Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto
Tuomas Kuisma

Opinnäytetyö

Tietoturva WLAN mesh-verkoissa

Työn ohjaaja koulutuspäällikkö Ari Rantala
Työn tilaaja Nokia Research Center / Demola
Tampere 6/2010

Tekijä	Tuomas Kuisma
Työn nimi	Tietoturva WLAN mesh-verkoissa
Päivämäärä	26.10. 2010
Työn laajuus	22 sivua
Avainsanat	WLAN, mesh, tietoturva, 802.11s
Koulutusohjelma	Tietotekniikka
Suuntautuminen	Tietoliikennetekniikka

Työn teettäjä	Nokia Research Center (Demola projekti 37: Power of Mesh)
Työn ohjaaja	Koulutuspäällikkö Ari Rantala

Tiivistelmä

Mesh-verkko pohjautuu kehitysvaiheessa olevaan avoimen lähdekoodin 802.11s langaton-mesh standardiin, joka on vielä tätä kirjoitettaessa standardoimaton verkkomalliratkaisu. Ratkaisu perustuu Ad Hoc solukkoverkon tapaiseen tukiasemattomaan WLANia hyödyntävään tiedonsiirtotapaan, missä verkon laitteet keskustelevat toistensa kanssa ilman verkon kiinteitä laitteita tai paikallista verkon valvontaa.

WLAN mesh-verkoissa tietoturva on vielä ratkaisematta sen ongelmallisuuden vuoksi. Tässä työssä pääsääntöisesti pohditaan erinäisiä ratkaisuita ja toteutustapoja mesh-verkkojen tietoturvaan. Työssä määritellyt ratkaisut mukailevat 802.11s luonnoksessa esitettyä toteutusta.

Työ toteutettiin demolan järjestämänä projektina neljän hengen ryhmässä. Projektin tavoite oli saada aikaan toimiva ohjelma WLAN mesh-verkon hallintaan. Työn tilaajana toimi Nokia Research center. Nokian puolelta ohjaajana toimi Mika Kasslin ja demolasta vetäjänä Ville Kairamo.

Author	Tuomas Kuisma
Work label	Security in WLAN mesh-networks
Date	26.10. 2010
Number of pages	22 pages
Keywords	WLAN, mesh, Security, 802.11s
Education programme	Computer systems engineering
Line	Telecommunications engineering

Commission company	Nokia Research Center (Demola project 37: Power of Mesh)
Thesis supervisor	Head of degree programme Ari Rantala

Abstract

Mesh network is based on the wireless Mesh standard of the open source code 802.11s which is still under development. At the moment the wireless Mesh network is not yet a standardized network model solution. The data transfer method that Mesh uses is similar to an ad hoc cell network where WLAN is working without a base station. In these kinds of systems all the networks devices communicate with each other without any wired local devices or local network monitoring.

The data security issues of the Mesh network are still without a solution because of their complexity. The objective of thesis is to examine different alternatives to solve these problems. The solutions defined in thesis are based on the implementation described in the 802.11s draft.

Demola organized this project and it was carried out in a group of four. The objective of the project was to create a functional software to control the Mesh network. The software was ordered by Nokia Research Center. The project was coordinated by Ville Kairamo from Demola and supervised by Mika Kasslin from Nokia.

Alkusanat

Tämä työ on tehty Tampereen ammattikorkeakoulun tietoliikennetekniikan suuntautumisvaihtoehdon insinöörityönä.

Työssä selvitän ja kuvailen WLAN mesh-verkkojen rakennetta, ominaisuuksia ja tulevaisuuden mahdollisuuksia. Työn pääpaino on mesh-verkkojen tulevaisuuden turvallisuus- ja tietoturvaratkaisuissa.

Erityisesti haluan kiittää projektin kanssani toteuttaneita kanssaopiskelijoita ja kiitokset kaikille muillekin projektiin osallistuneille. Kiitokset Tampereen ammattikorkeakoulussa minua opettaneille opettajille ja muullekin henkilökunnalle. Suurkiitokset myös Demolan väelle ja tietysti projektin toimeksi antajalle Nokia Research Centerille ja sen edustajille.

Tämä työ on julkinen.

Tampereella 26.10.2010

Tuomas Kuisma

Sisällys

Käytetyt lyhenteet ja merkinnät

AAA	*Authentication* (Todentaminen ja autentikointi), *Authorization* (valtuutus) *and Accounting* (tilastointi). AAA-protokollalla kyetään tunnistamaan verkossa toimiva toinen osapuoli.
AES	*Advanced Encryption Standard.* Työn kirjoitus hetkellä murtamaton lohkosalausmenetelmä.
CBC-MAC	*Cipher Block Chaining Message Authentication Code.* Ks. CCMP.
CCK	*Complement Code Keying.* Matemaattisesti koodisanoilla suojattu tiedonsiirtotapa.
CCMP	*Counter-Mode with CBC-MAC Protocol.* Tulevaisuuden salausprotokolla langattomiin lähiverkkoihin.
CTR	*Counter Mode.* Ks. CCMP.
GTK	*Group Temporal Key.* Ryhmäavain.
GTKSA	*Mesh Group Temporal Key Secure Associatio.* Ryhmien käyttämä kättelyprotokolla.
EAP	*Extensible Authentication Protocol.* Käyttäjien tunnistusprotokolla.
EAPoL	*EAP encapsulation over LANs.* Paketointitekniikka, jolla 802.1X protokollan viestit kuljetetaan.
FT	*Fast BSS transition.* 802.11r on standardi yhteyden ylläpitoon liikkeessä oleville langattomille verkoille.
IEEE	*The Institute of Electrical and Electronics Engineers.* Standardeja kehittävä tekniikan alan järjestö.
MBSS	*Mesh Basic Service Set.* Mesh-asemien muodostama mesh-verkko.
Mesh STA	*Mesh Station.* Mesh-asema on mesh-verkon käyttäjäosapuoli.

MIC *Message Integrity Check.* IEEE 802.11i standardin alainen tarkistusalgoritmi.

MIMO *Multiple Input, Multiple Output.* Useamman kuin yhden antennin tietoliikennejärjestelmä, missä antennit toimivat niin lähetys- kuin vastaanottosuuntaankin.

OFDM *Orthogonal Frequency-Division Multiplexing.* DMT-modulointi. Siinä tieto siirretään eri taajuuskanavilla samaanaikaan.

PAE *Port Authentication Entity.* Porttien hallintaan pohjautuva autentikointimenetelmä.

PBCC *Packet Binary Convolutional Coding.* Tehokas tiedonsiirtomenetelmä, mikä sisältää myös virheenkorjauksen.

PMKSA *Pair-wise Master Key Secure Association.* IEEE 802.11s työryhmän määritelmä autentikointiprotokollaksi. Se määrittelee autentikoinnin niin lähetys- kuin vastaanottosuuntaan

PSK *Pre-Shared Key.* Jonkin tunnistusmenetelmän käyttämä esijaettu salaisuus.

