WLAN-turvallisuus

Juha Niemi

Helsinki 18. huhtikuuta 2003

Tietoturvallisuus nykyaikaisessa liiketoimintaympäristössä -seminaari

HELSINGIN YLIOPISTO

Tietojenkäsittelytieteen laitos

Sisältö

1 Johdanto

Langattoman tiedonsiirron mahdollisuuksista ollaan jo pitkään oltu kiinnostuneita. Erityisesti viime vuosina tietoverkkojen merkityksen kasvaessa on oman tietokoneen ulkopuolelta haettavan tiedon tarve jatkuvasti lisääntynyt, joten erilaisissa palavereissa ja neuvotteluissa tarvitaan yhteys esimerkiksi internettiin tai lähiverkon palvelimelle. Ajatus langattomasta lähiverkosta tuntuu houkuttavalta, sillä enää ei kannettavalla tietokoneellakaan olla sidottuja lähimpään verkkopistokkeeseen vaan voidaan käyttää verkkoa vapaasti koko sen kuuluvuusalueella.

Näissä *WLAN-verkoissa* (Wireless Local Area Network) on niiden tarjoamien hyötyjen lisäksi myös useita erilaisia ongelmia. Tieto siirtyy ilmateitse hitaammin kuin kiinteissä verkoissa, joten langattomuuden aiheuttama viive ja toisaalta kiinteitä yhteyksiä pienempi 11 MBps tiedonsiirtonopeus (kyseinen nopeus on tällä hetkellä se yleisimmin käytetty – suurempia nopeuksia on tietysti jatkuvasti kehitteillä) tekee WLAN-ratkaisusta riittämättömiä moniin tämän päivän käyttökohteista.

Hidasta liikennöintinopeutta suurempi ongelma on kuitenkin langattomien verkkojen riittämätön tietoturva. Oletusasetuksillaan WLAN-laitteet päästävät usein kenet tahansa käyttämään verkkoa. Mutta vaikka monenlaisia suojauksia voidaankin kytkeä päälle, eivät ne kuitenkaan tee IEEE 802.11 –standardin langattomasta verkosta täysin turvallista.

Seuraavassa esitellään WLAN-verkkojen ongelmia ja etsitään niihin ratkaisuja. Lisäksi tutustumme myös uusiin, IEEE 802.11:n korvaaviin standardeihin ja selvitämme, onko niissä jo opittu aiemmin tehdyistä virheistä.

2 IEEE 802.11:n turvallisuus

Langattoman tiedonsiirron historia seuraa tietoturvan näkökulmasta hyvin pitkälti langattomien puhelinten tekniikan kehitystä. Kuka tahansa pystyi salakuuntelemaan analogisia kännyköitä ja melkein samanlaisella tavalla alkoi myös WLAN-verkkojen aikakausi, kun IEEE:n langattomien verkkojen standardi 802.11 saatiin vihdoin vuonna 1997 valmiiksi. Standardin suojaustavat jäivät kuitenkin kiireen iskettyä hieman keskeneräisiksi ja toisaalta luotettiin siihen, että langattomassa tiedonsiirrossa käytetään huomattavasti aiempia ratkaisuja laajempaa taajuusaluetta, minkä salakuuntelemiseen olisi erittäin vaikea kehittää sopivia välineitä. Kuitenkin unohdettiin, että WLAN-käyttöön suunnitelluilla vastaanottimilla liikenteen kuunteleminen onnistui käden käänteessä ja pian osoitettiin myös standardin muiden tietoturvaominaisuuksien heikkoudet.

IEEE 802.11 –standardin tietoturvan kulmakivi on kryptografiaan perustuva *WEP-protokolla* (Wired Equivalent Privacy). WEP-salausta pidettiin kuitenkin jo alusta alkaen riittämättömänä suojauksena, sillä salausjärjestelmien voimakkuuksia sääteli vielä viime vuosikymmenellä USA:n tiukat salauksen vientirajoitukset joten salaisen avaimen pituus oli tuolloin rajoitettu 40 bittiin. Mutta vaikka nykyään voidaankin jo käyttää 64- ja 128-bittisiä avaimia, on myös todettu, että WEPin ja sitä myöten WLANin suurimmat heikkoudet ovat itse salauksen toimintatavassa eikä niinkään avainten pituudessa [Cra02].

