Mika Mononen

Hannes Nurmi

Langattoman lähiverkon tietoturva

Opinnäytetyö

Tietoverkkotekniikka

Marraskuu 2015

KYAMK

University of Applied Sciences

Tekijä/Tekijät	**Tutkinto**	**Aika**
Mika Mononen Hannes Nurmi	Insinööri	Marraskuu 2015
Opinnäytetyön nimi Langattoman lähiverkon tietoturva		41 sivua
Toimeksiantaja Kymenlaakson Ammattikorkeakoulu		
Ohjaaja Yliopettaja Martti Kettunen		

Tiivistelmä

Langattomien verkkotekniikoiden hyödyntäminen eri käyttöympäristöissä yleistyy jatkuvasti. WLAN-verkkojen kehittämisen tarve näkyy kuluttaja- ja yritysympäristöissä. Jatkuvasti lisääntyvät älylaitteiden määrät luovat painetta kehittää tietoturvaa ja standardeja parantamaan verkon toimivuutta.

Tämän opinnäytetyön tavoitteena oli tutkia langattoman lähiverkon tietoturvaa yleisellä tasolla ja testata sen toimivuutta. Työssä käydään läpi yleiset 802.11 standardit, 802.1x ja WIDS/WIPS-järjestelmät yritysverkoissa. Käytännön osuus sisältää langattoman lähiverkon tukiasemaan kohdistetun hyökkäyksen, jossa tarkoituksena on murtaa sen WPA2-salaus.

Työssä käytettiin kuluttajille suunnattua Netgear WNDR4500-reititintä, jonka ympärille testiympäristö rakennettiin. Testit suoritettiin käyttämällä Kali Linux:n tunkeutumistyökaluja. Testissä tukiasemasta pudotettiin asiakas käyttämällä deauth-hyökkäystä ja kaapattiin WPA-kättelyviesti. Talteen otetusta kättelyviestistä selvitettiin salausavain hyödyntäen sanakirjahyökkäystä.

Työn tuloksena saatiin selville, mitä vaaditaan riittävään langattoman verkon suojaamiseen. Testissä todettiin WPA2-salaus riittäväksi, mikäli salausavain on pitkä ja monimutkainen.

Asiasanat

WLAN, tietoturva, WPA2

Author (authors)	Degree	Time
Mika Mononen Hannes Nurmi	Bachelor of Engineering	November 2015
Thesis Title Wireless local area network security		41 pages
Commissioned by Kymenlaakso University of Applied Sciences		
Supervisor Martti Kettunen, Principal Lecturer		

Abstract

Utilization of wireless network technologies on different operating environments is becoming increasingly widespread. The need for the development of WLAN networks is displayed for consumers and corporate environments. Constantly increasing number of smart devices will create pressure to develop data security, as well as new standards to improve the functionality of the network

The main objective of this study was to examine the wireless LAN security in general, and to test its functionality. The thesis examines the general 802.11 standards, as well as 802.1x and WIDS / WIPS systems in corporate networks. The practical part contains the targeted attack on the access point, where the goal is to break the WPA2 encryption

The test environment was built around Netgear WNDR4500 router, which is a basic consumer product. The tests were performed using Kali Linux's penetration tools. In tests a client was dropped from access point using deauth-attack and hijacked the WPA handshake. The encryption key was recovered from the captured handshake using dictionary attack.

As a result it was to find out what is required for the adequate protection of your wireless network. The tests found out that the WPA2 encryption method is adequate if the encryption key is long and complex enough.

Keywords

WLAN, network security, WPA2

SISÄLLYS

LYHENNELUETTELO

AAD	Additional Authentication Data eli MAC-kehyksen yhtenäisyyden varmistamiseen käytettävä informaatio
AES	Advanced Encryption Standard, eräs lohkosalausmenetelmä
AP	Access Point eli tukiasema
ARP	Adress Resolution Protocol eli protokolla, jolla selvitetään IP:tä vastaava MAC-osoite Ethernet verkoissa
AS	Authentication Server eli todentamispalvelin 802.1x verkossa
BSSID	eli tukiaseman MAC-osoite
CBC	Cipher Block Chaining eli salaus lohkojen ketjutus
CCMP	Counter mode with CBC-MAC Protocol, eräs langattomien verkkojen tietoturva protokolla
CRC	Cyclic Redundancy Check on tarkistusavaimen luomisen tarkoitettu algoritmi, jolla voidaan havaita ja korjata pieniä virheitä tiedonsiirrossa.
EAP	Extensible Authentication Protocol eli alun perin PPP-protokollan yhteydessä kehitetty käyttäjien tunnistusprotokolla
FCS	Frame Check Squence eli kehykseen lisätty virheen tarkistuskoodi
GMK	Group Master Key eli RSNA prosessissa käytetty pääavain
GTK	Group Temporal Key eli avain, jolla salataan broadcast- ja multicast-liikenne
ICV	Integrity Check Value eli eheyden tarkistus arvo

IEEE	Institute of Electrical and Electronics Engineers on kansainvälinen tekniikan alan järjestö
IP	Internet Protocol eli Internet Protokolla, joka huolehtii pakettien toimittamisesta perille pakettikytkentäisessä verkossa
ISM	Industrial Scientific and Medical eli lisenssoimaton taajuusalue, jonka käyttö ei vaadi erillistä lupaa
LAN	Local Area Network eli lähiverkko
LEAP	Cisco Lightweight Extensible Authentication Protocol eli Ciscon laitteille käyttäjien tunnistusprotokolla
LLC	Logical Link Control eli 802-verkkojen yhteinen osa siirtoyhteyskerrosta
MAC	Media Access Control eli Ethernet-verkoissa verkkosovittimen yksilöivä osoite.
MIC	Message Integrity Check eli pakettien eheyttä valvova toiminto
MPDU	Media Access Control Protocol Data unit eli viesti, joka vaihdetaan MAC ja OSI-malliin pohjautuvan kommunikaatiojärjestelmän välillä.
MSDU	MAC Service Data Unit eli tietue, joka on saatu LLC:tä
NFC	Near Field Communication eli RFID-tekniikkaa hyödyntävä kättely ja tiedonsiirto tekniikka
OSI-malli	Open Systems Interconnection Reference Model eli tiedonsiirtoprotokollien kuvaus seitsemällä kerroksella.
PC	Personal Computer eli tietokone
PEAP	Protected Extensible Authentication Protocol eli salattu käyttäjien tunnistusprotokolla

PMK	Pairwise Master Key eli RSNA prosessissa käytetty jaettuavain
PN	Packet Number eli kehykset yksilöivä numero
PPP	Point-to-Point Protocol eli protokolla jota käytetään muodostamaan suora yhteys verkkolaitteiden välillä
PTK	Pairwise Transient Key eli avain, jolla salataan unicast-liikenne
QoS	Quality of Service eli palvelun laatu
RADIUS	Remote Authenticaion Dial-In User Sevice eli keskitetty verkkoon kirjautumis- ja tunnistaumisprotokolla
RC4	Rivest Cipher 4 on Ronald Rivestin suunnittelema salausalgoritmi.
RSNA	Robust Security Network Association
SSL	Secure Socets Layer eli salausprotokolla, jolla voidaan suojata tietoliikennettä
STA	Station eli 802.11 yhteensopiva laite
TA	Transmitter Address eli lähettimen osoite
TKIP	Temporal Key Integrity Protocol, eräs langattomien verkkojen tietoturva protokolla
UNII	Unlicenced national Information Infrastructure eli lisensoimaton 5GHz taajuusalue
WEP	Wired Equivalent Privacy on ensimmäinen työaseman ja tukiaseman välistä langatonta yhteyttä suojaamaan kehitetty salausmenetelmä.
WIDS	Wireless Intrusion Detection System eli langattoman lähiverkon tunkeutumisen havaitsemisjärjestelmä.
WIPS	Wireless Intrusion Prevention System eli langattoman lähiverkon tunkeutumisen estojärjestelmä.

WLAN	Wireless Local Area Network eli langaton lähiverkko
WNMS	Wireless Network Management System eli langattoman lähiverkon hallinnointijärjestelmä.
WPA	Wi-Fi Protected Access on langattoman lähiverkon salausprotokolla, joka on WEP:n seuraaja.
WPS	Wi-Fi Protected Setup eli langattoman verkon tietoturvastandardi, joka helpottaa verkkoon kirjautumista
XOR	Exclusive OR eli ehdoton tai

1. JOHDANTO

Opinnäytetyön tarkoituksena on tutustua langattoman lähiverkon tietoturvaan ja tekniikkaan. Työssä esitellään myös yritysverkkojen hallintaan tarkoitettuja tekniikoita tietoturvanäkökulmasta.

Tarkoituksena on myös tutkia yleisesti käytössä olevien langattomien verkkojen salaustekniikoita. Testauksessa keskitytään nykyään laajalti käytössä olevaan WPA2-salaukseen.

Testiympäristö on tarkoitus rakentaa erilleen käytössä olevasta verkosta hyödyntäen kuluttajille suunnattua Netgear WNDR4500 reititintä. Testauksessa käytetään Kali Linux käyttöjärjestelmää, joka sisältää testaukseen tarvittavat työkalut.

2. LANGATON LÄHIVERKKO

Langattomien lähiverkkojen (WLAN) perusominaisuudet tekevät siitä huomattavasti erilaisen verraten kiinteään lähiverkkoon. Suunniteltaessa LAN-verkkoja, voidaan olettaa, että laitteen osoite vastaa sen fyysistä sijaintia. WLAN-verkkojen suhteen tämä ei pidä paikkansa. IEEE 802.11 standardissa osoitteen saavasta laiteesta käytetään nimitystä station (STA). STA voi olla esimerkiksi kannettava tietokone, PC, AP tai älypuhelin. Laitteiden fyysisten ominaisuuksien perusteella STA-laitteelle voidaan antaa etuliite: fixed, portable tai mobile. (IEEE Std. 802.11-2012, 44.)

3. WLAN-STANDARDIT

Suurin osa langattomista lähiverkoista(WLAN) käyttää Institute of Electrical and Electronics Engineers (IEEE) 802.11 WLAN-standardeja. Yleisimmin käytössä olevat WLAN radiolähetysstandardit ovat IEEE 802.11b ja IEEE 802.11g, jotka toimivat 2.4GHz taajuudella, sekä IEEE802.11a ja IEEE 802.11n, jotka käyttävät 5GHz taajuutta. 802.11a/b/g sisältää useita tietoturvaominaisuuksia, jotka kantavat nimitystä Wired Equivalent Privacy (WEP). WEP-suojauksessa on useita tunnettuja tietoturvaongelmia, joiden takia IEEE

802.11i (WPA2) on luotu. Uudempi 802.11i toimii aiempien 802.11a/b/g standardien kanssa yhdessä parantaen tietoturvaa. (Boob & Jadhav 2010)

3.1. 802.11b-standardi

Ensimmäinen laajassa julkisessa käytössä ollut WLAN-standardi on 802.11b, joka on otettu käyttöön 1999. 802.11b käyttää 2.4 - 2.4835GHz lisensoimatonta taajuusaluetta. Sen tarjoamat siirtonopeudet ovat 1, 2, 5.5 ja 11Mbps. (Coleman & Westcott 2009,157.)

3.2. 802.11a-standardi

Toinen 1999-vuonna käyttöönotettu standardi on 802.11a. Sen käyttämä taajuus on lisensoimaton 5Ghz. Suurin hyöty 5GHz taajuudesta on vähäisempi ruuhka verraten 2.4GHz taajuuteen, jota käyttävät mikroaaltouunit, Bluetooth ja useat muut langattomat laitteet. Siirtonopeudet 802.11a standardilla ovat 6, 9, 12, 18, 24, 36, 48 ja 54 Mbps. (Coleman & Westcott 2009, 158.)

3.3. 802.11g-standardi

Vuonna 2003 julkaistu 802.11g oli tarkoitettu parantamaan 802.11b standardin tiedonsiirtonopeutta. Tiedonsiirtonopeus 802.11g standardilla on enintään 54Mbps. 802.11g tukiasema on mahdollisuus konfiguroida kolmeen eri tilaan:

- B- Mode hyödyntää 802.11b standardia, jolloin siirtonopeus on maksimissaan 11Mbps.
- G-Mode ei ole yhteensopiva 802.11b laitteiden kanssa. Siirtonopeus tällöin maksimissaan 54Mbps
- B/G-Mode tukee 802.11b ja 802.11g standardeja yhdenaikaisesti. Mikäli tukiasemaan on yhteydessä molempia standardeja hyödyntäviä laitteita yhdenaikaisesti, tukiaseman tiedonsiirtonopeus laskee huomattavasti. B/G-Mode teoriassa tarjoaa 54Mbps tiedonsiirtonopeuden. Käytännössä kuitenkin nopeus vaihtelee 8-20Mbps välillä, riippuen yhteydessä olevista laitteista. (Coleman & Westcott 2009, 159.)

