VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Timo Tammela

LANGATTOMAN LÄHIVERKON TIE-TOTURVA

Liiketalous ja matkailu
2015

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Timo Tammela
Opinnäytetyön nimi	Langattoman lähiverkon tietoturva
Vuosi	2015
Kieli	suomi
Sivumäärä	34
Ohjaaja	Antti Mäkitalo

Opinnäytetyön tavoitteena on luoda kattava opas langattomista verkoista ja niiden tietoturvasta. Teorian lisäksi on tarkoitus tehdä käytännön ohjeet langattoman verkon suojaamiseen. Langattomat verkot ovat yleistyneet paljon ja sen vuoksi niiden tietoturva on käsiteltävänä aiheena ajankohtainen.

Työssäni käytin materiaalina useita kirjoja, jotka käsittelivät langattomia verkkoja ja niiden tietoturvaa. Kirjojen lisäksi käytin paljon verkosta löytyvää materiaalia, sillä osassa kirjoista oli vanhentunutta materiaalia. Työn seurauksena tieto langattomista verkoista ja niiden tietoturvasta on kasvanut.

Aluksi kerron työssäni langattomista verkoista ja niiden standardeista. Tämän jälkeen kerron itse tietoturvasta ja yleisimmistä langattomien lähiverkkojen uhista ja lopuksi esittelen, miten langattomasta verkosta saadaan tietoturvallinen.

Avainsanat WLAN, Tietoturva, 802.11, langaton lähiverkko, opas

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittely

ABSTRACT

Author	Timo Tammela
Title	Security of Wireless Local Area Network
Year	2015
Language	Finnish
Pages	34
Name of Supervisor	Antti Mäkitalo

The aim of this thesis was to create a comprehensive guide about Wireless Local Area Networks and their security. As a result of a great increase in WLANs has become a topical subject. In addition to theory a guide on how to secure Wireless Local Area Network was created

A lot of different books about WLANs and security were used in the study. Also, some material available on the internet was used because some books had old information in them.

The theoretical study first explains what WLAN is and introduces some of the most important standards. Then the security of WLAN and the most common threats to WLANs are explained. The final chapter shows how to secure your own Wireless network and last the result of the thesis are discussed

Keywords WLAN, information security, guide

SISÄLLYS

KUVIO- JA TAULUKKOLUETTELO

KÄSITTEET

WLAN	Wireless Local Area Network, Langaton lähiverkko
WEP	Wired Equivalent Privacy, salausmenetelmä
WPA	Wi-fi Protected Access, Tietoturvaprotokolla
WPA2	Wi-Fi Protected Access, Uudempi tietoturvaprotokolla
TKIP	Temporal Key Integrity Protocol, salausprotokolla
SSID	Service Set Identifier, WLAN-verkon tunnus
IP	Internet Protocl, Protokolla, joka reitittää paketteja verkon laitteiden välillä.
IP-Osoite	Numerosarja jolla yksilöidään verkkosovittimia
CCMP	Counter Mode Encryption with CBC-MAC Data Origin Authenticity Protocol, salausprotokolla
AES	Advanced Encryption Standard, salausalgoritmi
ARP	Address resolution Protocol, Protokolla, joka selvittää IP-osoitetta vastaavan MAC-osoitteen
USB	Universal Serial Bus, väylä jonka avulla oheislaitteet voidaan liittää tietokoneeseen
Ethernet	Pakettipohjainen lähiverkkotekniikka.
LAN	Rajoitetulla alueella toimia tietoliikenneverkko.

1 JOHDANTO

Langattomia verkkoja löytyy lähes kaikkialta, kotitalouksista, kahviloista, kouluista, hotelleista ja työpaikoista. WLAN-verkot ovat yleistyneet paljon. Yksi syy tähän on niiden helppo ja halpa asennus. Lisäksi langattomat laitteet, kuten älypuhelimet ja tabletit, ovat yleistyneet erittäin paljon, mikä on nostanut langattomien verkkojen kysyntää. Yleistymisen myötä myös tietoturvan tärkeys kasvaa. Langattomuus tulee melko varmasti vain kasvamaan, sillä nykypäivänä langattomuus ja liikkuvuus ovat ihmisille tärkeitä. Työssä tullaan käymään läpi langattoman verkon ominaisuuksia, historiaa, standardeja, tietoturvaominaisuuksia sekä tietoturvauhkia.

Tutkimusongelmat

Opinnäytetyön tutkimusongelmana on selvittää, miten saadaan toteutettua tietoturvallinen langaton lähiverkko helposti. Lisäksi selvitetään mikä on langaton lähiverkko, mitä on langattoman verkon tietoturva, millaisia uhkia langattomiin verkkoihin kohdistuu sekä työn lopuksi toteutetaan yksinkertainen langaton lähiverkko.

Tavoitteet

Työn teoriaosuudessa tutustutaan ensin siihen, mikä on langaton lähiverkko ja kerrotaan hieman langattomien verkkojen taustoista. Lisäksi kerrotaan, millaisia laitteita langattomien verkkojen luomiseen käytetään sekä mitä positiivista ja negatiivista langattomissa lähiverkoissa on. Tämän jälkeen teoriaosuudessa esitellään yleisimpiä langattoman verkon standardeja. Standardien jälkeen tutustutaan tietoturvaan. Aluksi esitellään, millaisilla keinoilla tietoturvaa voidaan parantaa ja kerrotaan kattavasti näistä asioista. Teoriaosan lopuksi kerrotaan hieman langattomiin verkkoihin kohdistuvista uhista

Käytännön osuudessa näytetään, miten luodaan tietoturvallinen langaton lähiverkko ja mitä tulee ottaa huomioon langatonta lähiverkkoa luodessaan. Lisäksi näytetään, miten voidaan liittyä omaan suojattuun langattomaan verkkoon.

2 WLAN

WLAN (lyhenne sanoista Wireless Local Area Network) on langaton lähiverkkotekniikka, jonka avulla erilaiset verkkolaitteet pystytään yhdistämään verkkoon ilman kaapeleita. WLAN perustuu IEEE 802.11-standardeihin ja sitä markkinoidaan Wi-Fi-tuotemerkillä. WLAN-laitteet keskustelevat samoilla 2,4GHz- ja 5GHz-radiotaajusalueilla huolimatta siitä, missä päin maailmaa yhteys on pystytetty. Nämä kyseiset taajuusalueet jaetaan useiksi kanaviksi. Kanavien käyttöluvat vaihtelevat maantieteellisesti. (Taulukko 1) Yhteensä kanavia on 14. (Viestintävirasto 2014, 4.)

Taulukko 1. Kanavat jotka ovat käytössä eri alueilla. (Cisco 2008.)

Kanava	**Keskitaajuus**	**USA ja Kanada**	**Eurooppa/Lähi-itä/Afrikka**	**Japani**
1	2412 MHz	x	x	x
2	2417 MHz	x	x	x
3	2422 MHz	x	x	x
4	2427 MHz	x	x	x
5	2432 MHz	x	x	x
6	2437 MHz	x	x	x
7	2442 MHz	x	x	x
8	2447 MHz	x	x	x
9	2452 MHz	x	x	x
10	24157 MHz	x	x	x
11	2462 MHz	x	x	x
12	2467 MHz		x	x
13	2472 MHz		x	x
14	2484 MHz			x

1980-luvun puolivälissä Motorola esitteli ensimmäisen WLAN-tuotteensa, Altairin. Motorolan Altair ja muut 80- ja 90-luvun alkupuolen tuotteet olivat kuitenkin valmistajakohtaisia. Tämä seurauksena uuden tekniikan ensimmäiset käyttäjät joutuivat sitoutumaan yhden valmistajan tuotteisiin ja luottamaan valmistajien epävarmoihin lupauksiin tulevaisuudesta. (Puska 2005,15.)

Vuonna 1990 IEEE:n (Institute of Electrical and Electronics Engineers) standardointiryhmä aloitti kehittämään langattoman lähiverkon standardeja. Ensimmäinen 802.11-standardi julkaistiin vuonna 1997. Se mahdollisti 2 Mbps:n enimmäisnopeuden, mutta jäi huomattavasti alle aiemmin julkaistun Fast Ethernet–lähiverkon suorituskyvyn. Lisäksi ongelmana olivat yhteensopivuusongelmat, sekä käyttölupaongelmat käytetyssä taajuuskaistassa. 802.11-standardia pidetään langattoman lähiverkon perusstandardina ja siihen on kehitetty paljon erilaisia laajennusosia. (Puska 2005, 15.)

2.1 Laitteet

2.1.1 Langaton verkkosovitin

Verkkosovitin on laite, jonka avulla tietokone vastaanottaa tukiaseman tai langattoman reitittimen radiosignaaleja. Langaton verkkosovitin käyttää antennia kommunikoidakseen radioaaltojen avulla tukiasemien ja langattomien reitittimien kanssa. Verkkosovittimia käytetään tietokoneiden liittämisessä verkkoon niin langallisissa kuin langattomissakin verkoissa. Nykypäivänä verkkosovitin on usein sisäänrakennettu moniin laitteisiin esimerkiksi kannettaviin tietokoneisiin. Pöytäkoneisiin täytyy yleensä ostaa erillinen verkkosovitin, joka liitetään esimerkiksi tietokoneen USB-väylään.

2.1.2 Tukiasemat

Tukiaseman tehtävä on tarjota langaton yhteys langalliseen Ethernet-verkkoon. Tukiasema sisältää verkkosovittimen, joka lähettää langattomia signaaleja. Näiden signaalien avulla laitteet voivat muodostaa yhteyden tukiaseman kautta langalliseen verkkoon. Tukiasemat eivät itsessään sisällä internet-yhteyden jakamistekniikkaa, joten tukiasema pitää olla liitettynä reitittimeen, jotta pääsy internettiin on mahdollista. (Microsoft 2015.)

