Bezpečnost a Hacking WiFi (802.11) - 1. Úvod a príprava

Vložil/a matej [1], 5 Květen, 2009 - 21:47

- Hacking [2]
- Hacking method [3]
- Networks & Protocols [4]
- Security [5]
- WiFi & Wireless [6]

Protokoly a iné prvky zabezpečujúce bezdrôtové siete IEEE 802.11 sú prelomiteľné. Táto práca sa venuje popisu jednotlivých možností zabezpečenia, ktorými sú skrývanie SSID, filtrovanie MAC adries, šifrovanie a autentifikácia pomocou WEP, WPA, WPA2, zabezpečenie na vyšších vrstvách a iné. Ukazuje praktické útoky na tieto bezpečnostné prvky, útoky za účelom zamietnutia služby a možnosti útokov muža v strede. Navrhuje možné opatrenia proti týmto útokom, odporúčania pre používateľa, administrátora, ako aj výrobcov zariadení.

Poďakovanie

Ďakujem Ing. Martinovi Rakúsovi, PhD., vedúcemu diplomovej práce, za odborné vedenie a pomoc pri zabezpečovaní podkladov pre túto prácu, Ing. Rudolfovi Urbanovskému, Odbor štátneho dohľadu Trenčín, Telekomunikačný úrad SR a pracovníkom oddelenia metodického riadenia a podpory štátneho dohľadu, Telekomunikačný úrad SR, za ochotu pri zodpovedaní otázok.

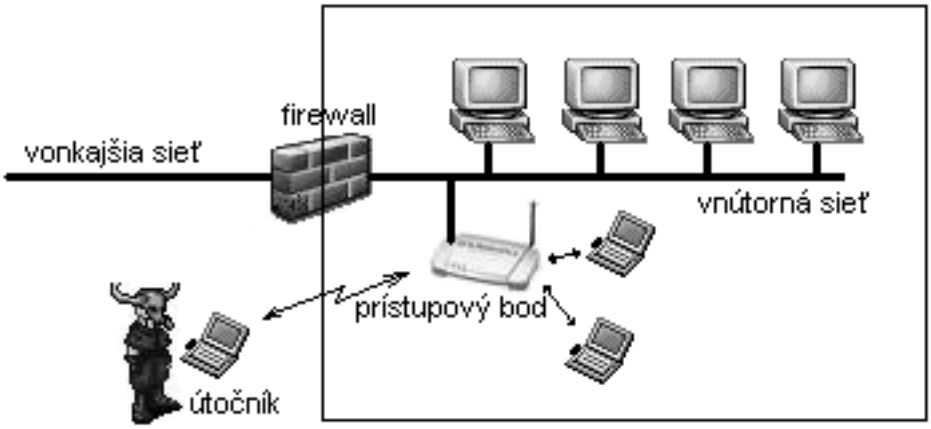
Anotácia

Slovenská technická univerzita v Bratislave
Fakulta elektrotechniky a informatiky
Študijný program: Telekomunikácie
Autor: Bc. Matej Šustr
Diplomový projekt: Analýza bezpečnosti štandardu IEEE 802.11
Vedenie diplomovej práce: Ing. Martin Rakús, PhD.
Dátum: máj 2007

1. Motivácia

Bezdrôtové siete založené na štandarde IEEE 802.11 sú v súčasnosti najpoužívanejšími bezdrôtovými počítačovými sieťami na svete. Vďaka prenositeľnosti, ľahkej inštalácii a dobrým parametrom oneskorenia a prenosovej rýchlosti si nachádzajú uplatnenie v domácnostiach, malých aj veľkých firmách a aj na budovanie prístupovej siete poskytovateľov internetu. Pri takomto rozšírení bezdrôtových sietí je nutné dbať na ich zabezpečenie.

Sieť IEEE 802.11 pracuje na prvej vrstve (fyzickej) a druhej vrstve (nižšia podvrstva MAC, riadenie prístupu na médium) referenčného modelu Open Systems Interconnection. Pri nesprávnom (ale úplne bežnom) a nezabezpečenom zapojení do existujúcej drôtovej siete predstavuje „dieru“ do siete, ktorá môže byť inak pred vonkajšími útokmi zabezpečená, ako napr. na obr. 1-1.