3.4. 802.11n-standardi

Standardi on kehitetty parantamaan langattomien yhteyksien laatua verrattuna edeltävään 802.11g-standardiin. 802.11n tarjoaa mahdollisuuden hyödyntää kahden taajuuden lähetystekniikkaa, jolloin 2,4Ghz ja 5Ghz taajuudet ovat yhtä aikaa käytössä. 802.11n-standardi mahdollistaa jopa 900Mbps tiedonsiirtonopeuden. (Cisco White Paper 2009.)

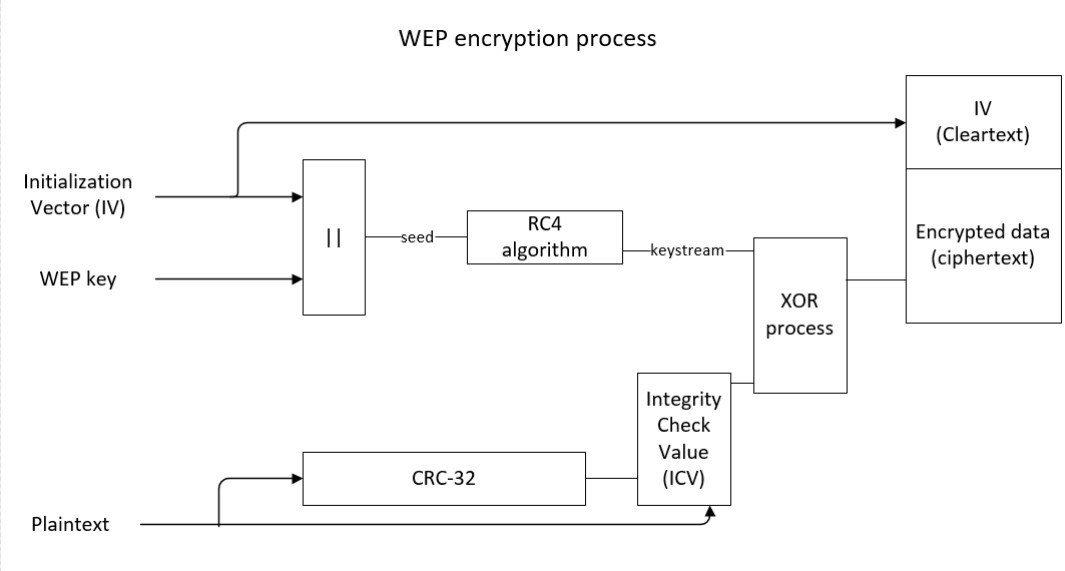
3.5. 802.11ac-standardi

Standardi edustaa uusinta WLAN-tekniikkaa, joka on otettu käyttöön vuonna 2014. Standardi mahdollistaa jopa 3,2Gbps tiedonsiirtonopeuden langattomasti. Se hyödyntää samoja taajuuksia kuin 802.11n, mutta kanavan kaista on kaksinkertainen (80Mhz) verraten 802.11n-standardin kanavan kaistaan. (IEEE Standards Association 2013.)

4. WEP-SALAUS

WEP eli Wired Equivalent Privacy on ensimmäinen langattomissa verkoissa käytössä ollut salaustekniikka, joka on otettu käyttöön ensimmäistä kertaa vuonna 1997. Kyseinen salaustekniikka on pystytty murtamaan jo pitkään, joten sen käyttöä ei suositella. (Coleman & Westcott 2009, 167.)

WEP-salausprosessissa suoritetaan salattavalle datalle Cyclic Redundancy Check (CRC), jonka jälkeen salattavaan datan loppuun lisätään Integrity Check Value (ICV). Tämän jälkeen luodaan 24-bittinen Initialization Vector (IV), joka yhdistetään staattisen salausavaimen kanssa. Seuraavaksi WEP luo avainjonon, käyttäen lähdemateriaalina aiemmin luotua IV-tietoa ja staattista avainta. Lopuksi XOR-prosessi yhdistää selkokielisen datan ja avainjonon, jonka lopputulemana on salattu data. (Coleman & Westcott 2009, 443.)



Kuva 1. WEP-salausprosessi (Coleman & Westcott 2009, 443.)

4.1. Hyökkäykset WEP-salausta vastaan

WEP-salauksessa on useita heikkouksia, jotka mahdollistavat salauksen murtamisen. Yleisimpiä hyökkäyksiä WEP-salausta vastaan ovat:

- IV collisions-hyökkäys**.** Koska 24-bittinen IV on selväkielinen ja erilainen jokaisessa lähetetyssä kehyksessä, kaikki 16 miljoonaa IV:tä tulevat ajallaan toistamaan itseään. Rajoitetusta IV-avaruudesta johtuen IV-törmäyksiä pääsee syntymään, tällöin hyökkääjän on mahdollista saada salausavain huomattavasti helpommin. (Coleman & Westcott 2009, 443.)

- Weak key-hyökkäys. RC4 avain-aikataulutus algoritmista johtuen, heikkoja IV avaimia pääsee muodostumaan. Hyökkääjä pystyy täten selvittämään salausavaimen helpommin hyödyntämällä heikkoja tiedettyjä IV avaimia. (Coleman & Westcott 2009, 444.)

- Reinjection-hyökkäys. Hyökkäystä varten on olemassa hakkerointityökaluja, jotka sisältävät paketin uudelleen injektointi hyökkäyksen. Tätä hyödynnetään hiljaisissa verkoissa, missä halutaan nopeuttaa heikkojen IV avainten keräystä. (Coleman & Westcott 2009, 444.)

WEP-salaus pystytään murtamaan minuuteissa käyttäen hyödyksi Deauth-menetelmää (Deauthentication attack) ja ARP-injektointia. 104-bittinen WEP-avain murtuu 50% todennäköisyydellä, kun 40 000 pakettia on onnistuttu kaappaamaan. 60 000 paketilla todennäköisyys on jo 80% ja 85 000 paketilla 95% todennäköisyys. Ideaalitilanteessa alle minuutissa saadaan kaapattua 40 000 pakettia ja murrettua siten verkonsalaus. (Tews, Weinmann & Pyshkin 2007.)

4.2. TKIP-salaus

Temporal Key Integrity Protocol (TKIP) luotiin korvaaman WEP-salaustekniikka, sen jälkeen kun WEP:n haavoittuvuudet tulivat julki. Tarkoitus TKIP-salauksessa oli hyödyntää vanhoja WLAN-tukiasemia ja päätelaitteita, suurin osa laitteista oli mahdollista päivittää yhteensopivaksi TKIP-tekniikan kanssa. (Coleman, Westcott, Harkins & Jackman 2010, 75.)

Huhtikuussa 2003 WI-FI Alliance esitteli uuden Wi-Fi Protected Access (WPA) sertifioinnin, joka hyödyntää TKIP-salausta. TKIP käyttää WEP-salauksesta tuttua RC4-algoritmiä. (Coleman, Westcott, Harkins & Jackman 2010, 75.)

Eroavaisuudet WEP-salaukseen ovat seuraavat:

- TKIP-salaus hyödyntää dynaamisia salausavaimia (Temporal keys) staattisten avaimien sijasta. Laitteet käyttävät neljäsuuntaista kättelyprosessia muodostaakseen dynaamisen unicast avaimen, joka on yksilöllinen näille laitteille. Staattiset salausavaimet ovat haavoittuvaisia social engineering-hyökkäyksille. (Coleman, Westcott, Harkins & Jackman 2010, 75.)

- TKIP käyttää MPDU TKIP sequence counter (TSC) MPDU lähetysten sekvensointiin. Tukiasema hylkää kaikki paketit, jotka saapuvat väärässä järjestyksessä. Tämä estää replay- ja reinjection-hyökkäykset, joita pystyi käyttämään WEP-salausta vastaan. (Coleman, Westcott, Harkins & Jackman 2010, 75.)

- TKIP hyödyntää kaksivaiheista kryptografista sekoitusprosessia (Key Mixing) luodakseen vahvemman lähde materiaalin RC4 salaukseen.

Kyseinen prosessi on suunniteltu estämään IV:n törmäykset ja heikko avain-hyökkäykset, joita käytettiin WEP-salauksen murtamiseen. (Coleman, Westcott, Harkins & Jackman 2010, 77.)

- Enhanced Data Integrity. TKIP käyttää vahvempaa datan eheystarkastusta, joka tunnetaan nimellä Message Integrity Code (MIC). MIC tunnetaan myös nimeltä Message Integrity Check. MIC on suunniteltu estämään bit-flipping- ja forgery-hyökkäykset. (Coleman, Westcott, Harkins & Jackman 2010, 77.)

- TKIP Countermeasures. TKIP MIC:n suunnittelurajoituksista johtuen on mahdollista, että hakkeri pystyy vaikuttamaan viestin eheyteen. Tätä varten TKIP sisältää myös vastatoimia, joilla pyritään rajaamaan salausavaimesta saatavan tiedon määrää. (Coleman, Westcott, Harkins & Jackman 2010, 77.)

4.3. WPA- ja WPA 2-salaus

Wi-Fi Protected Access (WPA) on Wi-Fi Alliancen kehittämä langattomien verkkojen salaustekniikka. WPA-tekniikka on ensimmäistä kertaa esitelty vuonna 2003, mutta jo vuonna 2004 se sai uuden version WPA 2. WPA otettiin käyttöön korvaamaan WEP-salaus, jonka tietoturvassa on puutteita. Alkuperäinen WPA-tekniikka oli käytännössä siirtymäajan tekniikka, ennen WPA 2-standardin ratifiointia. (Coleman, Westcott, Harkins & Jackman 2010, 88.)

WPA-tekniikassa korjattiin WEP-salauksessa havaitut heikot aloitusvektorit ja salausavain vaihtuu 10000 paketin välein. Syyskuussa 2004 Wifi Alliance esitteli WPA-salauksen version kaksi, jota kutsutaan WPA2-salaukseksi. Sen vaatimuksena on CCMP/AES-salauksen käyttö. WPA2-salaus vaatii laitteen suorittimelta enemmän laskentatehoa kuin 802.11 WEP-ja TKIP-tekniikoita käyttävät laitteet kykenevät tarjoamaan. Tästä syystä laitteet joudutaan usein vaihtamaan CCMP/AES:ia tukeviin laitteisiin. (Coleman, Westcott, Harkins & Jackman 2010, 88.)

Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol (CCMP) on tietoturvaprotokolla, joka on kehitetty osaksi 802.11i-tietoturvaparannusta. Tarkoituksena on ollut korvata TKIP- ja WEP-salaukset. CCMP käyttää AES-lohkosalausta RC4-salauksen sijasta, jota käytettiin WEP- ja TKIP-salauksissa. (Coleman, Westcott, Harkins & Jackman 2010, 83.)

CCMP koostuu useista eri komponenteista, joten on tyypillistä että komponentteihin viitataan erikseen. Counter Mode (CTR) käytetään datan luottamuksellisuuteen. Cipher-Block Chaining (CBC) ja Message Authentication Code (CBC-MAC) käytetään autentikointiin ja datan eheyden tarkistamiseen. (Coleman, Westcott, Harkins & Jackman 2010, 83.)

CCMP-tekniikasta käytetään lyhennettä CCM, kun viitataan lohkosalaukseen, eikä itse protokollaan. CCMP perustuu CCM osaan AES-salauksesta. CCM yhdistää CTR- ja CBC-MAC-osat tarjoten datan luottamuksellisuuden, autentikaation ja eheyden. CCM-prosessi käyttää samaa avainta salatakseen MSDU-tiedon ja tarjotakseen salauksen eheyden tarkistuksen. Salauksen eheys tarkistus suoritetaan MSDU-datalle ja MPDU:n MAC-osoitteen tunnisteen osille.
(Coleman, Westcott, Harkins & Jackman 2010, 83.)

AES-lohkosalaus pystyy hyödyntämään erikokoisia salausavaimia. Kun käytössä on CCMP-salausmetodi, AES-salaus käyttää 128-bittistä avainta ja salaa datan 128-bittisiin lohkoihin. (Coleman, Westcott, Harkins & Jackman 2010, 83.)

- Kuten TKIP, myös CCMP aloittaa 128-bittisellä TK-avaimella. 128-bittinen avain on joko (Pairwise Transient Key) PTK, jolla salataan unicast-liikenne tai (Group Temporal Key) GTK, jolla salataan broadcast- ja multicast-liikenne. (Coleman, Westcott, Harkins & Jackman 2010, 83.)