2.1.3 Langaton reititin

Reitittimen tehtävä on siirtää verkkojen välillä paketteja. Tämä mahdollistaa verkkojen välisen liikenteen esimerkiksi kotiverkon ja internetin välillä. Langaton reititin sisältää yleensä sisäänrakennetun tukiasematoiminnon, joten erillistä tukiasemaa ei välttämättä tarvita ollenkaan. Langattomat reitittimet sisältävät myös mahdollisuuden liittää laitteita langallisesti verkkoon. Useimmiten langattomat reitittimet sisältävät neljä Ethernet-porttia, joihin voi liittää esimerkiksi pelikonsoleita tai pöytäkoneita. (Microsoft 2015.)

2.2 Hyödyt

Langattomuuden ansiosta käyttäjät voivat käyttää internetiä ja sitä vaativia sovelluksia ja ohjelmistoja vapaasti ilman fyysisiä rajoitteita. Tämän myötä käyttäjä voi liikkua rakennuksessa vapaammin. Esimerkiksi, ihmiset jotka tekevät työtä kotoa käsin ja tarvitsevat työnsä tekoon internetyhteyttä, voivat langattoman yhteyden ansiosta liikkua vapaasti huoneesta toiseen. (Geier 2005, 3.)

Langaton lähiverkko on myös helpompi, halvempi ja nopeampi keino luoda lähiverkko kuin asentaa yleiskaapelointiin perustuva lähiverkko. Varsinkin kodeissa joissa internet-yhteys halutaan jakaa useammalle työasemalle, on langaton lähiverkko siisti ja helppo ratkaisu. (Puska 2005, 19.)

2.3 Riskit

Langattoman verkon dataliikenne perustuu radioaaltoihin. Radioaaltojen eteneminen ei pysähdy rakennuksen sisälle. Tämän vuoksi langattoman verkon salakuuntelu ja häirintä ulkopuolelta on yksi langattoman verkon haasteista. Sen vuoksi on syytä kiinnittää huomiota oman WLAN-verkon tietoturvaan. (Puska 2005, 21.)

Radiosignaalin etenemisen kontrollointi ja mallinnus on vaikeaa, sillä kentän voimakkuuteen ja suoritustehoon vaikuttavat monet asiat, kuten elektronisten laitteiden sähköinen kohina, kalusteet, ihmiset, kasvillisuus ja sääolosuhteet. Tämän vuoksi langattoman lähiverkon toteutus luotettavasti on hankalaa. Lisäksi lähistöllä

olevat muut yhteyspisteet vaikuttavat toisiinsa ja siten koko verkon toimintaan. (Puska 2005, 21-22.)

3 LANGATTOMAN VERKON STANDARDIT

IEEE on kansainvälinen organisaatio. Se kehittää sähköteknisiä tieteitä valmistelemalla ja julkaisemalla standardeja. Kuten aiemmin toin esille, 802.11 oli IEEE:n ensimmäinen langattomien verkkojen standardi. 802.11-standardin jälkeen IEEE on julkaissut lukuisia päivityksiä standardeihin ja tämän luvun tarkoituksena on esitellä niistä olennaisimmat. Taulukossa 2 on lyhyt koonti standardeista ja niiden ominaisuuksista, joista kerron myöhemmin tarkemmin.

Taulukko 2. Yhteenveto standardeista.

Standardi	**Ratifioitu**	**Taajuusalue**	**Nopeus teoriassa**	**Kanavia yht.**
802.11	1997	2,4 GHz	1 ja 2 Mbit/s	14
802.11b	1999	2,4 GHz	1, 2, 5,5 ja 11Mbit/s	14
802.11a	1999	5 GHz	6 – 54 Mbit/s	12
802.11g	2003	2,4 GHz	1 – 54 Mbit/s	12
802.11n	2009	5 ja 2,4 GHz	600 Mbit/s	
802.11ac	2014	5 GHz	6933 Mbit/s	

IEEE:n 802.11-standardit kuuluvat OSI-mallin (Open System Interconnection) (Kuva 1) kahteen alimpaan kerrokseen eli fyysiseen kerrokseen ja siirtokerrokseen. Nämä molemmat kerrokset on jaettu kahteen osaan. Siirtokerros muodostuu siirtoyhteyden ohjauksesta (LLC, Logical Link Control) ja kaistanvarauksesta (MAC, Medium Access Control). Fyysinen kerros muodostuu konvergenssikerroksesta ja mediariippuvaisesta kerroksesta. (Puska 2005, 25.)

Kuva 1. OSI-malli. (Geier 2004)

3.1 IEEE 802.11a

Vuonna 1999 IEEE julkaisi uuden 802.11a-standardin. Se mahdollisti 54 Mbit/s nopeuden ja käytti siirtotekniikkana monikantoaaltomodulointia (Orthogonal Frequency Divison Multiplexing, OFDM). Yhteyden kantama voi olla 30 metriä riippuen siitä, mikä on todellinen tiedonsiirtonopeus (Geier 2005, 124-125.)

802.11a-standardi toimii 5Ghz:n taajuusalueella toisin kuin 802.11-standardi, joka toimii 2,4Ghz:n taajuusalueella. Useimmat langatonta lähiverkkoa häiritsevät laitteet, esimerkiksi mikroaaltouuni, langattomat puhelimet ja bluetooth toimivat 2,4 Ghz:n taajuudella. Tämän vuoksi on alhaisempi todennäköisyys RF-interferenssille. Suurimmat ongelmat 802.11b-standardissa on yhteensopimattomuus 2,4Ghz:n taajuudella toimivien laitteiden kanssa, sekä lyhyt kantama verrattuna 2,4Ghz:n taajuutta käyttäviin laitteisiin. (Geier 2005, 124-125.)

3.2 IEEE 802.11b

Samaan aikaan IEEE 802.11a-standardin kanssa julkaistiin 802.11b-standardi. Se toimi samalla 2,4Ghz:n taajuudella kuin alkuperäinen suorasekvenssistandardi, mutta oli huomattavasti nopeampi. 802.11b laajennus mahdollisti 11Mbps:n enimmäisnopeuden. Suuremman nopeuden lisäksi etuna oli pidempi kantama. 802.11b–standardilla voidaan saavuttaa jopa 100 metrin kantama. Pitkän kantaman ansioista langattomien lähiverkkojen toteuttamiseen tarvittiin vähemmän tukiasemia kuin 802.11a:ta käytettäessä. (Geier 2005, 126.)

802.11b-standardilla on 14 kanavaa käytettävissä tukiasemien konfigurointiin sen 2,4Ghz:n taajuusalueella. Ongelmana tässä kuitenkin on, että jokainen kanava varaa signaalin lähetykseen lähes kolmasosan 2,4Ghz:n kokonaiskaistasta. Tämän vuoksi taajuusalueelle mahtuu ainoastaan kolme ei-päällekkäistä kanavaa. Lisäksi 802.11b:n käyttämä taajuusalue on alttiimpi RF-interferenssille toisin kuin 802.11a. (Geier 2005, 126.)

3.3 IEEE 802.11g

Vuonna 2003 IEEE ratifioi jälleen uuden 802.11-standardin. Tämä 802.11g-standardi on yhteensopiva 802.11b:n kanssa. 802.11g käyttää siirtotekniikkana OFDM:ää ja toimii 2,4Ghz:n taajuudella. Lisäksi 802.11g-standardin maksimaalinen tiedonsiirtonopeus on jopa 54Mbps.

802.11g-standardin merkittävin etu on yhteensopivuus 802.11b:n kanssa ja laitteet, jotka käyttävät 802.11b-standardia, on helppo päivittää 802.11g-standardiin laiteohjelmistopäivityksen avulla. On kuitenkin tärkeää huomata, että tilanteessa, jossa verkossa on sekä 802.11b- ja 802.11g-standardia käyttäviä laitteita samanaikaisesti, tulee käyttöön ottaa suojelumekanismeja. Suojelumekanismin tarkoituksena on estää laitteita lähettämästä samaan aikaan. Tämän johtuu standardien eriävästä moduloinnista. 802.11b-laitteet eivät tajua, milloin 802.11g-laitteet lähettävät. Siksi molempien laitetyyppien tulee ilmoittaa siirtotien käytöstä modulointityypillä, jota molemmat laitetyypit ymmärtävät.

3.4 IEEE 802.11i

Kesäkuussa 2004 IEEE ratifioi uuden 802.11i–standardin. Tämän standardin tarkoituksena oli parantaa langattomien verkkojen tietoturvaa ja tuoda se nykyaikaiselle tasolle. Tietoturvaa pyrittiin kehittämään esimerkiksi TKIP ja CCMP-salausprotokollilla, joiden tarkoituksena oli korvata WEP-salauksen tietoturvapuutteet. Näistä salausprotokollista tehokkaampi CCMP-salausprotokolla käyttää salaukseen lohkosalausta ja TKIP käyttää jonosalausta. Lisäksi standardi toi uudenlaisen 802.1x todennus- ja avaintenhallintamenetelmän. (Puska 2005.)

3.5 IEEE 802.11n

Vuonna 2009 IEEE julkaisi uuden standardin nimeltä 802.11n. Uuden standardin pääasiallinen tarkoitus oli kasvattaa langattomien verkkojen tiedonsiirtonopeutta. Teoriassa tiedonsiirtonopeus voi olla jopa 600Mbit/s, mutta siihen vaikuttavat monet tekijät, kuten käytettävät laitteet, konfigurointi ja laitteiden sijoitus. Jotta suuri tiedonsiirtonopeus olisi mahdollista 802.11n-standardi käyttää Multiple Input Multiple Output (MIMO) – tekniikkaa. MIMO moniantennitekniikka hyödyntää signaalien lähetykseen useita eri antenneja. Tämän lisäksi 802.11-standardi käyttää suurempaa kaistanleveyttä kuin vanhemmat standardit. Vanhat standardit käyttävät 20 MHz:n kaistanleveyttä, 802.11n-standardi pystyy käyttämään 20MHz:n ja 40MHz:n kaistanleveyttä. Suuremmalla kaistanleveydellä saavutetaan suuremmat tiedonsiirtonopeudet. (AirMagnet 2008.)

