Tietoturva langattomissa verkoissa

Anekdootti

Tapio Väättänen
21.04.2005

Tiivistelmä

Tässä tutkimuksessa on tutkittu kattavasti langattomien verkkojen tietoturvaa. Tutkimuksen välineinä on käytetty kannettavaa tietokonetta, johon on liitetty useampi langaton PC-kortti. Käytettyjen WLAN-korttien ajurit on päivitetty versioihin, jotka mahdollistavat ns. monitor- ja scanning-moodit kattavaan tulokseen pääsemiseksi.

Ohjelmistoina on käytetty julkisesti saatavilla olevia työkaluja. Metodeina on käytetty passiivista langattoman verkon kuuntelua sekä aktiivista pakotettua hyökkäystä, jossa datana on käytetty passiivisessa kuuntelussa kerättyä dataa. Tutkimuksen tarkoituksena ei ole ollut murtaa tai käyttää hyväksi tutkimuksessa havaittuja verkkoja, ainoastaan selvittää, kuinka moni verkoista olisi ollut murrettavissa niin sanotulla heittometodilla [1].

Sisältö

1 Johdanto

Langattomien verkkojen tietoturva on niiden yleistyessä arveluttanut suurta määrää käyttäjäkunnasta. Yleisin tällä hetkellä käytössä oleva salausmuoto on WEP-salaus eri implementaatioineen. WEP-salauksen ongelmakohtia on pyritty korjaamaan WPA-implementaatiossa. Osassa langattomia verkkoja ei käytetä salausta lainkaan, tai laitteisto on otettu käyttöön tehdasasetuksilla, jotka ovat yleisesti tiedossa. Tämän tutkimuksen tarkoituksena on selvittää näiden kolmen eri tilanteen prosentuaalista esiintymistä pääkaupunkiseudulla.

Ohjemistoiksi on valittu Airsnort [2], Kismet [3] sekä Aircrack [4]

2 Selostus mittauksista

Mittaukset suoritettiin viikon aikana harjoittamalla ns. "wardrivingia". Yksinkertaistettuna havaitsija ajoi ympäri pääkaupunkiseutua ja keräsi passiivisesti dataa kannettavalla tietokoneellaan.

Kerätty data analysoitiin jälkikäteen ja sen perusteella tehtiin seuraavassa kappaleessa esitetyt johtopäätökset.

3 Mittaustulokset

Prosentuaaliset osuudet:

- WEP 128bit 48%
- WPA 34%
- Avoimet verkot sekä verkot tehdasasetuksilla 18%

Tutkimuksessa ei löydetty verkkoja, jotka olisivat olleet murrettavissa "heittämällä". Pääkaupunkiseudun langattomat verkot ovat tämän tutkimuksen perusteella tietoturvaltaan erinomaisessa kunnossa. Pohjois-Amerikassa on mm. Markus Janssonin toimesta suoritettu lukuisia tutkimuksia [5], joita paikalliset alan lehdet ovat sankoin joukoin julkaisseet. Näissä tutkimuksissa langattomat verkot ovat olleet jopa yli 90 prosenttisesti murrettavissa niin sanotulla heittometodilla [1]. Kotoisen pääkaupunkiseutumme verkot ovat sitä vastoin pääosin janssoninkestäviä [6].

Tutkimuksessa ei tutkittu täysin avoimien verkkojen, eli ns. "hot-spotien"tarkoituksellisuutta. Osa näistä verkoista on tarkoituksella kaikkien käytettävissä, osa tarkoituksetta ja osa käyttää suojauksenaan jotain muuta tapaa kuin langattomaan verkkoon suoraan integroidut suojaustavat.