Príklad implementácie, kde bezdrôtová sieť kompromituje (inak zabezpečenú) drôtovú sieť. Táto práca nadväzuje na bakalársku prácu, v ktorej bol štandard IEEE 802.11 a jeho prvotné zabezpečenie WEP popísané všeobecne. Diplomová práca má za cieľ opis a realizáciu rôznych, najmä nových útokov na bezdrôtové siete IEEE 802.11, zabezpečené pomocou štandardizovaných aj proprietárnych prvkov ochrany. Analyzuje možnosti útočníka na prienik, ako aj administrátora alebo používateľa na zabezpečenie siete lepšími, resp. viacerými spôsobmi ochrany.

2. Príprava

Testovanie útokov je možné robiť na reálnych bezdrôtových sieťach, ale kvôli praktickým, etickým a právnym dôvodom bola použitá sieť zostrojená na tento účel. Použité operačné systémy (OS) boli Microsoft Windows 2000 a GNU/Linux distribúcie Slackware (GNU is Not Unix, GNU Nie je Unix) – dôvody sú popísané nižšie v časti 2.3. V nasledujúcom texte sú rámčekoch používané príkazy zadávané do konzoly GNU/Linux alebo iných *nix-ových systémov (hrubým písmom) a ich výstup. Mreža „#“ na začiatku riadku pred príkazom znamená, že je nutné púšťať ho s právami administrátora (root); dolár „$“ pred príkazom znamená, že program je možné púšťať ako bežný používateľ. Mreža za príkazom je vždy poznámka.

2.1 Monitorovací režim (monitor mode)

Pre odchytávanie komunikácie na „drôtových“ LAN (Local Area Network, lokálna sieť) je známe použitie promiskuitného režimu. V ňom sieťová karta umožňuje zachytávanie rámcov, ktorých cieľová MAC (Medium Access Control, riadenie prístupu na médium) adresa je ľubovoľná. V prípade WLAN (Wireless LAN, bezdrôtová LAN) v promiskuitnom režime môžeme po asociovaní sa na sieť zachytávať všetky rámce v danej sieti. Je však nutné najprv byť asociovaný. Navyše veľa ovládačov WLAN kariet ani nepodporuje promiskuitný režim.

V režime monitor, tiež známom ako RFMON (Radio Frequency Monitor, monitorovanie rádiových frekvencií), sieťová karta WLAN zachytáva rámce bez asociovania sa na AP (Access Point, prístupový bod), alebo do ad-hoc (príležitostná, sieť bez AP) siete – pri monitorovaní prevádzky chránenej šifrovaním to znamená, že budú odchytené celé rámce v zašifrovanej forme. Umožňuje „monitorovať“ konkrétny kanál bez toho, aby bol vyslaný akýkoľvek rámec – pri niektorých ovládačoch dokonca ani nie je možné v režime monitor vysielať. Ďalšou vlastnosťou monitorovacieho režimu je to, že karta zachytáva a posúva ďalej aj rámce s nesprávnymi kontrolnými súčtami, takže sa môže stať, že niektoré prijaté rámce budú poškodené.

2.1.1 Zapnutie monitorovacieho režimu

Po zavedení ovládačov, či už automaticky pomocou služieb hotplug (Linux 2.4), udev (Linux 2.6) alebo manuálne pomocou modprobe, sa zariadenie uvedie do režimu monitor jedným z nasledujúcich spôsobov:

```
# iwconfig rausb0 mode monitor # pre Ralink chipsety
# iwpriv eth2 monitor 2 1 # pre Prism chipsety, kanál ?. 1
```

Občas sa stalo, že sieťová karta neprepla režim správne. Vtedy pomohlo asociovanie sa na existujúce AP (ľubovoľné) v režime managed (manažovaný, infraštruktúrny) a následné prepnutie do režimu monitor.