WLANiin kohdistuvat murtautumisyritykset voidaan karkeasti jakaa viiteen ryhmään: Fyysisiin hyökkäyksiin, imitointiin, eheyden säilyttäviin hyökkäyksiin, kuunteluhyökkäyksiin sekä palvelunestohyökkäyksiin [SAM00].

Fyysisellä hyökkäyksellä tarkoitetaan yrityksen tietokoneen varastamista. Tällöin hyökkääjä saa haltuunsa WLAN-verkon salaisen avaimen ja saattaa päästä käyttämään yrityksen verkkoa hyvinkin pitkän aikaa. Jos varas saa vaikkapa haltuunsa WLAN-verkkokortin ja varkautta ei heti havaita tai siitä ei raportoida, voi varas verkon toteutuksesta riippuen saada itselleen pääsyn verkkoon hyvinkin helposti. Lisäksi, koska IEEE 802.11 –pohjaisissa langattomissa verkoissa ei ole käyttäjäkohtaista tunnistusta, on tällaista tavallisesta poikkeavaa aktiviteettia usein hyvin vaikea havaita.

Imitoinnissa hyökkääjä väittää olevansa toinen, verkkoon käyttöoikeudet omaava henkilö. Imitointi vaatii yleensä langattoman liikenteen salakuuntelua ja oikean henkilön pääsyn estämistä esimerkiksi denial of service –tekniikkaa käyttäen.

Eheyden säilyttävässä hyökkäyksessä hyökkääjän päämääränä on muuttaa langattomassa verkossa liikkuvaa tietoa omien etujensa mukaiseksi niin, etteivät muut verkon solmut havaitse muutosta.

Kuunteluhyökkäyksessä eli passiivisessa hyökkäyksessä ei varsinaisesti murtauduta langattomaan verkkoon vaan tyydytään kuuntelemaan sen liikennettä. Tällä tavalla pystytään kuuntelemaan liikennettä pitkiäkin aikoja, sillä organisaatio ei voi mistään arvata, että verkkoa kuunneltaisiin salaa.

Palvelunestohyökkäyksessä estetään käyttöoikeudet omaavan käyttäjän pääsy verkkoon esimerkiksi kuormittamalla verkkoyhteyttä.

2.1 WEP

WEP (Wired Equivalent Privacy) on IEEE 802.11-standardissa määritelty RC4-salaukseen perustuva tietoturvaprotokolla, jonka käyttäminen on standardissa kuitenkin jätetty vapaaehtoiseksi. WEP pyrittiin suunnittelemaan sellaiseksi, että sen avulla voitaisiin varmistua tiedon luottamuksellisuudesta ja aitoudesta sekä suorittamaan luotettava autentikointi.

WEPissä salainen avain (klassinen WEP avaimen koko 40 bittiä, standardista kehitetyssä laajennetussa versiossa 104 bittiä) yhdistetään 24-bittiseen alustusavaimeen, jolloin tuloksena saadaan 64- tai 128-bittinen avain. Tämä alustusavaimen liittäminen salaiseen avaimeen tehdään jokaisen salattavan paketin yhteydessä, jotta lopputuloksena jokaiselle paketille saataisiin samasta salaisesta avaimesta huolimatta erilainen RC4-avain [Eat02].

Paketissa kuljetettavalle tiedolle lasketaan tarkistussumma (CRC), jotta paketin purkava osapuoli voi varmistua tiedon aitoudesta. Kuljetettava tieto ja tarkistussumma kryptataan tämän jälkeen bittitason XOR-funktiolla ja saadun salatun sanoman oheen lisätään vielä selväkielisessä muodossa salaisen avaimen muodostamiseen käytetty alustusavain, minkä jälkeen tieto on valmis lähetettäväksi vastaanottajalle [Cra02].