3.6 IEEE 802.11ac

Vuonan 2014 IEEE julkaisi jälleen uuden standardin. Uuden standardin tarkoituksen oli edelleen nopeuttaa tiedonsiirtoa langattomassa verkossa. Tämä uusi 802.11ac-standardi käyttää vain 5GHz:n taajuusaluetta. Kaistanleveyttä on uudessa standardissa kehitetty. 802.11ac-standardi käyttää 20-, 40-, 80- ja 160MHz:n kaistanleveyttä. Tämän lisäksi 802.11ac-standardi tukee MU-MIMO –tekniikkaa (Multi-user MIMO). Toimintaperiaate on sama kuin MIMO:ssa, mutta MU-MIMO tukee jopa kahdeksaa antennia, kun 802.11n-standardi tukee vain neljää. (Cisco 2014.)

4 LANGATTOMAN VERKON TIETOTURVA

Tietotekniikassa tietoturva on aina ollut erittäin tärkeässä osassa. Tietoturvan tarve on vain kasvanut entistä enemmän. Tämä johtuu siitä, että tietotekniikan läsnäolo yhteiskunnassa on kasvanut huomattavasti. Erityisen tärkeää tietoturva on langattomissa verkoissa, koska tukiasemien ja langattomien reitittimien lähettämiä signaaleja ei voi pysäyttää. Tämän vuoksi nämä viestisignaalit ovatkin vapaasti tavoitettavissa niiden edetessä ilmassa. Langattomaan verkkoon kohdistuvia uhkia on kuitenkin mahdollista ehkäistä muutamilla yksinkertaisilla keinoilla, joita käydään lävitse seuraavaksi.

4.1 MAC-Suodatus

Nykyään suuri osa langattomista tukiasemista mahdollistaa MAC-osoitteiden suodatukseen. MAC-osoitetta (Media Access Control) käytetään liikenteen ohjaamiseen ja jokaisella verkkokortilla on oma yksilöllinen MAC-osoite. MAC-suodatuksen käyttö tarkoittaa, että tukiasema tarkistaa saapuvien kehyksien MAC-lähdeosoitteet. Mikäli osoitetta ei löydy sallittujen MAC-osoitteiden listalta, se hylätään. (Geier 2005, 187.)

MAC-suodatus ei ole kuitenkaan täydellinen tietoturvaratkaisu, koska esimerkiksi WEP-salaus ei salaa MAC-osoitekenttää kehyksessä. Tämän vuoksi hakkeri voi helposti salakuunnella verkon liikennettä ja selvittää sallittuja MAC-osoitteita. Saatuaan selville sallitun MAC-osoitteen hakkeri voi muuttaa oman verkkokorttinsa MAC-osoitteen verkossa sallituksi osoitteeksi. Tällä tavoin hakkeri voi naamioitua sallituksi käyttäjäksi. (Geier 2005, 187.)

Puutteellisen tietoturvan lisäksi MAC-suodatuksen ongelmana on työläs ylläpito. Järjestelmänvalvojan täytyy syöttää verkon käyttäjien MAC-osoitteet listaan ja tehdä muutoksia aina, kun uusi käyttäjä liittyy verkkoon. Tämän vuoksi MAC-suodatus sopii parhaiten verkkoihin, joilla on vähän käyttäjiä. (Geier 2005, 187.)

4.2 SSID:n naamiointi

SSID (Service Set Identifier) on langattoman verkon verkkotunnus. Sen avulla voidaan kytkeytyä haluttuun verkkoon ja erotetaan samalla alueella olevat WLAN-verkot toisistaan. Tukiasemat lähettävät verkkojensa SSID-tunnusta verkon kuuluvuusalueen laitteille. Langattoman verkon SSID-tunnuksen voi kuitenkin naamioida, mikäli haluaa, että se ei näy verkon kuuluvuusalueella oleville laitteille. (Geier 2005, 107.)

Ongelmana kuitenkin on, että SSID-tunnus kulkee salaamattomana verkon laitteiden ja tukiaseman välillä. Niinpä jälleen salakuuntelun avulla voidaan selvittää verkon SSID-tunnus. Tämän vuoksi SSID-tunnuksen naamiointia ei pidetä erityisen tehokkaana tietoturvaratkaisuna. (Coleman, Westcott, Harkins & Jackman 2010, 51-52.)

4.3 WEP

WEP (Wired Equivalent Privacy) oli ensimmäinen 801.11-standardin salausmenetelmä. WEP-salaus käyttää RC4-jonosalausta, joten salausavaimen täytyy olla saman pituinen kuin tavujono jota salataan. Salaus muodostuu 104- tai 40-bittisestä salausavaimesta ja 24-bittisestä alustusvektorista (IV, Initialization Vector). Yhdessä ne muodostavat joko 64 tai 128-bittisen RC4-avainvuon. RC4-salausavaimen luomiseen käytettävä alustusvektori kulkee lähettäjän ja vastaanottajan välillä selväkielisenä WEP-kehyksessä. Tämän avulla vastaanottaja kykenee luoda RC-avaimen, jota käytetään salauksen purkamiseen. (Puska 2005.)

Ennen kuin lähetettävä data salataan, WEP laskee datalle nelitavuisen eheystarkisteen (ICV, integrity check value). Eheystarkiste on tarkistussumma, jonka vastaanottava laite laskee uudelleen ja vertaa laskennan tulosta lähetettävältä asemalta saatuun tarkisteeseen. Tällä pyritään turvaamaan kehyksen eheys. Mikäli aseman laskema eheystarkiste ei ole sama kuin kehyksessä, on se merkki siitä, että lähetystä on peukaloitu ja kehys hylätään. (Geier 2005, 181)

Nykyään ei suositella käytettäväksi WEP-salausta. Se on erittäin haavoittuvainen ja helppo murtaa. Pääosin siksi, että alustusvektorit ovat lyhyitä ja avaimet kiinteitä.

WEP käyttää samoja alustusvektoreita eri datapaketeissa tietyn ajan jälkeen. Tämä on ongelma varsinkin isommissa verkoissa, sillä suuren liikennöinnin vuoksi alustusvektori voi toistua alle tunnissa. Tämän vuoksi lähetettävien kehysten avainmerkkijonot alkavat olla hyvin samanlaisia. Keräämällä tarpeeksi kehyksiä, joilla on sama alustusvektori, voi hakkeri selvittää salausavaimen. (Puska 2005, 182)

4.4 WPA

WPA (Wi-Fi Protected Acces) on päivitys WEP-salausprotokollaan. WPA:n tarkoituksena oli paikata WEP:ssä ilmenneet puutteet ja tietoturva-aukot. Yksi suurin päivitys WPA:ssa oli TKIP (Temporal Key Integrity Protocol) -salausprotokolla. WPA käyttää TKIP:tä liikenteen salaukseen. Tämän lisäksi WPA tarjoaa kaksi versioita: WPA-Personal ja WPA-Enterprise. Näistä WPA-Personal on suunnattu lähinnä koteihin ja pieniin verkkoihin ja WPA-Enterprise suurten yritysten verkkoihin. WPA-Personal ja WPA-Enterprise eroaa toisistaan siten, että WPA-Personal käyttää PSK-todennusta (Pre-Shared Key) ja WPA-Enterprise IEEE 802.1x- ja EAP -protokollia todentamiseen (Extensible Authentication Protocol), joista lisää myöhemmin. (Geier 2005. 184.)

4.5 WPA2

WPA2 on tällä hetkellä tehokkain tietoturvaluokitus WLAN-teknologiassa ja se perustuu IEEE 802.11i–standardiin. Suurin muutos WPA2:n ja WPA:n välillä on niiden käyttämä salaus. WPA2:n salaus perustuu CCMP-protokollaan, joka käyttää salaukseen AES-lohkosalausta. WPA2 on myös yhteensopiva vanhempien tietoturvaprotokollien kanssa. WPA2:sta on tarjolla kaksi eri versioita Personal-versio koteihin ja pieniin toimistoihin sekä Enterprise versio isojen yritysten käyttöön. Käyttäjien todentamiseen WPA:ssa käytetään PSK-todennusta, sekä IEEE 802.1x ja EAP-protokollia. (Wi-Fi alliance 2015)

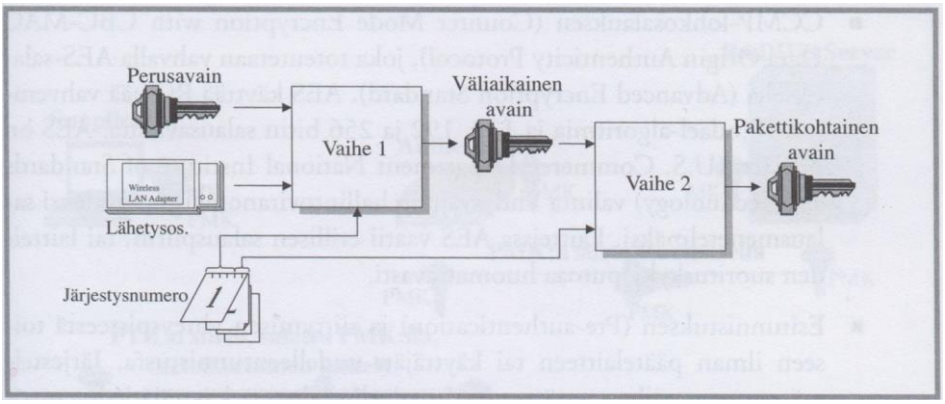
4.6 TKIP-Salausprotokolla

TKIP (Temporal Key Integrity Protocol) on salausprotokolla, jonka tarkoituksena oli korjata WEP-salauksen puutteet. Ohjelmistopäivityksen avulla WEP-laitteet

saatiin tukemaan TKIP-salausta. TKIP oli kuitenkin vain väliaikainen ratkaisu. Sen oli tarkoitus tarjota parempi suoja siihen asti, kunnes CCMP/AES-salausta tukevat laitteet yleistyy. (Coleman 2010 ym., 75.)

