustaneet WECA:n (Wireless Ethernet Compatibility Alliance), jonka tehtävänä on varmentaa eri valmistajien 802.11-tuotteiden yhteensopivuus. WECA:n yhteensopivuustestit läpäisseet laitteet ovat Wi-Fi -yhteensopivia (Wireless Fidelity). Wi-Fi pitää sisällään pakollisena tuen standardissa määritellylle 40-bittiselle WEP-salaukselle.

WEP

WEP-salaus suunniteltiin tarjoamaan vähintään samantasoinen luottamuksellisuus langattomasti siirrettävälle datalle kuin on hyvin fyysisesti suojatussa langallisessa verkossa [IEEE97]. WEP sijaitsee OSI-mallista puhuttaessa siirtoyhteyskerroksella, jolloin kyseessä on linkkitason salaus, eli salaus on tietoliikennelinkkikohtainen ja puretaan aina jokaisen linkin päässä [Eng01]. WEP on RC4-jonosalaimen toteutus, jossa käytetään standardin mukaan 40-bittistä symmetristä avainta (standardissa määritelty lyhyt avaimen pituus johtuu salaustuotteiden vientirajoituksista). Monet valmistajat ovat toteuttaneet myös 104-bittisiä avaimia käyttävän version.

RC4 on pseudosatunnaislukugeneraattori (pseudo-random number generator, PRNG) ja avainta käytetään sen siemenenä. RC4 siis laajentaa lyhyen avaimen mielivaltaisen pitkäksi pseudosatunnaiseksi bittivirraksi, jota kutsutaan avainvirraksi (key stream). Itse salaus tapahtuu niin, että salattava data ja avainvirta ajetaan biteittäisen XOR-operaation läpi.

WEP pyrkii välttämään jonosalaimiin liittyvän heikkouden käyttämällä 24-bittistä alustusvektoria (Initialization Vector, IV), joka liitetään salaisen avaimen kanssa peräkkäin. Avaimen ja alustusvektorin yhdistelmää (yhteensä siis pituudeltaan 64 tai 128 bittiä) käytetään RC4:n siemenenä. Alustusvektori liitetään salatun datan mukana pakettiin selkokielisenä, ja siten vastaanottaja voi muodostaa saman avainvirran mitä käytettiin salaukseen ja purkaa salauksen XOR-operaatiolla (exclusive OR). Alustusvektorilla pyritään välttämään saman avainvirran käyttöä kahdesti, mikä on erityisen tärkeää jonosalaimissa. Alustusvektorilla saavutetaan myös salauksen itsestään synkronoituvuus yksittäisen paketin tasolla, mikä on tärkeää linkkikerroksen salauksessa, koska pakettihävikki voi olla huomattavaa. WEP pyrkii havaitsemaan pakettien muuntelun laskemalla salattavasta datasta tarkistussumman (Integrity Check Value, ICV) CRC-32 –menetelmällä. Tarkistussumma lisätään lähetettävässä paketissa datan perään ja salataan samalla kuin data. Kuva 10 esittää WEPin toiminnan.
[IEEE97]



Kuva 10: WEP-salauksen toiminta [IEEE97]

Seuraavassa esitetään WEPin toiminnan vaiheet lyhyesti:

- Lasketaan datalle tarkistussumma.
- Liitetään tarkistussumma datan perään.
- Valitaan satunnainen alustusvektori ja liitetään se salaisen avaimen perään.
- Syötetään salainen avain ja alustusvektori RC4:lle. Tuloksena saadaan avainvirta.
- Salataan data ja tarkistussumma XORaamalla ne avainvirran kanssa.
- Asetetaan käytetty alustusvektori pakettiin datan eteen.

Vastaanottaja purkaa salauksen tuottamalla saman avainvirran kuin lähettäjä ja tekemällä uuden XOR-operaation. Puretusta datasta lasketaan tarkistussumma, jota verrataan paketin mukana tulleeseen. Jos luvut eivät täsmää, paketti hylätään.

RC4 on helppo toteuttaa sekä ohjelmallisesti että laitteistolla ja on erittäin nopea. Näiden ominaisuuksien ansiosta RC4 onkin varsin paljon käytetty salausmenetelmä. Salauksen vahvuus perustuu salaisen avaimen selvittämisen vaikeuteen kaikki avaimet läpikäymällä. Tähän taas vaikuttaa avaimen pituus ja yhden avaimen käytön ikä. [IEEE97]

Autentikointi ja pääsynhallinta

Ennen kuin langaton asiakasasema ja tukiasema voivat kommunikoida, asiakkaan täytyy assosioitua tukiaseman kanssa. Tähän tapahtumaan liittyen standardissa on määritelty kolme tilaa, joissa asiakas voi olla:

1. Autentikoimaton (todentamaton) ja ei-assosioitunut
2. Autentikoitu ja ei-assosioitunut
3. Autentikoitu ja assosioitunut

Assosioituminen tapahtuu kahdessa vaiheessa käymällä tilat järjestyksessä läpi. (muita mahdollisia tilasiirtymiä varten standardissa on määritelty täydellinen tilakone). Kun asiakas tulee langattoman verkon alueelle, se havaitsee tukiasemat niiden lähettämistä merkkipaketeista (beacon). Kun tukiasema on löytynyt, asiakas ja tukiasema autentikoituvat toinen toisilleen lähettämällä useita hallinnointipaketteja (management frame). Autentikoitumisen jälkeen seuraa assosioituminen, minkä jälkeen asiakas kuuluu verkkoon ja voi lähettää dataa. Standardi määrittelee kaksi

autentikointimenetelmää: avoin autentikointi (Open System Authentication) ja jaetun avaimen autentikointi (Shared Key Authentication). Avoin autentikointi on 802.11-standardin oletusarvo, ja siten pakollinen toteutettava. Kuten nimikin jo kertoo, avoin autentikointi autentikoi minkä tahansa asiakkaan, joka sitä vain pyytää. Näin ollen kaikki halukkaat pääsevät liittymään verkkoon, jossa käytetään avointa autentikointia. [IEEE97]

Jaetun avaimen autentikointi perustuu haaste-vastaus –menetelmään ja jaettuun salaiseen avaimeen. Kun asiakas haluaa autentikoitua, tukiasema lähettää asiakkaalle haasteen, joka salataan WEPillä ja lähetetään takaisin tukiasemalle. Tukiasema purkaa salauksen ja tarkistaa että saatu data vastaa lähetettyä haastetta ja varmistaa että tarkistussumma pitää paikkansa. Jos tarkistukset menevät läpi, on autentikointi onnistunut. Tämän jälkeen tukiasema ja asiakas vaihtavat rooleja, että saadaan aikaiseksi keskinäinen autentikointi. Jaetun avaimen autentikointi on standardin mukaan siinä mielessä vapaaehtoinen toteutettava, että jos WEP (standardi: vapaaehtoinen, WiFi: pakollinen) ei ole toteutettu, ei jaetun avaimen autentikointiakaan voi toteuttaa. Mutta jos WEP on toteutettu, myös jaetun avaimen autentikointi on toteutettava. Jaetun avaimen autentikoinnilla voidaan siis todentaa, että asiakas kuuluu joko niihin, jotka tuntevat salaisen avaimen tai niihin jotka eivät tunne. Pääsynhallinta seuraa siitä, että autentikoimaton asema ei pääse assosioitumaan tukiasemaan. [IEEE97] On yleensä myöskin mahdollista asettaa tukiasemissa, että ne hyväksyvät salausta käyttävien asiakkaiden lisäksi myös sellaiset, jotka eivät käytä WEP-salausta.

Standardiin kuulumattomia tietoturvaominaisuuksia

Useat valmistajat käyttävät tukiasemissaan pääsynhallintalistoja (Access Control List, ACL), vaikka niitä ei standardissa olekaan määritelty. Pääsynhallinta perustuu MAC-osoitteeseen (tunnetaan myös nimillä laitteisto-osoite, hardware-osoite, hw-osoite), joka on jokaiselle verkkokortille yksilöllinen. Pääsynhallintalistat ovat hyvä keino, jos pääsynhallinnan perusteena käytetty ominaisuus on vahva. MAC-osoite on kuitenkin mahdollista väärentää ja sallitut osoitteet voi saada selville salakuuntelemalla, koska MAC-osoitteet on oltava paketeissa salaamattomassa muodossa. Edelleen isossa verkossa listojen ylläpito jokaiselle tukiasemalle erikseen on erittäin työlästä, ellei sitä varten ole kehitetty tehokasta keskitettyä hallintamenetelmää. [Arb01]

802.11b-mukaisten laitteiden valmistajista Agere Systems (entinen Lucent) käyttää valmistajakohtaisena ei-standardin mukaisena pääsynhallintakeinona verkon nimeä (service set ID, SSID). Menetelmä voidaan asettaa päälle tukiasemista, ja tämän jälkeen verkkoon ei pääse mikäli verkon nimi ei ole tiedossa. SSID toimii siis jaettuna salaisuutena. Tämä ei ole erityisen turvallinen pääsynhallintakeino, koska SSID lähetetään useissa hallinnointipaketeissa selkotekstinä. WEP ei auta asiaan, koska sillä salataan vain pakettien hyötykuorma. SSID:n saa siis helposti selville salakuuntelemalla verkon liikennettä. [Arb01]

3.3.4 802.11-standardin tietoturvaominaisuuksien ongelmia

Ongelmat WEP-salauksessa

Kuten aiemmin jo todettiin, WEP käyttää salaukseen RC4 jonosalausalgoritmia, jossa salaamiseen ja purkamiseen käytetään XOR-operaatiota. Tällaista salausmenetelmää vastaan on useita hyökkäysmahdollisuuksia. XOR:n ominaisuuksista johtuu, että jos hyökkääjä muuttaa bitin salatusta tekstistä, vastaava bitti muuttuu salausta purettaessa. Samoin seurauksena XOR:n ominaisuuksista on, että jos salakuuntelija saa haltuunsa kaksi salasanomaa, jotka on salattu käyttäen samaa avainvirtaa, saadaan muodostettua selkotekstien XOR. Tämä tieto mahdollistaa tilastollisen hyökkäyksen, jolla voidaan saada selville alkuperäiset selkotekstit. Kun selkoteksti saadaan selville, selviää myös salaukseen käytetty avainvirta, minkä jälkeen voidaan purkaa kaikki samalla avainvirralla salatut datat. [Bor01]

WEPissä on suojaukset, joilla pyritään välttämään jonosalaimen ominaisuuksista johtuvat heikkoudet. Nämä suojaukset mainittiin jo aiemmin, ja ne ovat alustusvektori, jolla pyritään välttämään saman avainvirran käyttöä ja tarkistussumma, jolla havaitaan pakettien muuntelu. Valitettavasti molemmat keinot on toteutettu huonosti.

Tarkistussumma lasketaan tavallisella CRC-32 menetelmällä. CRC-32 on lineaarinen, mikä tarkoittaa että on mahdollista laskea kahden tarkistussumman ero niiden kahden datan erosta, joista tarkistussummat on laskettu. Pystytään siis laskemaan mitkä bitit

pitää muuttaa tarkistussummasta, että saadaan se oikeaksi sen jälkeen kun paketin dataa on muunneltu. Paketteja voidaan siis muunnella mielivaltaisesti ja siltikin saadaan se tarkistussumman puolesta näyttämään oikealta.

Alustusvektorille varattu 24-bittinen arvo on liian pieni tarkoitukseensa. Käytännössä on 2^{24} erilaista avainvirtaa jokaista salaista avainta kohti. Vilkkaasti liikennöity tukiasema, joka lähettää jatkuvasti 1500 tavun paketteja 11 Mb/s nopeudella, käyttää koko alustusvektoriavaruuden $1500*8/(11*10^6)*2^{24}$ = 18302 sekunnissa, eli noin viidessä tunnissa. Käytännön toteutuksissa sama salainen avain on usein jaettu kaikkien langattoman verkon laitteiden kesken, jolloin alustusvektoreiden törmäyksiä (eli samaa avainvirtaa käytetään uudestaan) sattuu melko suurella todennäköisyydellä. Standardin mukaan ei edes ole pakollista vaihtaa alustusvektorin arvoa jokaisen paketin kohdalla (vaikkakin sitä kyllä suositellaan). Mainituista ongelmista johtuen WEPillä salattua liikennettä vastaan on useita hyökkäyksiä, joiden tehokkuus ei edes riipu millään tavalla käytetystä salausavaimen pituudesta. [Bor01]

Hyökkäyksiä WEP-salausta vastaan

24-bittinen alustusvektori tekee mahdolliseksi löytää salakuuntelemalla alustusvektoreiden törmäyksiä ja johtaa niistä tilastollisella hyökkäyksellä selkotekstit ja käytetyt avainvirrat. Riittävästi liikennettä tallentamalla on mahdollista laajentaa hyökkäystä ja kasata kaikkiin alustusvektoreihin liittyvät avainvirrat minkä jälkeen kaikki liikenne voidaan purkaa, vaikka itse jaettu salainen avain ei olekaan tiedossa. Hyökkäyksestä käytetään nimitystä sanakirjahyökkäys. [Bor01] Tällaiset hyökkäykset ovat täysin passiivisia ja varsin mahdollisia toteutettavia. Tähän tarkoitukseen tehty ohjelmapaketti on vapaasti saatavilla Internetistä [New01]. Riittävän usein tapahtuva salausavaimen vaihto vaikeuttaa tällaista hyökkäystä.