2.1.2 Vysielanie v monitorovacom režime

Niektoré sieťové karty, resp. ich ovládače neumožňujú v režime monitor vysielať žiadne dáta. U niektorých je potrebné možnosť vysielania explicitne zapnúť, obvykle pomocou iwpriv, napríklad:
`# iwpriv rausb0 rfmontx 1`

2.1.3 Prism hlavička

Väčšina nových ovládačov pri použití monitorovacieho režimu pred zachytené rámce vkladá tzv. „Prism“ hlavičku (názov pochádza z Prism chipsetov, ktoré ako prvé podporovali monitorovací režim). Táto obsahuje informácie o sieťovej karte, na ktorej bol rámec zachytený, kanál, silu signálu, modulačnú rýchlosť, apod. Programy musia byť schopné rozoznať túto hlavičku, aby vedeli s rámcom pracovať. Väčšina použitých utilít s týmto problém nemala – či už pri zachytávaní naživo alebo pri čítaní z pcap (packet capture, zachytené pakety) súboru; iba tcpdump treba nastaviť na zachytávanie viac ako 96 bajtov z rámca, aby ho vedel analyzovať. Pre také programy, ktoré nedokážu Prism hlavičku spracovať, je možné ju z pcap súboru odstrániť, napríklad pomocou prism-strip z balíka Airbase tools.
Ďalšou možnosťou je vypnutie vkladania Prism hlavičky, čo niektoré GNU/Linux ovládače umožňujú pomocou programu iwpriv, napríklad:
`# iwpriv ra0 prismhdr 0`

U iných ovládačov je na tento účel možné upraviť ich zdrojový kód.

2.2 Zariadenia

Podľa informácií na stránke http://linux-wless.passys.nl/ [7] boli z dostupných IEEE 802.11b/g sieťových kariet vybrané také, ktoré mali mať Ralink chipset (čipovú sadu). Tento má k dispozícii open-source (s otvoreným zdrojovým kódom) ovládač pre operačný systém GNU/Linux, ktorý umožňuje monitorovací režim.

2.2.1 MSI US54G

Vendor ID/Device ID: 0db0:6861
MAC adresa: 00:11:09:29:62:38
Chipset: Ralink 2500USB
Linux ovládač dostupný z: http://rt2x00.serialmonkey.com/ [8] (rt2570, ver.1.1.0-b2)
Wi-Fi stick pripojiteľný cez USB rozhranie (Universal Serial Bus, univerzálna sériová zbernica), dodávaný s polmetrovým tvrdým predlžovacím káblom. Prekvapením bol veľmi krátky dosah zariadenia, signál prechádzajúci tenkou stenou nebolo možné zachytiť. Po zavedení ovládača rt2570 sa zariadenie identifikuje ako rausb0. Umožňuje aj prenosovú rýchlosť 54 Mbit/s v ad-hoc režime (porušenie 802.11g štandardu) pomocou príkazu `iwpriv rausb0 adhocmode 2`.

2.2.2 ASUS WL-107G

Vendor ID/Device ID: 1814:0201
MAC adresa: 00:17:31:BA:EF:E4
Chipset: Ralink 2500

Linux ovládač dostupný z: http://rt2x00.serialmonkey.com/ [8] (rt2500, ver.1.1.0-b4)
CardBus karta do notebooku. Po zavedení ovládača rt2500 sa identifikuje ako ra0. Vzhľadom na to, že s touto kartou boli najmenšie problémy s prepínaním režimov, bola používaná najmä na odchytávanie.

2.2.3 Micronet SP906GK

Vendor ID/Device ID: 10ec:8185
MAC adresa: 00:11:3B:0B:22:0C
Chipset: Realtek RTL-8185
Linux ovládač dostupný z: http://rtl8180-sa2400.sourceforge.net/ [9] (cez CVS)
PCI karta (Peripheral Component Interconnect, rozhranie na pripájanie periférií), o ktorej sa pôvodne predpokladalo, že bude mať Ralink chipset, ukázalo sa však, že je osadená Realtek-om. Dostupné ovládače pre Linux (rtl8180-sa2400-dev, rtl818x-newstack) po zložitom nakompilovaní a zavedení do jadra (kernel 2.6.18.3) spôsobili totálne zamrznutie systému pri viacerých pokusoch. Preto bola používaná pod OS Windows 2000, s ovládačom NDIS 5.1060.413.2006 (Network Driver Interface Specification, špecifikácia pre ovládače sieťových rozhraní) z inštalačného CD – karta bola teda použitá na simuláciu prevádzky, a nie útoky. Tieto ovládače obsahujú aj možnosť Host-AP (prístupový bod na počítači), to sa však nepodarilo uviesť do funkčného stavu.