Kuten WEP myös TKIP käyttää liikenteen salaukseen RC4–jonosalausta. TKIP eroaa kuitenkin monella tapaa WEP-salauksesta. TKIP-protokolla käyttää 128-bittisiä salausavaimia, jotka luodaan kehyskohtaisesti. Kehyskohtaisen avaimen käytöllä estetään avaimen uudelleenkäyttöön liittyvät ongelmat. Pidemmän salausavaimen lisäksi TKIP käyttää pidempää alustusvektoria, joka on laajennettu 48 bittiin. TKIP käyttää MIC-eheydentarkistusta (Message Integrity Check), joka paljastaa kehysten väärennysyritykset. Se paljastaa muutokset kehysten biteissä ja lähde- tai kohdeosoitteissa. (Puska 2005, 82.)

TKIP-salauksen alussa molemmilla osapuolilla on yhteinen 128-bittinen aloitusavain. Aloitusavain yhdistetään päätelaitteen MAC-osoitteeseen ja salattavan kehyksen järjestysnumeron neljään eniten merkitsevään bittiin (Kuva 2). Tästä saatu väliaikainen avain yhdistetään edelleen järjestysnumeron kahteen alimpaan bittiin, jonka seurauksena syntyy pakettikohtainen avain. Täten kaikki asemat käyttävät eri salausavainta ja se vaihtuu jokaiselle lähetetylle kehykselle. Istuntokohtaista salausavainta vaihdetaan 10000 kehyksen välein, jonka tarkoituksena on estää mahdollisia salakuuntelijoita kalastelemasta lähtödataa salauksen murtamiseen. (Puska 2005, 82-83.)



Kuva 2. TKIP-Salausavaimen generointi. (Puska 2005, 83)

4.7 CCMP-Salausprotokolla

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) on WPA2:n käyttämä tietoturvaprotokolla. CCMP käyttää salaukseen AES-lohkosalausta (Advanced Encryption Standard). CCMP:n tarkoituksena on korvata TKIP, koska CCMP tarjoaa tehokkaamman salauksen kuin TKIP. Suurin ongelma CCMP-protokollassa on AES-lohkosalauksen vaatima prosessointiteho ja sen vuoksi CCMP-AES ei ole yhteensopiva vanhojen laitteiden kanssa.(Coleman ym. 2010, 83)

AES on symmetrinen lohkosalausmenetelmä, joka perustuu Rijndael-algoritmiin ja käyttää salaukseen 128-bittisiä salausavaimia. AES-algoritmi on niin luotettava, että USA:n kauppaministeriön standardeista vastuussa oleva yksikkö, NIST (National Institute of Standards and technology) valitsi AES-algoritmin USA:n hallintoviranomaisten uudeksi salausmenetelmäksi. AES korvasi vanhentuvan DES:n (Data Encryption standard). (Coleman ym. 2010, 71; Geier 2005, 184)

4.8 Todentaminen

Kuten edellä mainitsin WPA ja WPA2 tarjoaa kaksi eri versioista. Toinen on Personal, joka on tarkoitettu pieniin verkkoihin, kuten kodit ja pienet toimistot, sekä Enterprise-versiot, joka on tarkoitettu isompien yritysten verkkoihin. WPA/WPA2-Personal käyttää todennukseen PSK (Pre-shared key)-todennusta WPA/WPA2-Enterprise käyttää todennukseen 802.1x-standardia, joka perustuu EAP:hen (Extensible Authentication protocol).

4.8.1 PSK salausavaimeen perustuva todennus

PSK (Pre-Shared Key) –avain, eli esijaettu avain muodostuu salasanasta, joka on määritelty langattomalle verkolle tukiaseman asetuksissa ja jota kaikki verkkoon liittyvät henkilöt käyttävät. Lisäksi PSK-avaimen muodostamiseen tarvitaan tukiaseman SSID:n pituus ja itse SSID, joka myös on määritelty tukiaseman asetuksissa. Nämä kolme tietoa salasana, SSID ja SSID:n pituus muutetaan automaattisesti 256-bittiseksi PSK-salausavaimeksi, jota käytetään todennukseen. Käyttäjän

itse ei tarvitse muistaa 256-bittistä avainta, vaan ainoastaan määritelty salasana, joka pituudeltaan on 8-63 -merkkiä. (Coleman ym. 2010, 223-224.)

4.8.2 IEEE 802.1x–todennus

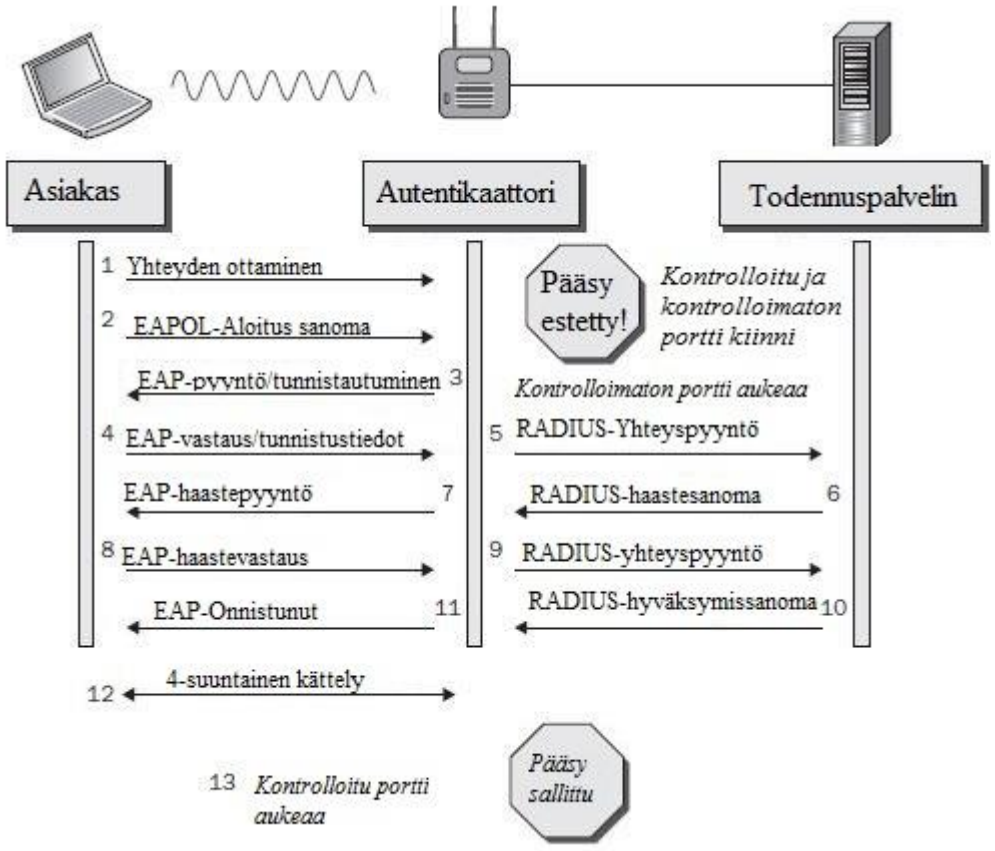
IEEE 802.1x–standardi on porttikohtaiseen todennukseen perustuva standardi. Tarkoituksena on rajoittaa pääsyä langattoman verkkoon. Siihen pyritään loogisten porttien sekä todennuspalvelimien avulla. Itse todennusprosessiin käytetään EAP (Extensible Authentication Protocol)-protokollaa. 802.1x muodostuu kolmesta osasta. autentikaattorista, todennuspalvelimesta ja asiakkaasta. 802.1x–standardia voidaan käyttää myös langallisissa verkoissa. (Coleman 2010, 108.)

Autentikaattori on laite, jonka tehtävänä on sallia ja estää liikennettä, joka kulkee sen porttien kautta. Autentikaattori ylläpitää kahta virtuaalista porttia: kontrolloitua ja kontrolloimatonta porttia, joista molemmilla on oma tehtävänsä. Kontrolloimaton portti sallii läpi kaiken liikenteen, joka liittyy käyttäjien todentamiseen. Kontrolloitu portti sen sijaan estää kaiken liikenteen, joka ei ole todennettu, läpi pääsee vain liikenne sen jälkeen, kun käyttäjä on todennettu onnistuneesti. Langattomassa verkossa autentikaattorina toimii tukiasema tai erillinen WLAN-kontrolleri. (Coleman ym. 2010, 110.)

Todennuspalvelimen tehtävän on käyttäjän käyttöoikeustietojen aitouden ja oikeellisuuden varmistaminen. Mikäli tiedot on varmistettu oikeiksi todennuspalvelin, antaa käyttäjälle oikeuden päästä verkkoon. Todennuspalvelin tarkastaa käyttäjätiedot sen omasta tietokannasta tai ulkoisesta tietokannasta, johon se on yhteydessä. Todennuspalvelimena toimii yleensä RADIUS (Remote Authentication Dial-In User Service)-palvelin. (Coleman ym. 2010, 110.)

Todennusprosessi alkaa, kun asiakaslaite yrittää ottaa yhteyttä langattomaan verkkoon (Kuva 3), mutta koska 802.1x-todennus on käytössä, ei hän vielä pääse verkkoon sisään. Asiakkaan yrittäessä liittyä verkkoon asiakas lähettää 802.11 EAPOL-aloitussanoman autentikaattorille, josta seuraa, että autentikaattori lähettää EAP-pyyntösanoman asiakkaalle, jossa vaatii tunnistautumista. Tähän asiakas vastaa EAP-vastaussanomalla, joka sisältää asiakkaan käyttäjätunnuksen selvänä tekstinä.