RC4:ään liittyen löytyi myös heikkous, joka mahdollistaa WEP-salauksen täydellisen murron (eli saadaan selville salausavain). Pelkästään salattua liikennettä keräämällä on mahdollista laskea käytetty salainen avain. Hyökkäys perustuu siihen, että tietyt alustusvektorin arvot tuottavat heikkoja avaimia. Näistä avaimista tuotetulla avainvirralla salattu data antaa tietoa itse salaisesta avaimesta. [Flu01] Hyökkäys on erittäin tehokas. Laskentatehoa ei tarvita juuri ollenkaan ja hyökkäykseen tarvittava aika

skaalautuu lineaarisesti salausavaimen pituuden mukaan. Vilkkaasti liikennöidyssä verkossa murto tapahtuu muutamassa tunnissa (joskus jopa nopeammin). Tämäkin hyökkäys on täysin passiivinen ja käytännössä erittäin toteutettavissa. Hyökkäyksen toteutti ensimmäisenä Adam Stubblefield, mutta hän ei julkaissut käyttämiään ohjelmia [Stu01]. Pian tämän jälkeen Internetiin ilmestyi vapaasti saataville kaksi hyökkäyksen toteuttavaa ohjelmaa: Airsnort (http://airsnort.shmoo.com/) ja Wepcrack (http://wepcrack.sourceforge.net/).

Liikenteen muuntaminen on mahdollista, koska standardissa käytetty tarkistussumma ei estä tahallista pakettien muuntamista. Myös kokonaisten pakettien väärentäminen on mahdollista, jos on tiedossa salatun paketin selkoteksti. Koska alustusvektoria ei tarvitse muuttaa, voidaan samaa pakettia käyttää väärentämisen pohjana koko ajan. Tällaiset hyökkäykset ovat tyypiltään aktiivisia ja hankalampia toteuttaa kuin pelkästään passiivista monitorointia vaativat hyökkäykset. Myös kerättyjen pakettien toistaminen on mahdollista ja sitä voidaan käyttää hyökkäyksissä.

Standardin mukaista, 40-bittisellä avaimella tehtyä, salausta vastaan on myös mahdollista tehdä raa'an voiman hyökkäys, eli käydä kaikki mahdolliset 40-bittiset avaimet läpi ja siten selvittää käytetty avain. Vuonna 1995 järjestetyssä murtamiskilpailussa 40-bittinen avain löytyi kahdeksassa päivässä. Tähän tarvittiin laiteresursseja muutaman kymmenen sen aikaisen hyvätasoisen PC-koneen verran. [Dol95] Kun laskentatehon kehitys otetaan huomioon, ei tällainen hyökkäys ole nykypäivänä kovinkaan vaikea toteutettava.

Heikkous jaetun avaimen autentikoinnissa

802.11:ssä käytettävä jaetun avaimen autentikointimenetelmä esiteltiin aiemmin. Salakuuntelemalla onnistunut autentikointi on mahdollista saada selville haasteen mittainen käypä avainvirta ja siihen liittyvä alustusvektori. Näillä tiedoilla ja laskemalla tarkistussumma on mahdollista luvattomien tahojen autentikoitua verkkoon, vaikka salainen avain ei olekaan tiedossa. Verkon käyttö tästä eteenpäin kuitenkin tarvitsee muiden hyökkäysmenetelmien käyttöä, koska jaettu WEP-avain ei ole tiedossa. [Arb01]

Avainten jakelu ja käyttö

Avainten hallinta on jätetty kokonaan määrittelemättä standardissa. Näin ollen suurin osa tuotteiden valmistajista on jättänyt toteuttamatta avainten jakelun missään muodossa. Siten loppukäyttäjälle jää ratkaistavaksi tunnettu kryptografian ongelma: kuinka toimittaa salaiset avaimet luotettavasti verkon tukiasemille ja verkkoa käyttäville tietokoneille. Manuaalisesti tehtynä työmäärä verkon koon suurentuessa käy nopeasti käytännössä liian suureksi. Ja mitä useammalle jaettu salaisuus on kerrottu, sitä heikommaksi salaisuus tulee. Käytännössä usein sama salainen avain on jaettu koko verkon laitteiden kesken. Jos käytetään samaa avainta kaikkien osapuolten kesken, olisi avaimet vaihdettava kohtuullisen usein WEP:n heikkouksista johtuen.

802.11 määrittelee kaksi tapaa kuinka WEP-avaimia voidaan käyttää. Ensimmäisessä tavassa verkon liikkuville asemille ja tukiasemille voidaan asettaa jokaiselle korkeintaan neljä eri avainta (yleensä siis kaikilla on samat neljä avainta). Salauksen purkamisen voi suorittaa millä tahansa näistä neljästä avaimesta, mutta salaamiseen käytetään vain yhtä valittua avainta kerrallaan (kun lähetetään WEP:llä salattuja paketteja, paketissa kerrotaan millä avaimella salaus on tehty). Tällä pyritään helpottamaan avainten kiertoa ja salausavaimia vaihdettaessa tapahtuvaa siirtymäajanjaksoa, kun kaikilla ei vielä välttämättä ole sama avain käytössä. Toinen tapa on avaintaulukko (WEP key mapping), jossa voidaan määritellä jokaista MAC-osoitetta kohden oma WEP-avain. Käyttäjäkohtaiset avaimet heikentävät salausta vastaan tehtyjen hyökkäysten onnistumismahdollisuuksia tehokkaasti, varsinkin jos avaimet vaihdetaan riittävän usein. Kaikkien avaimien vaihto manuaalisesti on työlästä ja suuremmissa verkoissa käytännössä mahdotonta. [IEEE97]

3.3.5 Liikenteen tarkkailu ja hyökkäykset käytännössä

802.11b-standardin mukaisen liikenteen tarkkailu on käytännössä helppoa. Tarvittava laitteisto on esimerkiksi tavallinen PC-kone (kannettava tietysti kätevin vaihtoehto) ja siihen 802.11b-mukainen langaton verkkokortti. Langattomissa verkkokorteissa käytettävien piirien valmistajia on muutamia ja itse korttien valmistajia enemmän. Kaikki tarkkailu- tai hyökkäysohjelmistot eivät toimi kaikkien korttien kanssa.

Aikaisemmin mainittiin jo kolme murto-ohjelmistoa, jotka ovat vapaasti saatavilla Internetistä. Tämän tyyliset ohjelmat tarvitsevat kaapattua liikennettä toimiakseen. Yleensä tietoliikennettä kaappaavia ohjelmia (analysaattori, snifferi) käytetään verkon häiriötilanteissa ongelman ratkaisemisessa. Langattoman liikenteen kaappaamiseen vapaasti saatavilla ovat mm. seuraavat ohjelmistot:

- Kismet 2.0 (Linux)
- prismdump, työkalu joka toimii Ethereal-analysaattorin kanssa (Linux)
- Mognet, Java-ohjelmointikielellä toteutettu työkalu
- BSD Airtools, BSD-käyttöjärjestelmille Airsnort, prismdump ja muita työkaluja

Langattomien verkkojen löytämiseen ja kartoittamiseen sopii mainiosti vaikkapa Netstumbler-niminen ohjelma. Netstumbler lähettää probe request –paketteja, joihin tukiasemat ja ad hoc-moodissa olevat verkkokortit vastaavat. Näistä paljastuu kaikenlaista hyödyllistä tietoa. Netstumbler toimii Windows-ympäristössä ja on ilmainen. Samaan tarkoitukseen on myös Aerosol (Windows), ApSniff (Windows 2000) ja Wellenreiter (Linux, BSD). Tällaisia ohjelmia käytetään usein ylläpidon apuna kuuluvuuskartoituksessa, asetuksien tarkastamisessa ja luvattomien tukiasemien löytämisessä.

3.3.6 802.11 tietoturvan tulevaisuus

Pahimpaan uhkaan, eli RC4:n heikkoja avaimia käyttävään hyökkäykseen on jo olemassa korjauksia. Kyseessä on ohjelmistopäivitys, joka estää heikkojen alustusvektoreiden käytön. Tällä tavalla päivitetyt laitteet toimivat myöskin päivittämättömien kanssa, koska lähettävä ja samalla salauksen suorittava osapuoli valitsee alustusvektorin. Jotta kyseisen hyökkäyksen uhka poistuisi kokonaan, on kaikkien verkon laitteiden oltava päivitetty.

Varsinaisia tulevaisuuden langattomien lähiverkkojen tietoturvaratkaisuja kehittää meneillään oleva IEEE:n työryhmä 802.11i. Työryhmältä syntyy tuloksena dokumentti, joka korvaa perusstandardin tietoturvaominaisuudet määrittelevän pykälän (eli 802.11:n pykälä 8). Tällä hetkellä (tilanne 08/2002) on julkaistuna ehdotelman toinen versio, ja siinä esitellään käsite RSN (Robust Security Network). Määritelmän mukaan RSN

turvallisuusalgoritmit toteuttava laitteisto on RSN-pystyvä ja nykyiset vuoden 1999 802.11 standardin mukaiset laitteet ovat RSN-edeltäjiä (pre-RSN). RSN:n turvallisuus koostuu kahdesta perusalijärjestelmästä:

- Datan luottamuksellisuusmekanismi. RSN määrittelee näitä kaksi:
    - TKIP (Temporal Key Integrity Protocol), kokoelma algoritmeja joilla parannetaan WEP-protokollaa. Mahdollistaa nykyisten laitteiden turvallisuuden parantamisen ohjelmistopäivityksellä.
    - AES-pohjainen (Advanced Encryption Standard) protokolla uuden sukupolven laitteille. Tarjoaa vahvan salauksen. Uuden sukupolven laitteissa voidaan toteuttaa myös TKIP, jotta saavutetaan taaksepäin yhteensopivuus.
- Turvallisuusassosiaatioiden hallinta (Security association management). RSN määrittelee useita komponentteja tähän tarkoitukseen:
    - RSN-neuvottelu, jolla muodostetaan turvayhteys.
    - IEEE 802.1X mukainen autentikointi, joka korvaa IEEE 802.11 autentikoinnin.
    - IEEE 802.1X mukainen avaintenhallinta, jolla hoidetaan avainten jakelu.

[IEEE02]

802.1X määrittelee MAC-siltaustason toimintaan vaadittavat muutokset, jotta voidaan tarjota porttipohjainen verkon pääsynhallintamenetelmä (Port based network access control capability). Sen mukaan verkkoonpääsyportti (network access port) on paikka, josta järjestelmä liitetään verkkoon. Portti voi siis olla fyysinen portti (esim. keskitin tai kytkin), tai looginen kuten esimerkiksi 802.11 tapauksessa liikkuvan aseman ja tukiaseman välinen assosiaatio. Liitettävä järjestelmä voi olla työasema, palvelin, silta jne. Standardin mukaan laite, jossa on portteja toimii autentikaattorina. Porttiin kiinnittyvän laitteen on kerrottava todentamiseen tarvittavat tiedot autentikaattorille ennen kuin se voi kommunikoida muun verkon kanssa. Autentikaattori keskustelee autentikointipalvelimen kanssa. Autentikointipalvelin suorittaa varsinaisen autentikoinnin ja kertoo tuloksen autentikaattorille. Osana autentikointiprosessia luodaan MAC-tason salausavaimet, jotka 802.1X toimittaa autentikaattorin ja verkkoon kiinnittyvän järjestelmän MAC-kerroksille. [IEEE01]

802.1X on menetelmä, jolla suoritetaan todentaminen ja sitä kautta saadaan pääsy IEEE 802-lähiverkkoihin. Myös laskutus ja yksilöllistetty pääsy verkkoon ovat mahdollisia. Standardissa määritellään protokolla, jolla verkkoon pääsyä haluava laite ja verkon reunalla oleva pääsyn tarjoava laite keskustelevat. Tämä protokolla on IETF:n (Internet Engineering Task Force) määrittelemä EAP (Extensible Authentication Protocol, RFC 2284), joka kapseloidaan 802-kehyksiin, jolloin se saa nimen EAPOL (Extensible Authentication Protocol Over LAN). EAP on yleinen protokolla, joka tukee useita erilaisia todentamismenetelmiä. 802.1X:ssä määritellään myös vaatimukset autentikaattorin ja autentikointipalvelimen väliselle protokollalle. Eräs vaihtoehto tähän on RADIUS (Remote Authentication Dial-In User Service). Näin voidaan käyttää jo olemassa olevaa autentikointi-, autorisointi- ja kirjanpitoinfrastruktuuria (Authentication, Authorization and Accounting).