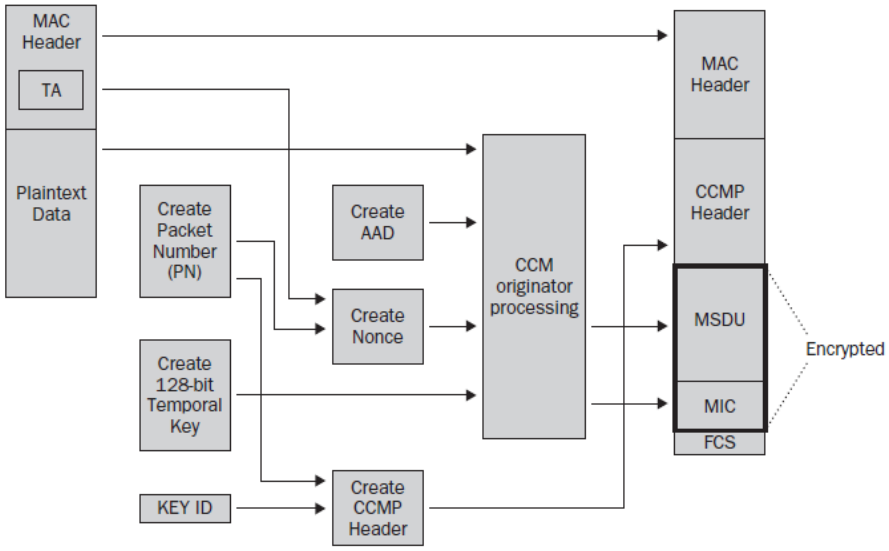
- 48-Bittinen Packet Number (PN) on kuin TKIP-sekvenssi numero. PN yksilöi kehykset ja osana jokaista kehystä. Tämä suojaa CCMP toisto ja injektointi hyökkäyksiltä. (Coleman, Westcott, Harkins & Jackman 2010, 83.)

- Nonce on sattumanvarainen numeerinen arvo, joka muodostetaan vain kerran. 104-Bittinen yksilöllinen nonce koostuu PN, QoS käyttämästä

prioriteetti datasta ja lähettimen osoitteesta. (Coleman, Westcott, Harkins & Jackman 2010, 84.)

- 802.11-data kehys (MPDU). Kehyksen runko kapsuloi MSDU:n ylemmän kerroksen kuorman, joka salataan ja suojataan käyttäen MIC:ä. MPDU tunniste, joka tunnetaan myös MAC tunnisteena ei ole salattu, mutta on osittain suojattu MIC:n toimesta. (Coleman, Westcott, Harkins & Jackman 2010, 84.)

- Additional Authentication Data (AAD). AAD koostuu MPDU-tunnisteen osista. Tätä informaatiota käytetään datan yhtenäisyyden varmentamiseen MAC-kehyksessä. (Coleman, Westcott, Harkins & Jackman 2010, 84.)



Kuva 2. CCMP salaus ja datan eheys prosessi. (Coleman, Westcott, Harkins & Jackman 2010, 84.)

CCMP salaa selkokielisen MPDU:n vaiheittain:

1. 48-bittinen PN luodaan. Jokaiselle MPDU:lle luodaan yksilöllinen PN, joka pysyy samana lähetyksen erivaiheissa. (Coleman, Westcott, Harkins & Jackman 2010, 84.)

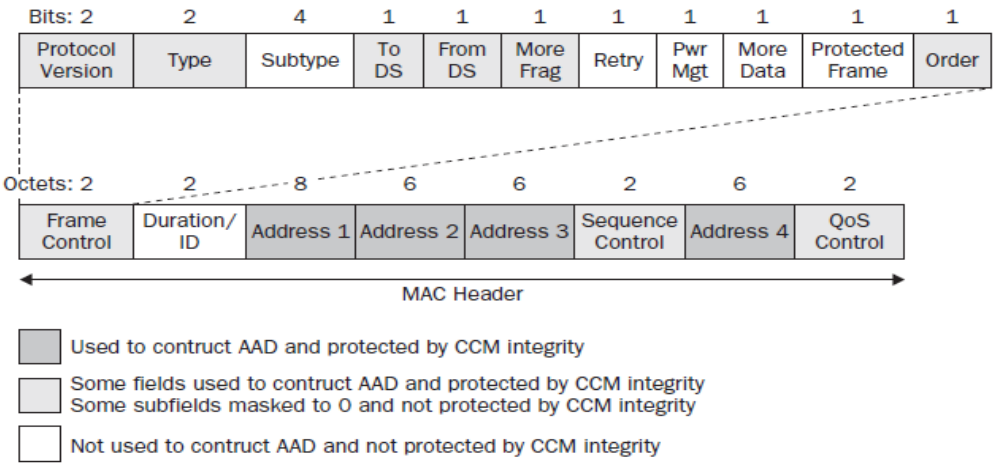
2. Osaa MPDU-tunnisteesta käytetään AAD:n muodostamiseen. MIC takaa eheys suojan näille osille MAC-kehyksestä. Kaikki MAC-osoitteet, MAC-kehyksen osat ja BSSID ovat suojattu. MAC-kehyksen osilla vastaanottava laite varmistaa eheyden. (Coleman, Westcott, Harkins & Jackman 2010, 84.)

3. NONCE luodaan käyttäen PN, TA ja QoS-dataa. (Coleman, Westcott, Harkins & Jackman 2010, 85.)

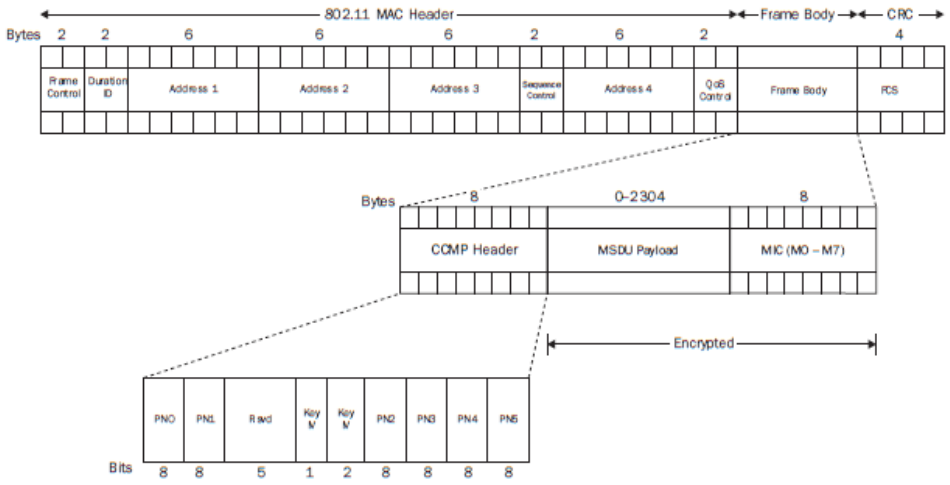
4. Kahdeksan oktetin CCMP-tunniste luodaan. CCMP-tunniste sisältää avain tunnisteen ja PN-tiedon, joka on jaettu kuuteen oktettiin. (Coleman, Westcott, Harkins & Jackman 2010, 85.)

5. CCM-moduuli, joka käyttää AES-lohkosalausta luo datan eheyden tarkistuksen ja salaa ylemmän data kerroksen. 128-bittinen TK, nonce, AAD ja selkokielinen data prosessoidaan luoden kahdeksan tavuinen MIC. Tämän jälkeen MSDU-kehys yhdessä MIC-kehyksen kanssa salataan 128-bittisiksi lohkoiksi. Tätä prosessia kutsutaan CCM alkuunpanijaprosessiksi. (Coleman, Westcott, Harkins & Jackman 2010, 85.)

6. Alkuperäinen MAC-tunniste liitetään CCMP-tunnisteeseen, salattuun MSDU-kehykseen ja salattuun MIC-kehykseen. FCS lasketaan tunnisteen osille ja kehyksen rungolle. Lopputulemana 32-bittinen CRC on lisätty FCS-kenttään. (Coleman, Westcott, Harkins & Jackman 2010, 85.)



Kuva 3. Additional authentication data (AAD)



Kuva 4. CCMP MPDU

Ensimmäiset 32 tavua ovat 802.11 MAC-tunniste, joka ei muutu. Kehyksen runko koostuu CCMP-tunnisteesta, MSDU-kehyksen ylemmän kerroksen kuormasta ja MIC-kehyksestä. CCMP-tunniste sisältää avaintunnisteen ja PN-tiedon, joka on jaettu kuuteen oktettiin. MSDU-kehys ja 8-tavuinen MIC-kehys on salattu. Kun CCMP on käytössä, kehyksen rungon koko MPDU-kehyksessä kasvaa 16-tavulla, maksimissaan 2320-tavuun. Eli CCMP-salaus lisää 16-tavua 802.11 MPDU-kehykseen. (Coleman, Westcott, Harkins & Jackman 2010, 86)

5. WPS - WI-FI PROTECTED SETUP

WPS-tekniikka määrittää automaattisesti WPA/WPA2-salausasetukset koti- ja pienyritys käyttäjille. Käyttäjät voivat helposti määrittää verkon käyttämällä WPS-painiketta tai PIN-koodia. WPS-tekniikan tarkoituksena on helpottaa verkon suojaamista ja yhteyksien muodostamista verkkoon. (Coleman, Westcott, Harkins & Jackman 2010, 232.)

IEEE ei määritä WPS-tekniikan mekanismeja. Ennen kaikkea WPS-tekniikka on määritelmä tietoturva-asetuksille ja verkonhallinnalle helpoimmalla mahdollisella tavalla. WPS-tekniikan tarkoituksena on estää luvaton verkkoon pääsy ja suojella verkkoliikennettä. On olemassa monia muita tapoja toteuttaa sama asia, mutta WPS-tekniikka tarjoaa käyttäjälle helpoimman tavan sen toteuttamiseen. (Coleman, Westcott, Harkins & Jackman 2010, 232.)

5.1. WPS arkkitehtuuri määrittää kolme roolia:

- AP on 802.11-langattomanverkon tukiasema. (Coleman, Westcott, Harkins & Jackman 2010, 233.)

- Enrollee on laite, joka haluaa liittyä WLAN-verkkoon. Saatuaan pääsyavaimen, laite hyväksytään verkon jäseneksi. (Coleman, Westcott, Harkins & Jackman 2010, 233.)

- Registrar-laite on osa verkkoa, joka hyväksyy tai evää pääsyavaimen verkkoon pyrkijältä. (Coleman, Westcott, Harkins & Jackman 2010, 233.)

Registrar on usein osana tukiasemaa tai se voi toimia erillisessä laitteessa, joka sijaitsee useamman tukiaseman takana. Silloin kun se ei ole tukiasemassa, siitä käytetään nimitystä External Registrar. Verkossa voi olla useita tukiasemia, jotka kaikki käyttävät samaa registrar-laitetta. WPS-tekniikka on pääsääntöisesti tarkoitettu kotiin ja pieni toimisto käyttöön. Registrar on tästä syystä yleensä osana tukiasemaa. (Coleman, Westcott, Harkins & Jackman 2010, 233.)

5.2. Rekisteröintiprotokolla

Rekisteröintiprotokolla on määritetty toimimaan in-band-, out-of-band- tai näiden yhdistelmä toteutuksena. In-band konfiguraatiossa Diffie-Hellman avaimen vaihto suoritetaan, jotta voidaan varmistua kirjautujan tietävän salasanan. Salasana itsessään voi olla lähtöisin käyttäjältä itseltään, USB-muistista tai NFC-tekniikkaa käyttävältä laitteelta. Out-of-Band-konfiguraatiossa USB- ja NFC-laitteet ovat WPS-järjestelmän määrittämiä. (Coleman, Westcott, Harkins & Jackman 2010, 234.)

Rekisteröinti-protokolla toimii kahdessa vaiheessa. Ensimmäisessä vaiheessa vaihdetaan tietoa julkisista avaimista, kirjautujasta ja registrar-laitteesta. Ensimmäinen vaihe myös mahdollistaa ominaisuuksien ja laitteen löytämisen.

Vaiheen aikana kirjautuja voi kommunikoida useamman kuin yhden tukiaseman tai registrar-laitteen kanssa, jonka jälkeen käyttäjä voi valita haluamansa tukiaseman. Kun laitteet päättävät siirtyä seuraavaan vaiheeseen, voidaan suorittaa kolme kierrosta, joilla viimeistellään tunnistautuminen ja kirjautumistietojen jakaminen. Toisessa vaiheessa on tarkoituksena muodostaa yhteinen tunnistautuminen perustuen kirjautujan laiteen salasanaan. (Coleman, Westcott, Harkins & Jackman 2010, 234.)