Mikäli tämä käyttäjätunnus hyväksytään kontrolloimaton portti avaa liikenteen kontrolloituun porttiin. Tämän jälkeen autentikaattori tiivistää EAP-vastaussanoman RADIUS-pakettiin ja lähettää sen eteenpäin todennuspalvelimelle yhteyspyyntönä. RADIUS-palvelin lähettää vielä RADIUS-haastesanoman autentikaattorille, joka lähettää sen eteenpäin asiakkaalle EAP-haastepyynnön muodossa. Asiakas vastaa tähän ja lähettää takaisin EAP-haastevastauksen. Mikäli RADIUS-palvelimella on varmuus asiakkaan aitoudesta RADIUS-palvelin lähettää RADIUS-hyväksymissanoman. Viimeinen vaihe on 4-suuntainen kättely autentikaattorin ja asiakkaan välillä. Tässä prosessissa luodaan dynaamiset salausavaimet. Todennuksen ja avainten luonnin jälkeen kontrolloitu portti aukeaa ja asiakas saa pääsyn verkkoon. (Coleman 2010, 140)



Kuva 3. EAP-Todennusprosessi.

5 TIETOTURVAUHAT

Tietoverkkoihin kohdistuvia tietoturvauhkia on hyvin paljon. Langattomalla ja langallisella verkolla on olemassa samanlaisia uhkia, mutta langattomuus on tuonut mukanaan uudenlaisia uhkakuvia. Langaton lähiverkko onkin monesti langallista verkkoa alttiimpi erilaisille hyökkäyksille ja ulkopuolisille. Nämä uhat jaetaan usein kahteen ryhmään, aktiivisiin ja passiivisiin uhkiin. Aktiivisissa tapauksissa langattoman verkon liikennettä pyritään häiritsemään ja manipuloimaan. Passiivisissa tapauksissa langattoman verkon liikennettä salakuunnellaan ja analysoidaan, mutta liikennettä ei manipuloida tai häiritä. (Puska 2005, 69.)

5.1 Salakuuntelu

Salakuuntelu on verkossa kulkevan tiedon kaappaamista. Salakuuntelun avulla kerätyistä tiedoista voidaan kerätä mm. tunnistetietoja ja muuta verkkoinformaatioita, jotka kiinnostavat hyökkääjää. Liikenteen salakuunteluun on olemassa ilmaisia ohjelmia kuten Kismet tai Wireshark. Ratkaisu tähän ongelmaan on käyttää tukiaseman ja asiakaslaitteen välillä salausta, josta aiemmin kerroin. Salauksen ansioista salakuuntelijan on erittäin vaikea purkaa salattua dataa ja päästä käsiksi verkossa liikkuvaan dataan. (Geier 2005, 172)

5.2 Palvelunestohyökkäys

Palvelunestohyökkäys on hyökkäys, jonka tarkoituksena on häiritä langatonta lähiverkkoa ja tehdä se käyttökelvottomaksi. Tämä häirintä tapahtuu esimerkiksi langattoman verkon radioliikenteen häirinnällä ja hallintakehysten muokkaamisella. Palvelunestohyökkäykset tapahtuvat OSI-mallin kahdella alimmalla kerroksella, fyysisellä kerroksella ja siirtokerroksella.(Coleman & Westcott 2009, 479-480.)

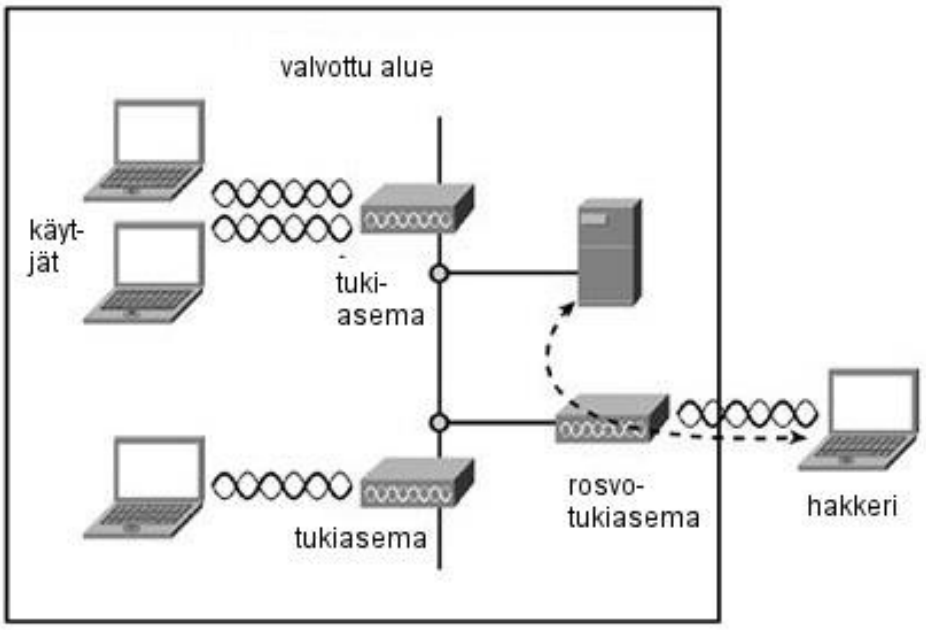
OSI-mallin fyysisessä kerroksessa tapahtuvilla hyökkäyksillä pyritään häiritsemään langattoman verkon radioliikennettä. Radiohäirintää on sekä tahatonta että tahallista. Tahallisessa häirinnässä hyökkääjä käyttää signaaligeneraattoria, jonka lähettämillä häiriösignaaleilla pyritään estämään langattomien laitteiden kommunikointi

mahdottomaksi. Tahatonta radiohäirintää aiheuttaa kodin elektroniikka, joka käyttävät usein samoja taajuuksia kuin langattomat verkot. (Coleman & Wescott 2009, 480.)

Paljon yleisempi hakkerien aiheuttama palvelunestohyökkäys on OSI-mallin siirtokerroksen hyökkäykset. Suurin osa näistä hyökkäyksistä tapahtuu peukaloimalla 802.11–kehyksiä. Yksi yleisimmistä keinoista, jolla hyökkääjä voi tehdä verkon käytön mahdottomaksi, on muokata yhteyden katkaisuun käytettävää kehystä (deauthentication frame). Hyökkääjä muuttaa kehyksen lähettäjäkentän MAC-osoitteeksi tukiaseman MAC-osoitteen ja vastaanottajaksi asiakaslaitteen MAC-osoitteen. Seuraavaksi hyökkääjä uudelleen lähettää muutettua kehystä jatkuvalla syötöllä asiakaslaitteelle. Hyökkäyksen kohteena oleva asiakaslaite luulee, että katkaisupyynnöt tulevat oikealta tukiasemalta ja täten katkaiseen yhteyden. (Coleman ym. 2010, 311.)

5.3 Rosvotukiasema

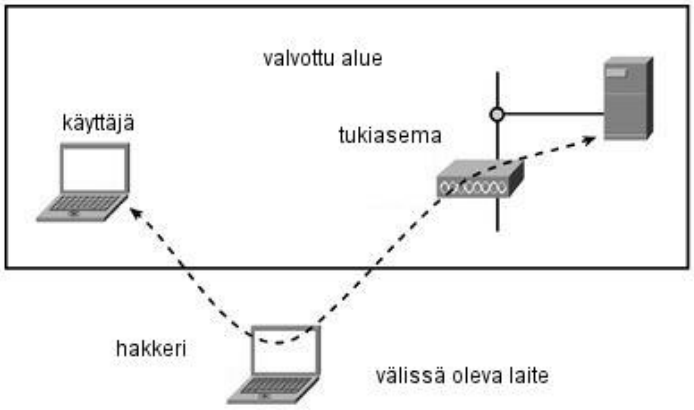
Rosvotukiasema on lähiverkossa toimiva luvaton tukiasema. (Kuva 4) Rosvotukiasemat ovat enemmänkin uhka yrityksille, mutta on hyvä tuoda asia silti esille, koska kotikäyttäjä voi omalla tietämättömyydellään luoda tietoturva-aukon yritykselle. Rosvotukiasema voi siis olla työntekijän itse asentama tukiasema tai hakkerin tuoma tukiasema. Rosvotukiasemassa ei todennäköisesti ole käytössä salauksia, joten se tarjoaa ulkopuolisille avoimen reitin yrityksen verkkoon. Siksi on tärkeää, että yritykset pitävät silmällä verkkoaan ja koukuttavat työntekijöitään tietoturva-asioissa.(Geier 2005, 173.)



Kuva 4. Rosvotukiasema (Puska. 2005. 173.)

5.4 Man-in-the-middle

Man-in-the-middle-hyökkäyksessä verkkoon hyökkäävä henkilö pyrkii asettumaan langattoman tukiaseman ja sitä käyttävän laitteen väliin siten, että langattoman verkon liikenne kulkee hänen kauttaan.(Kuva 5) Kun liikenne kulkee hyökkääjän kautta voi hän vapaasti muokata hänen kauttaan kulkevaa tietoa. Tyypillisesti Man-in-the-middle-hyökkäyksessä hyökkääjä käyttää ARP (Address Resolution Protocol)-myrkyttämistä ottaakseen haltuun langattoman verkon.(Geier 2005, 174.)