3.3.7 Yhteenveto

Nykyisellään 802.11 mukaisten verkkojen tietoturva on helposti murrettavissa. Tällaisia langattomia verkkoja käytettäessä tietoturvan puute on syytä tiedostaa, jotta osataan varautua muilla keinoilla. Tarvittava tietoturvan taso on mahdollista saavuttaa nykyisin saatavilla olevilla tekniikoilla ylemmillä protokollatasoilla. Mahdollisia salauksen ja todentamisen tekeviä protokollia ovat esimerkiksi IPSec, SSL (Secure Sockets Layer) ja SSH (Secure Shell). Mikäli langattomassa lähiverkossa siirretään arvokasta tietoa, on riittävän tietoturvatason saavuttamiseksi oltava muitakin menetelmiä kuin 802.11-standardin tarjoamat tietoturvapalvelut. Huonoin tilanne on kuitenkin se, jossa ei käytetä minkäänlaisia tietoturvamenetelmiä. Heikkokin suoja on parempi kuin ei suojaa ollenkaan, kunhan vain tiedostaa heikkouksien ja hyökkäysten mahdollisuudet.

Kannattaa myös muistaa, että kyseessä on lähiverkkotekniikan tietoturvaominaisuudet. WEP on linkkitason salaus, jolla pyritään vain ilmalinkin salaamiseen, koska radiolähetyksiä on helppo salakuunnella. Verkkojen väliset päästä-päähän –yhteydet on tarvittaessa suojattava muilla keinoilla. Langattoman verkkolinkin uhkat rajoittuvat käytännössä lähettimen kantaman kokoiseen fyysiseen ympäristöön.

802.11-standardin tietoturvamääritykset osoittavat, että tietoturvaprotokollan suunnitteleminen on vaikeaa. Tässä tapauksessa epäonnistuttiin selvästi. Salaustekniikan primitiivien toiminta on ymmärretty väärin ja seurauksena, periaatteessa toimivista osasista, on koottu turvaton kokonaisuus. Jonosalaimia käytettäessä on ehdottoman tärkeää muistaa, että samaa avainvirtaa ei saa käyttää uudestaan.

802.11-standardin tietoturvan tulevaisuus vaikuttaa lupaavalta 802.11i-työryhmän myötä. Määrittelyihin kuuluu vahvempi salaus ja 802.1X-pääsynhallinnan käyttö langattomassa lähiverkossa. 802.1X:n kehittämisen taustalla on 802-lähiverkkojen lisääntynyt käyttö julkisilla ja puolijulkisilla paikoilla. Tämä pätee erityisesti langattomiin lähiverkkoihin, joiden voidaan katsoa olevan oikeastaan aina julkisella paikalla. Työryhmä i:n työ on kuitenkin vielä ehdotelman asteella, ja siitä on pitkä tie valmiiksi tuotteiksi. RSN-pystyvyys vaatii laitteistomuutoksia ja sekin viivästyttää käyttöönottoa. Nykyisiin laitteisiin on jo investoitu huomattavasti rahaa, eikä niistä haluta luopua ihan heti. Työryhmä i:n määrittelemä siirtymäajan tekniikka auttanee sen suhteen.

3.4 WLAN käytännössä

IEEE 802.11b-standardin mukaiset laitteet ovat tällä hetkellä saavuttaneet suuren suosion ja muiden standardien mukaisia tuotteita on myynnissä vain vähän. Tästä syystä käsitellään tässä työssä tästä eteenpäin 802.11(b)-standardiin perustuvia langattomia verkkoja. Tästä eteenpäin käsitteet langaton lähiverkko ja WLAN viittaavat tässä työssä kyseisen standardin mukaisiin verkkoihin ja laitteisiin ellei toisin mainita. WLAN-verkkoja on asennettu varsinkin toimistoihin ja muutenkin enimmäkseen yrityssektorille. WLAN-tuotteet alkavat kuitenkin jo löytää kuluttajasektorille ja koteihin. WLAN-tekniikkaan perustuvat erilaiset julkiset kaupunkiverkot ovat myös tulleet suosituiksi. Ne käsitellään tuonnempana laajemmin omassa osiossaan.

3.4.1 WLAN kotikäytössä

WLAN-verkon yleisin käyttö kotona lienee laajakaistaiseen Internet-yhteyteen liitetty tukiasema, jonka kautta omaan langattomaan lähiverkkoon liitetyt laitteet jakavat yhteyden Internetiin. Laajakaistayhteyksien tekniikoita ovat esimerkiksi kaapelimodeemi ja DSL (Digital Subscriber Line). Laajakaistayhteydet ovat jatkuvasti päällä olevia yhteyksiä ja kotikäyttäjän on syytä olla selvillä Internet-yhteyden tuomista tietoturvauhkista sekä lisäksi mahdollisen käytössä olevan WLAN-tekniikan tuomista lisähuolista.

Internet-yhteyteen liittyviin tietoturvauhkiin ei tässä kohtaa syvällisemmin puututa, koska ne käsiteltiin jo kohdassa 2.4.3. WLAN-tekniikkaan liittyvissä tietoturvaongelmissa paras lähtökohta on, että tiedostaa kyseiset ongelmat. Näin ongelmiin osaa varautua ja osaa ottaa tekniikassa olevat puutteet huomioon tehdessään ratkaisuja. Kotikäytössä oleva langaton lähiverkko lisää lähialueen uhkia. Internet-yhteys toisaalta avaa paljon suuremmalle yleisölle mahdollisuudet tunkeutua omaan lähiverkkoon. Internetistä hyökkäyksiä tekevät eivät useinkaan etsi kotikoneilta mitään tietoja (siitä syystä, että siellä ei useinkaan ole mitään kovin mielenkiintoista), vaan haluavat koneen hallintaansa, jotta voisivat käyttää sitä hyväkseen muissa hyökkäyksissä naamioiden näin hyökkäyksen todellisen alkuperän.

Vastaavasti kuluttajan langatonta lähiverkkoa uhkaavat lähellä asuvat ihmiset, jotka mahdollisesti haluavat esimerkiksi käyttää ilmaiseksi toisen Internet-yhteyttä joko ihan vain surffaillakseen tai tehdäkseen pahojaan toisen Internet-yhteyden taakse naamioituneena. On kyllä mahdollista, että joku murtautuu varta vasten juuri sinun verkkoosi ja tämän takia kannattaa miettiä miten arvokasta koneilla oleva tieto on ja kuinka paljon kuluttaa resursseja suojautumiseen. Kannattaa käyttää ainakin tuotteissa olevia tietoturvaominaisuuksia, eli tässä tapauksessa asettaa WLAN-laitteissa salaus päälle ja asettaa kunnon salasana sekä tehdä ohjelmistopäivitykset. Mahdolliset pääsylistat kannattaa myöskin asettaa. Salasanat kannattaa vaihtaa riittävän usein ja käyttää ylempien protokollakerrosten salausmenetelmiä aina kun se on mahdollista. Pääteyhteyksissä kannattaa käyttää SSH:ta, webissä asioidessa SSL:ää ja arkaluontoiset sähköpostit salata vaikka PGP:llä (Pretty Good Privacy). Internet-yhteyden ja

kotiverkon rajalle voi laittaa palomuurin. Nämä keinot takaavat riittävän tietoturvan useimmissa tapauksissa.

3.4.2 WLAN yrityskäytössä

WLAN-tuotteet olivat aluksi yrityskäyttöön suunnattuja jo pelkästään hinnoittelunsa vuoksi. WLAN-ratkaisut ovat olleet varsin suosittuja mitä erilaisimmissa kohteissa liikkuvuuden tuoman joustavuuden ansiosta. WLAN-tekniikasta löytyneet tietoturvaongelmat jarruttivat suosiota jossain määrin. Tietoturvaongelmien ratkaisemiseksi on keinot olemassa jo tällä hetkellä. On vain valittava tilanteeseen sopivat ratkaisut tarvittavan tietoturvan tason ja käytössä olevien resurssien pohjalta.

Pien- tai kotitoimistossa ei välttämättä ole resursseja huipputietoturvaratkaisujen toteuttamiseen, eikä myöskään ehkä tarvetta. Tällaisissa tapauksissa samanlaiset toimenpiteet, kuin edellä esitetyssä kotiverkon tapauksessa, ovat varsin riittävät. Ratkaisut ovat tietysti tapauskohtaisia ja riippuvat verkossa olevan tiedon arvosta.

Kun suuremmissa yrityksissä käytetään WLAN-tekniikkaa täydentämään langallista verkkoa, ovat käyttäjämäärät suurempia ja verkossa oleva data arvokkaampaa. Suurempien käyttäjämäärien myötä nykyisen WLAN-standardin tietoturvaominaisuudet käyvät hankaliksi hallita, ja ovat vikojensa vuoksi riittämättömiä suojaamaan arvokasta tietoa päättäväiseltä ja osaavalta hyökkääjältä. Avainten jakelu suureen määrään tukiasemia ja langattomia päätelaitteita on käytännössä liian työlästä. Tukiasemakohtaisten, MAC-osoitteeseen perustuvien, pääsylistojen asettaminen ja ylläpito manuaalisesti on työlästä, eikä edes kovin varma turvakeino. Yleinen ja suositeltu ratkaisu on eriyttää langaton verkko luotetusta langallisesta verkosta ja sijoittaa niiden rajalle palomuuri. Langatonta verkkoa kohdellaan siis kuin Internet-yhteyttä ja langattomat päätelaitteet ottavat turvallisena pidettyyn verkkoon yhteyden samalla tavalla kuin Internetin yli. Käytännössä tämä tarkoittaa sitä, että langattomat päätelaitteet varustetaan sopivalla VPN-ohjelmistolla ja palomuuri päästää läpi vain VPN-yhteydet langattomasta verkosta. VPN-palvelin voi sijaita vaikka palomuurin yhteydessä.

Joidenkin valmistajien tukiasemissa on RADIUS-tuki. Päätelaitteiden autentikointiin käytetään MAC-osoitetta, ja päätelaitetta ei päästetä asioimaan langattomaan verkkoon mikäli osoitetta ei löydy RADIUS-palvelimen tietokannasta. Toiminta on saman tapainen kuin MAC-pääsynhallintalistoilla, mutta tässä tapauksessa saadaan keskitetyn hallinnan hyödyt. Vaikka MAC-osoitteeseen perustuva autentikointi ei olekaan erityisen varma, toimii se silti hyökkäyksiä vaikeuttavana turvakerroksena. Huonona puolena tässä ratkaisussa on se, että jos RADIUS-palvelin hajoaa, ei kukaan pääse käyttämään WLAN-verkkoa.

Kannettaviin päätelaitteisiin sisältyy aina ylimääräisiä uhkakuvia, jos niitä käytetään työmatkoilla ja kotona. Tällöin laitteiden fyysinen turvaaminen on täysin käyttäjän varassa. Kannettavat on syytä varustaa riittävällä käyttäjän todentamisella ja levyn kryptaamisella, ettei arvokasta tietoa päädy vääriin käsiin ja ettei laitetta voida käyttää hankkimaan pääsy yrityksen sisäverkkoon mikäli laite häviää tai varastetaan. Henkilökohtaiset palomuurit ovat myös suositeltavia kannettavissa, joita käytetään vieraissa verkoissa jolloin ne eivät ole turvassa yrityksen palomuurin takana. Etätyökoneelle voidaan murtautua verkon kautta ja käyttää sitä linkkinä hyökättäessä yrityksen sisäverkkoon. Pelkkä VPN-yhteys ei suojaa yrityksen verkkoa, jos hyökkääjällä on pääsy koneelle, josta on VPN-yhteys yritysverkkoon. Etätyökoneen kunnollisesta palomuurisuojauksesta on paljon apua. Nämä huomiot eivät suoranaisesti liity WLAN-tekniikkaan, mutta kannettavat päätelaitteet ja etätyö yleistyvät mm. WLAN-tekniikan ansiosta ja kannettaviin liittyvät tietoturva-asiat ovat tärkeitä huomioida.