5.3. In-Band tila

Kun konfiguroidaan in-band tilaa, Diffie-Hellman avaimen vaihto suoritetaan ja tunnistautuminen käyttäen laitteen salasanaa. Laiteen salasana on saatu kirjautujalta ja syötetty registrar-laitteeseen. WPS in-band konfiguraatio on suunniteltu suojaamaan passiivisilta kuunteluhyökkäyksiltä ja huomaamaan/suojaamaan aktiiviset brute-force hyökkäykset. (Coleman, Westcott, Harkins & Jackman 2010, 235.)

5.4. Out-of-Band tila

Käytettäessä out-of-band tilaa, WPS:llä on kolme eri asetus vaihtoehtoa. Ensimmäisessä vaihtoehdossa asetukset ovat salaamattomana NFC laitteella tai USB-muistilla. Tällöin asetukset sisältävän laitteen fyysiseen suojaukseen tulisi kiinnittää huomiota, esimerkiksi säilyttää lukitussa tilassa. (Coleman, Westcott, Harkins & Jackman 2010, 235.)

Toinen vaihtoehto sisältää asetukset salattuna Diffie-Hellman julkisella avaimella. Kolmas vaihtoehto on NFC-laitteella peer-to-peer yhteydellä tapahtuva asetusten vaihto. NFC-tekniikkaa pidetään turvallisena tiedonsiirtomuotona, tässä tapauksessa WLAN asetukset ovat myös suojattu 128-bittisellä AES salauksella. (Coleman, Westcott, Harkins & Jackman 2010, 235.)

6. 802.1X-STANDARDI JA EAP-PROTOKOLLA

IEEE 802.1x-standardi ei ole varsinaisesti langattomien verkkojen standardi, koska siihen usein viitataan virheellisesti käyttäen 802.11x. 802.1x-standardi tarkoittaa porttikohtaista todentamista. Kyseinen standardi tarjoaa tunnistautumisympäristön, jolla sallitaan tai evätään liikenne kyseisen portin kautta ja sitä kautta pääsy verkkoon. 802.1x-standardia pystytään hyödyntämään langattomissa ja kiinteissä verkoissa. 802.1x-standardi koostuu kolmesta pää komponentista. (Coleman & Westcott 2009, 447.)

6.1. Supplicant-laite

Supplicant-laite on isäntälaite, jonka ohjelmisto pyytää oikeutta päästä kirjautumaan verkkoon ja siten käsiksi verkon resursseihin. Jokaisella laitteella on yksilölliset tunnistetiedot, jotka varmennetaan todentamispalvelimen toimesta. (Coleman & Westcott 2009, 447.)

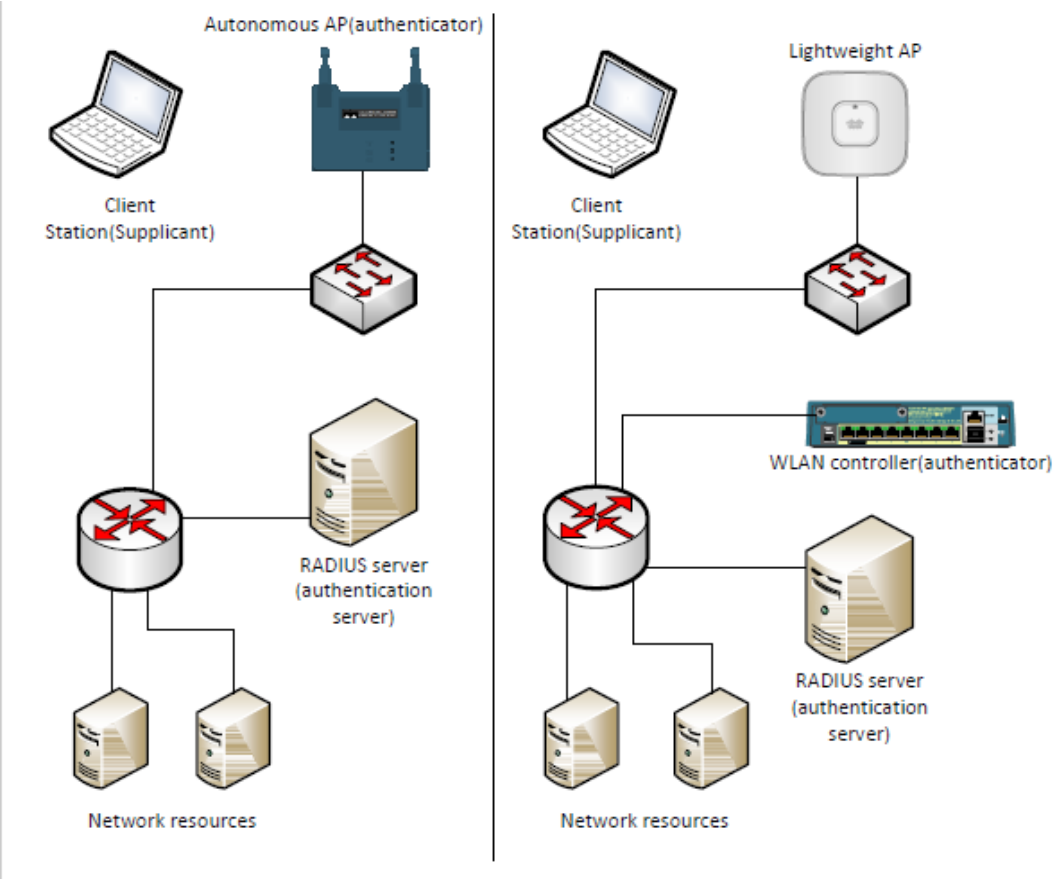
6.2. Authenticator-laite

Authenticator-laite eli varmentajalaite sallii tai evää pääsyn verkkoon portin kautta. Tunnisteliikenne sallitaan päästä normaalisti authenticator-laitteen lävitse. Kaikki muu liikenne on estetty, kunnes supplicant-laite on tunnistettu. Authenticator-laitteella on käytössä kaksi virtuaalista porttia, joista toinen on tarkoitettu tunnisteliikenteelle ja toinen tunnistetulle liikenteelle. (Coleman & Westcott 2009, 447.)

6.3. Authentication server-laite

Authentication server-laite varmentaa supplicant-laitteen tunnistetiedot ja ilmoittaa authenticator-laitteelle, että supplicant-laitteelta on sallittu tai evätty pääsy verkkoon. Authentication server ylläpitää käyttäjätietokantaa tai käyttää ulkoista tietokantaa käyttäjän todentamiseen. (Coleman & Westcott 2009, 448.)

Langattomissa verkoissa supplicant on päätelaite, joka pyytää pääsyä verkon resursseihin. Tukiasema voi toimia authenticator-laitteena, mikäli langaton-verkko ei ole kontrolleri pohjainen, jolloin kontrolleri toimisi authenticator-laitteena. Authentication server-laitteena toimii yleisesti RADIUS-palvelin. (Coleman & Westcott 2009, 448.)

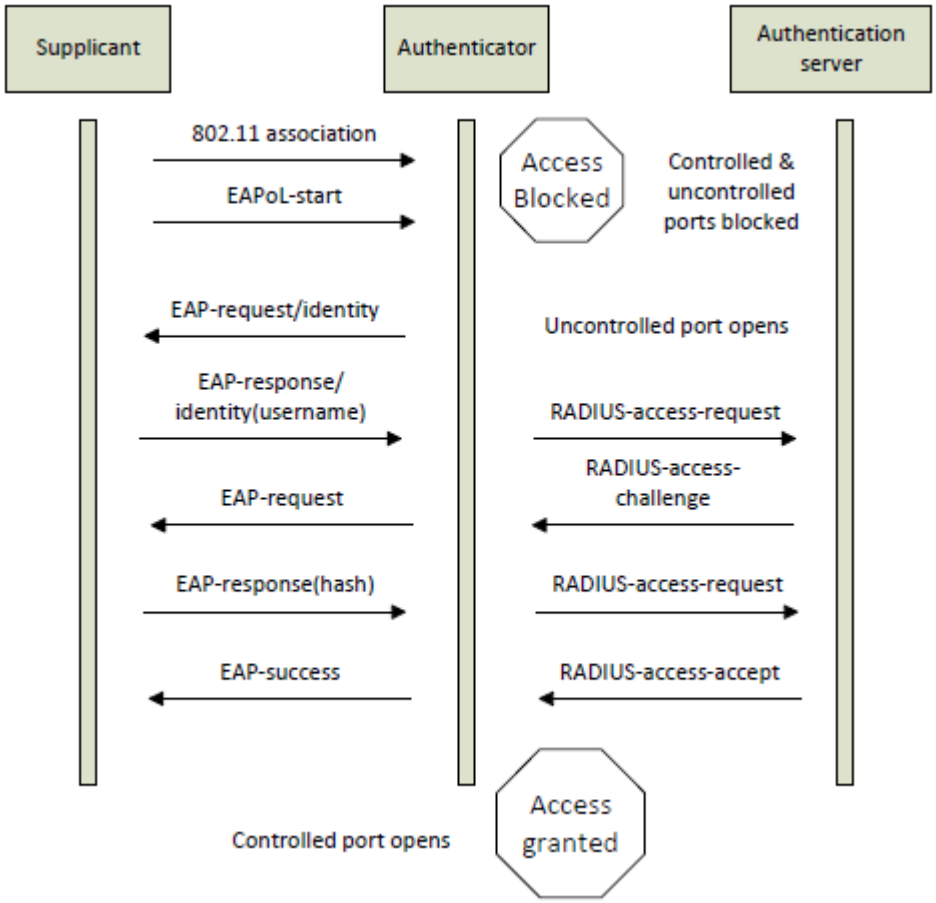


Kuva 5. 802.1x infrastruktuuri(Coleman & Westcott 2009, 448.)

6.4. Extensible Authentication Protocol

Supplicant, authenticator ja authentication server muodostavat kehyksen 802.1x:lle, jonka lisäksi tarvitaan todentamisprotokolla. Extensible Authentication Protocol(EAP) on todentamisprotokolla, jota käytetään käyttäjän todentamiseen. EAP-protokolla on joustava OSI-mallin kerroksella kaksi toimiva todentamisprotokolla, joka sijaiseet Point-to-Point Protokollan (PPP) alla. supplicant ja authentication server kommunikoivat toisilleen käyttäen EAP-protokollaa. Authenticator sallii EAP-liikenteen avoimesta virtuaaliportista. Kun authentication server on varmentanut supplicant-laitteen oikeudet, palvelin lähettää

viestin authenticator-laitteelle, että supplicant-laite on varmennettu. Authenticator-laite avaa tämän jälkeen portin liikenteelle. (Coleman & Westcott 2009, 449.)



Kuva 6. EAP todentaminen(Coleman & Westcott 2009, 449.)

6.5. EAP-tyypit

EAP-protokollasta on monia eri tyyppejä. Ciscon Lightweight Extensible Authentication Protocol (LEAP) on valmistajan oma malli EAP-protokollasta, kun puolestaan Protected Extensible Authentication Protocol (PEAP) on standardiin perustava malli. Osa käyttää yhdensuuntaista todentamista, kun osa käyttää kahdensuuntaista todentamista. Molemminpuolinen todentaminen vaati, että authentication server-laite varmentaa käyttäjän ja supplicant-laitteen pitää myös varmentaa todentamispalvelimen oikeellisuus. Authentication server-laitteen varmentamalla, supplicant-laite voi varmistua, että käyttäjätunnus ja sala-

sana eivät päädy haitalliselle todentamispalvelimelle. Suurin osa EAP-tyypeistä vaatii molemminpuolisen varmentamisen käyttämiseen palvelin puolen digitaalista sertifikaattia, jolla varmennetaan authentication server-laite. (Coleman & Westcott 2009, 450.)

	EAP-MD5	EAP-LEAP	EAP-TLS	EAP-TTLS	PEAPv0 (EAP-MSCHAPv2)	PEAPv0 (EAP-TLS)	PEAPv1 (EAP-GTC)	EAP-FAST
Security Solution	RFC-2284	Cisco proprietary	RFC-2716	IETF draft	IETF draft	IETF draft	IETF draft	IETF draft
Digital Certificates—Client	No	No	Yes	Optional	No	Yes	Optional	No
Digital Certificates—Server	No	No	Yes	Yes	Yes	Yes	Yes	No
Client Password Authentication	No	Yes	N/A	Yes	Yes	No	Yes	Yes
PACs—Client	No	No	No	No	No	No	No	Yes
PACs—Server	No	No	No	No	No	No	No	Yes
Credential Security	Weak	Weak (depends on password strength)	Strong	Strong	Strong	Strong	Strong	Strong (if Phase 0 is secure)
Encryption Key Management	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mutual Authentication	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunneled Authentication	No	No	No	Yes	Yes	Yes	Yes	Yes
Wi-Fi Alliance supported	No	No	Yes	Yes	Yes	No	Yes	No
Man-in-the-Middle Protection	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Dictionary Attack Resistance	No	No	Yes	Yes	Yes	N/A	Yes	Yes

Kuva 7. EAP-tyypit(Coleman & Westcott 2009, 451.)