Kuva 5. Man-In-The-Middle-hyökkäys. (Puska. 2005. 174)

Jokaisella verkossa toimivalla laitteella on MAC-osoite, jotta laitteet voisivat kommunikoida toistensa kanssa, täytyy laitteen tietää toisen laitteen MAC-osoite. MAC-osoite saadaan selville ARP-protokollaa käyttäen. Laite saa toisen laitteen MAC-osoitteen selville lähettämällä kaikille lähiverkon laitteille ARP-kyselyn. ARP-kyselyn sisältää sen laitteen IP-osoitteen, jonka kanssa halutaan kommunikoida. ARP-kyselyn saavuttua tälle laitteelle se vastaa pyynnön lähettäneelle laitteelle takaisin ARP-vastauspaketin, joka sisältää halutun MAC-osoitteen. Vastauksen saatuaan laite kyselyn lähettänyt laite päivittää ARP-taulunsa, johon merkitään IP-osoitetta vastaava MAC-osoite. (Geier 2005, 175.)

ARP-myrkyttäminen tapahtuu siten, että hyökkääjän rosvotukiasemalta lähetetään ARP-pyyntöön väärennetty ARP-vastaus. Väärennetty ARP-vastaus sisältää hyväksytyn IP-osoitteen, mutta MAC-osoitteeksi on muutettu rosvolaitteen MAC-osoite. Tämän seurauksena kaikki verkon asemat päivittää ARP-taulunsa näillä väärennetyillä tiedoilla ja kaikki paketit saapuvat rosvolaitteelle. Tämän seurauksena hyökkääjä voi saada käsiinsä mm. salasanoja. (Geier 2005, 175.)

5.5 Väsytyshyökkäys

Väsytyshyökkäys on hyökkäystekniikka, jolla pyritään selvittämään henkilökohtaista tietoa esimerkiksi salasanoja ja PIN-numeroita. Tämä tekniikka perustuu yritys- ja erehdys-tekniikkaan. Tämä tarkoittaa, että hyökkäyksessä automatisoitu oh-

jelma on valjastettu murtamaan salasana syöttämällä erilaisia merkkijonoja salasanasuojatulle tiedostolle tai ohjelmalle. Tyypillisesti väsytyshyökkäyksiä-hyökkäyksiä on kahdenlaisia. Ensimmäinen tunnetaan nimellä sanakirjahyökkäys, jossa käytetään koko sanakirjan sisältöä yrityksessä päästä suojauksen läpi. Toisessa tavassa murtamiseen käytetään esimerkiksi eniten käytettyjä salasanoja tai erilaisia kirjain- ja numeroyhdistelmiä. (Janssen 2015.)

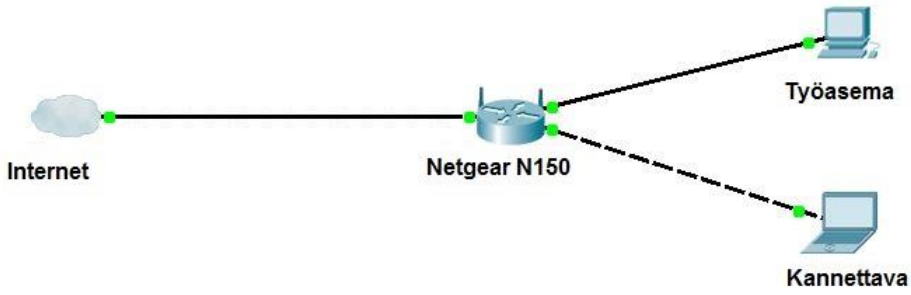
6 TIETORUVALLINEN LANGATON LÄHIVERKKO

Tässä luvussa käydään läpi miten käyttäjä voi tehdä verkostaan tietoturvallisen. Ensimmäisessä luvussa esittelen miten langaton reititin olisi syytä konfiguroida, jotta se olisi mahdollisimman tietoturvallisen ja toimivan. Lisäksi lopussa esittelen miten käyttäjä voi vaikuttaa langattoman verkon ja siihen liitettyjen laitteiden tietoturvaan.

Langattomana reitittimenä toimii Netgear N150 (Kuva 6), joka on hyvä valinta käyttäjille, joilla ei ole kokemusta langattomista reitittimistä. Asetussivun käyttöliittymä on selkeä ja helppo oppia. Netgear N150 IEEE 802.11b/g standardeja, sekä joitain 802.11n-standardin ominaisuuksia. Lisäksi tämä langaton reititin tarjoaa 4 LAN-porttia, joihin voi yhdistää esimerkiksi pöytäkoneita Ethernet-kaapelilla.

Kuva 6. Netgear N150 langaton reititin.

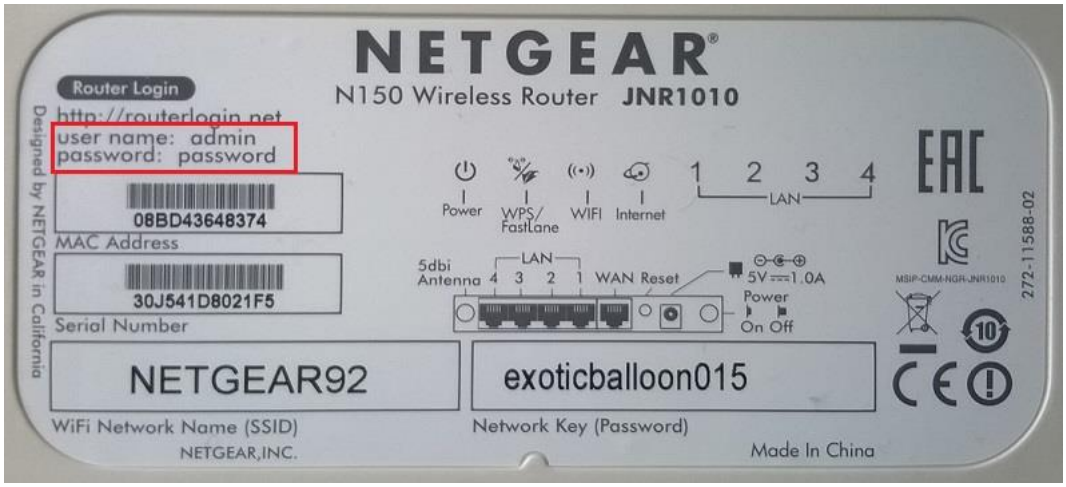
Testattava verkko koostuu Netgear N150 reitittimestä, yhdestä työasema sekä minikannettavasta. (Kuva 7) Erilliselle tukiasemalle ei ole tarvetta, sillä Netgear N150 reitin sisältää sisäänrakennetun tukiaseman. Langattomasta reitittimestä jaetaan langaton yhteys kannettavaan tietokoneeseen. Työasema on yhdistettynä Ethernet kaapelilla langattoman reitittimen LAN-porttiin.



Kuva 7. Verkkokaavio.

6.1 Langattoman reitittimen asetukset

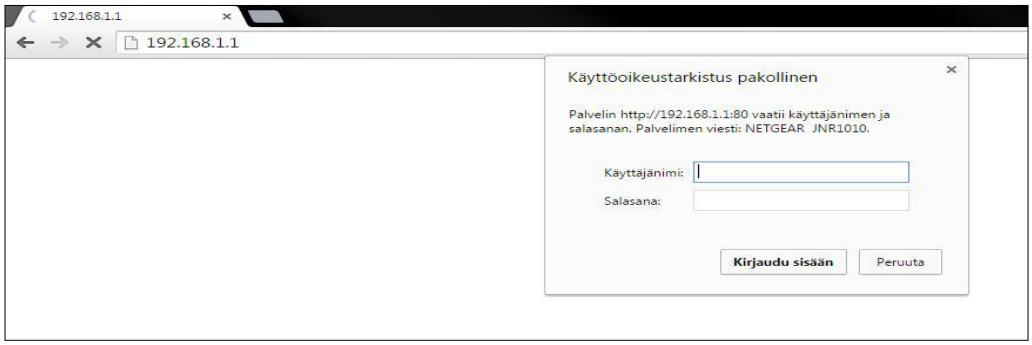
Reitittimien asetuksia pääsee muuttamaan tietokoneen internetselaimen kautta. Selaimen kautta siihen pääsee käsiksi kirjoittamalla osoitekenttään reitittimen IP-osoitteen. Tämä IP-osoite vaihtelee valmistajan mukaan, mutta yleisimmät IP-osoitteet jotka ovat käytössä 192.168.0.1, 192.168.1.1 tai 192.168.2.1. IP-osoite tai asetussivun osoite löytyy yleensä reitittimen pohjasta. (Kuva 7)



Kuva 8. Reitittimen pohja.

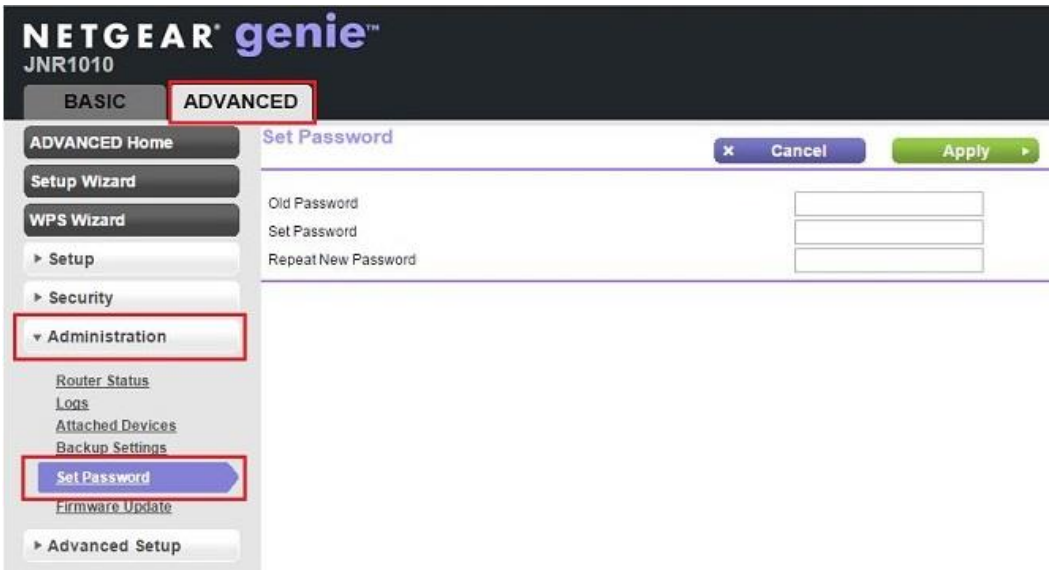
Tässä tapauksessa IP-osoite on 192.168.1.1 tai vaihtoehtoisesti reitittimen pohjassa oleva osoite: http://routerlogin.net. Seuraavaksi selain kysyy käyttäjätunnusta ja salasanaa. (Kuva 9) Samoin kuin IP-osoite tai asetussivun osoite myös käyttäjätunnus

ja salasana löytyvät reitittimen pohjasta. Myös nämä tiedot ovat valmistajakohtaisia.