4 WLAN-TEKNIIKKAAN PERUSTUVA JULKINEN VERKKO

WLAN-tekniikkaa on alettu käyttää innokkaasti julkisten verkkojen rakentamiseen. Julkiset langattomat verkot voidaan jakaa kahteen pääluokkaan: avoimet yhteisöverkot ja julkiset hallinnoidut verkot. Avoimet yhteisöverkot ovat vapaaehtoisvoimin rakennettuja ja yleensä kaikkien käytettävissä ilmaiseksi. Julkinen hallinnoitu verkko on yhden organisaation omistuksessa oleva kokonaisuus. Kummankinlaisten verkkojen tavoitteena on tarjota niin sanottu verkkoyhteyden viimeinen linkki niille, joilla ei jo muutoin sellaista ole. Toisin sanoen tarjolla on Internet-yhteys langattomasti. Verkkojen asiakkaat voidaan jakaa myöskin karkeasti kahteen ryhmään: tavalliset kuluttajat ja liikemiehet. Tässä osiossa tarkastellaan käyttäjien tietoturvatarpeita ja erilaisia julkisia WLAN-verkkoja tietoturvaratkaisuineen. Lopuksi esitellään Lappeenrannan teknillisessä yliopistossa tietoliikennetekniikan laitoksen WLAN-hankkeessa kehitetty malli ja testiverkko WLAN-tekniikkaan perustuvalle kaupunkiverkolle tietoturvaratkaisuineen.

4.1 Käyttäjät ja tietoturvatarpeet

Jokaisen yksittäisen tietokonetta ja verkkoa käyttävän tietoturva käsittää perinteiset kolme pääosa-aluetta: luottamuksellisuus, eheys ja saatavuus. Monesti ollaan sitä mieltä, että tavallisen peruskuluttajan tietokone ja verkon käyttö eivät ole tärkeitä, mutta silti tietoturvan peruskäsitteet pätevät tavalliseen Internet-käyttäjään siinä missä suuryrityksen tai valtion verkkoihin. Kukaan ei halua vapaaehtoisesti antaa tuntemattomien lukea tärkeitä dokumenttejaan. Samoin jokainen haluaa varmaankin pitää luottamuksellisena sen mitä tietokoneellaan tai verkkoyhteydellään tekee. On myöskin yleensä varsin toivottavaa, että tietokoneelle talletettu tieto pysyy muuttumattomana ja on saatavilla aina tarvittaessa. [CERT01]

Kaikille avointen verkkojen käyttöön liittyy tietoturvauhkia. Nämä uhkat liittyvät mahdollisuuteen, että joku tai jokin luvaton taho tahallisesti tunkeutuu verkon välityksellä tietokoneelle ja käyttää sitä väärin. Toinen mahdollisuus on, että verkon yli lähetettyä liikennettä salakuunnellaan tai muunnellaan jossain matkan varrella. Muita

uhkia, jotka voivat kohdata vaikka ei olekaan minkäänlaista verkkoyhteyttä, ovat esimerkiksi laitteistoviat, varkaudet ja onnettomuudet.

Verkkojen käyttäjät voidaan jakaa tietoturvatarpeiden osalta karkeasti kahteen luokkaan: tavallisiin kuluttajiin ja liikemiehiin. Kuluttajalla on yleensä varsin rajallinen tietämys verkon teknologioista ja niihin liittyvistä uhkakuvista. Kuitenkin voidaan olettaa heillä olevan seuraavanlaisia vaatimuksia tietoturvan osalta:

- Verkkoyhteys on saatavilla aina tarvittaessa, varsinkin jos siitä maksaa.
- Rahaan liittyvien verkkoasiointien yksityisyys ja turvallisuus.
- Palvelujen saatavuus.
- Sähköpostin ja muun kommunikoinnin yksityisyys.
- Palvelun käytön estäminen oltava mahdollista (esimerkiksi tilanteessa, jossa päätelaite on varastettu ja voitaisiin käyttää vaikkapa verkkoyhteyttä oikean omistajan laskuun).

Osaan tietoturvaan liittyvistä asioista verkkopalvelun tarjoaja voi vaikuttaa jossain määrin, mutta ei kaikkiin. Aina jää osa kuluttajan itsensä harteille hoidettavaksi ja opittavaksi. Yleisin tapa Internet-palveluntarjoajilla on olla ottamatta kantaa yksityisasiakkaan tietoturvaan, paitsi ehkä lisäpalveluna.

Liikemiesten tietoturvavaatimukset eivät periaatteessa eroa paljoakaan tavallisen kuluttajan vaatimuksista. Liikemiehen tapauksessa verkon yli liikuteltava tieto on usein arvokasta. Lisävaatimuksena on yleensä turvallisen yhteyden saaminen yrityksen verkkoon. Useimmiten tämä tarkoittaa jonkinlaista VPN-yhteyttä. Ainakin suuremmissa yrityksissä liikemiehillä on turvanaan yrityksen ylläpito ja tarvittava koulutus. Ylläpito asentaa tarvittavat tietoturvaohjelmistot laitteisiin ja yritys kouluttaa (toivottavasti) henkilökuntansa tietoturva-asioissa päteviksi. Näin ollen liikemiehillä on tavallaan etu tietoturva-asioissa tavallisiin kuluttajiin verrattuna.

4.2 Avoimet yhteisöverkot

Avoimia yhteisöverkkoja alkoi ilmaantua sen jälkeen, kun WLAN-tuotteiden hinnat putosivat kuluttajaystävälliselle tasolle. Tällaiset yhteisöverkot ovat vapaaehtoisvoimin käytännössä tyhjästä rakennettuja ja voivat kattaa suuriakin alueita (luokkaa kaupunginosa tai kaupunki). Yksinkertaisimmillaan vapaa yhteisöverkko muodostuu ihmisistä, joilla on pelkkä WLAN-tukiasema, jonka kautta he haluavat jakaa omia palveluitaan kaikille halukkaille. Tarjolla voi olla myös pääsy Internetiin. Yhteisö verkon takana saattaa antaa teknistä tukea sekä ”asiakkaille” että palveluiden tarjoamiseen osallistuville yhteisön jäsenille. Tarjolla on myös kuuluvuuskarttoja ja ohjeita. Vapaita yhteisöverkkoja on muodostunut eri puolille maailmaa. Suuremmissa projekteissa tavoitteena on luoda kokonainen kaupungin kattava langaton verkkoinfrastruktuuri siten, että tarjolla on täysin kehittynyt verkko omine palveluineen, eikä pelkästään Internet-yhteyksiä.

Tietoturva jää avoimissa yhteisöverkoissa yleensä käyttäjän vastuulle. WLAN-tekniikan omia tietoturvaominaisuuksia ei voi mitenkään järkevästi käyttää ja koska ne ovat muutenkin todistettavasti heikot, on ne yleensä jätetty vapaissa yhteisöverkoissa suosiolla pois käytöstä. Näin helpotetaan verkkoon liittymistä. Käyttäjälle arvokas verkkoliikenne on suojattava kuten aina normaalisti mitä tahansa Internet-yhteyttä käytettäessä. Luottokortin numeroa ei kannata lähettää verkkokauppaan, jos se ei käytä SSL-suojausta. Sähköpostit kannattaa lukea suojatun yhteyden yli (esim. SSH tai SSL) vaikka ne kulkevat sähköpostipalvelimien välillä salaamattomina normaalisti. Yleensäkin on kannattavaa käyttää salausta kaikissa palveluissa, joissa se on mahdollista, koska näin varsinaisen datan lisäksi myös palveluihin tarvittavat salasanat kulkevat verkon yli salattuina. Normaalin Internet-liittymän käyttöön liittyvän varovaisuuden katsotaan usein olevan riittävää, riippumatta viimeisenä linkkinä käytetyn verkkotekniikan turvattomuudesta.

Yhteisöverkoissa verkkoliittymää tarjoava henkilö on myös verkon käyttäjä ja vastaa osaltaan saatavuudesta. Oman kotiverkon suojaaminen häiriköiltä on tärkeää. Tärkeä yksityiskohta on muistaa rajoittaa tukiaseman etähallintaa ja muuttaa oletussalasana, ettei kukaan käy muuttamassa asetuksia luvatta. Verkkoliittymän tarjoaja tarvitsee yleensä enemmän osaamista kuin muut verkon käyttäjät.

4.3 Julkiset hallinnoidut verkot

Julkinen hallinnoitu verkko on yhden organisaation omistuksessa oleva kokonaisuus. Tällaiseen verkkoon pääsy voi olla ilmaista tai maksullista. Julkisia verkkoja on olemassa eri tyylisiä. Suomessa yleisiä ovat kaupunkialueita kattavat WLAN pääsyverkot (access network), jota hallinnoi ja jonka omistaa Internet-palveluntarjoaja. Monet organisaatiot ovat myös kattaneet erikseen WLAN-verkolla julkisia sisätiloja, joissa liikkuu paljon matkustavia ihmisiä, jotka tarvitsevat Internet-yhteyksiä (esim. lentokentät, hotellit jne.). Asiakkaat maksavat yhteyksistään ja huomattavaan osaan tietoturvan puolesta nousee laskutuksen toimivuus.

4.3.1 WLAN-operaattorit

Kaupunkialueita kattavien WLAN-operaattorien kohderyhmänä ovat tavallisesti kuluttajat, jotka eivät muuten helposti saa Internet-yhteyttä kotiinsa. Tässäkään tapauksessa eivät WLAN-standardin tietoturvaominaisuudet ole käyttökelpoisia. Jotkut operaattoreista järjestävät asiakkailleen suojatun yhteyden Internetin rajalle saakka, eli jokaista asiakasta varten järjestetään oma VPN-tunneli, mitä kautta kaikki asiakkaan liikenne kulkee. Näin on tehty esimerkiksi MSOYNETissä [Ran02]. Järjestely vaatii yleensä VPN-asiakasohjelman asentamisen asiakkaan tietokoneelle. Kyseinen järjestely poistaa WLAN-tekniikan tuoman ylimääräisen tietoturvahuolen korkeamman tason salauksella, ja sen seurauksena Internet-yhteys on niin turvallinen kuin se yleensäkään voi olla käyttäjän kannalta. Laskutus on monesti kuukausimaksupohjainen, jolloin palveluntarjoajan puolesta asiakkaiden pääsynhallintaan riittävä keino sisältyy VPN-ratkaisuun ja palomuuriin.

4.3.2 WLAN-palvelualueet

Kaikki tahot eivät pyri kattamaan suuria aloja WLAN-verkolla, vaan pystyttävät ns. hotspotteja eli suhteellisen pieniä WLAN-palvelualueita, joista pääsee Internetiin. Tällaisia hotspotteja on yleensä paikoissa, joissa käy paljon matkustavia ihmisiä, jotka tarvitsevat Internet-yhteyksiä asioidensa hoitamiseen. Yhdellä toimijalla on myöskin oltava näitä hotspotteja kattavasti erilaisissa paikoissa, jotta asiakkailla olisi tarpeeksi

kiinnostusta käyttää palvelua. Jotkut WLAN-operaattorit ovat tehneet keskenään verkkovierailusopimuksia, ja näin kasvattaneet tarjoamansa palvelun kattavuutta. Verkkovierailuille ei ole vielä mitään standardia ratkaisua, joten sopimukset ovat vielä varsin harvinaisia. Suomessa tällaisia hotspot-palveluita tarjoavat mm. Sonera ja Telia.

Soneran wGate-palvelu tarjoaa WLAN-yhteyksiä julkisilla paikoilla, esimerkiksi lentokentillä, hotelleissa, laivoissa ja koulutus- ja konferenssitiloissa. Yritykset voivat myös tilata tiloihinsa wGate-yrityspalvelualueen. Palvelun toimimiseksi on oltava WLAN-verkkokortilla varustettu tietokone ja selainohjelma. Palvelua varten on tehtävä sopimus Soneran kanssa, jolloin saa Internet-yhteyttä varten tarvittavat käyttäjätunnuksen ja salasanan. Palveluun kirjautuminen tapahtuu selaimella ja yhteyden lopettaminen pitää myöskin muistaa tehdä selaimella. WLAN-standardin tietoturvaominaisuudet eivät ole käytössä. Mitään muitakaan tietoturvapalveluita ei wGate tarjoa vaan asiakkaan on itse huolehdittava turvallisuudesta. Hinnoittelu on kuukausimaksuun perustuva ja julkisilla paikoilla wGate-palvelusta peritään vielä minuuttitaksa (tilanne 01/2003). [Son02]

Telian HomeRun toimii valikoiduilla lentokentillä, hotelleissa, kahviloissa ja kongressikeskuksissa kaikissa pohjoismaissa. Telialla on myöskin WLAN-verkkovierailusopimus italialaisen MegaBeamin ja ahvenanmaalaisen Ålcomin kanssa. HomeRun toimii samaan tapaan kuin wGate - käyttämiseen tarvitaan luonnollisesti WLAN-verkkokortti sekä selain. Palveluun tarvittavat käyttäjätunnukset ja salasanat saa tekemällä sopimuksen Telian kanssa. Liittymätyyppejä on kolmenlaisia: liittymä jossa maksetaan pelkkä kuukausimaksu, liittymä jossa maksetaan kuukausimaksu ja minuuttitaksa sekä liittymä, joka on voimassa vain 24 tuntia ensimmäisestä kirjautumisesta palveluun. Tietoturva-asioihin pätee sama kuin wGatessa, eli ne ovat käyttäjän vastuulla. [Telia]