QoS *Quality of Service.*

RADIUS *Remote Authentication Dial In User Service.*

SAE *Simultaneous Authentication of Equals.*

TKIP *Temporal Key Integrity Protocol.*

TKSA *Mesh Transient Key Secure Association.*

WAVE *Wireless Access for the Vehicular Environment.*

Wi-Fi *Wireless Local Area Network.*

WLAN *Wireless Local Area Network (Langaton lähiverkko).*

WPA2 *Wi-Fi Protected Access.*

WPP *Wireless Performance Prediction.*

1 Johdanto

Pohjana tälle opinnäytetyölle toimi projekti, joka toteutettiin Demolan (demola.fi) järjestämänä Nokia Research Centerin tilauksena neljän hengen ryhmässä vuonna 2009 kevään ja syksyn välillä. Projektiryhmän kokoontumispaikkana toimi Demolan tilat Tampereella Finlaysonin alueella. Projektissa oli tarkoituksena ideoida, toteuttaa ja testata WLAN mesh-verkkoon helppokäyttöinen sovellusratkaisu, joka selventäisi mesh-verkkojen ongelmia, mahdollisia tulevaisuuden käyttömahdollisuuksia ja ominaisuuksia. Projektin keskeisin toteutus oli lopputuloksena saatu linux-pohjainen ohjelmisto.

Wlan mesh-verkko on standardina vielä keskeneräinen, mutta IEEE:n työryhmä työstää sitä parhaillaan, ja sen on tavoite olla valmiina vuoden 2010 aikana. Standardia on auttanut kehittymään open80211s. Se pohjautuu IEEE:n 802.11s työryhmän luonnokseen. Työryhmä on nimennyt projektin nimellä o11s mesh. O11s mesh on täysin avoimen lähdekoodin linux-pohjainen ratkaisu, joka pyrkii kehittämään mesh-verkkoa eteenpäin.

Mesh-verkot ovat tulevaisuuden verkkoratkaisu. Se tarjoaa toimiessaan käyttäjille helpon ratkaisun verkostoitumisesta ilman erillisiä servereitä tai muita modeemeita. Langattomina mesh-verkot voivat tarjota monipuolisesti liikkuvia ja muokattavissa olevia ratkaisuita lähiverkoille.

Kuten missä tahansa verkossa, myös mesh-verkoissa sen tietoturva muodostaa sen suurimpia haasteita. Maailma on täynnä verkon väärinkäyttäjiä ja omien etujensa ajajia, jotka pyrkivät käyttämään tavallisia kuluttajia hyödykseen kaikin mahdollisin keinoin. Juuri siksi mesh-verkkojen kehityksen kannalta on tärkeää kehittää niiden tietoturva parhaalle mahdolliselle tasolle heti standardin alkutaipaleella.

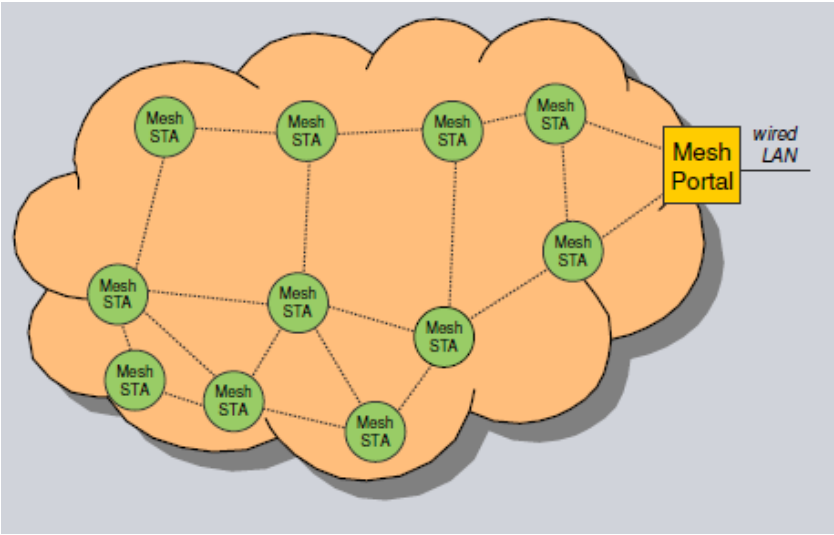
2 Mesh-topologia käsitteenä

Yleisesti mesh-verkolla tarkoitetaan verkkoa, jossa kaikki sen komponentit osat yhdistetty toisiinsa, joko suoraan, tai yhden tai useamman solmupisteen kautta. Mesh-verkkoja on monenlaisia ja ne voivat sisältää monenlaisia osia, joilla jokaisella voi olla oma tehtävänsä mesh-verkossa.

2.1 Mesh-verkko

Mesh-verkolla tarkoitetaan itsenäisesti toimivaa reitittävää verkkoa, jossa ei ole tukiasemia. Normaalisti tässä verkossa ei ole mitään keskitettyä osaa, vaan kaikki verkon osat ovat samanarvoisia. Mesh-verkko voi muodostua kahdesta tai useammasta laitteesta, mesh-asemasta (mesh STA; mesh station), jotka muodostavat fyysisesti täysin mielivaltaisen topologian. Jokainen laite toimii verkossa solmupisteenä ja tiedon reitittäjänä muihin ympärillä oleviin laittesiin. Tällä tavalla verkosta saadaan todella häiriösietoinen, kun mikään solmu ei ole periaatteessa ehdoton verkon muodostumisen suhteen. Kuvassa 1 on havainnollistettu kuvitteellinen mesh-verkko.

Käytännössä, kun halutaan yhteys johonkin toiseen verkkoon tai laitteeseen, tarvitaan mesh-verkkoon jokin sen mahdollistava reitityspiste (Mesh portal). Verkossa saattaa olla myös muita korkeampi käyttäjä, valvoja tai palveluntarjoaja, jolla on oikeudet hallita verkkoa. /2/



Kuva 1. Kuvaus mesh-verkosta. /5/

2.2 Langaton mesh-verkko

Langaton mesh-verkko perustuu samaan topologiaan tavallisen mesh-verkon kanssa ja on täten myös kuvan 1 topologian mukainen. Nimensä mukaisesti kaikki yhteydet on vain toteutettu langattomasti, mutta periaate pysyy samana. Langaton mesh voidaan toteuttaa monilla eri langattomilla tekniikoilla, kuten 802.11 (WLAN) tai 802.16 (langaton laajakaista). /3/

Langattomuus luo verkosta huomattavasti kustannustehokkaamman verrattuna kiinteään verkkoon. Tämä tuo kuitenkin haasteita verkon tehokkuudelle tietysti verkon käyttötarkoitusta mukaillen. Esimerkiksi videon videovirta kuormittaa verkkoa huomattavan paljon. Myös verkon hyvä liikuteltavuus voidaan laskea mesh-verkon hyväksi puoleksi. Jatkuvalle tietoyhdeydelle on tarvetta esimerkiksi mobiilisti liikkuvassa verkossa. Langaton mesh-verkko, joka tarvitsee ylläpitäjältä vain valvontaa ilman tukiasemia tai kaapelointia ja niiden huoltokustannuksia, on varmasti äärimmäisen kustannustehokas, luotettava ja käytännöllinen.

Vertaillaan langatonta mesh-verkkoa tavalliseen langattomaan lähiverkkototeutukseen.

Erot tavalliseen WLAN-verkkoon.