6.6. Dynaamisen salausavaimen luominen

Vaikka 802.1x/EAP-kehys ei vaadi salausta, on se silti suositeltavaa. 802.1x/EAP sivutuotteena luodaan ja levitetään dynaamisia salausavaimia. EAP-protokolla tarjoaa lähdemateriaalin, jonka avulla dynaamiset salausavaimet luodaan. Etu dynaamisissa avaimissa on tietoturva, avaimet ovat yksilöllisiä ja ne ovat turvassa sosiaaliselta manipulaatiolta.

EAP-kehyksien vaihdon jälkeen todennuspalvelin ja supplicant-laite saavat toisistaan tarvittavat tiedot. Kyseistä tietoa käytetään lähdemateriaalina tai avainmateriaalina supplicant-laitteen ja authentication server-laitteen dynaamisen

salausavaimen luomiseen. Nämä dynaamiset avaimet luodaan istuntokohtaisesti käyttäjille. Aina kun käyttäjä tunnistautuu, luodaan uusi avain ja jokaiselle käyttäjälle yksilökohtainen ja erillinen avain. (Coleman & Westcott 2009, 452.)

6.7. 4-suuntainen kättely

Kahden STA-laitteen täytyy muodostaa menettely, jolla ne tunnistautuvat ja muodostavat kumppanuuden toistensa kanssa. Ne muodostavat myös prosessin aikana dynaamisen salausavaimen, joka tunnetaan neljä suuntaisena kättelynä. (Coleman & Westcott 2009, 452.)

RSNA-prosessi hyödyntää dynaamista salausavaimen hallinta menettelyä, joka pitää sisällään viiden eri avaimen luomisen. Osa RSNA prosessista sisältää kahden pääavaimen luomisen, jotka kantavat nimiä Group Master Key (GMK) ja Pairwise Master Key (PMK). Nämä avaimet ovat seurausta 802.1X/EAP todennuksesta. PMK voidaan luoda myös PSK todennuksesta. Nämä pääavaimet ovat lähde materiaalia, jota käytetään lopullisen dynaamisen avaimen luomiseen. Lopulliset dynaamiset avaimet tunnetaan nimillä PTK ja GTK, joita käytetään salaukseen ja salauksen purkamiseen. GTK salaa ja purkaa salauksen broadcast- ja multicast-liikentestä. PTK puolestaan salaa ja purkaa unicast-liikenteen. (Coleman & Westcott 2009, 452)

7. TUNKEUTUMISEN HAVAITSEMIS- JA ESTOJÄRJESTELMÄT

Suunniteltaessa langattomia verkkoja tulisi kiinnittää huomiota verkkoon pääsyn lisäksi myös tietoturvaan hyökkäysten ja tunkeutumisten osalta. Nykyään on entistä tärkeämpää valvoa jatkuvasti langattoman verkon liikennettä. WIDS eli tunkeutumisen havaitsemisjärjestelmä on langattomien verkkojen valvontaan tarkoitettu ohjelmisto- tai laitteistoratkaisu, jota käytetään useissa yritysverkoissa. WIPS on puolestaan langattomien verkkojen tunkeutumisen estojärjestelmä.(Coleman, Westcott, Harkins & Jackman 2010, 371.)

WIDS ja WIPS sisältävät monia yhteisiä ominaisuuksia, jotka helpottavat verkkoliikenteen valvontaa ja ylläpitoa. Molemmat käyttävät laitteiden ja sensoreiden yhdistelmää tiedon keräämiseen ja analysoimiseen. Jotkut käyttävät myös

kytkimiltä, tukiasemilta ja WLAN-kontrollereilta saatua tietoa hyväkseen. Järjestelmänvalvojan olisi mahdollista kerätä samat tiedot verkkoliikenteestä manuaalisesti, mutta tämä vaatisi ympärivuorokautista valvontaa. (Coleman, Westcott, Harkins & Jackman 2010, 371.)

WIDS-järjestelmä kerää tietoa 802.11 radioliikenteestä käyttäen sensoreita, kerätty tieto tarkistetaan tämän jälkeen. Hajautettu WIDS-järjestelmä on mukautuvampi kuin yhden protokollan authenticator-järjestelmä. (Coleman, Westcott, Harkins & Jackman 2010, 372.)

WIPS käyttäytyy samalla tavalla, mutta lisäksi se pystyy eristämään luvattomat laitteet WLAN-verkosta. Jotkut WIPS-järjestelmät estävät myös luvattomat tukiasemat verkosta. WIPS pystyy myös valvomaan WLAN-käytäntöjä ja estämään luvattomien laitteiden haitallisen toiminnan. Esimerkkinä luvattoman tukiasemaan yhdistämisen ja ad hoc yhteyksien luominen. (Coleman, Westcott, Harkins & Jackman 2010, 372.)

WIDS pystyy havaitsemaan suurenosan hyökkäyksistä ja verkon tapahtumista. WIDS pystyy havaitsemaan: Luvattomat laitteet, väärät konfiguroinnit laitteissa, yhteysongelmat, verkonhäirinnän (Jamming), Man-in-the-middle hyökkäys, Wardriver, verkon skannauksen ohjelmilla kuten (Netstumbler/Kismet), RF häirintä, MAC Spoofing, Denial of Service (DoS) hyökkäys, Brute Force yritykset ohittaa 802.1X (Boob & Jadhav 2010.)

7.1. WIDS/WIPS infrastruktuuri

WIDS/WIPS-komponentit ja ominaisuudet vaihtelevat eri valmistajilla. Ydintoiminnot ja rauta ovat kuitenkin samankaltaisia valmistajasta riippumatta. Yleinen WIDS/WIPS-järjestelmä on hajautettu käyttäjä/palvelin malli, joka sisältää kolme pääkomponenttia:

- WIDS/WIPS-palvelin
- Hallinnointikonsoli
- Sensorit

WIDS/WIPS-palvelin on ohjelma- tai rautapalvelin, joka on keskeisessä roolissa tiedonkeruun ja analysoinnin osalta. Palvelin hyödyntää allekirjoitus analysointia, käyttäytymisen analysointia, protokolla analysointia ja radiotaajuus spektrin analysointia huomatakseen mahdolliset uhat. Allekirjoitus analyysi etsii verkosta yleisimpien WLAN-hyökkäyksien kaavoja. Käyttäytymisanalyysi etsii 802.11-poikkeavuuksia. Protokolla analyysi tutkii MAC-kerroksen informaatiota 802.11-kehyksistä. Protokolla analyysi pystyy myös tutkimaan 3-7 kerroksen informaatiota, jota ei ole salattu. Spektrianalyysi valvoo radiotaajuus tilastoja, kuten signaalin voimakkuutta, signaali-kohinasuhdetta. Suorituskyky analyysiä voidaan käyttää tutkimaan WLAN-verkon tilannetta, kuten kapasiteetti ja peittävyys. (Coleman, Westcott, Harkins & Jackman 2010, 372.)

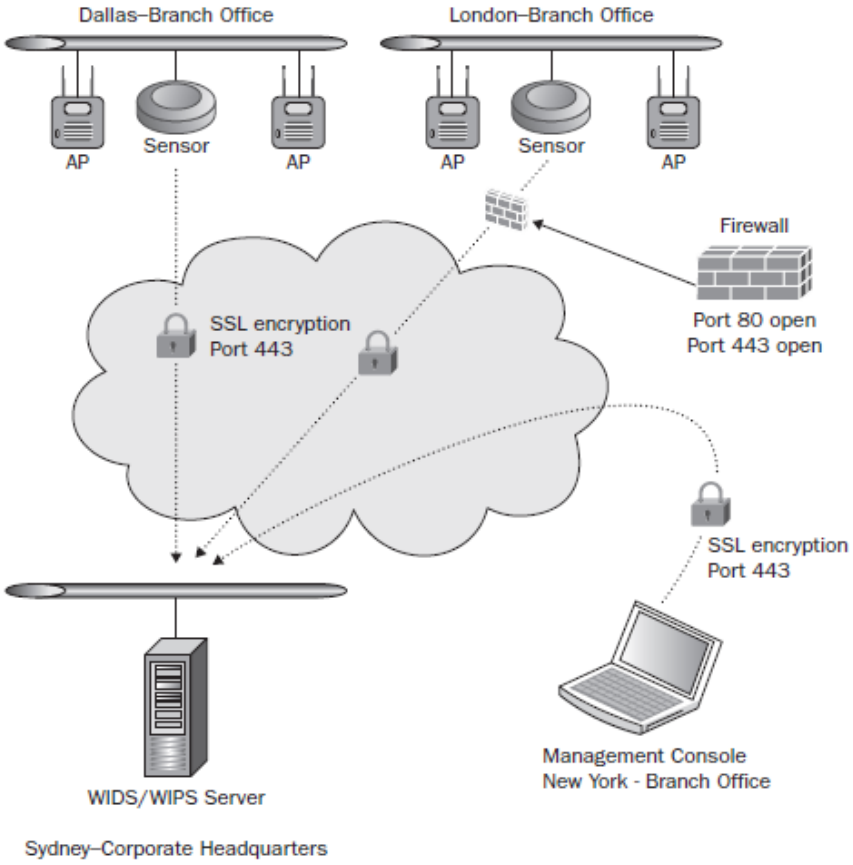
Ohjelmistopohjaista hallinta konsolia käytetään kommunikointiin työasemalta WIDS/WIPS palvelimelle. Hallinta konsolia voidaan käyttää myös ympärivuorokautiseen valvontaan 802.11 verkoissa. (Coleman, Westcott, Harkins & Jackman 2010, 373.)

Rauta- tai ohjelmistopohjaiset sensorit tulisi sijoittaa verkon tärkeimpiin kohtiin, jotta voidaan kuunnella ja ottaa talteen kaikki 802.11-liikenne. Sensorit käyttävät 802.11-radioita tiedon keruuseen, jota käytetään WLAN-yhteyksien turvaamiseen ja analysointiin. Sensorit käyttävät usein samaa rautaa, kuin tukiasemat. Kuitenkin sensorien tarkoituksena on kuunnella verkkoa, eikä tarjota siihen pääsyä kuten tukiasemalla. Sensorit tarkkailevat jatkuvasti kaikkia 14 kanavaa 2,4GHz ISM-alueella ja 23 kanavaa 5GHz UNII-taajuudella. Kanavan skannaus tiheys vaihtelee 100 millisekunnista yhteen sekuntiin. Skannaus tiheyttä voidaan kuitenkin vaihtaa tarpeen mukaan, lyhemmäksi tai pidemmäksi. Yleensä sensorit asetetaan skannaamaan jatkuvasti kaikki 802.11-kanavat. Sensorit voidaan myös asettaa tarkkailemaan määriteltyä kanavaa. (Coleman, Westcott, Harkins & Jackman 2010, 374.)

Suurin osa WIDS/WIPS-sensoreista on rautapohjaisia, joissakin tapauksissa sensorit voivat olla myös ohjelmistopohjaisia. Sensori ohjelmisto hyödyntää tietokoneen WLAN-radiota skannaukseen.

Yhteydet sensorilta ja hallinta konsolilta takaisin palvelimelle ovat yleensä suojattu SSL-tunneloiduilla valmistajakohtaisilla protokollilla. Sensorit lähettävät palvelimelle myös jatkuvasti viestejä, jolla ilmaisevat olevansa toiminnassa. Sensoreita voidaan keskistetysti hallita konsolin kautta, tai yksitellen käyttämällä verkkoselainta, telnet- tai SSH-yhteyttä. Hallintayhteyttä varten portit 80 ja 883, pitää olla avoinna palomuurista. Joidenkin valmistajien laitteet saattavat käyttää myös muita portteja hallintayhteyteen. Sensoreilla voidaan myös etänä kaapata paketteja. (Coleman, Westcott, Harkins & Jackman 2010, 374.)

FIGURE 10.3 WIDS/WIPS distributed architecture



Kuva 8. WIDS / WIPS hajautettu arkkitehtuuri. (Coleman, Westcott, Harkins & Jackman 2010, 375.)

Kolmen komponentin hajautettu WIDS/WIPS-järjestelmä arkkitehtuuri pystytään toteuttaa yhden toimipisteen WLAN:n verkossa tai voidaan laajentaa valvomaan useamman toimipisteen verkkoja. WIDS/WIPS-palvelin voi sijaita eri

toimipisteessä, kuin valvottava verkko. Hallinta konsoli sijaitsee yleensä samassa toimipisteessä, mistä verkkoa hallitaan. (Coleman, Westcott, Harkins & Jackman 2010, 375.)