4.4 Case WLAN-hanke

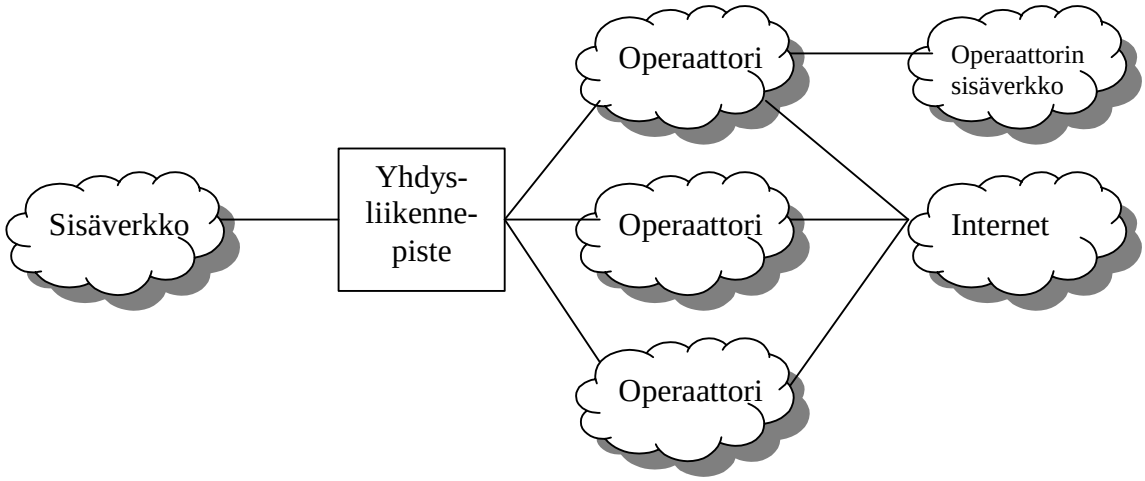
WLAN-hankkeessa tutkitaan langattoman lähiverkkotekniikan käyttöä kaupungin kattavan verkon toteutuksessa. Kaupunkiverkon käytön tulisi olla mahdollista kenelle tahansa, joka kuuluvuusalueelle tulee yhteensopivan laitteiston kanssa.

Lähiverkkotekniikaksi valittiin toteutuksessa 802.11b, koska sen mukaisia tuotteita on saatavilla useilta valmistajilta ja koska kilpailevien standardien mukaisia tuotteita ei oikeastaan ole tarjolla. Näin verkko saa mahdollisimman paljon käyttäjiä ja siitä on useammille hyötyä.

Hankkeen verkko eroaa muista tavallisista WLAN-operaattoreiden verkoista siinä, että verkkoon on toteutettu yhdysliikennepiste, johon eri Internet-palveluntarjoajat (tai muut organisaatiot) voivat liittyä. Kyseessä on ns. monioperaattoriverkko. Eli kaupungin alueelle tulee vain yksi langaton access-verkko, joka on tässä tapauksessa niin kutsuttu sisäverkko. Tähän sisäverkkoon voi kuka tahansa liittyä käyttäjäksi ja yhdysliikennepisteen kautta operaattorit voivat tarjota halukkaille pääsyä hallinnoimaansa verkkoon. Eli esimerkiksi Internet-palveluntarjoajat voivat tarjota sisäverkon käyttäjille pääsyä Internetiin. Hyötynä tästä on esimerkiksi se, että vältetään mahdolliset kilpailevien WLAN-operaattoreiden päällekkäiset verkot, jotka voivat häiritä toisiaan.

4.4.1 Monioperaattoriverkon ja yhdysliikennepisteen toimintaperiaate

Monioperaattoriverkon varsinainen toiminnallisuus on yhdysliikennepisteessä. Yhdysliikennepiste on rajapinta verkkojen välillä, ja käytännössä se on palvelinrypäs sisä- ja ulkoverkon välissä. Sisäverkko voi olla mikä tahansa verkko, ja tämän hankkeen puitteissa se on langaton alueverkko, joka on avoin kaikille kuuluvuusalueella oleville käyttäjille. Peruskäyttöön riittää tietokone, jossa on WLAN-kortti ja kortin tarvitsemat ajurit. Yhdysliikennepisteeseen liitetään sisäverkon lisäksi käyttäjille ulkopuoliseen verkkoon yhteyden tarjoavat operaattorit. Ulkopuolinen verkko voi olla esimerkiksi Internet tai organisaation oma sisäverkko. Kuvassa 11 on esitettynä yhdysliikennepisteen ja monioperaattoriverkon periaate. Jos sisäverkon käyttäjä haluaa päästä käyttämään jonkin yhdysliikennepisteeseen kytkeytyneen operaattorin hallinnoimaan ulkoiseen verkkoon, täytyy käyttäjän tehdä erillinen sopimus kyseisen operaattorin kanssa. Monioperaattoriverkko eroaa perinteisestä yhden operaattorin verkosta siinä, että sisäverkosta on yhden sijasta useita reittejä ulospäin.



Kuva 11: Esimerkki monioperaattoriverkosta yhdysliikennepisteineen [Juu01]

Yhdysliikennepisteen päätehtävä on toimia solmupisteenä kaikelle verkkojen väliselle tietoliikenteelle sekä hallinnoida sisäverkkoa käyttäjineen ja yhteyksiä operaattoreille. Yhdysliikennepisteen tehtävänä on myös tunnistaa sisäverkon käyttäjät ja auktorisoida heidän yhteytensä operaattoreille yhteistyössä operaattoreiden kanssa. Yhdysliikennepiste huolehtii myös käyttäjien verkko-osoitteista ja reitityksestä. Yhdysliikennepisteeseen on kehitetty palvelurajapinta, jonka kautta saadaan sisäverkkoon tarjolle palveluita (esimerkiksi paikannuspalvelu). Verkon käytöstä kerätään lokitietoja toiminnan seurantaa varten. [Juu01]

4.4.2 Tietoturvallisuuden toteuttaminen hankkeessa

Yhdysliikennepisteen toimintaan liittyy monia tietoturvakysymyksiä. Verkon toiminnan kannalta tärkeimpiä ongelmia ovat käyttäjien tunnistaminen ja auktorisointi, jotta heidät voidaan ohjata oikealle operaattorille. Auktorisoinnilla tarkoitetaan valtuuttamista palveluiden ja yhteyksien käyttämiseen. Yhdysliikennepisteessä ei voida ottaa kantaa käyttäjän ja operaattorin väliseen sopimukseen, joten kun käyttäjä haluaa päästä ulos sisäverkosta, on välitettävä todentamistiedot operaattorille ja sieltä tulevan valtuutusvastauksen perusteella avataan yhdysliikennepisteellä tie kyseiselle käyttäjälle ulos verkosta tuon tietyn operaattorin kautta. Näihin kysymyksiin sekä sisäverkon ja yhdysliikennepisteen ylläpidon kannalta tärkeisiin tietoturva-asioihin on paneuduttu muissa projektista tehdyissä töissä.

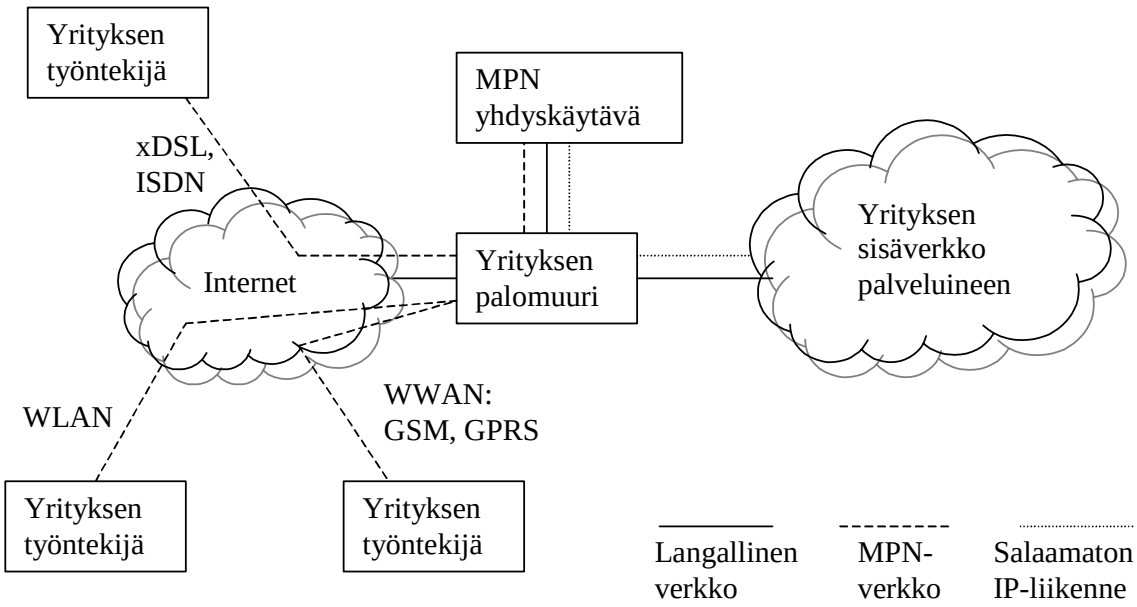
Tässä työssä keskityttiin tarkastelemaan käyttäjän perustietoturvaa ja etenkin WLAN-tekniikan vaikutusta käyttäjän tietoturvan kannalta. Varsin nopeasti WLAN-verkkoihin liittyvän tietoturvan tutkinnan aloittamisen jälkeen havaittiin, että standardissa olevat tietoturvaominaisuudet ovat heikot. Lisäksi standardin tietoturvaominaisuudet ovat täysin sopimattomat avoimessa verkkoympäristössä käytettäväksi. Näihin asioihin ja Internet-käyttöön liittyen tehtiin WLAN-hankkeen verkon käyttäjille tietoturvaohjeistus ja tietopaketti, joka on liitteenä 1.

WLAN-verkkoliikenteen salakuuntelu ja tallentaminen ovat helposti toteutettavissa Internetistä vapaasti saatavilla työkaluilla. Tätä vastaan voidaan käyttää joissain tapauksissa salattuja yhteyksiä, kuten verkkopankissa asioidessa yleensä SSL-salaus ja pääteyhteyksissä SSH. Vielä jää kuitenkin valtaosa verkkoliikenteestä salaamatta, esimerkiksi web-sivuja selaillessa lähes kaikki on kaapattavissa. Vaikka mitään varsinaisesti arvokasta tietoa ei siinä liikkuisikaan, pystyy tunkeilija loukkaamaan verkon käytön yksityisyyttä. Liikennettä voidaan kuunnella missä tahansa verkon pisteessä, mutta kaapeleihin ja verkkolaitteisiin käsiksi pääseminen on paljon vaikeampaa kuin WLAN-lähetysten kuunteleminen. Lisäksi WLAN-salakuuntelusta on oikeastaan mahdotonta jäädä kiinni.

WLAN-salakuuntelun helppous on käytännössä ainoa ero tietoturvan kannalta muihin tekniikoihin, joilla Internet-yhteyden viimeinen linkki toteutetaan. Tätä eroa tasoittamaan etsittiin sopivaa ratkaisua. Yleisesti suositellun ratkaisun todettiin olevan VPN. Hankkeessa oli alun perin suunnitelmana toteuttaa eri kaupunginosia kattavat WLAN-verkot erillisinä aliverkkoina. Tämä taas aiheuttaa sen, että verkkojen välillä liikuttaessa yhteydet katkeavat, koska WLAN-standardin roaming toimii vain alemmilla verkkotasoilla eikä toimi ylemmän verkkotason yhdyskäytävien läpi. Tähän ongelmaan haettiin samalla ratkaisua. Löydettiin tuote, joka ratkaisisi molemmat ongelmat: Netseal-yhtiön MPN (mobile private network), eli ”mobiili yksityisverkko”. MPN on eräänlainen mobile-ip:n ja VPN:n yhdistelmä. Tuotetta testattiin WLAN-hankkeen testiverkossa.