Hyvältä kuulostavista ominaisuuksista huolimatta WEP-protokollan rakenne sisältää merkittäviä puutteita tietoturvan kannalta ja sekä passiiviset (murtautuja tyytyy salakuuntelemaan liikennettä) että aktiiviset (murtautuja osallistuu liikennöintiin esimerkiksi kaappaamalla yhteyden) hyökkäykset ovat mahdollisia.

Yhtä näistä WEP-protokollassa havaituista haavoittuvuuksista kutsutaan alustusavaimen törmäykseksi. Koska käytännössä salainen WEP-avain muuttuu vain harvoin (jos koskaan), käytetään alustusavainta varmistamaan se, että koko RC4-avain olisi jokaisella lähetyskerralla erilainen. Avaimen erilaisuus on siksi tärkeää, että samoilla salausavaimilla salattujen kahden paketin purkaminen on mahdollista siinä tapauksessa, että pystytään eristämään liikenteestä salattuja sanomia niin, että tiedetään myös niiden selväkielinen merkitys. Alustusavaimen kierrätyksessä on kuitenkin usein heikkouksia, sillä WEP-määrittelyssä vain suositellaan (mutta ei pakoteta) alustusavaimen vaihtamista jokaisen siirretyn paketin jälkeen. Useilla langattoman verkon laitteilla alustusavain nollataan aina yhteyden muodostuksen yhteydessä ja toisaalta avaimen pituus (24 bittiä) tarkoittaa, että uniikkeja arvoja riittää normaalisti liikennöidyssä langattomassa verkossa noin puoleksi päiväksi [BGW01].

Salatun sanoman yhdistäminen selväkieliseen sanomaan kuulostaa aluksi miltei mahdottomalta mutta sitäkin varten on omat keinonsa. Langattomassa verkossakin siirtyvässä IP-liikenteessä on standardin myötä useita ennalta ennustettavia kenttiä. Toisaalta myös sisältöä pystytään ennakoimaan, kuten sisäänkirjautumiset palveluihin salasanankyselyineen noudattavat usein tiettyä kaavaa. Toinen lähestymistapa on joidenkin langattoman verkon laitteiden kautta syntyvä mahdollisuus lähettää selväkielinen sanoma langattomaan verkkoon niin, että tukiasema kaiuttaa sen takaisin salatussa muodossa [BGW01]. Toisiinsa täsmäävien salatun ja selväkielisen tiedon saatuaan murtautuja pystyy purkamaan kaikki paketit jotka käyttävät samaa alustusavainta. Samaa menetelmää murtautuja voi vähitellen hankkia itselleen myös muihin alustusavaimiin täsmäävät purkukoodit. Kaikki alustusavaimet sisältävä sanakirja (decryption dictionary) tosin veisi tilaa useita kymmeniä gigatavuja.

Keksijöidensä mukaan nimetyssä Fluherin, Mantinin ja Shamirin (FMS) hyökkäyksessä lähestysmistapa on hieman erilainen, sillä se perustuu WPA:ssä käytetyn RC4-salauksen avaintenjakoalgoritmissa ilmenneeseen heikkouteen [SIR01]. RC4 on yksi yleisimmistä salauksessa käytetyistä algoritmeista ja sitä pidetään turvallisena oikein käytettynä. Kuitenkin WPA:n yhteydessä ilmenee kaksi heikkoutta, joilla RC4 on murrettavissa.

Käytännössä näin tapahtuva avaimen selvittäminen vaatii vain suuren datamäärän kuuntelemista, mihin menee verkon käyttöasteesta riippuen tunneista viikkoihin. Toisaalta riittävän tietojen kuuntelun jälkeen avaimen selvitys vie valmiita ohjelmia kuten AirSnortia käyttäen vain muutamia sekunteja.