Edut

- tukiasemattomuus eli liikuteltavuus
- häiriösietoisuus
- kustannustehokkuus (ei kaapelointeja tai ylimääräisiä laitehankintoja)
- luotettavuus (yhteys ei ole kiinni yhdestä reitittimestä)

Heikkoudet

- luotettavuus (verkon fyysisen topologian hajotessa runsaasti, saattaa jokin käyttäjä olla vain yhden solmun takana ja tämän jättäessä verkon, myös etäisin käyttäjä tippuu verkosta)
- tehokkuus (siirtonopeus rajoitettu)

- taloudellisuus (laitteiden on jatkuvasti tarkkailtava verkkoa ja tarvittaessa siirrettävä myös itselle kuulumatonta tietoa eteenpäin, joka kuluttaa valtavasti energiaa)

- kehittämättömyys (ei standardoitu, joten vielä paljon kehitettävää: kapasiteetin riitoisuus pitkällä etäisyydellä, helppokäyttöisyysratkaisut, kaistan tarve, pakettilähetyksien virhesietoisuudet, turvallisuusratkaisut, virrankulutus yms.) /6/

Ad hoc-verkko toimii langattomasti käyttäen verkon laitteita reitittiminä, kuten langaton mesh-verkko. Ero näissä kahdessa verkossa piilee niiden verkon toteuttamistavassa. Ad-hoc-verkossa laitteet toimivat yleensä käyttäjältä käyttäjälle tekniikalla, kun taas langaton mesh on sidottu enemmän reitityksen osalta infrastruktuurin eri tapoihin. /4/

2.3 WLAN mesh-verkko 802.11s

802.11s -tekniikka perustuu IEEE:n standardiin WLAN 802.11. 802.11-standardi jakautuu moniin eri alastandardeihin. Jokaista alastandardia kehittää oma työryhmänsä.

2.3.1 802.11 standardit

Virallisen WLAN-standardin IEEE julkaisi heinäkuussa 1997. Tätä ennen työryhmä oli ehtinyt kehitellä kuusi eri versiota tulevasta 802.11-standardista. Nykyään 802.11-standardiin sisältyy useita eri alastandardeja alkuperäisen 802.11 lisäksi. Niistä tällä hetkellä yleisimmät käytössä olevat ovat 802.11b ja 802.11g. 802.11 käyttää toimintaansa radiotietekniikkaa taajuusalueenaan 2,4 – 2,4835 GHz:n vapaa ISM-taajuusalue. /7/

Standardit voidaan jaotella neljään tärkeimpään päästandardiin, ja loput ovat lähinnä lisäominaisuuksia tuovia täydennyksiä näille. Taulukossa 1 kerrotaan tärkeimpien standardien tärkeimpiä ominaisuuksia.

Taulukko 1. Tärkeimpien 802.11-standardien tärkeimmät ominaisuudet

Standardi	Standardoitu	Nopeus (Mbit/s)	Taajuus (GHz)	Laajennus
802.11	1997	1 / 2	2,4-2,4835	-
802.11b	1999	5,5 / 11	2,4	Nopeus sekä CCK-tai PBCC-tekniikan käyttöönotto
802.11a	1999	54	5.150-5.350 / 5.475-5725.0	Toimintataajuus, tekniikaksi OFDM-tekniikka
802.11g	2003	54 / 11	2,4	a:n ja b:n sekoitus, tekniikkana CCK-ODFM
802.11e	2005			Kehitti palvelunlaatua pienentämällä mm. Viiveitä
802.11f	2003-2006			Parantamaan laitteiden yhteensopivuuksia
802.11d	2001		2,4	Tuki eri maiden taajuuskaistojen tunnistamisiin
802.11h	2003		5	5GHz:n taajuusalueen laitteiden toiminnalle
802.11i	2004		2,4	Tietoturva parannuksia; WPA2, AES, autentikointi
802.11n	2009	600	2,4	Nopeus, MIMO-tekniikan tuki
802.11s	7/2010 ?		2,4 / 5	Langaton mesh-tuki

Yllä olevan taulukon lisäksi IEEE:n työryhmä on kehittänyt muitakin päivityksiä 802.11:sta. Vähemmän merkittäviä alastandardeja esitellään taulukossa 2.

Taulukko 2. Vähemmän merkittäviä 802.11 alastandardeja. /8/

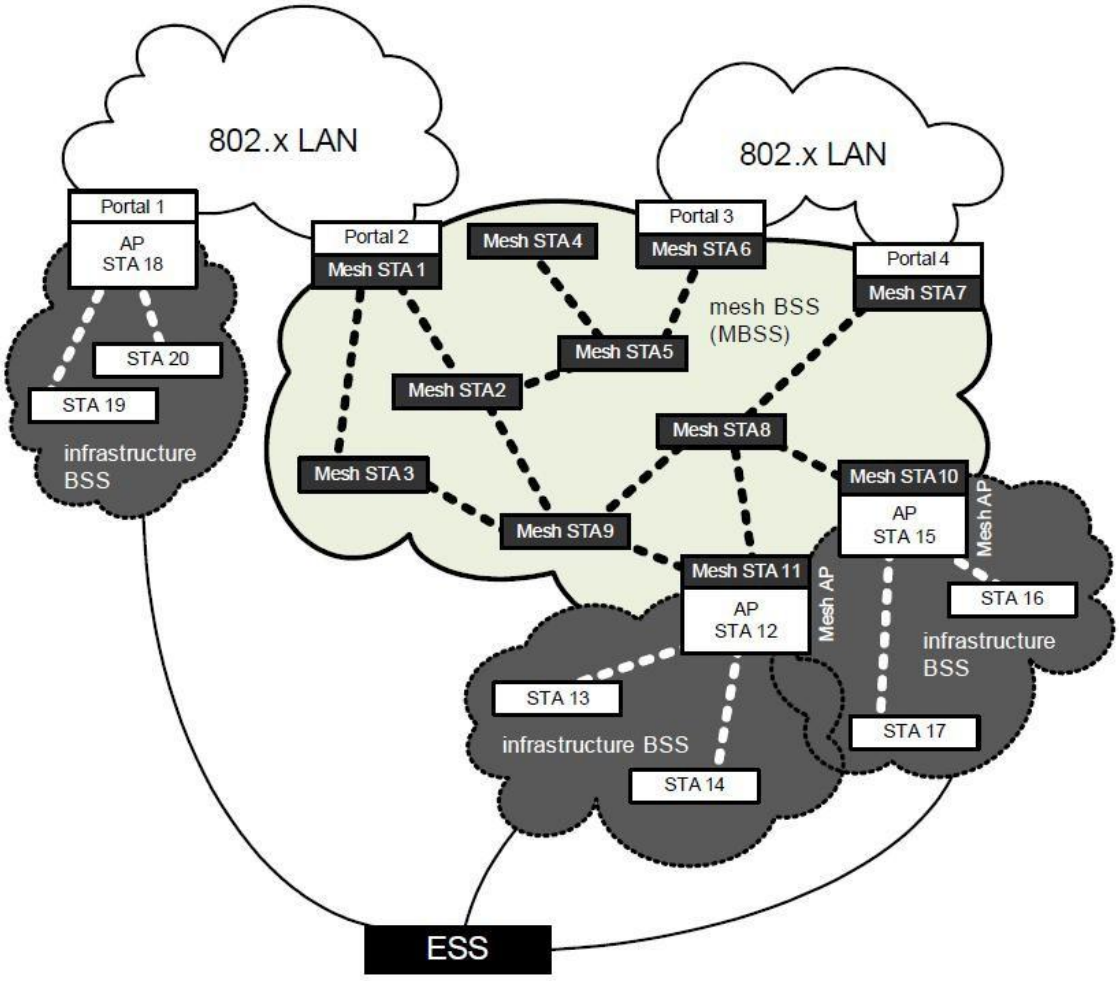
Standardi	Selitys
802.11c	siltaus
802.11d	maasta toiseen siirtyminen
802.11j	laajennus Japania varten
802.11k	radiotien parannus
802.11p	WAVE-tekniikka
802.11r	Nopea ja turvallinen tiedonsiirto
802.11T	Langattoman lähiverkon tarkkaan testaukseen
802.11u	muihin verkkoihin sulautuminen
802.11v	langaton verkon hallinta
802.11w	suojatut hallintakehykset
802.11y	Yhdysvaltojen verkon integraatio
802.11z	DLS-operaation parannus
802.11aa	audio- ja videovirran parannus
802.11mb	standardi ylläpidolle, tulossa 2011
802.11ac	korkean tason suoritusteho <6GHz
802.11ad	korkean tason suoritusteho 60GHz
802.11ae	QoS hallinta
802.11af	TV whitespace