4.4.3 Netseal MPN

Kuvassa 12 on esitetty yksinkertainen esimerkki MPN:n käytöstä. MPN-järjestelmään kuuluu MPN-yhdyskäytävä ja MPN-asiakkaita. MPN-asiakasohjelma asennetaan esimerkiksi yrityksen työntekijöiden kannettaville tietokoneille, jotka ovat mukana esimerkiksi työmatkoilla. MPN toimii IPv4-verkoissa. MPN-asiakas saa staattisen IP-osoitteen, joka annetaan ylläpidon toimesta. Kaikki koneen verkkosovellukset näkevät vain tämän osoitteen, jolloin ne tavallaan luulevat olevansa koko ajan samassa verkossa. Kun MPN-käyttäjät/asiakkaat liikkuvat maantieteellisesti (esim. työmatkalla), he kytkeytyvät Internetiin useiden erilaisten Internet-palveluntarjoajien kautta. Usein noissa verkoissa annetaan IP-osoite automaattisesti DHCP:llä (Dynamic Host Configuration Protocol). MPN-asiakasohjelma ottaa tämän osoitteen käyttöönsä ja ottaa sen avulla yhteyttä MPN-yhdyskäytävään, joka on yrityksen verkon reunalla ja muodostaa salatun IPSec-pohjaisen tunnelin. Tämän jälkeen kaikki liikenne, mitä MPN-asiakaskoneelta lähtee, tunneloidaan ensin MPN-yhdyskäytävälle ja vasta sieltä paketit jatkavat aiottuun kohteeseen. Vastauspaketit kohteesta palaavat MPN-yhdyskäytävän kautta tunnelointiin ja sitä pitkin MPN-asiakaskoneelle.



Kuva 12: Yksinkertainen esimerkki MPN:n käytöstä [Net02]

MPN-ohjelmisto pitää huolta IP-mobiliteetistä ja ylläpitää IPSec-tunnelia liikuttaessa verkosta toiseen. MPN tukee myös verkko-osoitemuunnosten (NAT/PAT, Network Address Translation/Port Address Translation) yli kulkemista ilman että IPSec-tunnelointi hajoaa. [Net02]

4.4.4 MPN WLAN-hankkeen testiverkossa

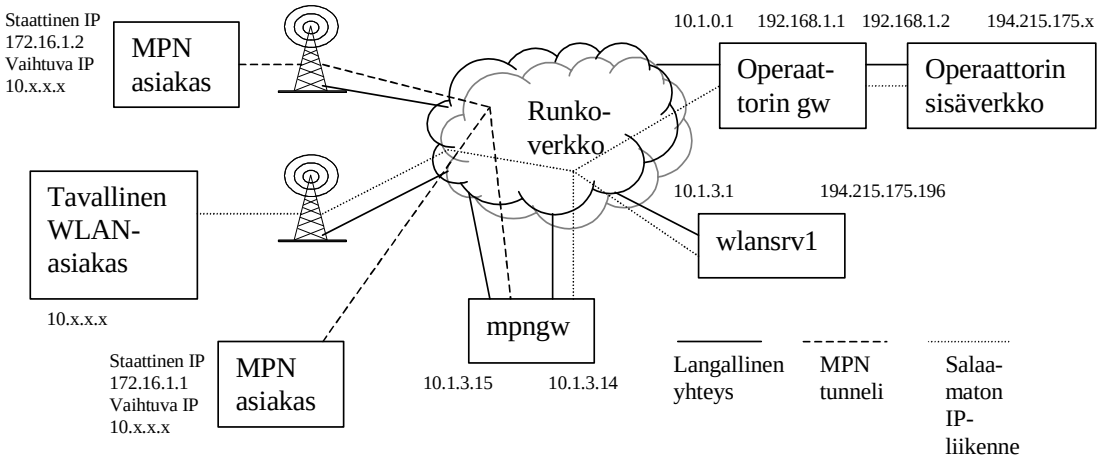
MPN-yhdyskäytäväksi tarvitaan kahdella verkkokortilla varustettu tavallinen pc-kone, johon ohjelmisto asennetaan. Yhdyskäytäväohjelmiston voi asentaa myös korkean saatavuuden versiona, jolloin tarvitaan toinenkin kone. Itse ohjelmisto on helppo asentaa. Asennusvaiheessa pitää olla selvillä kummallekin verkkokortille annettavat osoitteet, sekä asiakaskoneille jaettava kiinteä osoitteistoalue. Toinen verkkorajapinnoista määritellään ’julkiseksi’ ja toinen ’yksityiseksi’. Julkinen rajapinta ottaa vastaan vain MPN-asiakasohjelmien salattuja yhteyksiä, ja on normaalissa verkkoasennuksessa turvattoman verkon puolella (eli esim. Internetin). Yksityinen rajapinta on suojatun yksityisverkon puolella. MPN-palvelun käyttäjillä on oltava MPN-asiakasohjelma asennettuna. Asiakasohjelman asennus on myöskin helppo toimenpide.

MPN:n päätarkoitus WLAN-hankkeen verkossa on turvata datan luottamuksellisuus ilmatiellä. Toinen tavoite on tarjota roaming aliverkkojen välillä, mikäli testiverkko jaetaan aliverkkoihin. Toistaiseksi testiverkko on päätetty pitää yhtenä suurena verkkona, joten MPN:n pääominaisuus jää tässä tapauksessa käyttämättä.

MPN-yhdyskäytävä asennettiin osaksi yhdysliikennepistettä. Käytännössä MPN-yhdyskäytävä kytkettiin testiverkon langalliseen runkoverkkoon kummastakin verkkokortistaan. Kuva 13 esittää asennuksen periaatteen. WLAN-verkkokortilla varustettu MPN-asiakas muodostaa salatun tunnelin MPN-yhdyskäytävään (kuvassa mpngw) minkä jälkeen kaikki liikenne kulkee salattuna MPN-yhdyskäytävälle ’julkiseen’ verkkorajapintaan asti ja siitä eteenpäin ’yksityisen’ puolen verkkokortilta salaamattomana kohti lopullista kohdeosoitetta. Mikäli kohteena on toinen MPN-asiakas, liikenne menee luonnollisesti koko matkan salattuna. Sisäverkossa on käytössä yksityisverkoille varattu osoiteavaruus 10.0.0.0 – 10.254.254.254, ja yhdyskäytävä sai

osoitteet tältä alueelta. MPN-asiakkaiden staattisiksi osoitteiksi annettiin alue toisesta yksityisverkoille varatusta osoiteavaruudesta: 172.16.1.1 – 128.

Tällainen järjestely vaatii lisäyksiä kaikkien verkon yhdyskäytäväkoneiden (kaikki koneet joilla on verkkorajapintoja ainakin kahdessa verkossa) reititystauluihin, jotta MPN-asiakkaille osoitetut paketit osataan ohjata MPN-yhdyskäytävän kautta perille. Järjestely saatiin toimimaan WLAN-hankkeen testiverkossa.



Kuva 13: MPN WLAN-hankkeen testiverkossa

Tuote itsessään todettiin toimivaksi ja melko helpoksi asentaa. Testauksen aikana tuli esiin seuraavia ajatuksia tuotteen sopivuudesta avoimeen kaupunkiverkkoon:

- Verkon peruskäyttöön pitää riittää WLAN-kortti ja sen ajurit, joten ilmatiellä liikkuvan datan vahva salaus voitaisiin tarjota erillisenä palveluna.
- Tavoitteena on, että verkkoa voi käyttää mahdollisimman monilla erilaisilla käyttöjärjestelmillä ja alustoilla, täten tarjottujen palveluiden pitäisi olla järjestelmäriippumattomia, mukaanlukien mahdolliset tarjottavat tietoturvapalvelut.
- Jos WLAN-liikenteen salausta tarjotaan palveluna, olisi ratkaisun syytä olla standardoitu ja sellainen jolle löytyy tuki mahdollisimman laajasti.
- MPN on IPSec-pohjainen, mutta mobiliteetin takia IPSec-toteutus ei ole täysin standardin mukainen. Tämän vuoksi tavallisilla IPSec-asiakasohjelmilla ei voi

ottaa yhteyttä MPN-yhdyskäytävään. MPN-asiakasohjelmia taas ei ole saatavilla kuin Windows-käyttöjärjestelmille. Windows-pohjaisille PDA-laitteille (Personal Digital Assistant) sopivaa versiota MPN-asiakasohjelmasta ei ollut tarjolla testauksia suoritettaessa.

- MPN:n vahvuus, eli verkkosovelluksille näkymätön verkosta toiseen liikkuvuus jää käyttämättä, koska testiverkko on päätetty pitää yhtenä kokonaisena verkkona.

Edellä mainituista syistä johtuen päädyttiin tulokseen, että MPN ei ole paras mahdollinen ratkaisu tämän testiverkon tietoturvaongelmien poistajaksi. Sen sijaan joku standardin mukainen IPSec-yhdyskäytävä saattaisi olla toimiva ratkaisu. Niitä ovat kaupalliset WLAN-operaattoritkin käyttäneet. Toisaalta, jos langattomassa sisäverkossa keskenään liikennöivistä käyttäjistä vain toinen käyttää ylemmän protokollatason salausohjelmistoa, johon liittyy yhdyskäytävä (kuten MPN tai tavallinen IPSec), jää toinen ilmalinkeistä salaamatta. Tällöin tämän tyylisen ratkaisun käyttö saattaa antaa käyttäjälle valheellisen turvallisuuden tunteen. Tämä taas herättää kysymyksen tällaisen tietoturvapalvelun tarpeellisuudesta yleensäkin. Toistaiseksi päädyttiin olemaan tarjoamatta mitään erillistä ilmalinkin salaukseen tarkoitettua palvelua.

5 JOHTOPÄÄTÖKSET

Tehtävänä oli tarkastella kuinka langattomuus vaikuttaa verkon käyttäjän tietoturvaan. Havaittiin, että langattomissa lähiverkkotekniikoissa kommunikointiin käytettävät radioaallot leviävät lähettimien ympäristöön läpäisten jonkun verran fyysisiä esteitäkin. Tämä helpottaa langattomaan lähiverkkoon hyökkäämistä, koska hyökkääjän ei tarvitse tehdä fyysisiä erikoisjärjestelyitä hyökkäämistä varten. Langalliseen verkkoon hyökätessä pitää yleensä päästä verkkoon fyysisesti käsiksi, jolloin hyökkääjä joutuu alttiiksi kiinni jäämiselle. Kun verkon fyysinen turvaaminen ei ole mahdollista, paras ratkaisu verkon yhteyksien suojaamiseen on käyttää kryptografisia menetelmiä.

Työssä tutkittiin WLAN-hankkeeseen valitun langattoman lähiverkkotekniikan, eli IEEE 802.11b-standardin mukaisten laitteiden tietoturvaominaisuuksia. Havaittiin standardin tietoturvaominaisuudet monella tavoin heikoiksi ja avoimeen kaupunkiverkkoon sopimattomiksi. Tulevassa standardin laajennuksessa 802.11i on luvassa parannuksia tietoturvaan. Avointa alueverkkoa käytetään yleensä Internetiin pääsemiseksi, ja tällöin on syytä muistaa, että vaikka langattoman lähiverkkotekniikan tarjoamat tietoturvaominaisuudet olisivat vahvat, auttavat ne vain langattoman linkin salaamiseen. Lähiverkkotekniikan tietoturvaominaisuudet eivät vaikuta päästä-päähän – tietoturvaan mitenkään, eli Internetissä data kulkee selkokielisenä mikäli jotain korkeamman protokollatason salausta ei käytetä.

Lisäksi tutkittiin muutamaa tapausta, joissa 802.11b-verkkoja on käytetty julkisina access-verkkoina. Kaikissa tapauksissa standardin sisältämät tietoturvaominaisuudet oli jätetty pois käytöstä. Lähes aina tietoturvasta huolehtiminen on jätetty käyttäjän omaksi tehtäväksi, kuten muunkinlaisten Internet-yhteyksien tapauksessa. Jotkut WLAN-operaattorit ovat järjestäneet niin, että käyttäjien ilmalinkki on turvattu VPN-ratkaisulla.

Projektissa päätettiin testata tuotetta, joka parantaisi WLAN-asiakkaiden tietoturvaa salaamalla kaiken ilmalinkin yli kulkevan tietoliikenteen. Vaikka tuote on teknisesti täysin toimiva, todettiin se silti avoimeen verkkoympäristöön sopimattomaksi, koska

kyseessä on kaupallinen ja valmistajakohtainen ratkaisu. Asiakasohjelmia ei ole saatavilla kaikille suosituille alustoille.

VPN-ratkaisun käyttäminen ilmalinkin salaamiseen saattaa antaa WLAN-asiakkaalle valheellisen turvallisuuden tunteen, joten tällaisen palvelun tarjoamisesta WLAN-hankkeen verkossa päätettiin toistaiseksi luopua. Huomattavasti tärkeämpää on ohjeistaa verkon käyttäjiä normaaliin Internet-käyttöön liittyvistä tietoturvariskeistä. Verkon käyttäjille suunnattu tietoturvaohjeistus nähtiin tarpeelliseksi joten sellainen tehtiin. Ohjeet ovat liitteessä 1.

LÄHDELUETTELO

[Arb01] Arbaugh, William & Shankar, Narendar & Wan, Justin. 2001. Your 802.11 Wireless Network Has No Clothes. [Kokoomateos]. Proceedings of the International Conference on Wireless LANs and Home Networks, 2001, sivut 131-141. ISBN 981-02-4826-1. Saatavissa: http://www.cs.umd.edu/~waa/wireless.pdf, viitattu 28.4.2002.