Vaikka WEP-protokollassa onkin havaittu lukuisia teknisiä puutteita, pystyy WEP kuitenkin yhdessä muiden myöhemmin käsiteltävien suojaustapojen kanssa tarjoamaan kohtalaisen (tieto ei ainakaan ihan selväkielisenä liiku) suojauksen, mikä riittää ainakin osaan langattomien verkkojen käyttötarkoituksista. Usein tämäkin suojaus onnistutaan kuitenkin pilaamaan joko välinpitämättömyydellä (miksi kukaan haluaisi murtautua juuri meidän organisaatiomme verkkoon) tai tietämättömyydellä. Tärkeä osa WEP-suojausta on WEP-avainten hallinta ja niiden vaihtaminen säännöllisin väliajoin [Cra02]. Useassa langatonta verkkoa käyttävässä organisaatiossa avaimia ei vaihdeta välttämättä koskaan. Joku yrityksen tietokoneista saatetaan vaikka varastaa, jolloin varas saa langattoman verkon salaisen avaimen haltuunsa – mutta kenellekään ei välttämättä tule mieleenkään päivittää tämän jälkeen salainen avain uuteen.

Lisäksi IEEE 802.11 standardi tukee muutamia WEP-protokollan luotettavuutta lisääviä ominaisuuksia. Esimerkkejä tällaisista ovat mahdollisuus käyttää neljää WEP-avainta rinnakkain sekä mahdollisuus käyttää asiakaskohtaisesti eri avaimia. Kumpikaan ominaisuuksista ei poista murtautumisen mahdollisuutta mutta tekee siitä jälleen vähän vaikeampaa vähentämällä alustusvainten törmäämisen todennäköisyyttä.

2.2 Autentikointi

Jotta laite voisi kytkeytyä käyttämään langatonta verkkoa, on sen ensin tunnistauduttava verkon tukiasemalle. IEEE 802.11:ssä tämä on mahdollista tehdä joko standardiin pakollisena kuuluvalla ja yleensä oletusasetuksena päällä olevalla *avoimella autentikoinnilla* tai vaihtoehtoisesti *jaetun avaimen autentikoinnilla*.

Avoin autentikointi perustuu *palvelutunnisteeseen* (Service Set Identification, SSID) joka tarkoittaa käytännössä verkon nimeä, jonka sekä asiakkaalla että tukiasemalla on oltava sama, jotta autentikointi olisi mahdollinen [Cra02]. Koko avoin autentikointi onkin tietoturvamielessä lähinnä vitsi, sillä langattoman verkon yhteyspisteet lähettävät tätä verkon nimeä toimintatavastaan johtuen jatkuvasti selväkielisenä ilmoittaakseen mahdollisille verkon uusille asiakkaille läsnäolostaan.

Jaetun avaimen autentikointi on tunnistustavoista hieman avointa autentikointia turvallisempi. Siinä autentikointiin tarvittavaa tunnusta ei siirretä selväkielisenä ilmateitse vaan käytetään ns. haaste-metodia: Tukiasema pyytää asiakaslaitetta salaamaan tälle lähettämänsä viestin. Jos sekä asiakaslaitteella että tukiasemalla on käytössään sama (siis oikea) avain, pystyy asiakas salaamaan viestin ja lähettää

seuraavaksi puolestaan salatun viestin tukiasemalle, joka pystyy vuorostaan tästä purkamaan esiin alkuperäisen viestin [ASW01]. Jaetun avaimen autentikoinnissa käytetty avain on kuitenkin se sama, mitä myös WEP käyttää liikenteen suojaamiseen, joten tämän avaimen varastamalla murtautuja saa siis itselleen pääsyn sekä autentikoinnin että WEPin läpi.

Koska molemmissa autentikointimalleissa asiakkaan tunnistaminen perustuu yhdelle ja samalle avaimelle, on käyttäjäkohtaisen tunnistamisen tekeminen mahdotonta. Toisaalta myöskään tukiasemaa ei voida tunnistaa, mikä avaa mahdollisuudet yhteyksien kaappaamiselle.