2.3.2 802.11s

Langattoman mesh-verkon pohja rakentuu käyttöasemista eli mesh-asemista. Nämä asemat muodostavat niin kutsutun pilven ja toimivat reitittiminä ja solmupisteinä olete-tussa verkossa. Tätä itsenäisistä mesh-asemista muodostuvaa verkkoa kutsutaan

MBSS:ksi (Mesh Basic Service Set). Esimerkki langattomasta mesh-verkosta on kuvassa 2. Jonkin muun infrastruktuuriverkon yhdistämiseksi MBSS:tiin voidaan jokin mesh-asema konfiguroida toimimaan yhdistävänä käytävänä tässä välissä, mesh AP:na (mesh access point). Tällöin mesh-asema toimii samanaikaisesti mesh-verkon työasemana ja samalla reitittävänä solmupisteenä toisen verkon työasemille (STA). /9/

MBSS voidaan myös yhdistää johonkin muuhun 802.x -verkkoon. Silloin joku mesh-asema määrätään toimimaan portaalina verkkojen välissä. Yhdistämisen jälkeenkin kuitenkin vain mesh-asemat voivat toimittaa mesh-verkon tehtäviä, kuten esimerkiksi reitittää tietoa./9/



Kuva 2. Mesh-verkon topologia /9/

3 Mesh-verkon tietoturva

Mesh-verkon tietoturvan tavoitteet.

1. Verkon luvattoman käytön estäminen.
2. Tietosuojan määrittäminen.
3. Palvelun häirinnän estäminen.

Työtä tehdessä langattoman mesh-verkon tietoturvaratkaisut olivat vielä ratkaisematta. Tässä osuudessa esitetyt tietoturvaratkaisut pohjautuvat siten saatavilla olevaan alan kirjallisuuteen ja IEEE 802.11s työryhmän suunnitelmaan mahdollisista ratkaisuista. Mitään käytännön kokeiltua ratkaisua ei siis ollut olemassa.

3.1 Tietoturvauhat

Mesh-verkon topologiasta johtuen aran tiedon liikuttelu varsinkin julkisessa verkossa on varsin turvatonta. Uhkia ja hyökkäyksiä verkkoa ja sen käyttäjiä kohtaan voi olla monenlaisia. Ne voidaan jaotella passiivisiin ja aktiivisiin. Motiivit tietourkinnoille voivat olla erilaisia. Väärinkäyttäjä voi näin pyrkiä keräämään verkosta tietoa käyttäjistä, päätelaitteista ja käytetyistä protokollista.

Liikenteen salakuuntelu on yksi passiivinen uhka. Salakuuntelulla pyritään seuraamaan liikkuvaa dataa muiden käyttäjien sitä huomaamatta. Näin saadaan mahdollisesti urkittua esimerkiksi taloudellista hyötyä antavaa tietoa. Kohdennettu salakuuntelu on langattomassa mesh-verkkossa tavallista helpompaa. Mesh-verkossa tieto etsii parhaan mahdollisen reitin liikkuessaan määränpäähänsä. Jos maantietteellisesti tiedetään lähtöpaikka ja kohdepaikka, on tähän välille salakuuntelupaikan saaminen äärimmäisen helppoa tarjoamalla liikkuvalla datalle paras mahdollinen reitti. Tällöin data kulkee automaattisesti salakuuntelupaikkana toimivan päätelaitteen kautta. Tämän vuoksi liikuteltava tieto onkin syytä olla salattu mahdollisimman hyvin. Samalla täytyy kuitenkin muistaa, että langattoman mesh-verkon kapasiteetti on rajattua. Tieto on siis syytä suojata vain sen arvon verran, jolloin ei turhaan kuormiteta verkkoa ylimääräisellä salauksella ja sen purkamisella.

Käyttämällä laitonta liikenneanalyysiä väärinkäyttäjä tutkii datasta sen ominaisuuksia, kuten viestin pituutta, lähettäjän ja vastaanottajan osoitetta, lähetysaikaa, viestien tiheyttä ja viesteihin reagoitia sekä muutoksia viestinnässä; ei niinkään viestin sisältöä. Passiivisia hyökkäyksiä on sen vuoksi melko vaikea havaita.

Passiivisista toimista verkkoa vastaan aktiiviset toimet eroavat siten, että ne muuttavat dataa jollakin tavalla tai lisäävät jotain siihen kuulumatonta. Tällaisia aktiivisia tietoturvauhkia on esimerkiksi luvaton tietokantojen selailu, jolloin väärinkäyttäjä etsii verkossa olevia tietoturva-aukkoja tai pyrkii saamaan käyttäjän reagoimaan toimintaansa jotenkin häiritsemällä verkon toimintaa.

Identiteettihuijaus tapahtuu silloin, kun väärinkäyttäjä kertoo olevansa jotain mitä ei ole. Väärinkäyttäjä voi tällä tavalla huijata itselleen verkon todennustietoja ja käyttää niitä myöhemmin lisätäkseen oikeuksiaan verkossa.

Hyökkääjä saattaa myös pyrkiä muuttamaan tai tuhoamaan dataa tai muuten estämään hyödyllistä verkkoliikennettä. Tätä kutsutaan tietosisällön manipuloimiseksi.

Aktiivisista uhista nykyaikaisin on palvelunestohyökkäykset. Sillä verkon muita käyttäjiä estetään käyttämästä sitä esimerkiksi kuormittamalla verkkoa niin paljon, että tavalliset käyttäjät estyvät sen käytöltä. /1/

Merkittävin uhka on kuitenkin käyttäjä itse. Käyttäjän huolimattomuus ja tietämättömyys maksaa vuosittain miljoonia euroja, korvaamattomia tunteja ja satoja gigoja tietoa. Kovin moni ei vain viitsimättömyyttään ota selvää käyttölaitteensa tietoturvatasosta ja päivitä sitä ajantasalle.

Myös jatkuvasti lisääntyvät julkiset ohjelmat ja kehittyvät multimedialaitteet keräävät varmasti väärinkäyttäjiä puoleensa, jolloin käyttäjien pitää ymmärtää suojautua entistä paremmin ajantasalla olevin keinoin. Varsinkin älypuhelimiin kohdistuvat uhat kasvavat jatkuvasti suurenemissa määrin.