2.2.4 Micronet SP917G Access Point

MAC adresa: 00:11:3B:07:00:14
Pre zostavenie infraštruktúrnej siete bolo potrebné použitie AP. Zariadenie podporuje WEP (Wired Equivalent Privacy, dôvernosť ekvivalentná drôtovej sieti – v kapitole 4 ukážeme, že názov je zavádzajúci), WPA (Wi-Fi Protected Access, zabezpečený prístup Wi-Fi) aj WPA2.

2.2.5 Kompatibilita

Všetky zariadenia vedeli spolupracovať v ad-hoc aj infraštruktúrnom zapojení, bez použitia šifrovania a pri použití WEP. Pri snahe o použitie WPA-TKIP (Temporal Key Integrity Protocol, protokol s integritou dočasných kľúčov) aj WPA-AES (Advanced Encryption Standard, rozšírený šifrovací štandard) však nastali problémy s nekompatilitou (aj pri testovaní všetkých kariet na Windows s použitím ovládačov od výrobcu) a nebola možná komunikácia STA (station, stanica) a AP medzi:

» Asus-STA « Micronet-AP – AP neodpovedá na 2. správu EAPOL handshake (Extensible Authentication Protocol over LAN, podanie si rúk pomocou rozšíriteľného autentifikačného protokolu cez lokálnu sieť), pretože mu na konci tela správy chýbajú dva nulové bajty (ktoré Micronet neštandardne používa);

» MSI-STA « Micronet-AP – po odpovedi na Probe request broadcast (celoplošná vyhľadávacia požiadavka) sa MSI nepokúsi o pripojenie;

» Asus-STA « Micronet-STA – (ad-hoc) posielajú nekompatibilné Beacon (signálne rámce);

» MSI-STA « Micronet-STA – (ad-hoc) neznáma príčina, odchytávanie nebolo k dispozícii;

Pri zabezpečení pomocou WPA/WPA2 bolo teda nutné prevádzku simulovať pomocou špeciálneho zapojenia (viď. 2.4), pretože jediná fungujúca dvojica (tak, aby bola ešte k dispozícii karta v monitor režime) bola Micronet-STA « Micronet-STA. Žiadne z použitých zariadení nemá Wi-Fi certifikáciu, Micronet ani nie je členom Wi-Fi aliancie.

2.3 Softvér

Najviac vývoja v oblasti analýzy bezpečnosti bezdrôtových sietí sa deje v *nixovom prostredí. Je to najmä kvôli dostupnosti knižníc (najmä knižnica pcap na zachytávanie a ukladanie sieťovej

komunikácie), jednoduchej interakcii programov navzájom (skriptovanie) a možnosti nízkoúrovňového prístupu hardvéru. Zapnutie monitorovacieho režimu je s ovládačmi pre OS Windows obtiažne a často nemožné a podpora aplikácií potrebných na testovanie útokov je veľmi nízka. Na simuláciu prevádzky bol použitý počítač s OS Windows 2000 (s Micronet PCI kartou) vždy spolu s jedným z ďalších dvoch PC. Na pasívne aj aktívne útoky boli použité počítače s nainštalovaným OS Linux distribúcie Slackware 10.1 a 10.2, dostupný z http://www.slackware.org [10]. Boli použité kernely (jadrá) verzie 2.4.29 a 2.6.18.3, oba nakompilované pre použitie na danom systéme.

2.3.1 Použité utility

Okrem programov štandardne prítomných v distribúcii Slackware a ovládačov, ktoré boli popísané vyššie, boli použité nasledovné:

· **WireShark**, verzia 0.99.5 – pôvodným názvom Ethereal, http://www.wireshark.org [11], zachytávanie a prehľadná analýza v grafickom režime;

· **AirSnort**, verzia 0.2.7e – http://airsnort.shmoo.com [12], zistenie WEP kľúča pomocou FMS a KoreK útokov (viď. 4.7 a 4.8) v grafickom režime;

· **Aircrack-ng**, verzia 0.8 – http://www.aircrack-ng.org [13], balík programov na rôzne útoky;

· **Aircrack-ptw**, v. 1.0.0 – http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw [14], utilita na zistenie WEP kľúča Kleinovým útokom (viď. 4.9);

· **Airbase**, verzia svn-233 – http://www.802.11mercenary.net/ [15], balík programov na lámanie WEP, využitá z neho bola najmä utilita prism-strip na odstraňovanie Prism hlavičiek z pcap súborov;