[Aso95] Asokan, N. 1995. Security Issues in Mobile Computing. University of Waterloo. [Verkkodokumentti]. Saatavissa: http://www.semper.org/sirene/people/asokan/research/proposal.ps.gz, viitattu 26.3.2002.

[Ber98] Berg, Venla. 1998. TIVEKEn tietoturvasivut. [Verkkodokumentti]. Saatavissa: http://palvelut.tieke.fi/arkisto/tiveke/turva.htm, viitattu 7.3.2002.

[Bor01] Borisov, Nikita & Goldberg, Ian & Wagner, David. 2001. Intercepting Mobile Communications: The Insecurity of 802.11. [Verkkodokumentti]. Saatavissa: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf, viitattu 18.4.2002.

[CERT01] CERT Coordination Center. 2001. Home Network Security. Software Engineering Institute, Carnegie Mellon University. [Verkkodokumentti]. Saatavissa: http://www.cert.org/tech_tips/home_networks.html, viitattu 10.1.2003.

[CERT02] CERT Coordination Center. 2002. Home Computer Security. Software Engineering Institute, Carnegie Mellon University. [Verkkodokumentti]. Saatavissa: http://www.cert.org/homeusers/HomeComputerSecurity/home_computer_security.pdf, viitattu 10.1.2003.

[Cis01] Cisco Systems, Inc. 2001. Overview, Wireless LAN Security. [Verkkodokumentti]. Saatavissa: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm, viitattu 26.3.2002.

[Dea97] Dearden, James. 1997. Wireless Networks. [Verkkodokumentti]. Saatavissa: http://www.jisc.ac.uk/jtap/htm/jtap-014-1.html, viitattu 20.3.2002.

[Dif76] Diffie, W. & Hellman, M. 1976. New directions in cryptography. ISSN 0018-9448. Saatavissa: http://ieeexplore.ieee.org/iel5/18/22693/01055638.pdf, viitattu 23.1.2003.

[Dol95] Doligez, Damien. 1995. I broke Hal's SSL challenge. [Verkkodokumentti]. Saatavissa: http://pauillac.inria.fr/~doligez/ssl/index.html, viitattu 18.4.2002.

[Eng01] Engdahl, Tomi. 2001. Prosessori 5/2001: Salaus Internetissä ja muissa verkoissa. ISSN 0357-4121.

[Flu01] Fluhrer, Scott & Mantin, Itsik & Shamir, Adi. 2001. Weaknesses in the Key Scheduling Algorithm of RC4. [Verkkodokumentti]. Saatavissa: http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps, viitattu 28.4.2002.

[Gei99] Geier, Jim. 1999. Wireless LANs: Implementing Interoperable Networks. ISBN 1-57870-081-7.

[Gra02] Granneman, Scott. 2002. Securing Privacy, Part Two: Software Issues. [Verkkodokumentti]. Saatavissa: http://www.securityfocus.com/infocus/1573, viitattu 10.3.2003.

[IEEE97] The Institute of Electrical and Electronics Engineers, Inc. 1997. IEEE Std 802.11-1997. ISBN 1-55937-935-9. Saatavissa: http://ieeexplore.ieee.org/iel4/5258/14251/00654749.pdf, viitattu 23.1.2003.

[IEEE99a] The Institute of Electrical and Electronics Engineers, Inc. 1999. IEEE Std 802.11, 1999 edition. ISBN 0-7381-1658-0. Saatavissa: http://standards.ieee.org/getieee802/download/802.11-1999.pdf, viitattu 23.1.2003.

[IEEE99b] The Institute of Electrical and Electronics Engineers, Inc. 1999. IEEE Std 802.11a-1999. ISBN 0-7381-1810-9. Saatavissa: http://standards.ieee.org/getieee802/download/802.11a-1999.pdf, viitattu 23.1.2003.

[IEEE99c] The Institute of Electrical and Electronics Engineers, Inc. 1999. IEEE Std 802.11b-1999. ISBN 0-7381-1812-5. Saatavissa: http://standards.ieee.org/getieee802/download/802.11b-1999.pdf, viitattu 23.1.2003.

[IEEE01] The Institute of Electrical and Electronics Engineers, Inc. 2001. IEEE Std 802.1X-2001. ISBN 0-7381-2927-5. Saatavissa: http://standards.ieee.org/getieee802/download/802.1X-2001.pdf, viitattu 28.4.2002.

[IEEE02] The Institute of Electrical and Electronics Engineers, Inc. 2002. Proposed Tgi D1.8 Clause 8 Editing Changes. [Verkkodokumentti]. Saatavissa: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/2-178.zip, viitattu 10.6.2002.

[IEEE03] The Institute of Electrical and Electronics Engineers, Inc. 2003. Status of Project IEEE 802.11g. [Verkkodokumentti]. Saatavissa: http://grouper.ieee.org/groups/802/11/Reports/tgg_update.htm, viitattu 23.1.2003.

[ISO94] International Organization for Standardization. 1994. Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. ISO/IEC 7498-1.

[Juu01] Juutilainen, Matti. 2001. Yhdysliikennepisteen suunnittelu. Diplomityö, Lappeenrannan teknillinen yliopisto. Saatavissa: http://edu.lut.fi/LutPub/web/nbnfi-fe20011637.pdf, viitattu 3.3.2003.

[Ker99] Kerttula, Esa. 1999. Tietoverkkojen tietoturva. 2., uudistettu painos. ISBN 951-37-2904-4.

[Net02] Netseal. 2002. Netseal MPN 3.0 Gateway Setup and Configuration Guide.

[New01] Newsham, Timothy. 2001. 802.11 Wireless LANs. [Verkkodokumentti]. Saatavissa: http://www.lava.net/~newsham/wlan/, viitattu 18.4.2002.

[Oha99] O'Hara, Bob & Petrick, Al. 1999. The IEEE 802.11 Handbook: A Designer's Companion. ISBN 0-7381-1855-9.

[Pfl97] Pfleeger, Charles P. 1997. Security in Computing – International Edition, Second Edition. ISBN 0-13-185794-0.

[Ran02] Rantala, Pekka. 2002. Tietoviikko 25.4.2002: Mäntsälän Sähkö myy nyt langatonta laajakaistaa.

[Rus01] Russell, S. F. 2001. Wireless network security for users. [Julkaisusarja]. Proceedings of the International Conference on Information Technology:

Coding and Computing, 2001, sivut 172-177. ISBN 0-7695-1062-0. Saatavissa: http://ieeexplore.ieee.org/iel5/7336/19864/00918786.pdf, viitattu 26.3.2002.

[Sch00] Schneier, Bruce. 2000. Secrets and Lies: Digital Security in a Networked World. ISBN 0-471-25311-1.

[Sch90] Schilling, Donald & Pickholtz, Raymond & Milstein, Laurence. 1990. Spread spectrum goes commercial. ISSN 0018-9235. Saatavissa: http://fp.ieeexplore.ieee.org/iel3/6/2121/00058433.pdf, viitattu 19.3.2002.

[Sch96] Schneier, Bruce. 1996. Applied Cryptography Second Edition: protocols, algorithms, and source code in C. ISBN 0-471-12845-7.

[Sep00] Seppänen, Lasse. 2000. Langattomat lähiverkot, kurssimateriaali. Hämeen ammattikorkeakoulu. [Verkkodokumentti]. Saatavissa: http://trade.hamk.fi/~lseppane/courses/wlan/doc/WLANmat.doc, viitattu 8.3.2002.

[Shi00] Shirey, R. 2000. RFC 2828: Internet Security Glossary. [Verkkodokumentti]. Saatavissa: ftp://ftp.isi.edu/in-notes/rfc2828.txt, viitattu 1.10.2003.

[Son02] Sonera Oyj. 2002. Sonera wGate – kiinteän verkon nopeus langattomasti, työmatkalla ja yrityksesi tiloissa. [Verkkodokumentti]. Saatavissa: http://www.sonera.fi/CDA.FI.ArticleFrame/0,1362,articleId%3D17651%26expandSize%3D2%26expandLevelId%3D1778_429_331_%26hierarchyId%3D1778,00.html, viitattu 21.1.2003.

[Sta97a] Stallings, William. 1997. Data and Computer Communications, Fifth Edition. ISBN 0-02-415425-3.

[Sta97b] Stallings, William. 1997. Local & Metropolitan Area Networks, Fifth Edition. ISBN 0-13-190737-9.

[Stu01] Stubblefield, Adam & Ioannidis, John & Rubin, Aviel D. Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. AT&T Labs Technical Report TD-4ZCPZZ, Revision 2. [Verkkodokumentti]. Saatavissa: http://www.cs.rice.edu/%7Eastubble/wep/wep_attack.pdf, viitattu 28.4.2002.

[Telia] Telia AB. Telia HomeRun. [Verkkodokumentti]. Saatavissa: http://www.homerun.telia.com/fin/start/default.asp, viitattu 21.1.2003.

[Tou00] Tourrilhes, Jean. 2000. A bit more about the technologies involved… Hewlett Packard Laboratories, Palo Alto. [Verkkodokumentti]. Saatavissa: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.Overview.pdf, viitattu 26.3.2002.

[Usk97] Uskela Sami. 1997. Security in Wireless Local Area Networks. Department of Electrical and Communications Engineering. Helsinki University of Technology. [Verkkodokumentti]. Saatavissa: http://www.tml.hut.fi/Opinnot/Tik-110.501/1997/wireless_lan.html, viitattu 5.6.2002.

[WLANA] The Wireless LAN Association. 1999. Introduction to Wireless LANs. [Verkkodokumentti]. Saatavissa: http://www.wlana.org/learn/intro.pdf, viitattu 8.3.2002.

LIITE 1: TIETOTURVAOHJEITA WLPR.NETIN KÄYTTÄJILLE

Suositeltavat toimenpiteet verkon käyttäjille

Ohjeistuksen aluksi muistilista suositeltavista toimenpiteistä ja toimintatavoista tietoturvallisen käytön saavuttamiseksi:

- käytä virustentorjuntaohjelmistoa
- ole varovainen sähköpostin liitetiedostojen kanssa
- käytä salattuja yhteyksiä (SSL, SSH, PGP jne.)
- pidä käyttöjärjestelmä ja sovellukset ajan tasalla päivittämällä niitä
- ota varmuuskopioita
- käytä palomuuria
- käytä vahvoja salasanoja

Seuraavassa kappaleessa käydään läpi hieman tarkemmin ohjeita laajaan avoimeen verkkoon (yleensä Internetiin) liitetyn kotitietokoneen suojaamisesta ja tietoturvallisesta käytöstä.

Ohjeita tietoturvasta ja kotikoneen suojaamisesta

Tietoturvallisuuden saavuttamiseen auttaa aina käytettävien sovellusten ja verkkoteknologioiden tuntemus; tietää kuinka niitä käytetään oikein ja mitä riskejä niihin liittyy. Kannattaa ottaa selvää sovelluksen toiminnasta ennen asentamista ja käyttöönottoa. Internetin avoimuuden tuntien kannattaa käyttää salausta aina kun se on mahdollista ja datan arvo niin edellyttää. Esimerkiksi web-lomakkeille annettavat salasanat olisi hyvä antaa vain SSL-salatun yhteyden yli, samoin verkkopankissa asioidessa on hyvä varmistaa että yhteys on koko ajan salattu. SSL:ää käyttäessä on hyvä tarkistaa palvelimen antama varmenne, ja varmistaa että todellakin asioi oikean palvelimen kanssa. Pääteyhteyksissä kannattaa käyttää myös salausta (esimerkiksi SSH:ta mikäli mahdollista). Tavallinen sähköposti ei ole tietoturvallinen tapa kommunikoida. Jos sähköpostissa lähetettävien tietojen on vahingollista päätyä sivullisten luettavaksi, kannattaa käyttää salausta. Tähän tarkoitukseen sopivia sovelluksia on useita, ja yksi yleisimmin käytetyistä on PGP.

Salasanoja käytetään monissa yhteyksissä käyttäjien todentamiseen. Salasana pitää valita niin, että se ei ole helposti arvattavissa. Samaa salasanaa ei saa käyttää monissa eri palveluissa. Tämä siksi, etteivät kaikki käyttämäsi palvelut joudu väärinkäytölle alttiiksi jos joku arvaa, tai muuten saa käsiinsä jonkun salasanoistasi. Salasanoja ei saa kertoa kenellekään.

Hanki, asenna ja käytä virustorjuntaohjelmistoa. Erilaisia vahinko-ohjelmia saattaa päästä tietokoneellesi huomaamatta. Käytä virustorjuntaohjelmistoa säännöllisesti tarkistamaan koneesi tila.