3.2 Mesh-verkon luvattoman käytön estäminen

Mesh-verkon käyttöön liittyy paljon sellaisia riskejä ja ongelmia, mitä ei tavallisessa lähiverkossa tai langattomassa lähiverkossa esiinny. Mesh-verkon käyttöä on siis tavallista tärkeämpää valvoa huolellisesti.

3.2.1 Käytön valvonta

Normaali mesh-verkko tarjoaa täysin avoimen käyttöratkaisun. Siinä jokainen käyttäjä on tasavertainen ja ottaa vastaan sekä reitittää jollekin muulle tarkoittua tietoa. Tällainen verkko on hyvin toimiva, varsinkin silloin, kun verkko voi jatkuvasti kasvaa uusilla käyttäjillä.

Tällöin ongelmaksi muodostuvat haittakäyttäjät. Haittakäyttäjä saattaa aiheuttaa verkkoon esimerkiksi tarpeettoman suurta kuormitusta (palvelunesto) ja täten estää muun liikenteen tai pahimmassa tapauksessa aiheuttaa koko verkon kaatumisen. Tällaisia tilanteita varten on verkossa hyvä olla olemassa yksi tai useampia käyttäjiä, joilla on muita suuremmat käyttöoikeudet. Useamman verkonvalvojan tilanteessa saatettaisiin päästä tilanteeseen, missä ainakin yksi olisi aina paikalla valvomassa verkkoa, jolloin uhkatilanteet voidaan pyrkiä havaitsemaan ja torjumaan mahdollisimman nopeasti.

Periaatteessa mesh-verkon käyttö voidaan jakaa kolmeen eri tapaukseen:

1. Avoin käyttö – Avoimessa käytössä jokainen mesh-asema saa samat oikeudet. Tällöin verkkoon liittyminen on helppoa ja suorituskyky verkossa ilman haittatekijöitä hyvä. Tämä kuitenkin aiheuttaa sen, että verkossa ei voida liikutella kovinkaan arkaa tietoa ilman salauksia. Verkon täytyy myös olla hyvinkin vastustuskykyinen palvelunestohyökkäyksille.

2. Autentisoitu käyttö – Tällöin pääsy verkkoon sallitaan vain ennalta määrätyn avaimen avulla. Autentisoinnin yhteydessä voidaan tällöin todentaa verkkoon pyrkijä sallituksi käyttäjäksi. Verkon käyttäjien autentisointi parantaa jo huomattavasti sen turvallisuutta. Toisaalta tällainen verkko ei voi toimia julkisena verkkona ja voidaankin puhua suljetusta verkosta. Lisäksi verkossa täytyy olla ratkaisu avainten kryptaukseen, liikuttamiseen ja todennuksen tapa.

3. Moninkertainen autentisoitu käyttö – Tässä tapauksessa jaossa on useita etukäteen määritettyjä avaimia. Tällöin samaan mesh-verkkoon voi päästä sisään eri avaimilla ja käyttäjien tunnistukset hoidetaan mesh ID:n tai muun vastaavan avulla. Mesh ID on käyttäjän työasemalleen määrittämä nimi. Jokaisella mesh-asemalla pitää olla saman verkon alla eri nimi. Usean eri avaimen salliminen sallii käyttäjän toiminnan useasssa suojatussa verkossa samanaikaisesti, kuten myös reitityksen näiden verkkojen välillä.

Mesh-verkkoon voi olla liittyneenä huomattavan monia erilaisia verkkoja ja sitä myötä kasvaa mahdollisten uhkien määrä huomattavasti. Ulkopuolisista verkoista tulevan uhan huomaaminen ja siihen reagoiminen vie enemmän resursseja kuin, jos hyökkäys tulisi verkon sisältä. Siksi myös mesh-verkon tietoturvaratkaisut on syytä olla yhtä ajan tasalla kuin tavallisenkin lähiverkon.

Itse autentisointi aiheuttaa myös lisäuhan. Sen suojan murtaminen saattaisi olla hyökkääjälle jokseenkin taloudellisesti tuottoisaa. Tällöin hyökkääjä voisi esimerkiksi käyttää haltuun saamaansa käyttäjätiliä hankkiakseen lisäoikeuksia tai hän voi yrittää myydä haltuun saamiaan tietoja.

3.2.2 Mesh PMKSA

PMKSA (Mesh Pair-wise Master Key Secure Association) on IEEE 802.11s työryhmän määritelmä autentikointiprotokollaksi. Se määrittelee autentikoinnin niin lähetys- kuin vastaanottosuuntaan. Mesh-verkoissa autentikointi voidaan suorittaa, joko jaotellusti eri käyttäjille tai sitten keskitetysti koko verkolle. Autentikointi suoritetaan kuitenkin aina täsmälähetyksenä (unicast).

Kun protokolla on onnistuneesti suorittanut osapuolten tunnistamisen, voidaan mesh PMKSA suorittaa. Mesh-asema käyttää sille määriteltyä PMKSA:ia niin kauan kuin se on verkossa. Mesh PMKSA:a käytetään todentamaan yhteys mesh TKSA:lle. /9/

3.2.3 Mesh TKSA ja GTKSA

TKSA (Mesh Transient Key Secure Association) on väliaikainen kättelyprotokolla. Se on myös kaksisuuntainen. Sen elinikä on määritelty.

GTKSA (Mesh Group Temporal Key Secure Association) on täydennetty kättelyprotokolla tai ryhmäavain kättelyprotokolla. Se on määritelty yksisuuntaiseksi. Ryhmäavaimen käyttö tapahtuu aina yleislähetyksenä (broadcast) tai ryhmälähetyksenä (multicast).

Mesh-verkossa jokainen mesh-asema määrittää oman lähetys-GTKSA:nsa sen jälkeen, kun mesh GTK (Group Temporal Key) on vaihdettu ja lähetetty verkon jokaiselle jäsenelle. GTKSA:ta käytetään enkryptaamaan ryhmitellyt lähetysosoitteet ja varastoimaan erilliset vastaanotto-GTKSA:t erikseen jokaiselle mesh-asemalle.

Vastaanotto-GTKSA luodaan sen jälkeen, kun TKSA on suoritettu onnistuneesti. Samaa vastaanotto-GTKSA:ta käytetään niin pitkään kuin sen eliniäksi on määritetty tai uusi vastaanotto-GTKSA luodaan samasta osoitteesta. /9/

3.3 Mesh-verkon tietosuoja

Mesh-verkon tietosuojan hoitaminen on vähintäänkin yhtä tärkeää kuin sen valvonnan hoitaminen. Suuremmat riskit

3.3.1 Tietosuojan määrittäminen

Tietosuojan pitäminen mesh-verkkojen tapaisessa verkossa vaatii paljon niin käyttäjiltä kuin tekniikalta. Ideaalinen tapaus olisi tietysti se, että kaikki mahdollinen liikenne ja kaikki solmut olisivat mahdollisimman hyvin turvattuja. Salasanat pitäisi olla murtamattomia ja ennustamattomia, liikkuva data pitäisi suojata manipuloinnilta ja muutoksilta, käyttäjien tiedot täytyy olla suojassa ja kaikki käyttäjät tunnistettavissa juuri siksi, mitä he oikeasti ovat. Käytännössä tämä on kuitenkin hyvin vaikea toteuttaa.