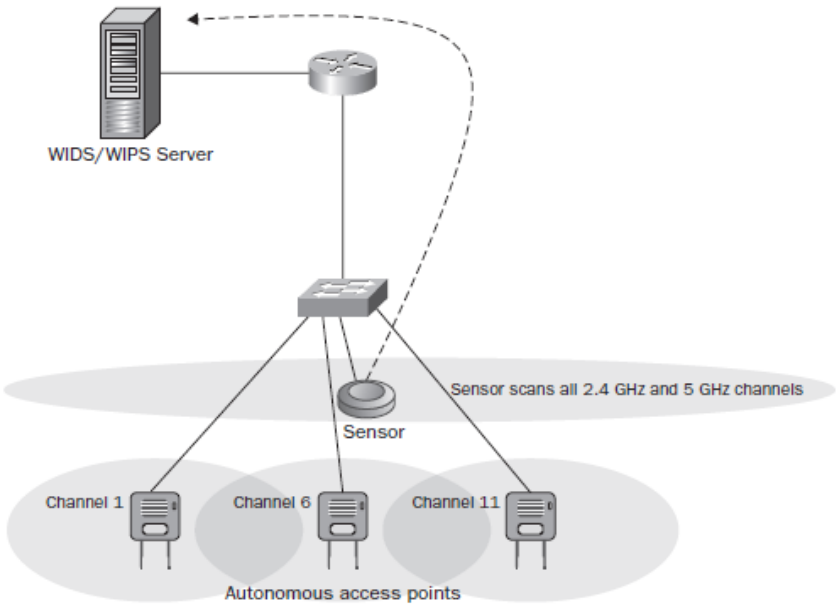
7.2. WIDS/WIPS arkkitehtuuri mallit

WIDS/WIPS-järjestelmä koostuu kolmesta keskeisestä komponentista. Nämä pystyvät valvomaan 802.11 WLAN-verkkoja käyttämällä jotain vaihtoehtoa kolmesta eri arkkitehtuuri mallista:

- Integroitu
- Peite
- Integraatio käytössä

Peite arkkitehtuurilla oleva WIDS/WIPS-järjestelmä sijoitetaan olemassa olevan WLAN-verkon päälle. Tällä mallilla voidaan valvova mitä tahansa olemassa olevaa tai suunnitteilla olevaa verkkoa. Kyseisellä mallilla on paremmat ominaisuudet ja valvonta mahdollisuudet, mutta se on myös kalliimpi toteuttaa kuin muut mallit. Peite malli koostuu WIDS-palvelimesta ja sensoreista, jotka eivät ole osana WLAN-verkkoa, joka tarjoaa yhteydet käyttäjille. (Coleman, Westcott, Harkins & Jackman 2010, 375.)

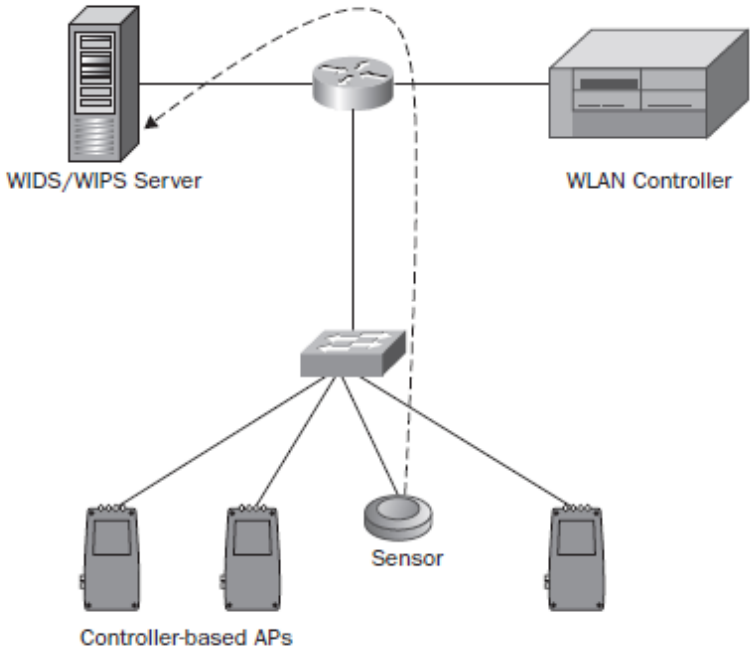
FIGURE 10.4 Overlay WIDS/WIPS—autonomous APs



Kuva 9. WIDS/WIPS peite arkkitehtuuri itsenäisillä tukiasemilla (Coleman, Westcott, Harkins & Jackman 2010, 376.)

Peite arkkitehtuuria voidaan käyttää WLAN-verkoissa, jotka käyttävät itsenäisiä tukiasemia. Voidaan hyödyntää myös useimmissa kontrolleri pohjaisissa WLAN-ratkaisuissa. Mallissa hyödynnetään itsenäisiä sensoreita olemassa olevan verkonvalvontaan. Itsenäiset sensorit hyödyntävät erillisiä radioita, jotka ovat varattuja vain valvontaan. Sensorit vaativat kiinteän verkkoyhteyden WIDS/WIPS-palvelimelle. Yhdellä sensorilla voidaan valvoa 2,4 GHz ISM ja 5 GHz UNII taajuuksia. (Coleman, Westcott, Harkins & Jackman 2010, 376.)

FIGURE 10.5 Overlay WIDS/WIPS—WLAN controller

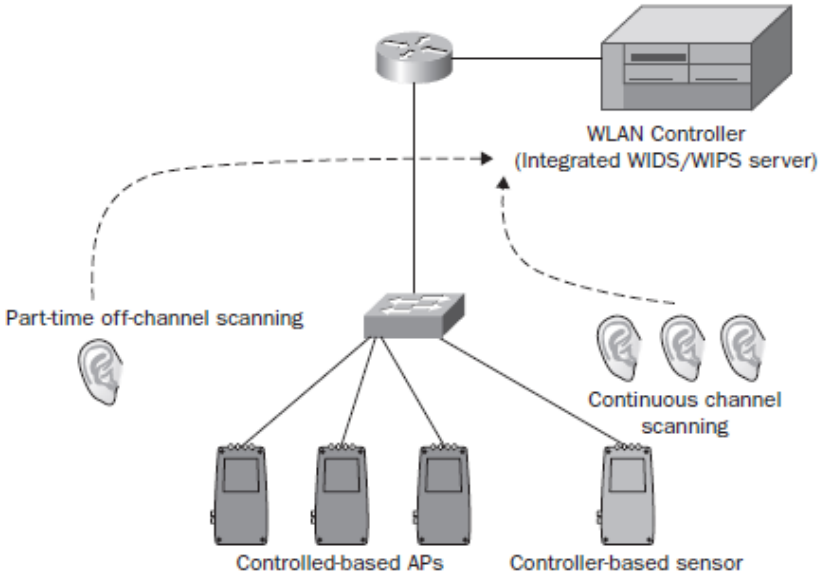


Kuva 10. WIDS/WIPS Peite arkkitehtuuri WLAN-kontrollerilla (Coleman, Westcott, Harkins & Jackman 2010, 377.)

Itsenäisillä sensoreilla voi olla kaksi radiota, joista toinen valvoo 2,4GHz taajuuksia ja toinen 5GHz taajuuksia. Peitemallin rauta ja käyttöönotto kustannukset ovat suuremmat, mutta tarjoavat enemmän toimintoja verkonvalvontaan. Peite WIDS-/WIPS-palvelimet pystyvät usein laajemmin valvomaan hyökkäyksien tuntomerkkejä, jolloin mahdollinen uhka tai tiedonkeruu pystytään havainnoimaan. Toinen suuri etu järjestelmässä on valvonnan jatkuvuus, vaikka WLAN-verkko menisi pois käytöstä. Kyseinen malli on erillään muusta WLAN-infrastruktuurista, joten verkon toiminnalla ei ole vaikusta WIDS/WIPS-järjestelmään. (Coleman, Westcott, Harkins & Jackman 2010, 377.)

Integroitu WIDS-/WIPS-arkkitehtuuri on käytössä useilla laitevalmistajilla WLAN-kontrollereissaan. WLAN-arkkitehtuuria hyödynnetään tarjoamaan verkkoon pääsy ja verkonvalvonta. (Coleman, Westcott, Harkins & Jackman 2010, 377.)

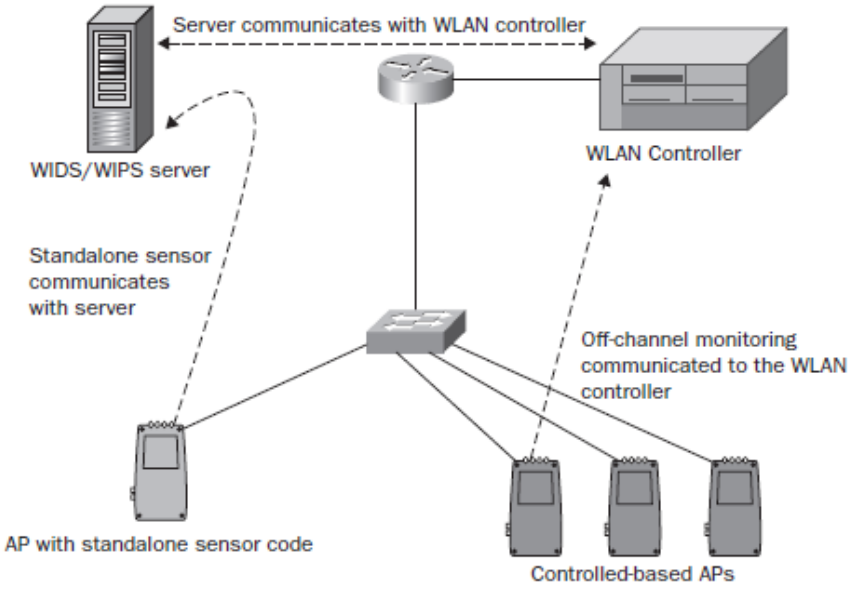
FIGURE 10.6 Integrated WIDS/WIPS



Kuva 11. Kontrolleriin integroitu WIDS/WIPS (Coleman, Westcott, Harkins & Jackman 2010, 378.)

WIDS/WIPS-palvelin sijaitsee WLAN-kontrollerissa osana ohjelmistoa. WLAN-kontrolleri pohjaiset tukiasemat, voidaan asettaa toimimaan täysi-aikaisina sensoreina tai osa-aikaisina sensoreina. Osa-aikainen tukiasema toimii sensorina riippuen tukiaseman ruuhkasta. Täysi-aikainen sensori ei tarjoa pääsyä verkkoon, vaan valvoo verkonliikennettä. (Coleman, Westcott, Harkins & Jackman 2010, 379.)

FIGURE 10.7 Integrated-enabled WIDS/WIPS

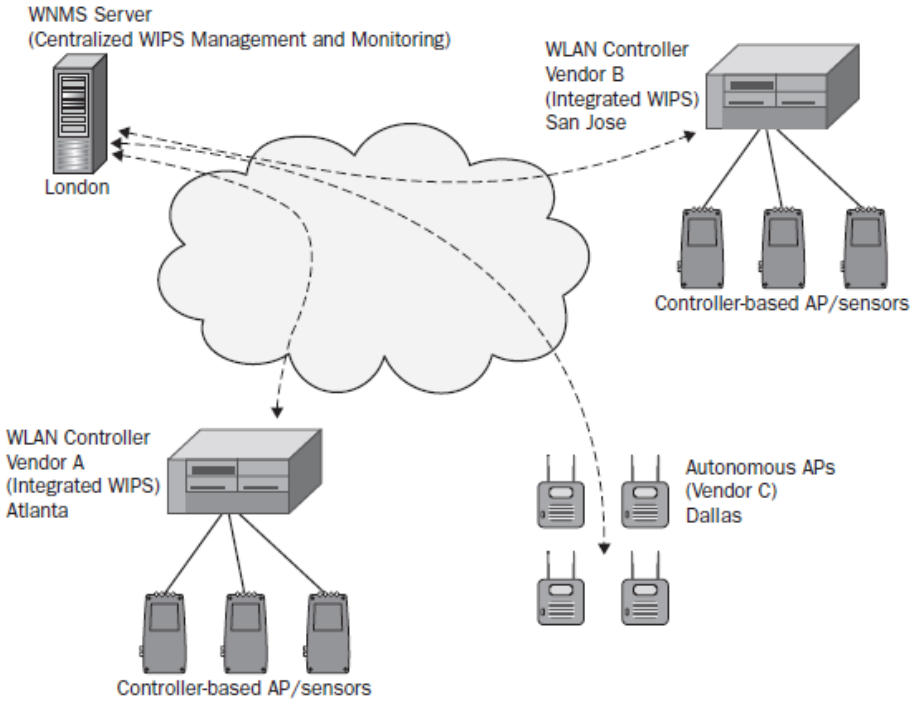


Kuva 12. Erillinen WIDS/WIPS-palvelin (Coleman, Westcott, Harkins & Jackman 2010, 380.)