2.3 Muita ongelmia

Eri valmistajien WLAN-verkkolaitteiden välillä on toisinaan havaittu yhteensopivuusongelmia. Laitteet saattavat toimia hieman eri tavoin niin etteivät onnistu muodostamaan yhteyttä toistensa välille. Viimeisenä keinona tällaiset laitteet saattavat yrittää yhteydenmuodostusta toimittamalla salaisen avaimen ilmateitse selväkielisenä. Tällöin avain on helppo poimimalla liikenteen joukosta. Lisäksi käyttäjän aitoutta ei IEEE 802.11-standardissa varmisteta millään tavalla, joten liikenteen kaappaamiselta on vaikea suojautua.

Vaikka WEP-salaus siis onkin murrettavissa kohtuullisen pienessä ajassa, on tilanne hyvin useissa langattomissa verkoissa tietoturvan kannalta tehty vielä sitäkin huonommaksi. Suurimpana syynä tilanteeseen on ihmisten huolimattomuus ja toisaalta tietämättömyys langattoman tekniikan toimintatavasta. Kukaan ei välttämättä tule edes ajatelleeksi, että työpaikalle

rakennettu langaton verkko saattaa ylettyä myös viereisiin toimistoihin ja jopa kokonaan rakennuksen ulkopuolelle. Esimerkkinä tästä voidaan pitää ns. parkkipaikkahyökkäystä - Yhdysvalloissa, Kalifornian Piilaaksossa on langattomien lähiverkkojen löytämiseksi riittänyt lähteä autoajelulle ja antaa kannettavan tietokoneen ja siihen yhdistetyn WLAN-verkkokortin hakea avoimia verkkoja. WEP-salauksen käyttäminen on standardissa määritelty vapaaehtoiseksi ja niinpä etenkin langattomien lähiverkkojen alkuaikoina markkinoilla oli useita laitteita, joissa koko salausta ei ollut toteutettu vaikkapa tiukasta aikataulusta johtuen [Joh02].

Usein WEP-salauksen tilalla on käytetty verkkokorttien MAC-osoitteisiin perustuvaa suojausta. Tällöin langattoman verkon tukiasema tai palomuuri estää oletusarvoisesti kaikki yhteydet ja vain ennalta määritellyille MAC-osoitteille avataan pääsy verkkooon. Tällainen verkkortin yksilöintitunnuksen käyttäminen on kuitenkin suojaustapana vähintäänkin kyseenalainen, sillä suurimmassa osassa verkkokorteista MAC-osoitteen voi ohjelmisto- tai laitteistopohjaisesti määritellä itse. Lisäksi MAC-osoitteet siirretään verkossa aina salaamattomassa muodossa, joten oikean osoitteen hankkiminenkin on helppoa [ASW01].

Vaikka IEEE 802.11-standardissa onkin edellä mainittuja vakavia heikkouksia, voidaan langaton verkko kuitenkin toteuttaa sitäkin käyttäen vähintään keskinkertaisen turvallisesti. Tällöin paras mahdollinen tietoturva saavutetaan kiinnittämällä huomiota pieniinkin yksityiskohtiin eli niin fyysiseen kuuluvuusalueen rajoittamiseen kuin esimerkiksi MAC-osoitteiden käyttöön.

Lisäksi tulee laatia yritykselle sopiva tietoturvapolitiikka, jonka perusteella huolehditaan WEP- ja MAC-tekniikoiden ajantasaisuudesta ja salaisen avaimen vaihtamisesta säännöllisin väliajoin. Erityisesti on muistettava, että usein tietoturvan kannalta suurin uhka tulee organisaation sisältä esimerkiksi taitamattoman tai omia ohjelmiaan asentelevan työntekijän muodossa.

Edellä mainittu MAC-osoitteiden tunnistaminen olisi kuitenkin vaikea toteuttaa suurissa organisaatioissa, missä tietokoneet ja työntekijät saattavat vaihtua tiheään tahtiin. Näissä tilanteissa usein käytetty ja pienillekin organisaatioille turvallinen ratkaisu on se, että estetään kokonaan suora pääsy yrityksen paikallisverkkoon langattoman yhteyden kautta eli kohdellaan langattoman yhteyden käyttäjää siis ulkopuolisena tahona eikä päästetä häntä automaattisesti palomuurin ohitse. Tämän jälkeen voidaan käyttää vaikkapa VPN-yhteyttä sisäverkkoon pääsemiseksi.