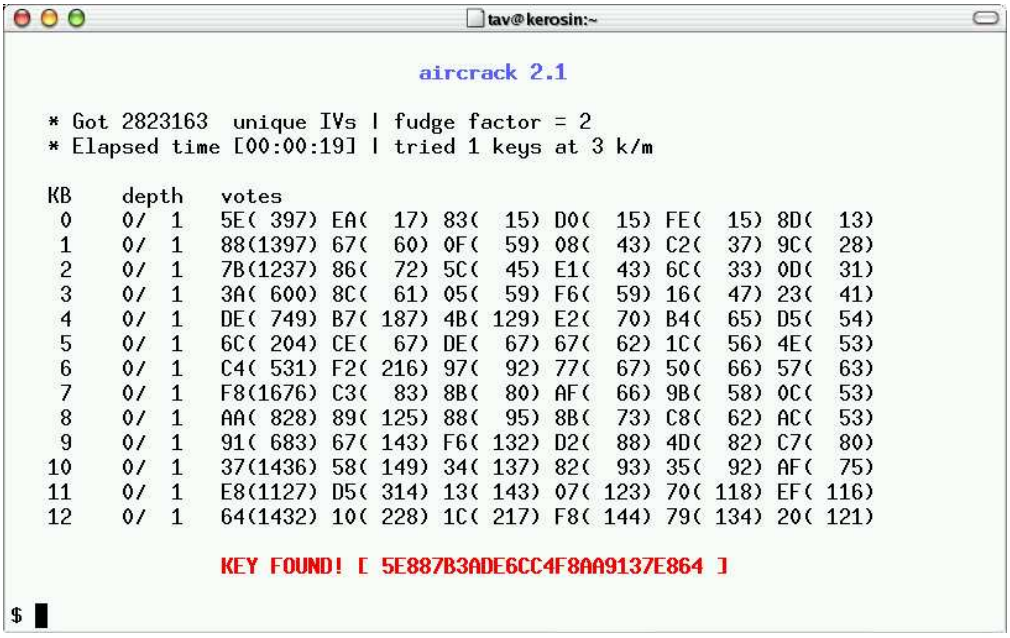
4 Loppusanat

Langattomien verkkojen käytetyin salausmuoto on tämän tutkimuksen tulosten perusteella 128bit WEP, jonka heikkoudet on ollut tiedossa pitkään. Tein pikaisen testin oman langattoman verkkoni, joka käyttää salaukseen 128bit WEPiä, turvallisuudesta. Monitoroidessani omaa langatonta verkkoani kykenen normaalioloissa keräämään kryptattua dataa vauhdilla, joka on noin viisi pakettia sekunnissa. Testiä varten liikuttelin 254MB kokoista tiedostoa koneelta toiselle. Näin kryptattua dataa oli mahdollista kerätä keskimäärin 500 pakettia sekunnissa. Kytkin langattomaan verkkoon kaksi kannettavaa konetta. Toisella koneella monitoroitiin ja kerättiin kryptattua dataa. Toisella generoitiin liikennettä mainittua suuri kokoista tiedostoa edestakaisin koneelta toiselle langattoman verkon yli siirtelemällä.

Monitoroiva kone oli niin ikään kytketty toisen langattoman verkkokortin, jolla siis ei suoritettu itse monitorointia, avulla testin kohteena olevaan langattomaan verkkoon. Tämän generoimaa liikennettä ei kuitenkaan ollut mahdollista kerätä, koska etäisyys monitoroivaan korttiin oli liian pieni. Dataa kerättiin kello yhdestätoista illalla kello kuuteen aamulla käyttäen tähän soveltuvaa Kismet-ohjelmistoa

[3]. Vaikkakin Kismet itsessään kykenee murtamaan salausavaimia, tätä ominaisuutta ei käytetty hyväksi. Monitoroidessa keskityttiin monitoroimaan yhtä lukittua kanavaa, jotta muiden kuuluvuusalueella olevien tukiasemien liikenne häiritsisi testiä mahdollisimman vähän. Samalla varmistettiin, että monitoroitavasta tukiasemasta saadaan mahdollisimman tehokkaasti dataa. Data kerättiin seitsemän tunnin aikana ja sitä kertyi lähes 3GB. Dataa olisi kertynyt enemmänkin, mutta monitoroivan koneen kiintolevy kerkesi täyttymään ennenaikaisesti. Kerätty data prosessoitiin Aircrack-ohjelmistolla [4], joka löysi datasta 2823163 yksilöllistä IV-pakettia. Näistä tämä pystyi kuvan 1 mukaisesti selvittämään salausavaimen 19 sekunnissa.