Kuva 9. Käyttäjätunnus ja salasana.

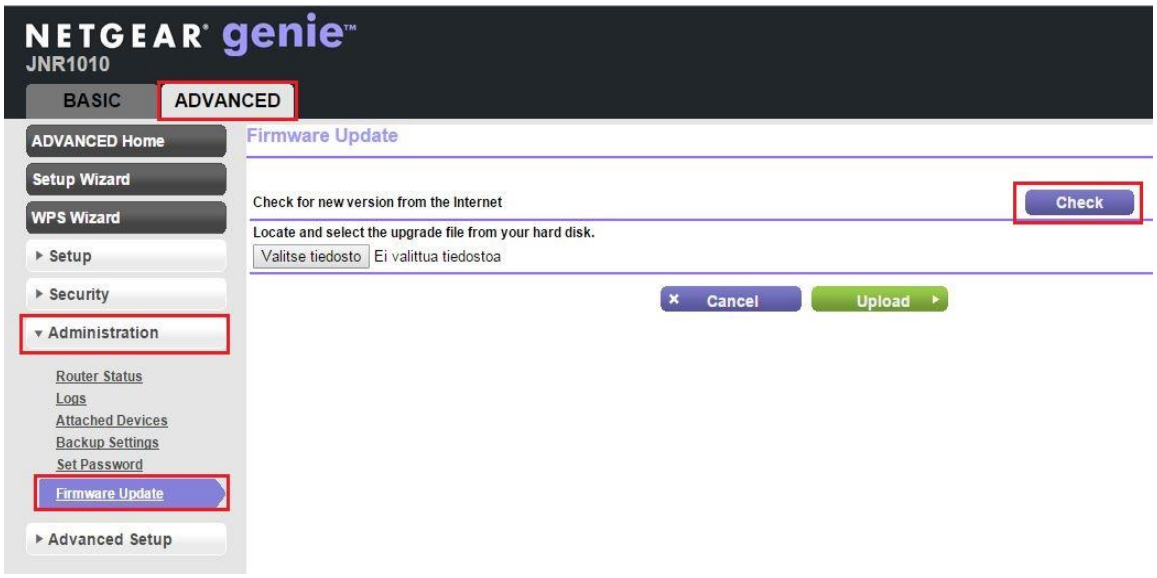
Ensimmäinen asia, joka tulisi vaihtaa, on edellä mainitun käyttäjätunnuksen salasana. Nämä kyseiset kirjautumistiedot ovat uusissa saman valmistajan laitteissa aina samat. Joten mikäli ulkopuolisella henkilöllä on pääsy langattomaan verkkoon, on todennäköistä, että he pystyvät kirjautumaan sisään langattomaan reitittimeen ja muuttamaan asetuksia miten tahtovat ja seuraamaan liikennettä. Hyvä salasana on mahdollisimman pitkä ja sisältää pieniä kirjaimia, isoja kirjaimia numeroita ja erikoismerkkejä. Mikäli on vaikeuksia muistaa salasanaa voi sen kirjoittaa esimerkiksi lapulle ylös ja säilyttää hyvässä tallessa. Netgearin reitittimissä salasanan vaihto tapahtuu Advanced-asetuksista. (Kuva 10) Seuraamalla kuvan punaisia ympyröintejä pääsee salasanan vaihtosivulle. Sivusto pyytää ensin vanhaa salasanaa ja sitten pyytää kirjoittamaan salasanan kahdesti. Lopuksi tulee vielä painaa ”Apply”, jolla hyväksytään uusi salasana.



Kuva 10. Pääsyn salasana.

Salasanan muuttaminen estää ulkopuolisilta pääsyn langattoman reitittimeen. Tämä ei kuitenkaan estä ulkopuolista yrittämästä murtaa salasanaa esimerkiksi väsytyshyökkäyksellä–hyökkäyksellä. Sen vuoksi onkin tärkeää, että salasana on tarpeeksi vahva.

Pääsyn salasana ei ole kuitenkaan ainoa asia, mikä on syytä tarkistaa reitittimestä ennen sen käyttöönottoa. On hyvä tarkastaa myös, että reitittimien firmware on päivitetty. Firmware on laiteohjelmisto, joka huolehtii laitteen toiminnoista. Ohjelmistopäivityksillä pyritään korjaamaan toiminnoissa esiintyviä virheitä tai luomaan uusia ominaisuuksia. Ohjelmiston päivitys tapahtuu myös reitittimen asetussivulta. Painamalla kuvassa (Kuva 11) ympyröityä ”check”-nappia, reititin tarkastaa, onko laiteohjelmistolle uutta versioita netistä. Mikäli sivu ilmoittaa, että uusi versio on saatavilla, sen voi päivittää saman tien.



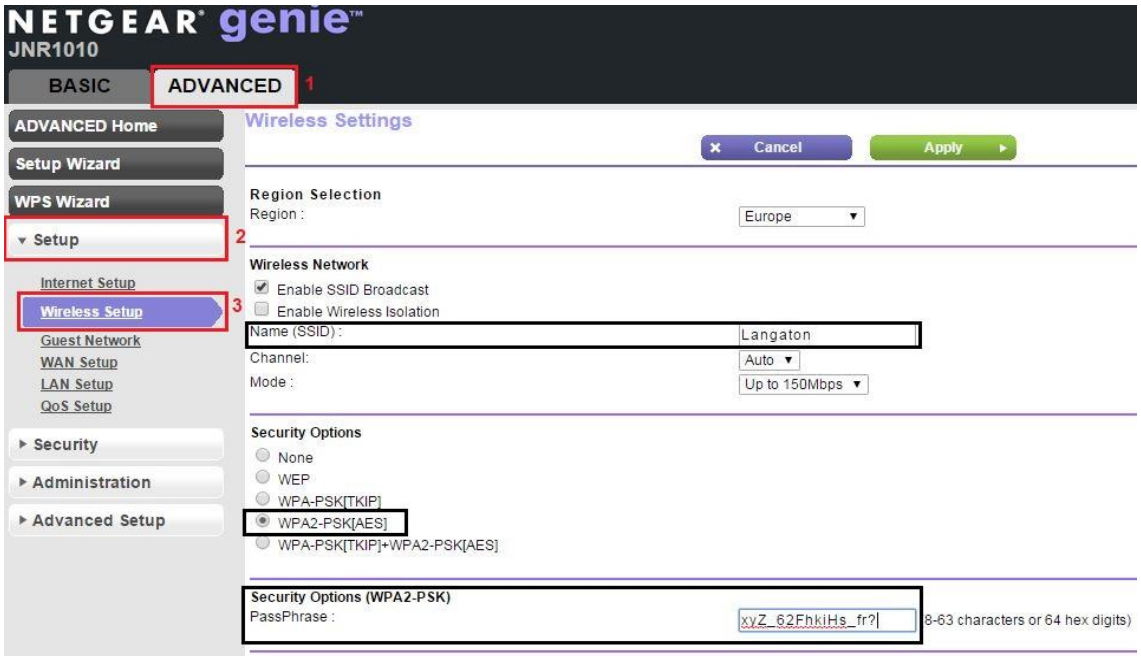
Kuva 11. Ohjelmiston päivitys.

6.2 Langattoman verkon asetukset

Seuraavaksi päästään itse langattoman verkon asetuksiin. Kuten teoriaosuudessa olen kertonut, on tärkeää, että langattoman verkon tietoturva on kunnossa. Langattoman verkon asetuksista tärkeintä on muuttaa salausmenetelmä, SSID ja tietenkin salasana. Kuvassa 12 näkee miten näihin asetuksiin pääsee ja mitä siellä tulee muuttaa. Ensimmäisenä on syytä muuttaa langattoman verkon nimi eli SSID, joka kuvassa on ensimmäinen mustalla ympyröity kohta. Nimeksi voi valita haluamansa nimen, joka on helppo tunnistaa, lähiympäristön muista langattomista verkoista.

Toisessa ympyröidyssä kohdassa päästään valitsemaan haluttu salaus. Kuten teoriaosassa kerroin on WPA2 vaihtoehdoista paras. WPA:n ja WPA2:n yhdistelmä tulee valita silloin, jos on niin vanhoja laitteita, etteivät ne tue WPA2-salausta. Mikäli kaikki laitteet tukee WPA2:sta, on syytä valita WPA2-PSK[AES].

Lopuksi tulee muuttaa passphrase eli tunnuslause. Tunnuslause on lähes sama kuin salasana. Salasana on yleensä vain merkkijono, kun taas tunnuslause on yleensä pidempiä kuin salasanat ja ne voivat sisältää useita sanoja joista syntyy kokonainen lause. Tärkeintä kuitenkin on, että tunnuslause tai salasana on tarpeeksi pitkä ja sisältää paljon erilaisia merkkejä. Kun asetukset on muutettu tulee vielä lopuksi painaa vihreää ”apply”-painiketta.