· **coWPAtty**, verzia 4.0 – na stiahnutie z http://www.churchofwifi.org/ [16], utilita na lámanie PSK vo WPA a WPA2 (viď. 5.2);

· **wep_crack** – http://www.thenewsh.com/~newsham/wlan [17], utilita na brute-force lámanie WEP založeného na passphrase (viď. 4.1.1). Použité neboli (či už pre nedostatočné štádium vývoja, nemožnosť použitia v testovacom prostredí, alebo závislosť programu od použitých ovládačov), ale za zmienku stoja nasledovné:

· **Airsnarf** – http://airsnarf.shmoo.com/ [18], balík určený na nastavenie falošného AP (viď. 8.1);

· **asleap** – http://asleap.sourceforge.net/ [19], utilita na lámanie LEAP (Lightweight EAP, odľahčený EAP) (viď. 5.3) a PPTP (Point-to-Point Tunneling Protocol, protokol na tunel medzi dvoma bodmi);

· **chopchop** – zverejnený na fóre http://www.netstumbler.org/ [20], pôvodný proof-ofconcept (dôkaz konceptu) pre chopchop útok (viď. 4.5);

· **HotSpotDK** – http://airsnarf.shmoo.com/ [18], WIDS (Wireless Intrusion Detection System, systém na detekciu prienikov na bezdrôtovej sieti) na personálne použitie (viď. 9.4);

· **lorcon** – http://802.11ninja.net/lorcon/ [21], knižnica, ktorá umožňuje manipuláciu so zariadeniami v režime monitor pre viaceré ovládače s transparentným prístupom – jedná sa o aktuálny projekt, ktorý zjednoduší vývojárom prácu o starosti s ovládačmi, takže sa čoskoro zrejme objavia úplne nové projekty ohľadom bezpečnosti WLAN,

· **MAC Changer** – http://www.gnu.org/software/macchanger [22], program na zmenu MAC adresy zariadenia.

2.3.2 Úprava ovládačov

Ovládače rt2500 boli upravené tak, aby v režime monitor poskytovali vyšším vrstvám nielen dátové

a management rámce, ale aj riadiace (control). Zmena bola urobená v súbore rt2500-1.1.0-b4/Module/rtmp_data.c, patch (záplata) je na priloženom médiu.

Rovnakú zmenu je možné urobiť aj pre rt2570, v súbore rt2570-1.1.0-b2/Module/rtusb_data.c, pre nutnú zapnutú bezpečnostnú politiku na danom počítači nebolo možné neúplné riadiace rámce poskytnúť cez firewall vyššej vrstve. Tieto ovládače boli upravené aj pre rýchle posielanie rámcov v režime monitor snulovým backoff time (časom cúvnutia), tiež zmenou v súbore rtusb_data.c. Záplata na priloženom médiu.

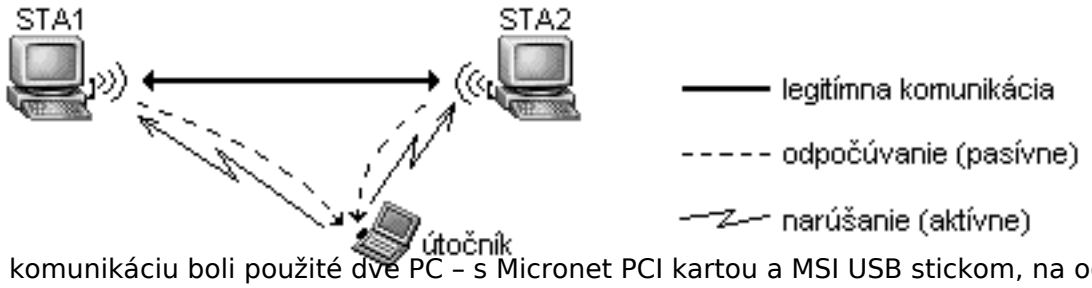
2.3.3 Nová utilita framespam

Pre potreby tejto práce, najmä pre implementáciu CTS flood útoku (viď. 6.3) bola vytvorená jednoduchá utilita nazvaná framespam. Umožňuje posielať rámce veľkou rýchlosťou („spamovať“ ich), alebo s pauzou po vyslaní každého rámca. Rámec na odoslanie je načítaný zo štandardného vstupu, ktorý je presmerovateľný zo súboru alebo z výstupu iného programu, a tak je utilita ľahko použiteľná aj v skriptoch. Parametre a príklad spustenia sú popísané v časti 6.3.3 Realizácia CTS útoku. Utilita je na priloženom médiu.