3.3.2 Salaustekniikat

Tuleva wlan mesh 802.11s turvallisuusprotokolla perustuu paljon IEEE:n toisen standardin 802.11i:n päälle. 802.11i eli WPA2 (Wi-fi Protected Access) on suunniteltu toimimaan kaikkien IEEE:n standardoimien langattomien lähiverkkotekniikoiden kanssa. Se on kehitetty sitä edellisestä tekniikasta, WPA:sta. WPA2 sisältää luonnollisesti samat ominaisuudet kuin WPA, lisäksi siihen on merkittävimpänä ominaisuutena lisätty uusi salausmenetelmä AES (Advanced Encryption Standard). AES on vielä toistaiseksi murtamaton lohkosalausmenetelmä.

WPA2 sisältää yksittäisistä tekniikoista seuraavia: TKIP (Temporal Key Integrity Protocol), PSK (Pre-Shared Key), CCMP (Counter-Mode/CBC-MAC Protocol), EAP (Extensible Authentication Protocol) ja EAPoL (EAP encapsulation over LANs).

WPA on kehitetty Wired Equivalent Privacy (WEP) pohjalta parantamaan sen heikkouksia. WEP oli IEEE:n ensimmäinen langattoman lähiverkon suojaukseen tarkoitettu salaustekniikka. WPA perusti paremman turvallisuutensa lähinnä TKIP:aan, joka on sittemmin murrettu. WPA2 käyttää kehittyneempää ja vahvempaa salausta CCMP:aa TKIP:n sijaan. WPA:iin sisältyy myös pakettien tarkistustoiminto MIC (message Integrity Check). Se tarkastaa kaikki vastaanotetut paketit siten, että kukaan ei ole voinut muokata niitä matkan varrella. Jos jotain muutoksia havaitaan, määrää MIC kaikki verkon käyttäjät autentikoitavaksi uudelleen. Tällä voidaan myös estää niin kutsutut toistohyökkäykset. Viestien siirto todennetaan nelinkertaisella kättelyllä. /11/

TKIP on langattomien lähiverkkojen salausprotokolla. Salausprotokolla muodostaa ja asentaa salausavaimet käyttäjälle. Se käyttää suojaamiseen staattista 128-bittistä pakettikohtaista salausavainta. Avainten dynaamisuus poistaa WEP:lle ominaisen heikkouden, avainten ennustettavuuden. TKIP:n heikkous on avainvirran palautumisesta aiheutuvat hyökkäykset.

Jotta WPA2 olisi turvallisempi kuin edeltäjänsä, vältetään TKIP:n käyttöä ja sen sijaan käytetään CCMP:aa. Se käyttää salausalgoritminään vielä murtatonta AESia. AES on symmetrinen lohkosalausalgoritmi, jonka salaus on 128-bittinen. Sen avaimet voivat olla 128, 196 tai 256 bittisiä, riippuen salaustason tarpeesta. Kun AES käytetään CCMP:n kanssa, se toimii CCM-tilassa. CCM-tilassa käytetään avainten salaukseen

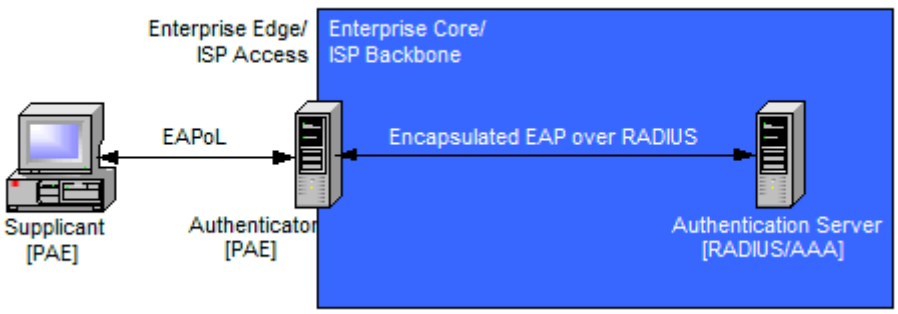
CTR:a (Counter Mode) ja niiden eheydentarkistamiseen CBC-MAC:a (Cipher Block Chaining Message Authentication Code). CTR käyttää satunnaisia lukuja (laskuri), jotka muuttuvat jokaisen salatun tekstiryhmän jälkeen. Laskuri on kryptattu ja tuloksesta otettu XOR-operaatio salakirjoituksella. Niin kauan kuin laskuri jatkaa tekstiryhmien muuttamista, ei ole mahdollista ennustaa tulevaa salakirjoitusta. CBC-MAC:n jokainen tieto-osio on salattu jatkuvalla XOR-operaatiolla. /12/

EAP on tunnistuskehys käyttäjän ja laitteen välille. Se ei itsessään ole tunnistusmenetelmä, vaan sen pohjalta on kehitetty 40 erilaista tunnistustapaa, joilla on yhteisiä ominaisuuksia. EAP:lle voidaan määritellä kolme tärkeää komponenttia tai ominaisuutta:

1. asiakas.
2. tukiasema.
3. autentikointiserveri.

EAPoL on paketointitekniikka, jolla EAP-viestit kuljetetaan. Se on EAP:n kaltainen ja suunniteltu toimimaan kaikkien 802.1x perheen LANien kanssa. Siinä on samat kolme komponenttia, mitkä löytyvät myös EAP:sta. EAPolin komponenttien toimintalogiikka on esitelty kuvassa 3.

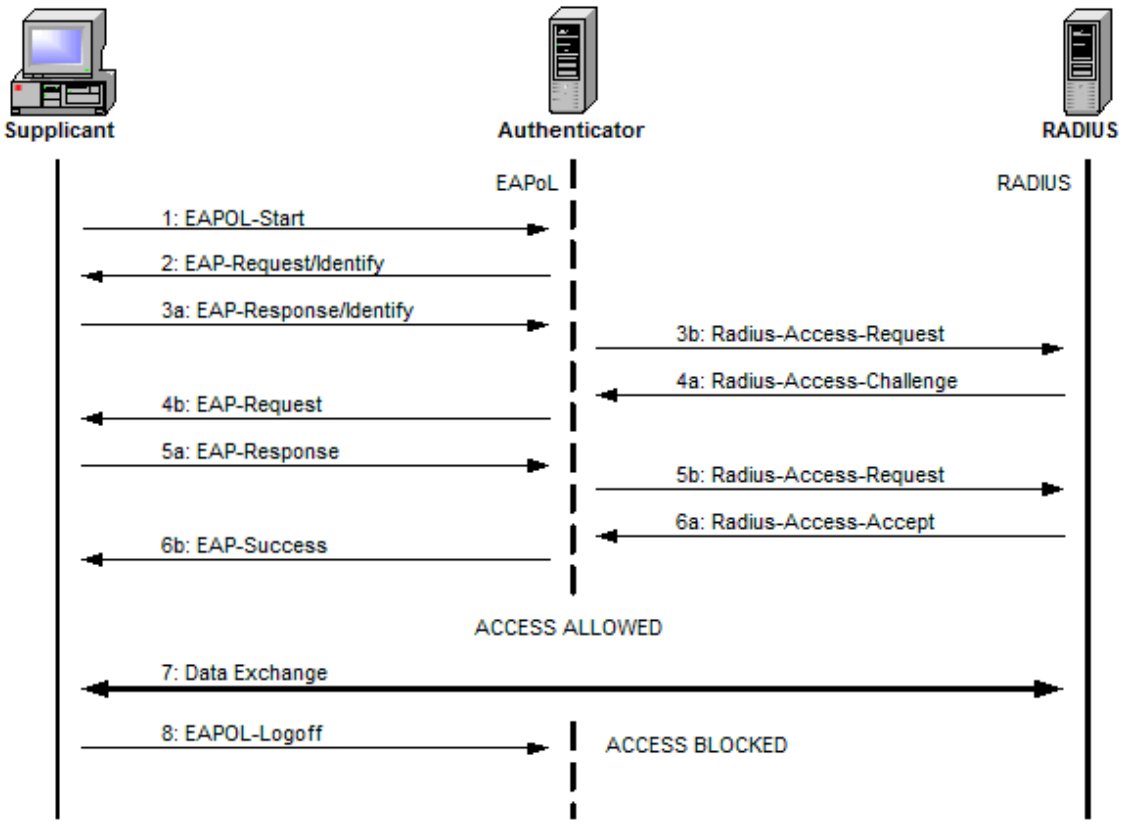
1. asiakas (Supplicant PAE (port Authentication Entity)).
2. autentikoija (Authentication PAE; hallitsee verkkoon pääsyä).
3. autentikointi server (Authentication server)