3 Uudet ratkaisumallit

Vuonna 1997 julkaistu IEEE 802.11 alkaa olla atk-maailmassa jo varsin vanha standardi. Tämän jälkeen on tullutkin jo useita IEEE 802.11:n korvaajia, joista osa on jo standardeja ja osa vielä keskeneräisiä.

Tietoturvaa parantavien standardien lisäksi on IEEE 802.11:n jälkeen julkaistu myös koko joukko esimerkiksi WLANin nopeutta tai laajennettavuutta koskevia standardeja, kuten verkon siirtonopeuden 1-2 Mbps tasolta 11 Mbps:n nopeuteen nostava IEEE 802.11b .

Tietoturvan kannalta keskeisimmät uudet standardit ovat IEEE 802.1x ja IEEE 802.11i. Nämä uudet standardit on suunniteltu joustaviksi niin, että käyttäjä voi esimerkiksi valita käyttämiään salauksia. Tämä lisää tietoturvaa mutta toisaalta siirtää entistä enemmän vastuuta WLAN-laitteiden valmistajille ja loppukäyttäjille.

3.1 IEEE 802.1x

Ensimmäinen edistysaskel langattomien verkkojen tietoturvan kannalta oli vuonna 2001 julkaistu IEEE 802.1x, jossa IEEE 802.11:een verrattuna on uutta lähinnä autentikointi. Uusi standardi on kuitenkin laadittu niin, että sitä on helppo laajentaa. Niinpä muunmuassa oikeuksienvalvonta ja avaintenhallinta on helposti toteutettavissa IEEE 802.1x:n päälle.

Asiakkaan tunnistamisessa käytetään IEEE 802.1x:ssä protokollaa nimeltä *EAP* (Extensible Authentication Protocol). EAP-määrittely on rakennettu niin, että se tukee useita erilaisia tunnistustapoja, kuten Kerberosta, kertakäyttösalasanoja, sertifikaatteja ja julkisen avaimen varmennusta [Cra02].

Uuden standardin mahdollistaman dynaamisen avaintenhallinnan myötä päästään eroon staattisten avainten aiheuttamasta ongelmasta. Nyt salausavaimia voidaan vaihtaa automaattisesti ja niin usein kuin vain halutaan. Tällä saadaan hyvä suoja niitä hyökkäyksiä vastaan, joissa suuret tietomäärät kaappaamalla yritetään murtaa WAP-suojaus [MiA02].

Kuitenkin jo muutaman kuukauden päästä IEEE 802.1x:n julkaisusta saatiin selville, että vaikka uusi standardi onkin alkuperäistä IEEE 802.11:a huomattavasti turvallisempi, on tämäkin ratkaisu edelleen alttiina hyökkäyksille. Esimerkiksi yhteyden kaappaus -hyökkäyksessä hyökkääjän on ensin odotettava, että asiakas tunnistautuu langattomaan verkkoon ja tämän jälkeen estettävä asiakkaan yhteydet ja esiinnyttävä asiakkaana.

Toinen tapa hyökätä IEEE 802.1x:n yli on langattomaan verkkoon tunnistautumisensa jälkeen saada asiakas QUIT-viestiä käyttäen uskomaan, että yhteys verkkoon on katkennut. Nyt langattoman verkon palvelin luulee asiakkaan edelleen olevan aktiivinen eikä huomaa yhteyden kaappausta [MiA02].