Joidenkin isojen yritysten verkoissa hyödynnetään WNMS-palvelinta. WNMS tarjoaa keskitetyn hallinnan WLAN-verkonlaitteille ja mahdollisuuden päivittää laitteet. WNMS voi olla valmistajakohtainen tai valmistajasta riippumaton. WLAN-kontrollerit on kuitenkin yleisesti syrjäyttäneet WNMS palvelimet verkonhallinnassa. (Coleman, Westcott, Harkins & Jackman 2010, 380.)

WNMS-palvelimia hyödynnetään pääsääntöisesti, kun verkossa on useampia WLAN-kontrollereita. Riippumatta WLAN-kontrollerin valmistajasta, voidaan sitä hallita WNMS-palvelimen avulla. WNMS ei ole siis riippuvainen laitevalmistajasta. WIDS/WIPS on mahdollista yhdistää WNMS-palvelimen toimintaan, jotta voidaan valvoa keskitetysti verkon hälytyksiä. (Coleman, Westcott, Harkins & Jackman 2010, 380.)

Figure 10.8 WNMS for security monitoring



Kuva 13. WNMS-palvelimella oleva WIDS/WIPS-arkkitehtuuri (Coleman, Westcott, Harkins & Jackman 2010, 381.)

8. KÄYTÄNNÖN TESTIT

Käytännön osuudeksi valittiin WPA2-salauksen testaaminen, koska kyseinen salaustekniikka on yleisin käytössä olevista. Testauksen tarkoituksena on havainnollistaa WPA2-salauksen murtamisen periaate.

Testissä käytettiin kuluttajille suunnattua Netgear WNDR4500-reititintä. Ainoa tehty muutos laitteen asetuksiin on SSID:n vaihtaminen, jotta laite on helposti eroteltavissa muista verkkolaitteista. Laitteen salausavain on testissä tarkoituksellisesti laitevalmistajan luoma.

Testaaminen itsessään suoritettiin kannettavalla tietokoneella, johon oli asennettu Kali Linux. Salausavaimen selvittämiseksi suoritettu sanakirjahyökkäys suoritettiin pöytäkoneella, jotta testi saatiin suoritettua nopeammin. Tietokoneen laskentateho ja sanalistan laatu ovat molemmat ratkaisevia tekijöitä salausavaimen selvittämiseen.

8.1. Kali Linux

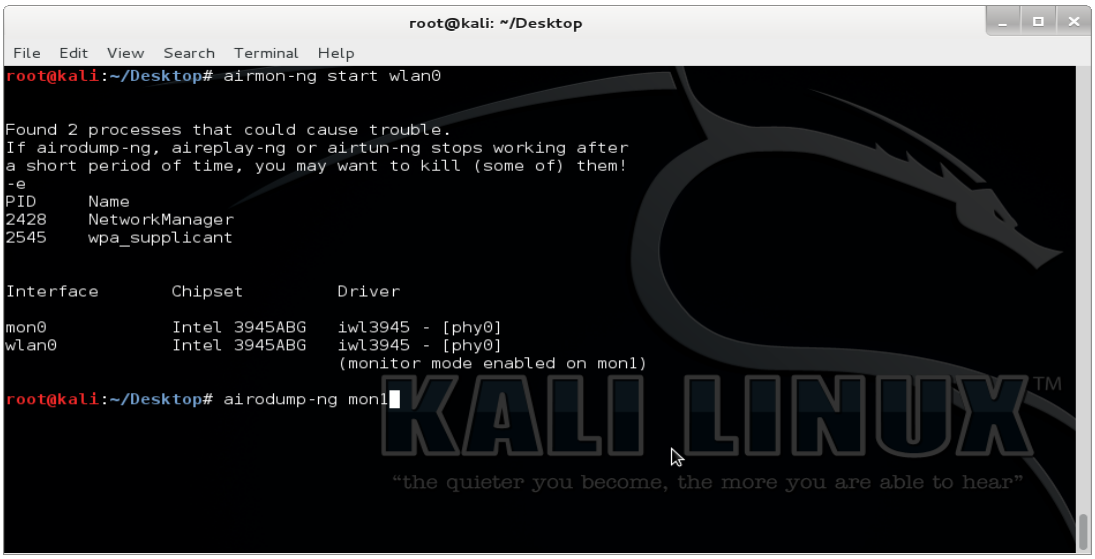
Kali Linux on Debian pohjainen Linux-jakelu, joka on tarkoitettu tietoturva-auditointiin ja tunkeutumistestaukseen. Kali sisältää yli 600 testaukseen tarkoitettua työkalua. Työkalut on tarkoitettu ensisijaisesti tunkeutusmistestaukseen, tutkintaan ja takaisinmallintamiseen. Kali Linuxin on kehittänyt, rahoittanut ja ylläpitää Offensive Security. (What is Kali Linux? 2015.)

8.2. Asentaminen

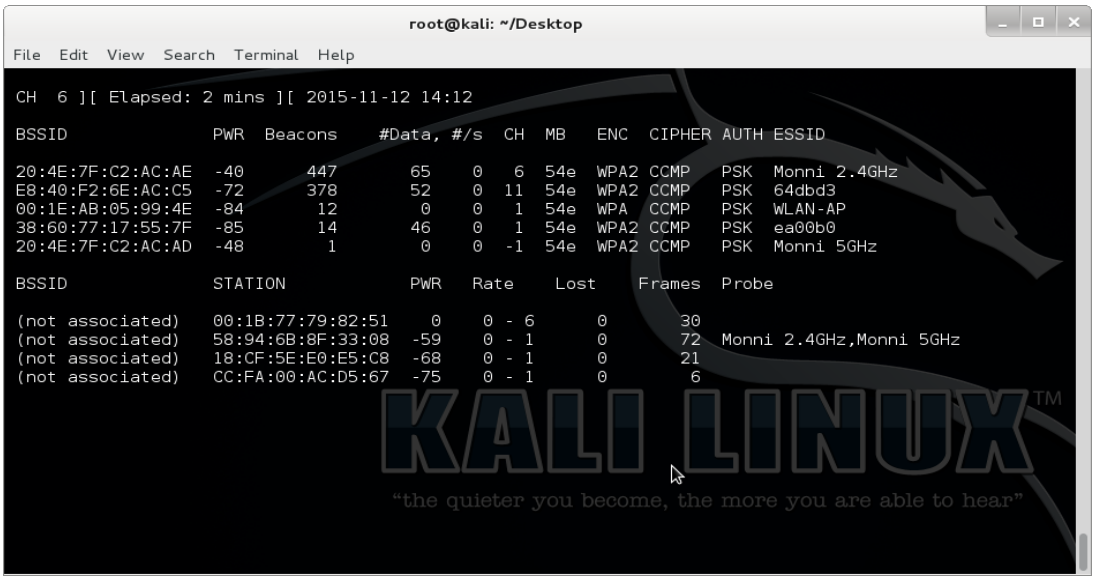
Kali Linux voidaan asentaa tietokoneelle tai sitä voidaan käyttää suoraan muistitikulta. Levykuva sisältää asentamiseen tarvittavat tiedostot sekä niin sanotun Live-USB:n. Live-USB mahdollistaa käyttöjärjestelmän suorittamisen suoraan USB-muistista, jolloin sitä ei tarvitse asentaa.

8.3. WPA2-salauksen murtaminen

Ensimmäiseksi asetetaan langaton verkkokortti valvomaan verkkoa. Käytössämme oli kannettavaan tietokoneeseen integroitu verkkokortti. Komento toiminnolle syötetään Kali Linuxin terminaalissa: ***airmon-ng start wlan0***. Tämän jälkeen aloitetaan verkkoliikenteen talteenotto komennolla: ***airodump-ng mon1***.



Kuva 14. Asetetaan verkkokortti kuuntelemaan

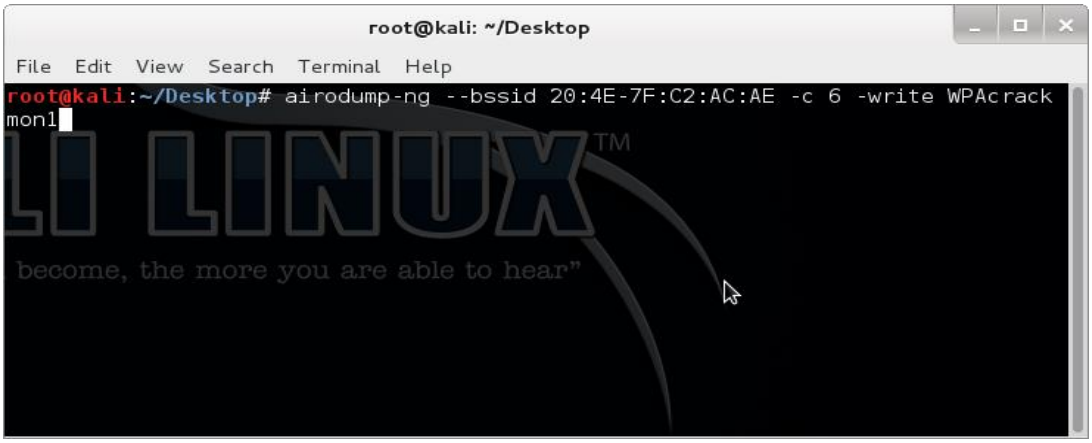


Kuva 15. Aktiiviset tukiasemat

Komento ***airodump-ng mon1*** kerää talteen kaiken verkkokortin havaitseman langattoman verkkoliikenteen. Komennolla nähdään mm. BSSID, hallintakehykset, kanava, data kehykset, salaus ja ESSID.

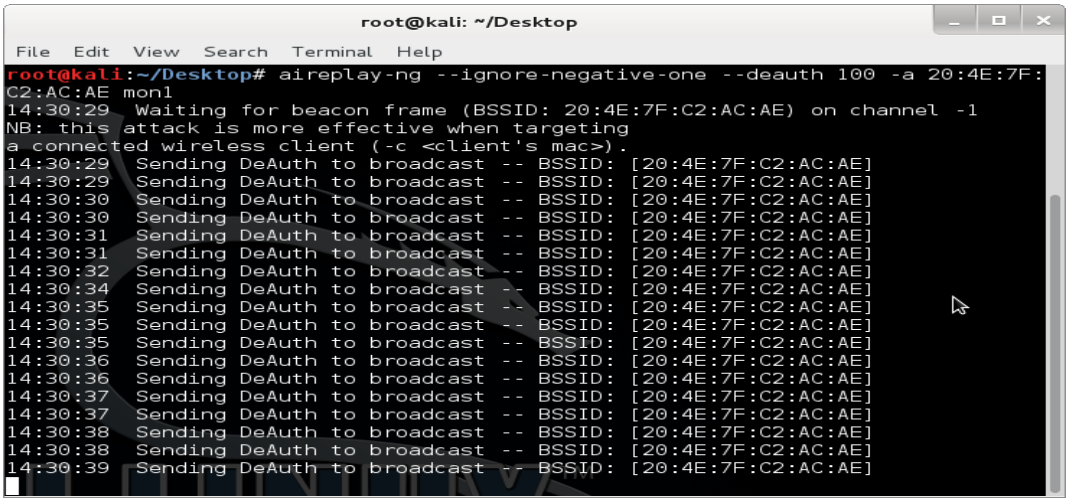
Seuraavaksi valitaan yksi tukiasema ja keskitytään kuuntelemaan yhtä kanavaa. Testaukseen valittuna on tukiasema, jonka SSID on Monni 2.4GHz. Komennolla: ***airodump-ng - -bssid 20:4E:7F:C2:AC:AE –c 6 - - write WPAcrack mon1***. Komennon osa bssid 20:4E:7F:C2:AC:AE määrittää tukiaseman, jota kuunnellaan. Kuunneltava kanava määritetään parametrilla –c 6, josta numero ilmaisee kuunneltavan kanavan. WPAcrack on tiedoston nimi, johon kuunneltu tieto kerätään.

Komento tulee suorittaa erillisessä terminaalissa, jotta myöhemmin voidaan tarkistaa WPA kättelyn talteenotto.