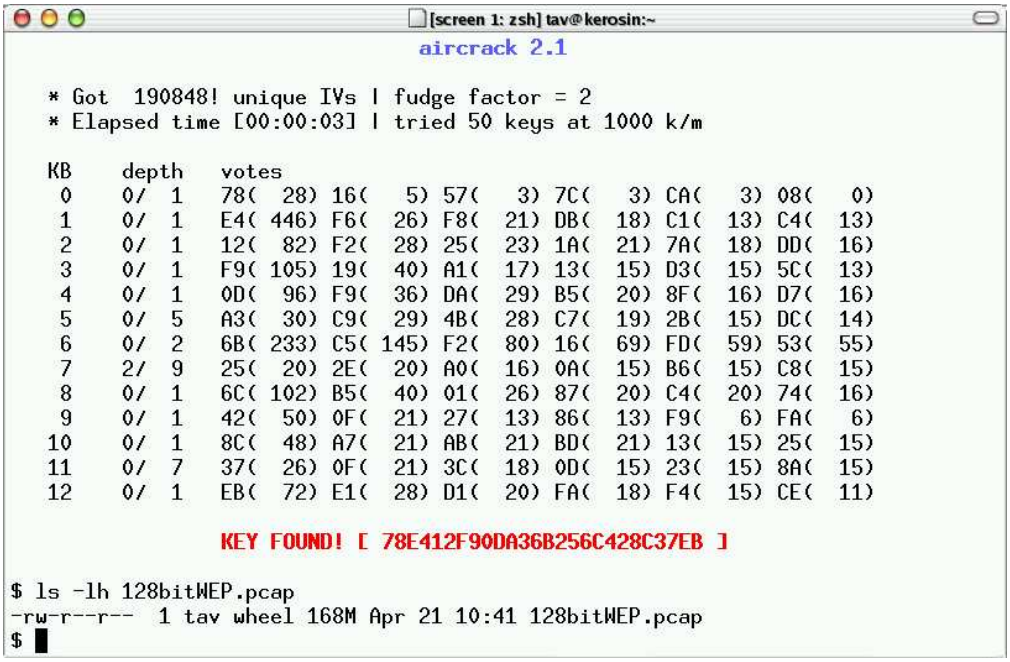
Kuva 1: WEPin murtaminen



Edellä kuvailtu salausavaimen selvitys tehtiin seitsemän tunnin aikana, jona dataa kertyi huomattavasti enemmän, kuin olisi ollut tarpeellista. Toistin kokeen useaan kertaan lyhyemmillä aikajaksoilla sekä 64bit että 128bit WEP:lle. Nopeimmillaan 64bit WEP murtui kolmessa minuutissa 40 sekunnissa. Dataa tuohon tarvittiin 21MB, jossa käyttökelpoisia IV-paketteja 39 930. 128bit murtaminen onnistui nopeimmillaan alta kahden kymmenen minuutin. Tällöin dataa kerättiin 168MB,

jossa oli käyttökelpoisia IV-paketteja 190 848, kuten kuva 2 osoittaa. Toisaalta onnellakin on aina osuutta asiaan. Niinpä murtaminen ei välttämättä onnistu suuremmallakaan datan määrällä ilman niin sanoattua "brute-forcea". Lienee kuitenkin turvallista sanoa, että 64bit WEP murtuu pääsääntöisesti hyvissä olosuhteissa alle kymmenessä minuutissa ja 128bit WEP alle kahdessakymmenessä minuutissa. 128bit WEPin murtamiseen tarvitaan 200k - 500k IV-paketteja. Tuota määrä varten on liikenteestä oltavaa dataa noin 200MB - 500MB. Mitä enemmän liikennettä verkossa on, sitä nopeammin tarvittava data saadaan kerättyä.

Kuva 2: 128bit WEPin nopea murtaminen



Viitteet

[1] Heitto- tai heilahdusmetodi - http://groups-beta.google.com/group/sfnet.atk.turvallisuus.kotikoneet/msg/c8e84900a4bd7f66

[2] Airsnort - http://airsnort.shmoo.com/

[3] Kismet - http://www.kismetwireless.net/

[4] Aircrack - http://www.cr0.net:8040/code/network/

[5] Laajat alan lehdissä julkaistut tutkimukset - http://groups-beta.google.com/group/sfnet.atk.turvallisuus.kotikoneet/msg/94cb0edb9235cbdd

[6] Janssoninkestävä - http://groups-beta.google.com/group/sfnet.atk.turvallisuus.kotikoneet/msg/c4543e2a72ceb58b