3.2 IEEE 802.11i

Vuodesta 2000 alkaen kehitteillä ollut ja tämän hetken ennustusten mukaan vuonna 2004 julkaistava IEEE 802.11i tulee sisältämään entisestään parannetun tietoturvan, jota kutsutaan nimellä Robust Security Network (RSN). Sen avulla pitäisi pystyä estämään kaikki tällä hetkellä tiedossa olevat hyökkäykset. RSN muodostuu kolmesta osasta; kahdesta avaintenjakomallista, joista toinen (Temporal Key Integrity Protocol, TKIP) on suunniteltu vanhemman WLAN-laitteiston yhteensopivuutta varten ja toista (Counter Mode with CBC-MAC Protocol, CCMP) päästään kunnolla hyödyntämään vasta tulevissa järjestelmistä [Eat02]. Näiden IEEE 802.11i-standardin kahden alemman kerroksen päällä on edellisessä kappaleessa käsitelty IEEE 802.11x.

Tällainen IEEE 802.11i:n ja IEEE 802.1x:n yhdistelmä mahdollistaa vahvan käyttäjätunnistuksen ja salausavainten jakamisen. Näiden kahden standardin yhdistäminen koetaan erittäin tärkeäksi, sillä yksittäin käytettynä kumpikaan näistä osista ei vielä olisi riittävän turvallinen.

4 Yhteenveto

IEEE 802.11 –standardiin perustuvien langattomien verkkojen tietoturvaan ei ole luottaminen. Standardin tietoturva perustuu hyvin pitkälti siinä käytettyyn WEP-salaukseen mutta siinä havaitut ongelmat tekevät verkkoon murtautumisen mahdolliseksi. Toisaalta kaikissa verkoissa ei edes käytetä koko salausta, joten niissä tapauksissa tietoturva on lähinnä muutamien hyvin helposti murrettavien esteiden varassa.

Helpotusta tilanteeseen ovat onneksi tuomassa uudet standardit, joiden pitäisi ainakin teoriassa poistaa heikkoudet. Erityisesti näillä näkymin vuonna 2004 julkaistavalta IEEE 802.11i –standardilta odotetaan paljon, sillä se kokoaa aiempien standardien ominaisuudet yhteen pakettiin tavoitteinaan vahva tietoturva.

Useat verkkolaitevalmistajat ovatkin jo lisänneet vastaavia ominaisuuksia laitteisiinsa tietoturvaongelmien korjaamiseksi. Usein tällaiset laitteet ovat myöhemmin päivitettävissä myös varsinaisen standardin mukaisiksi, joten langattoman verkon toteuttaminen tälläisilla laitteilla voi jo tässä vaiheessa olla perusteltua. Sen sijaan vain perus-IEEE 802.11:tä tukevaan laitteistoon ei kannata enää investoida, mikäli haluaa pitää lähiverkkonsa turvallisena. Muutoin on vähintään eristettävä langaton verkko lähiverkosta ja muodostettava pääsy esimerkiksi VPN:n kautta.

Lähteet

ASW01 Arbaugh, W., Shankar, N., Wan, Y., Your 802.11 Wireless Network has No Clothes. Department of Computer Science University of Maryland College Park, Maryland, March, 2001.

BGW01 Borisov, N., Goldberg, I., Wagner, D., Intercepting Mobile Communications: The Insecurity of 802.11. Proceedings of the seventh annual international conference on Mobile computing and networking, Italy, 2001.

Cra02 Craiger, J., 802.11, 802.1x, and Wireless Security. SANS, June, 2002.

Eat02 Eaton, D., 802.11 Security. Intersil White Papers, 2002.

Joh02 Johnson, B., Wireless 802.11 Security: Questions & Answers to Get Started. SystemExperts Corporation, 2002.

Kla02 Klaus, C., Wireless LAN Security FAQ version 1.7. Internet Security Systems, 2002, http://www.iss.net/wireless/WLAN_FAQ.php

MiA02 Mishra, A., Arbaugh, W., An Initial Security Analysis of the IEEE 802.1X Standard. University of Maryland, 2002.

Ned01 Nedeltchev, P., Wireless Local Area Networks and the 802.11 Standard. 2001.

Sam00 Simon, D., Aboba, B., Moore, T., IEEE 802.11 Security and 802.1X. Microsoft Corporation, 2000.

SIR01 Stubblefield, A., Ioannidis, J., Rubin A., Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. Rice University, Houston, 2001.