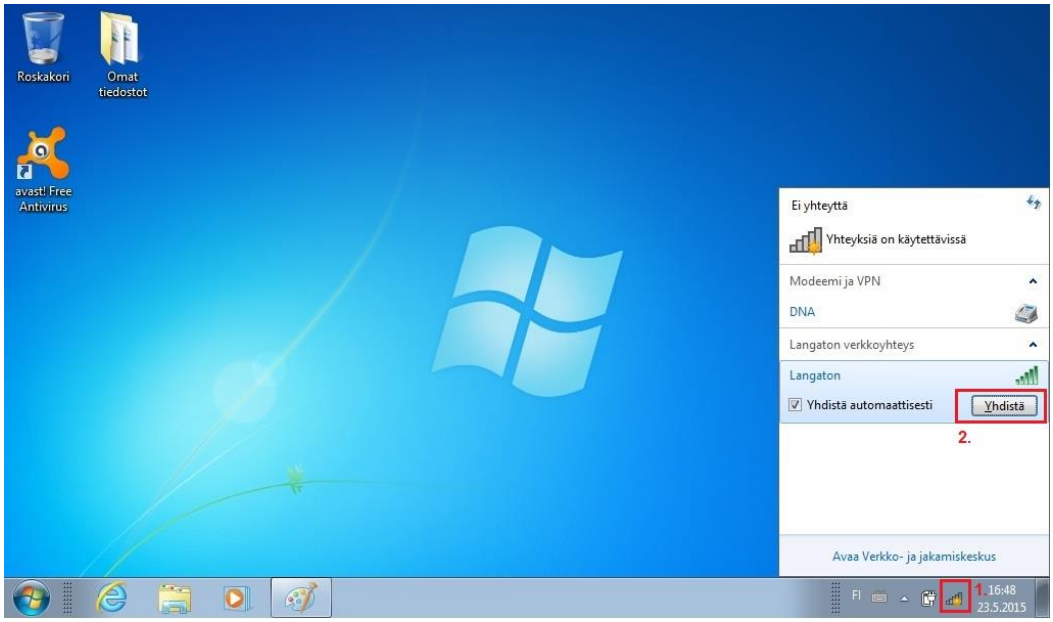
Kuva 12. Langattoman verkon asetukset.

6.3 Langattomaan verkkoon liittyminen

Langattomaan verkkoon liittyminen tapahtuu päätelaitteelta. Tässä tapauksessa päätelaitteena on Acer Aspire one D250 -minikannettava, jotta yhdistäminen on mahdollista, täytyy päätelaitteen tukea langattomia verkkoja. Tämä tarkoittaa sitä, että laitteessa tulee olla verkkosovitin, joka kykenee vastaanottamaan langattoman verkon signaaleja. Acer Aspire one D250:n verkkosovitin tukee langatonta lähiverkkoa ja 802.11b/g–standardeja.

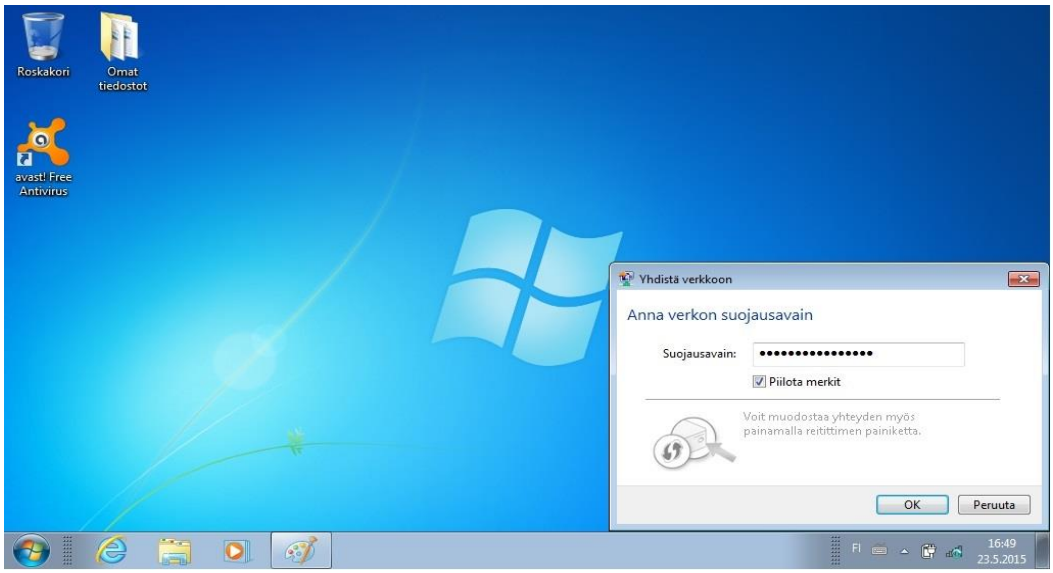
Kun langattoman verkon asetukset ovat valmiit, voidaan langattomaan verkkoon yhdistää laitteita. Langattoman verkon pitäisi näkyä langattomien verkkojen listassa (Kuva 13). Painamalla kuvassa kohta yksi tulee näkyviin saatavilla olevat langattomat verkot. Tässä tapauksessa näkyvissä on vain edellä luomamme langaton lähiverkko nimeltä ”Langaton”. Painamalla ”yhdistä” tietokone ottaa yhteyden

langattomaan lähiverkkoon. (Kuva 13)



Kuva 13. Aiemmin luotu langaton lähiverkko.

Seuraavassa vaiheessa tietokone kysyy käyttäjältä suojausavainta. (Kuva 14) Suojausavain on sama kuin langattoman verkon asetuksiin määrittelemämme ”passphrase”. Suojausavaimen antamisen jälkeen tietokone saa yhteyden langattomaan verkkoon ja saa pääsyn internettiin.



Kuva 14. Suojausavain

7 YHTEENVETO

Langattomuus on nykypäivänä erittäin yleistä ja sitä näkee lähes kaikkialla. Langattomuuden yleistymisen myötä langattoman laitteetkin ovat yleistyneet. Nykypäivänä langattomia laitteita löytyy huomattava määrä. Suurin syy yleistymiseen on varmasti langattoman verkon helppokäyttöisyys ja halpa käyttöönotto. On huomattavasti helpompaa käyttää langatonta yhteyttä, koska se tuo liikkuvuutta ja varsinkin koteihin vapautta rumista johdoista.

Yleistyminen on kuitenkin tuonut mukanaan tietoturvaongelmat, kuten verkon salakuuntelun ja palvelunestohyökkäykset. Langattoman verkon käyttö edellyttää, että tietoturva-asiat ovat kunnossa. On erittäin tärkeää, että langattoman verkon käyttäjä perehtyisi sen tietoturvaan ja tarkastaisi oman verkkonsa tietoturva-asetukset. Tärkeintä olisi muuttaa langattoman verkon ja tukiaseman hallintasivun oletussalasanat ja tietenkin tarkastaa, että käytössä on pätevä salaus.

Suurimmat ongelmat työtä tehdessäni olivat tiukka aikataulu ja vanhentunut kirjallisuus. Varsinkin suomenkielisiä ajankohtaisia kirjoja oli vaikea löytää. Lisäksi langattomat verkot ja tietoturva ovat aiheena niin kattavia, että suunnitteluvaiheessa oli vaikeuksia päättää, mitä teoriaa työssä kannattaa tuoda esille ja mitä jättää pois. Tästä huolimatta onnistuin mielestäni tuomaan kaikki oleellisimmat asiat langattomia verkkoja käyttäville henkilöille.

Langattoman verkon suojaaminen ei varsinaisesti ole haastavaa, mutta moni jättää sen tekemättä ja käyttää vain laitteiden tehdasasetuksia. Nyky-yhteiskunnassa ihmiset säilyttävät tietokoneillaan paljon yksityisiä asioita ja tämän vuoksi on tärkeää hoitaa tietoturva-asiat kuntoon.

Käyttäjä tulisi muistaa aina seuraavat asiat

1. Vaihda langattoman reitittimen/tukiaseman hallintasivun salasana.
2. Pidä laiteohjelmisto ajan tasalla.
3. Käytä tehokasta salausta.
4. Käytä tarpeeksi vahvaa ja pitkää salasanaa.

LÄHTEET

AirMagnet. 2008. 802.11n Primer. http://airmagnet.flukenetworks.com/assets/whitepaper/WP-802.11nPrimer.pdf (Viitattu 23.5.2015)

Cisco. 2014. 802.11ac: The Fifth Generation of Wi-Fi. Viitattu 23.5.2015. http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.pdf

Cisco. 2008. Enterprise Mobility 4.1 Design Guide. Viitattu 21.5.2015. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.pdf

Coleman, D., Westcott, D., Harkins, B., Jackman, S. 2010 CWSP: Certified Wireless Security Professional Official Stduy Guide. Indianapolis. Wiley Publishing.

Coleman, D. & Westcott, D. 2009. CWNA: Certified Wireless Network Administrator Official Stduy Guide. Indianapolis. John Wiley & Sons

Cory Janssen. 2015. Brute Force Attack. Viitattu. 1.5.2015. http://www.techopedia.com/definition/18091/brute-force-attack

Geier, J. 2005 Langattomat verkot. Helsinki. IT-Press

Microsoft. 2015 Mitä eroa on keskittimellä, kytkimellä, reitittimellä ja tukiasemalla. Viitattu 21.5.2015. http://windows.microsoft.com/fi-fi/windows/hubs-switches-routers-access-points-differ#1TC=windows-7

Puska, M. 2005. Langattomat Lähiverkot. Jyväskylä. Talentum Media Oy.

Viestintävirasto. 2014. Langattomasti, mutta turvallisesti. Viitattu 20.5.2015. https://www.viestintavirasto.fi/attachments/tietoturva/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

Wi-fi Alliance. 2015. WPA2 Security now mandatory for Wi-Fi Certified products. Viitattu 20.4.2015 http://www.wi-fi.org/news-events/newsroom/wpa2-security-now-mandatory-for-wi-fi-certified-products