2.4 Zapojenie

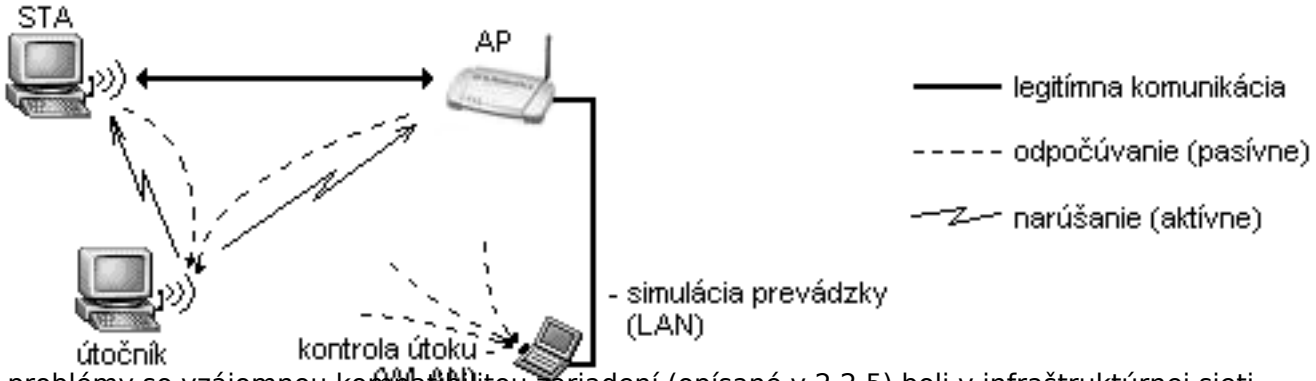
Boli použité dve rôzne zapojenia – jedno pre operáciu v režime ad-hoc a jedno infraštruktúrne (režim managed).

2.4.1 Ad-hoc zapojenie



Na komunikáciu boli použité dve PC – s Micronet PCI kartou a MSI USB stickom, na odpočúvanie a narúšanie notebook s Asus CardBus kartou.

2.4.2 Infraštruktúrne zapojenie



Pre problémy so vzájomnou kompatibilitou zariadení (opísané v 2.2.5) boli v infraštruktúrnej sieti (režim managed) použité na legitímnu wireless komunikáciu iba Micronet-AP a Micronet-STA. Ako útočník bolo použité PC s MSI USB stickom. Kvôli potrebe Linuxu (umožňuje flood ping) na aspoň jednej z komunikujúcich staníc bol ku AP pripojený pomocou ethernetu notebook, ktorý s STA komunikoval. Ten navyše robil aj pasívne sledovanie, pre kontrolu priebehu útoku pomocou programu WireShark. Väčšina práce (tam, kde nie je uvedené inak) bola vykonaná v infraštruktúrnom režime, práve pre možnosť nezávisle sledovať priebeh útoku.

URL článku:
https://security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-1-%C3%BAvod-p%C5%99%C3%ADprava

Odkazy:
[1] https://security-portal.cz/users/matej
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/hacking-method
[4] https://security-portal.cz/category/tagy/networks-protocols
[5] https://security-portal.cz/category/tagy/security
[6] https://security-portal.cz/category/tagy/wifi-wireless
[7] http://linux-wless.passys.nl/
[8] http://rt2x00.serialmonkey.com/
[9] http://rtl8180-sa2400.sourceforge.net/
[10] http://www.slackware.org
[11] http://www.wireshark.org
[12] http://airsnort.shmoo.com
[13] http://www.aircrack-ng.org
[14] http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw
[15] http://www.802.11mercenary.net/
[16] http://www.churchofwifi.org/
[17] http://www.thenewsh.com/~newsham/wlan
[18] http://airsnarf.shmoo.com/
[19] http://asleap.sourceforge.net/
[20] http://www.netstumbler.org/
[21] http://802.11ninja.net/lorcon/
[22] http://www.gnu.org/software/macchanger
[23] http://matej.sustr.sk/publ/dipl/
[24] http://creativecommons.org/licenses/by-nc/3.0/