Pidä käyttöjärjestelmäsi ja käyttämäsi sovellukset ajan tasalla. Ohjelmistoista löytyy ohjelmointivirheitä, joita voidaan käyttää tietokoneellesi tunkeutumiseen. Virheisiin tehdään myös korjauksia (päivityksiä) ja ne ovat usein saatavissa ohjelmiston valmistajan kotisivuilta. Ajan tasalle päivitettyyn koneeseen on vaikeampaa murtautua.

Ole varovainen avatessasi sähköpostin liitetiedostoja. Ne ovat suosittu tapa levittää vahinko-ohjelmia. Liitetiedosto kannattaa tarkistaa virustutkalla ennen avaamista. Tuntemattomien lähettämiin liitetiedostoihin kannattaa suhtautua erityisellä varovaisuudella. Sähköposti on tosin varsin helppo väärentää, joten lähettäjän nimi ei vielä takaa mitään.

Asenna ja käytä palomuuriohjelmistoa. Palomuurilla voidaan rajoittaa tehokkaasti pääsyä tietokoneelle verkosta. Käyttöönotto ja toimivien asetusten tekeminen vaatii jonkun verran tietoa verkkotekniikasta, mutta oikein säädetty palomuuri on yksi tehokkaimmista tietoturvatekniikoista.

Tee varmuuskopiot tärkeistä tiedostoista ja säilytä niitä fyysisesti eri tilassa kuin itse tietokonetta. Varmuuskopioilta voidaan palauttaa tiedot, jos ne jostain syystä ovat hävinneet (levyrikko, tulipalo, varkaus, viruksen tekemä tuho jne.). Varmuuskopiot kannattaa tehdä säännöllisesti.

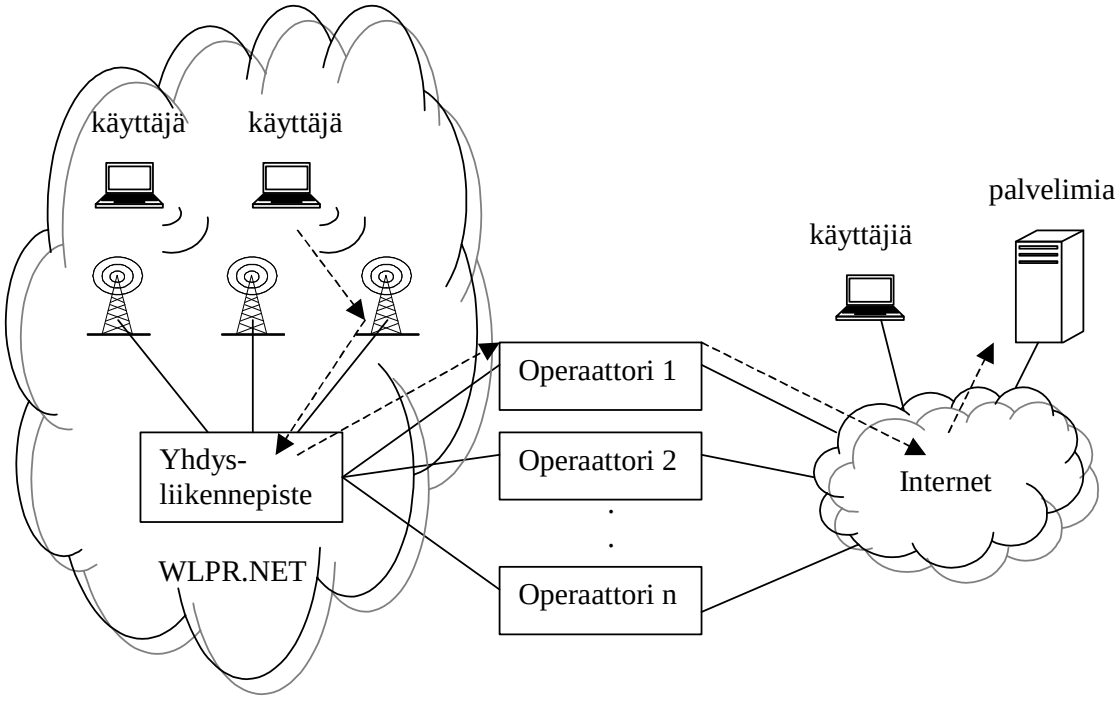
Kannattaa harkita arvokkaiden tiedostojen salaamista jollain tarkoitukseen sopivalla ohjelmistolla. Tällä estetään esimerkiksi varkauden tai verkkomurron tapauksessa

tietojen päätyminen vääriin käsiin. Usean käyttäjän järjestelmissä kannattaa käyttää pääsynhallintakeinoja (esim. pääsynhallintalistat), jotta kaikki eivät pääse käsiksi kaikkien tietoihin.

Seuraavissa kappaleissa käsitellään WLPR.NET-verkon rakennetta ja käyttöön liittyviä tietoturvauhkia. Koska verkkoa voidaan käyttää Internetissä asioimiseen, käsitellään myös Internetiin liittyvät tietoturvauhkat.

WLPR.NETin rakenne ja verkkoliikenteen tietoturva

WLAN-hankkeen testiverkkoa kutsutaan nimellä WLPR.NET. Kuva 1 esittää verkon periaatteellisen rakenteen. Tässä oletetaan, että käyttäjä on Internet-palveluntarjoajan asiakas ja käyttää verkkoyhteyttään Internetissä asioimiseen WLPR.NETin paikallisten palveluiden lisäksi. Verkkoon voi liittyä käyttäen langatonta 802.11b-standardin mukaista verkkokorttia (WLAN-kortti). Kyseessä on siis ns. langaton laajakaistaliittymä, jossa verkkoyhteys on aina päällä kun tietokonekin on päällä. Langaton verkko on periaatteessa muuten samanlainen kuin langallinen verkko, mutta laitteiden välille ei tarvitse kaapelointia vaan langattomat laitteet (kuten langaton verkkokortti ja tukiasema) keskustelevat käyttäen radioaaltoja.



Kuva 1: WLPR.NETin periaatekuva ja yhteys Internetiin

Käydään läpi tiedon kulkua verkossa yksinkertaistetun esimerkin avulla. Oletetaan, että WLPR.NETin langaton käyttäjä haluaa ottaa yhteyttä Internetissä olevaan palvelimeen. Selostuksen mukaista datan kulkua voi seurata kuvasta 1. Käyttäjän tietokoneen lähettäessä dataa palvelimelle se kulkee ensin langattoman linkin yli tukiasemalle. Langatonta linkkiä on suhteellisen helppo salakuunnella, koska radioaallot leviävät joka puolelle ympäristöön ja läpäisevät jonkun verran kiinteitä esteitä. Tukiasemalta data jatkaa langalliseen WLPR.NETin runkoverkkoon ja yhdyskäytävän läpi Internet-operaattorin verkkoon. Operaattorin verkon kautta data jatkaa matkaansa muiden organisaatioiden hallitsemien verkkojen kautta (jotka voivat sisältää mitä erilaisimpia tiedonsiirtoteknologioita) kohti lopullista kohdetta, eli haluttua palvelinta. Dataa voidaan salakuunnella myös langallisessa verkossa, mutta silloin kuuntelijan täytyy päästä käsiksi kaapelointiin tai verkkolaitteisiin. Dataa voidaan tallentaa ja käydä läpi myös yhdyskäytäväkoneilla. Koska data kulkee mitä erilaisimpien ja eri tavoin ylläpidettyjen verkkojen läpi, ei tiedonsiirtotietä kokonaisuudessaan voida pitää luotettavana. Palvelimelta tuleva vastausdata kulkee samoja reittejä takaisin käyttäjälle.

Salakuuntelu ja muut verkkoliikenteeseen kohdistuvat hyökkäykset voidaan estää salauksella ja muilla kryptografian keinoilla. 802.11b-langattomaan lähiverkkotekniikkaan sisältyy salausominaisuudet (linkkitason salaus, eli kahden suoraan keskenään keskustelevan laitteen välisen yhteyden salaus), mutta niitä ei voida käyttää WLPR.NETin kaltaisessa avoimessa verkkoympäristössä. Tämä johtuu siitä, että salaukseen käytetään kaikkien verkon laitteiden kesken jaettua salaisuutta ja salaisuus ei ole salaisuus, jos kaikki tietävät sen. Näin ollen salaus on tehtävä ylemmillä protokollatasoilla, kuten sovelluksissa tai verkkotasolla, jos verkkoliikenteen arvo niin edellyttää.

Tiivistetysti voidaan sanoa, että langatonta verkkoliikennettä on mahdollista salakuunnella lähettimien kantamalta. On kuitenkin huomioitavaa, että mikäli asioidaan esimerkiksi Internetissä, voidaan liikennettä salakuunnella missä tahansa oman tietokoneen ja kohdekoneen välillä. Langaton linkki on vain pieni osa kokonaisyhteydestä. Normaali Internet-yhteyden käyttöön liittyvä tietoturvallisuuden

hallinta ja varovaisuus ovat yleensä peruskäyttäjälle riittäviä liittymätekniikasta riippumatta.

Internetiin liitetyn kotitietokoneen uhkat

Internet on nopeasti muuttuva kokonaisuus rakenteeltaan ja käytettävien teknologioiden osalta. Internet on erittäin laaja ja avoin verkko, joten on mahdotonta tietää mitä kautta verkkoliikenne todellisuudessa kulkee kohteeseensa. Internetissä asioidessa on aina syytä olettaa, että liikennettä voidaan salakuunnella. Internetiin liitettyyn tietokoneeseen voidaan myös ottaa yhteyttä mistä tahansa toisesta Internetiin kytketystä koneesta. Internet-käyttäjän tietoturvauhkat voidaan jakaa karkeasti kolmeen osa-alueeseen:

- Internetissä siirrettävää dataa voidaan salakuunnella, muokata tai väärentää
- tunkeutujat voivat verkkoyhteyden kautta tahallisesti väärinkäyttää tietokonetta
- vahingot ja onnettomuudet, eli uhkat jotka ovat olemassa vaikka tietokone ei olisikaan liitetty mihinkään verkkoon

Seuraavaksi käydään läpi yllä luetellut uhkakuvat yksityiskohtaisemmin. Ohjeita uhkilta suojautumiseen annettiin jo aivan ensimmäisissä kappaleissa.

Suurin osa Internetissä liikkuvasta datasta kulkee salaamattomana. Salaamatonta liikennettä ovat yleensä esimerkiksi sähköposti ja web-selailu. Voidaan ajatella sähköpostin tietoturvan vastaavan postikortin tietoturvatasoa. Sähköposti voidaan lukea luvatta esimerkiksi kaikilta siirtoon käytetyiltä välityspalvelimilta. Sähköpostin sisältö voidaan myös helposti muokata tai väärentää kokonaan. Tietoliikennettä voi nuuskia ja tallentaa verkon kaapelointiin tai laitteisiin käsiksi pääsevä. Näin voidaan saada vaikkapa käyttäjätunnuksia ja salasanoja, joita annetaan salaamattomien yhteyksien yli esimerkiksi web-pohjaiseen palveluun.

Internetin käyttäjien joukkoon mahtuu suuri joukko potentiaalisia tunkeutujia. He etsivät toisten tietokoneilta tietoja tai ottavat tietokoneen haltuunsa käyttääkseen sitä hyökätäkseen muualle. Verkkoon liitettyyn koneeseen voi päästä käsiksi esimerkiksi sovelluksissa olevien viallisten asetuksien takia tai sovelluksissa ja käyttöjärjestelmässä olevien ohjelmointivirheiden ansiosta. Muuta tahallista pahantekoa ovat sähköpostin

mukana tulevat vahinko-ohjelmat (virukset, troijalaiset) ja verkosta ladattavien sovellusten mukana tulevat vahinko-ohjelmat.

Vahingot ja onnettomuudet käsittävät esimerkiksi laitteistorikon, virransyöttöön liittyvät ongelmat ja varkauden. Tietokoneen levyn rikkoutuminen voi johtaa kaiken levyllä olevan tiedon peruuttamattomaan menetykseen. Virransyötössä ilmenevät ongelmat, kuten virtapiikit, voivat rikkoa laitteistoa. Varas saattaa viedä koko tietokoneen ja päästä käsiksi siihen tallennettuun tietoon.

Loppusanat

Tämä ohje- ja tietopaketti on tehty verkon käyttäjien avuksi. Uhkista puhuttaessa ei ole tarkoitus pelotella vaan tuoda käyttäjien tietoisuuteen, että verkon käyttöön liittyy myös riskejä. Ikävät tilanteet pystyy välttämään kunhan vaan osaa varautua niihin.

Käytetyt lyhenteet

PGP Pretty Good Privacy – sovellus, jota käytetään salaamaan mm. sähköpostia

SSH Secure Shell – ohjelma, jolla voi muodostaa salattuja etäyhteyksiä

SSL Secure Sockets Layer – Internetissä yleisesti käytetty protokolla turvalliseen viestintään, esimerkiksi selaimissa web-liikenteen salaamiseen

WLAN Wireless Local Area Network – langaton lähiverkko