4. Kuva 3. EAPoLin toiminta. /13/

Autentikointi serveri käyttää RADIUS-protokollaa (Remote Authentication Dial In User Servic) ottaakseen yhteyttä autentikoijaan. RADIUSta tarvitaan, jos halutaan käyttää AAA-palveluita (Authentication, Authorization ja Accounting). AAA-palveluita taas käytetään tunnistamaan toinen osapuoli. Eli asiakas ottaa yhteyttä lähiverkkoa kontrolloivaan autentikoijaan, joka tarkistaa RADIUKSEN tietokannasta AAA:n avulla onko käyttäjä luotettava.

Kuvassa 4 kerrotaan miten viestintä toimii käytännössä EAPoLia käytettäessä.



Kuva 4. EAPoLin tiedon kulku /13/

1. asiakas lähettää EAPoLin käynnistysviestin
2. autentikoija lähettää EAP-tunnistautumiskyselyn
3. a. asiakas lähettää EAP-tunnistusviestin takaisin

b. autentikoija lähettää EAP-viestin eteenpäin RADIUS-protokollalle varmistettavaksi

4. a. RADIUS toimittaa oman haastekyselynsä eteenpäin

   b. autentikoija jatkaa edelleen asiakkaalle

5. a. asiakas ratkaisee haasteen ja lähettää vastauksen (tarkistussumma) jälleen EAP:n päällä

   b. autentikoija toimittaa asiakkaan vastauksen RADIUS-palvelimelle

6. a. RADIUS ratkaisee saman haasteen ja vertaa vastausta tietokantaansa, jonka jälkeen tekee päätöksen verkkoon pääsystä

   b. autentikoija välittää tiedon asiakkaalle

7. Yhteyden toimiessa voidaan tehdä tarvittava tiedon siirto

8. Asiakas lähettää EAPoLin lopetus viestin, jolloin yhteys katkaistaan.

Vaihtoehto EAPoLille avainten liikutteluun mesh-verkoissa on juuri mesh-verkoille suunniteltu, salasanalla suojattu avainten siirtotekniikka, SAE (Simultaneous Authentication of Equals). SAE:n käyttämä salakirjoituksella suojattu salasana on hyvin tehokas verkon suojaustapa. Se voidaan luokitella p2p-protokollaksi ja sen ominaisuuksiin kuuluu, että se voidaan lähettää useaan eri kohteeseen yhtäaikaa. Se on siis hyvä vaihtoehto silloin, kun ei voida käyttää keskitetysti haettavaa salausta.

SAE perustuu zero knowledge proof-tekniikkaan ja toimii niin aktiivisia, passiivisia kuin sanakirjahyökkäyksiäkin vastaan. Sanakirjahyökkäykset on suunniteltu nimenomaan salasanojen murtamista varten. Nimensä mukaisesti sillä on laaja tietokanta täynnä erilaisia sanoja, joita se hyökkäyksen aikana kokeilee erikseen.

Zero knowledge proof on tapa jollain toinen osapuoli todentaa toiselle, että jokin väite on tosi. Nimensä mukaisesti se ei paljasta mitään muuta tietoa kuin todenmukaisen vastauksen. Zero knowledge proofilla on kolme todennettavaa tilaa.

1. Täydellisyys; jos tosi, tarkistaja saa tiedon, että todistaja on luotettava
2. Luotettavuus; jos epätosi, epäluotettava todistaja ei pysty vakuuttamaan tarkistajaa sen luotettavuudesta
3. Tietämättömyys; jos tosi, epäluotettava tarkistaja ei saa tietoonsa mitään tärkeää tietoa. /14/

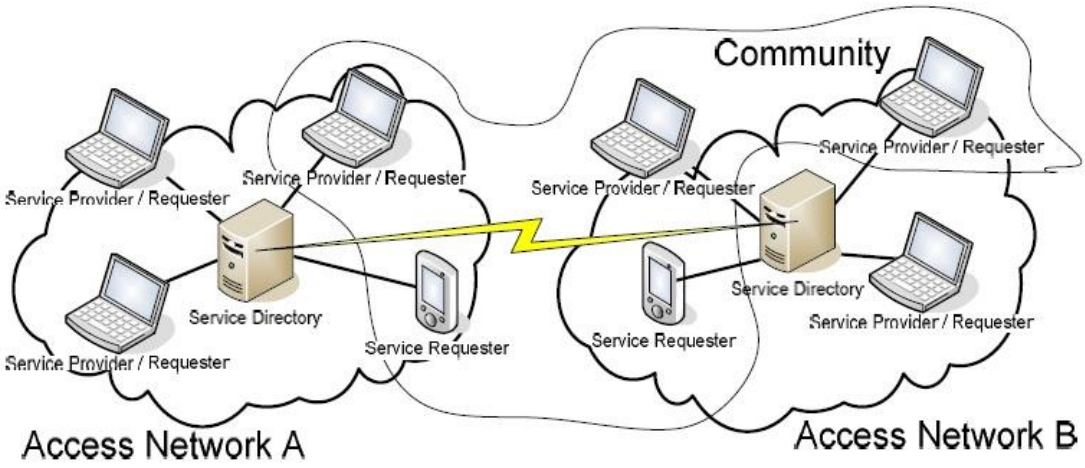
Salasanan ennustettavuus ja sen kirjaston koko, jossa se sijaitsee, määrittelevät paljolti salasanan vahvuuden. Mitä vahvempi salasana on, sitä vaikeampi sitä on ennustaa. Koska SAE on hyvin suojattu sanakirjahyökkäyksiltä, joutuu hyökkääjä tekemään sitä vastaan paljon aktiivisia hyökkäyksiä, jotta se voisi oppia sen. Salasanan vahvuus on siis äärimmäisen merkittävä mesh-verkkojen turvallisuudelle.

Aktiivisten hyökkäyksien toisto on ainoa keino hyökkääjälle pyrkiä oppimaan suojattu salasana. Tämä tarkoittaa, että hyökkääjälle ei ole hyötyä siitä, että se hyökkäisi monia mesh-asemia vastaan yhden sijaan. Tämä myös tarkoittaa sitä, että salasanan jakaminen mesh-verkossa ei heikennä sen tietoturvaa. SAE on siis vahva, suojattu mesh-verkoille ominainen autentikointi protokolla, joka tarjoaa jo heikoillekin salasanoille tehokkaan suojan.