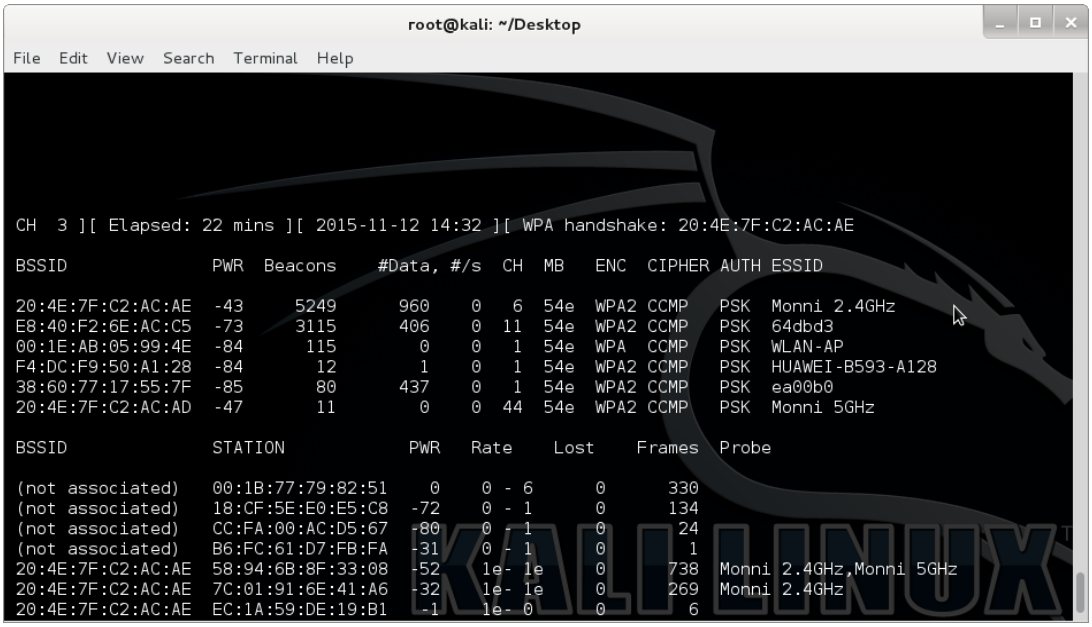
Kuva 16. Otetaan talteen tukiaseman paketit

Seuraavaksi tarkoituksena on saada taltioitua WPA-kättelyprosessi. Tätä varten suoritetaan deauthentication hyökkäys, jonka tarkoituksena on pudottaa laitteita kyseisestä tukiasemasta. Laitteiden kirjautuessa takaisin verkkoon, saadaan otettua talteen WPA kättely. Deauth toteutetaan komennolla ***aireplay-ng - - ignore-negative-one - - deauth 100 – a 20:4E:7F:C2:AC:AE mon1***.



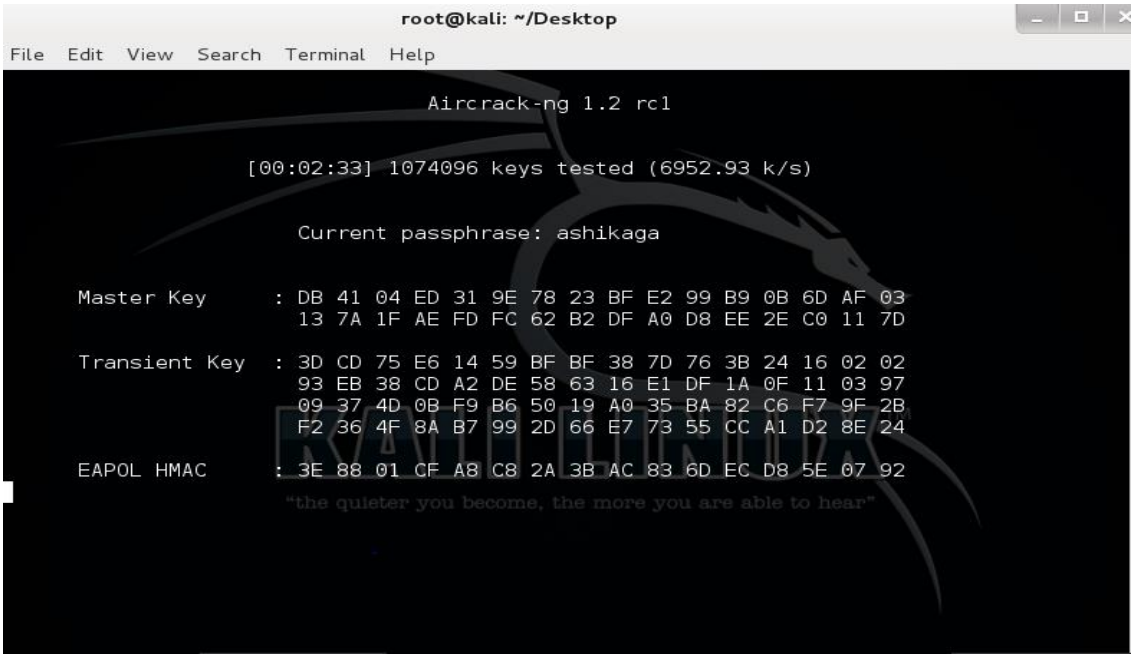
Kuva 17. Deauth-hyökkäys

Komennon osalla - - deauth 100 määritetään deauth-kehysten määrä. Komennossa tulee olla myös määritettynä kohde tukiaseman BSSID. WPA-kättelyn talteenoton onnistuminen ilmenee erillisestä terminaalista, joka aiemmin asetettiin kuuntelemaan kyseistä tukiasemaa.



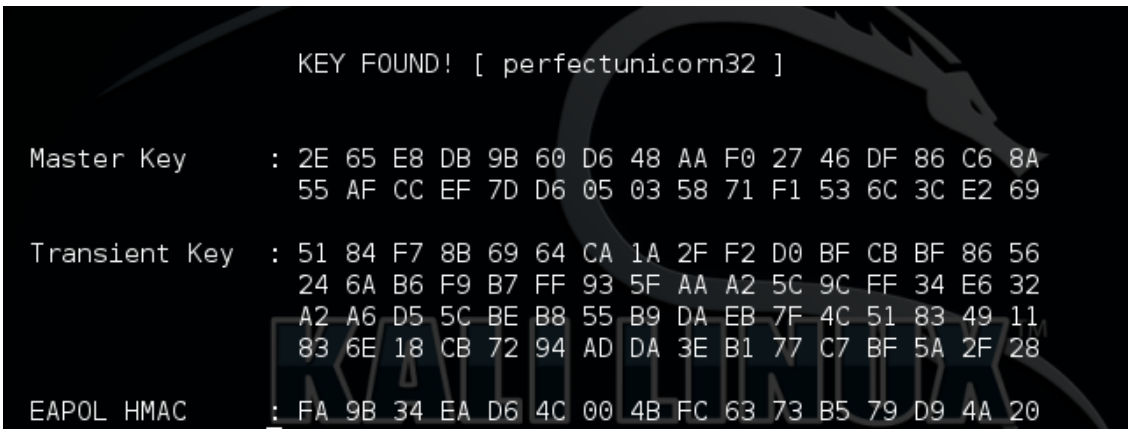
Kuva 18. WPA kättely otettu talteen

WPA kättelyn talteenoton jälkeen selvitetään verkon salasana. Talteen otettu salattu salasana on WPAcrack-01.cap tiedostossa. Salasanan selvittämiseksi käytetään rockyou-sanalistaa, joka on osa Kali Linuxia. Komennolla ***aircrack-ng WPAcrack-01.cap –w /usr/share/wordlists/rockyou.txt*** suoritetaan salasanan vertailu sanakirjaa vastaan.



Kuva 19. sanakirja hyökkäys

WPAcrack tiedostossa olevaa salasanaa vertaillaan sanalistaa vastaan, josta lopulta löytyi oikea salasana.



Kuva 20. Salausavain löytyi

9. YHTEENVETO

Lähtökohta opinnäytetyölle oli tarkastella langattoman lähiverkon tietoturvaa yleisellä tasolla ja yritysmaailmaan suunnatun 802.1x kannalta. Opinnäytetyön edetessä mukaan tuli myös verkonhallintaa ja valvontaa tietoturvanäkökulmasta.

Verkonhallinta ja valvonta-osiossa keskityttiin WIDS/WIPS-järjestelmiin, jotka ovat osa yritystason verkkoratkaisuja. WIDS/WIPS osio jätettiin teorian tasolle. Aihe itsessään riittäisi opinnäytetyön aiheeksi, mikäli siihen sisällyttäisi käytännön osuuden.

Työn painottui yleisesti käytössä oleviin WLAN-tekniikkaan teorian tasolla sekä laajasti käytössä olevan WPA2-salauksen testaamiseen. WLAN-tekniikan osalta suurin muutos on tapahtunut 802.11ac julkaisun myötä siirtonopeuksissa. Siirtonopeudet kohoavat uuden standardin ansiosta monin kertaisiksi verrattuna 802.11n standardiin.

Käytännön osuus työstä painottui WPA2-salauksen testaamiseen hyödyntämällä sanakirjahyökkäystä. Käytännön osuudessa käytössä oli kuluttaja käyttöön tarkoitettu Netgear WNDR4500 reititin, jonka salausavain on laitteen itse luoma.

Testaamiseen käytettiin Kali Linuxia, joka sisältää laajan valikoiman työkaluja tunkeutumistestaukseen. WPA kättelyn talteenotto oli helposti toteutettavissa, varsinainen haaste on selvittää talteen otetusta hash:sta varsinainen verkon salasana.

WPA kättelyn talteenotto suoritettiin deauthentication hyökkäyksellä, jolloin reitittimeen yhteydessä olleista laitteista osa joutui kirjautumaan verkkoon uudelleen. Tässä vaiheessa WPA kättely pystyttiin ottamaan talteen.

Sanakirjahyökkäyksen toimivuus riippuu käytössä olevan sanakirjan laajuudesta. Mikäli salasana on pitkä ja sisältää erikoismerkkejä, vaikeutuu sen selvittäminen. Sanakirjahyökkäyksessä salasanan selvittämiseen vaikuttaa myös oleellisesti käytössä olevan tietokoneen laskentateho, eli kuinka monta sanaa ehditään verrata salasanan hash-arvoa vastaan.

Testasimme sanakirja hyökkäystä kahdella eri tietokoneella, joista toinen oli 2.2GHz tuplaydinsuorittimella varustettu kannettavatietokone. Toinen testi

suoritettiin pöytäkoneella virtuaalikoneessa, jolle oli varattuna kahdeksan 4GHz ydintä. Kannettava kykeni vertaamaan noin 1100 sanaa sekunnissa, virtuaalikone vertasi sekunnissa 7100 sanaa. Vaihtoehtoisesti saman voi ostaa palveluna, jolloin kättelytiedosto luovutetaan palveluun laskettavaksi. CloudCracker palvelu lupaa verrata kättelyä 300:n miljoonaan sanaan 20 minuutissa.

Käytössämme olleessa sanakirjasta ei löytynyt testin aikana laitteen oikeata salausavainta. Lopulta päätimme lisätä oikean salausavaimen sanakirjaan, jotta pystyimme testaamaan sanakirjahyökkäyksen toimivuutta. Käytössämme ollut salasana ratkesi tämän jälkeen nopeasti.

Salausavaimen on syytä olla yli kahdeksan merkkiä pitkä ja sisältää vähintään kirjaimia ja numeroita, mutta myös erikoismerkkejä. Tällöin salausavaimen selvittäminen järkevässä ajassa on käytännössä mahdotonta. Tietokoneiden laskentatehon kasvaessa heikkojen salausavaimien selvittäminen nopeutuu entisestään.

LÄHTEET

Boob, S. & Jadhav, P. 2010. Wireless Intrusion Detection System. International Journal of Computer Applications (0975 - 8887) Nro. 8 Elokuu 2010.

Cisco White Paper 2009 Key Performance Benefits of 802.11n. Verkkojulkaisu. Saatavissa: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11n/white_paper_c11-513840.pdf [Viitattu 25.9.2015.]

Coleman, D. & Westcott, D. 2009. Certified Wireless Network Administrator. Indianapolis: Wiley Publishing Inc.

Coleman, D., Westcott, D., Harkins & B., Jackman, S. 2010. Certified Wireless Security Professional. Indianapolis: Wiley Publishing

IEEE Standards Association. 2013. IEEE Std. 802.11ac - 2013. Verkkojulkaisu. Saatavissa: https://standards.ieee.org/findstds/standard/802.11ac-2013.html [Viitattu 20.9.2015]

IEEE Standards Association. 2012. IEEE Std. 802.11 - 2012. Verkkojulkaisu. Saatavissa: https://standards.ieee.org/findstds/standard/802.11-2012.html [Viitattu 4.8.2015]

Tews, E., Weinmann & R., Pyshkin, A. 2007.. Breaking 104bit WEP in less than 60 seconds. Verkkojulkaisu. Saatavissa: http://eprint.iacr.org/2007/120.pdf [viitattu 1.10.2015]

What is Kali Linux? Verkkojulkaisu. Saatavissa: http://docs.kali.org/introduction/what-is-kali-linux [Viitattu 4.11.2015]