4 Palveluiden suojaaminen

Palvelut mesh-verkkoon toteutetaan service discoveryn avulla. Sen pääasiallinen tehtävä on muodostaa halutut palvelut automaattisesti ja mahdollisimman käyttäjäystävällisesti. Sen täytyy tarjota käyttäjille mahdollisimman hyvät tiedot tarjolla olevista palveluista, mahdollistaa palveluihin liittyminen sekä niiden hallinta.

Palveluiden käyttäminen ja halinta täytyy myös olla mahdollista eri verkkojen välillä. Katso kuva 5.



Kuva 5. Service discovery mesh-verkoissa. /15/

Palveluiden lisääminen verkkoon tuo lisähaasteita tietoturvan hallinnalle. Mesh-verkon topologia ei määritä verkolle fyysisiä ja tai määrällisiä rajoituksia, jolloin myös palveluiden määrä voi nousta lukumäärältään suureksi. Verkkojen integroituessa toisiinsa, syntyy jopa tuhansia, ehkä vieläkin suurempi joukko monenlaisia palveluita. Tähän joukkoon voi tietysti mahtua muille käyttäjille haitallisia palveluita.

Palveluiden suojaaminen tai vaihtoehtoisesti palveluilta suojautuminen on hyvin pitkälti käyttäjän vastuulla. Kun palveluita pitää pystyä tarjoamaan yleisesti julkiseen verkkoon, niiden luotettavuus täytyy olla jotenkin selvitettävissä. Olisi siis luotava jonkinlainen standardi palveluiden tunnistamiseen. Mesh-verkkojen tapauksessa puhutaan vielä monien erilaisten laitteiden kombinaatiosta, joten tunnistusmenetelmien pitää olla yhteensopivia erilaisille käyttöjärjestelmille.

Päätelaitteella käytettävistä sovelluksista vastaa ensi sijassa sen käyttäjä, joten suurin riski on siis tiedossa. Joskus haittaohjelman tai -palvelun tunnistaminen saattaa olla kuitenkin lähes mahdotonta tai ainakin vaikeaa. Tällöin laitteella olevat turvaohjelmistot on syytä olla kunnossa, jolloin ne osaavat varoittaa ja poistaa havaitut ongelmat. Tärkeää on myös, että käytetyt tietoturvaohjelmistot ovat ajan tasalla eli päivitettyinä viimeisimpiin ja tai ainakin lähes viimeisimpiin saatavilla oleviin versioihin.

Mesh-verkossa oleviin sovellus-tason uhkiin täytyy myös vastata sovellustasolta. Sitä ei voida kuitenkaan pitää ainoana tietoturvaratkaisuna vaan torjuminen on yleensä syytä hoitaa jo alemmilla OSI-mallin tasoilla.

5 Yhteenveto ja mesh-verkkojen tulevaisuus

Turvallisuussuunnitelman ja -toimenpiteiden tarkoitus on suojata verkkoa ja käyttäjiä mahdollisilta haittakäyttäjiltä. Sen tehtävä on tarjota käyttäjille mahdollisuus käyttää verkossa luottamuksellista tietoa ilman pelkoa tiedon katoamisesta, urkinnasta tai muuttumisesta. Sen tehtävä on myös tarjota verkolle mahdollisuus muodostaa sinne erilaisia resursseja, palveluita ja tietopankkeja.

Tässä työssä katsastelin mesh-verkkojen tietoturvan tulevaisuutta; mahdollisuuksia tietoturvan erilaisille ratkaisuille ja jo kehitettyjä menetelmiä. Kävin ratkaisuja läpi niin ideallisesti kuin teknisestikin.

Mesh-verkkojen tulevaisuus lienee siihen integroitavissa palveluissa ja niiden helppokäyttöisyydessä. Erilaisia tietoliikenne verkkoja on lukuisia ja niissä on lukuisia erilaisia käyttäjiä. Verrattaessa tämän hetken sukupolvia verkkojen käyttäjinä, uudet sukupolvet ovat teknisesti taidokkaampia kuin vanhat. Tästä huolimatta vain murto-osa kaikista käyttäjistä on halukkaita opettelemaan verkkojen teknisiä saloja ja niiden käyttöä perinpohjaisesti.

On selvästi nähtävissä, että tulevaisuus erilaisissa verkoissa ja palveluissa on niiden käytön toiminnassa, toimivuudessa ja ennen kaikkea käytettävyydessä. Mesh-verkolla on hyvä potentiaali tässä suhteessa. Se ei tarvitse ylimääräisiä laitteita ja niiden välisiä konfiguraatio-ongelmia.

Lähteet

1 Penttinen, Jyrki 2006. Tietoliikennetekniikka – 3G ja erityisverkot. Helsinki: WSOY.

2 Wikipedia [www-sivu] Mesh networking [viitattu 26.5.2010] Saatavissa:

http://en.wikipedia.org/wiki/Mesh_networking

3 Wikipedia [www-sivu] Wireless mesh [viitattu 26.5.2010] Saatavissa: http://fi.wikipedia.org/wiki/Wireless_mesh

4 Wiki answers [www-sivu] What is the difference between wireless mesh networks and mobile ad hoc networks [viitattu 26.5.2010] Saatavissa: http://wiki.answers.com/Q/What_is_the_difference_between_wireless_mesh_networks_and_mobile_ad_hoc_networks

5 Siemens [powerpoint] Overview and status of IEEE 802.11s [viitattu 26.5.2010] Saatavissa: http://www.ict-carmen.eu/workshop09/pdf/bahr.pdf

6 Microsoft research [www-sivu] Self Organizing Wireless Mesh Networks [viitattu 27.5.2010] Saatavissa: http://research.microsoft.com/en-us/projects/mesh/

7 Werebuild wiki [www-sivu] Mesh networking [viitattu 27.5.2010] Saatavissa: http://werebuild.eu/wiki/index.php?title=Mesh_networking

8 Wikipedia [www-sivu] IEEE 802.11 [viitattu 27.5.2010] Saatavissa: http://en.wikipedia.org/wiki/IEEE_802.11

9 IEEE 802.11s Draft [PDF dokumentti] IEEE P802.11s/D3.0 March 2009 [viitattu 3.6.2010]

10 Wikipedia [www-sivu] Wi-Fi protected access [viitattu 1.6.2010] Saatavissa: http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

11 Wikipedia [www-sivu] Langattoman lähiverkon tietoturva [viitattu 1.6.2010] Saatavissa: http://fi.wikipedia.org/wiki/Langattoman_l%C3%A4hiverkon_tietoturva

12 Techweb [www-sivu] Counter mode [viitattu 2.6.2010] Saatavissa: http://www.techweb.com/encyclopedia?term=counter%20mode

13 Vocal [www-sivu] EAPoL [viitattu 2.6.2010] Saatavissa: http://www.vocal.com/security/eapol.html

14 Wikipedia [www-sivu] Zero knowledge proof [viitattu 3.6.2010] Saatavissa: http://en.wikipedia.org/wiki/Zero_knowledge_proof

15 CiteSeerX [PDF dokumentti] Service discovery in wireless mesh networks: a survay on candinate solutions [viitattu 3.6.2010] Saatavissa:

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.2979&rep=rep1&type=pdf

Liitteet

Liite 1: Mesh control panel - lähdekoodi