UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Bezpečnost Wi-fi sítí

Dan Václavek

Bakalářská práce
2012

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2011/2012**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Dan Václavek**
Osobní číslo:	**I09301**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Bezpečnost Wi-fi sítí**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je popsat způsoby zabezpečení bezdrátových technologií pomocí šifrovacích metod. Autor uvede přehled standardu 802.11i a jeho komerční implementaci WEP, WPA a WPA2, dále popíše slabá místa šifrování WEP, porovná slabá místa WPA a WPA2, základy standardu 802.1x. V praktické části ověří pomocí vybraného sniffovacího programu zabezpečení vybraných šifrovacích metod. Dále navrhne a realizuje ukázkové testy útoku pro prolomení vybraného šifrování.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

PUŽMANOVÁ , Rita. Bezpečnost bezdrátové komunikace. 1. Praha : ComputerPress, 2005. 184 s. ISBN 80-251-0791-4.
BRANDON , James Carrol. Bezdrátové sítě Cisco. 1. Praha : ComputerPress, 2010. 480 s. ISBN 978-80-251-2884-8.

Vedoucí bakalářské práce: **Ing. Soňa Neradová**
Katedra softwarových technologií

Datum zadání bakalářské práce: **16. prosince 2011**
Termín odevzdání bakalářské práce: **11. května 2012**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 30. března 2012

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 10. 05. 2012 Dan Václavek

Poděkování

Na tomto místě bych rád poděkoval vedoucí bakalářské práce, Ing. Neradové za poskytnuté rady ohledně vypracování této práce. Dále bych chtěl poděkovat Mgr. Horálkovi za pomoc při návrhu tématu. Také bych rád poděkoval za povolený přístup do školní laboratoře a zapůjčení hardwaru.

Anotace

Tato bakalářská práce se zabývá problematikou zabezpečení bezdrátových sítí. Popisuje jednotlivé varianty standardu 802.11, metody zabezpečení a možnosti útoků.

V praktické části bakalářské práce jsou popsány provedené útoky. Jedna kapitola se také zabývá související problematikou volby bezpečných hesel a použitelnosti v praxi.

Klíčová slova

IEEE 802.11, Wi-Fi, WEP, WPA, WPA2, bezdrátové sítě, zabezpečení, šifrování, útoky

Title

Wireless Networks Security

Annotation

This bachelor thesis deals with the issue of wireless security. Describes the different variants of the 802.11 standard, methods of securing and potential attacks.

In the practical part of bachelor thesis describes some types of attacks. One chapter also deals with related issues of secure passwords selection and applicability in practice.

Keywords

IEEE 802.11, Wi-Fi, WEP, WPA, WPA2, wireless networks, security, encryption, attacks

Obsah

Seznam zkratek

ARP	Address Resolution Protocol
CCK	Complementary Code Keying
CRC	Cyclic Redundancy Check
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
FHSS	Frequency Hopping Spread Spectrum
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IrDA	Infrared Data Association
ISM	Industrial, Scientific and Medical band
LAN	Local Area Network
MIC	Message Integrity Check
MIMO	Multiple Input Multiple Output
MITM	Man In The Middle
OFDM	Orthogonal Frequency Division Multiplexing
PEAP	Protected EAP
PSK	Pre Shared KeyISM
RC4	Rivest Cipher 4
SS	Spread Spectrum
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTSL	Tunneled Transport Layer Security
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

Seznam obrázků

Seznam tabulek

Úvod

Cílem této bakalářské práce je popsat problematiku bezdrátových sítí především z pohledu bezpečnosti. V dnešní době jsou bezdrátové sítě věcí, se kterou se většina z nás setkává denně. Ať již doma, v práci, ve škole nebo i na veřejných prostranstvích či kavárnách nebo restauracích. Jejich využívání pochopitelně přináší různé výhody (snadná instalace, mobilita uživatelů), ale každé pro má i své proti. U bezdrátových sítí v podobě zabezpečení, které je složitější než u metalických sítí. Nejedná se pouze o zamezení přístupu do sítě prostřednictvím přístupového bodu, ale i o šifrování dat, která jsou přenášena vzduchem a jsou tak poměrně snadno zachytitelná. Převážná část uživatelů, kteří využívají bezdrátové technologie Wi-Fi v domácím prostředí, mají minimální znalosti ohledně nastavení potřebných zařízení. Často jsou pak tyto zařízení ponechána ve výchozím nastavení a stávají se tak snadným cílem pro útočníky. Ve firemním prostředí se očekává profesionální přístup a nastavení sítě tak, aby splňovala nejpřísnější bezpečnostní kritéria. Není to však psaným pravidlem a tak není problém se setkat i se špatně zabezpečenou firemní sítí. Taková síť je pro případného útočníka rozhodně zajímavější než domácí sít, kde prolomením zabezpečení získá většinou maximálně tak připojení k Internetu. V případě firemních sítí se může jednat o opravdu důležitá a citlivá data.

V teoretické části je třeba nejprve popsat jednotlivé zabezpečovací mechanismy, které se využívají při zabezpečování bezdrátových sítí. Přiblížit principy jejich fungování a poukázat na bezpečnostní slabiny. Na začátku se podíváme na něco málo z historie a principy fungování bezdrátové sítě. Další kapitola bude věnována standardu 802.11, kde budou kromě původního standardu 802.11 popsány jeho jednotlivé varianty (802.11a, b, g, n). S principem fungování bezdrátových sítí je třeba se zaměřit na metody bezdrátového přenosu dat (FHSS, DSSS, OFDM). Dále budou popsány principy autentizace a používané metody zabezpečení (WEP, WPA a WPA2). U protokolu WEP je především poukázáno na jeho nevhodnost využití v dnešní době z důvodu poměrně snadného prolomení klíče. Jeho hlavní nevýhodou je používání statického klíče. V další části je popsáno zabezpečení WPA, které odstraňuje známé nedostatky zabezpečení WEP. Důležité bylo především zaměřit se na použité šifrování a kontrolu integrity dat. U WPA2 bylo popsáno šifrování CCMP, které nahradilo TKIP u předchozího WPA. V následující kapitole jsou popsány jednotlivé typu útoku na bezdrátové sítě. Tyto útoku je možné provádět na základě znalostí získaných v předchozích kapitolách. Využívají námi známých bezpečnostních nedostatků jednotlivých zabezpečení. Dále jsou popsány možnosti jak jednotlivým útokům předcházet. Kapitola s názvem Zásady zabezpečení se věnuje především problematice hesel. Je zde popsáno jakým způsobem zvolit dostatečně bezpečné heslo. V další kapitole je stručný návod jakým způsobem lze zvýšit bezpečnost domácí nebo firemní sítě, ale i jak se bezpečně chovat při připojení do některé ze sítí veřejných (takzvané Free Wi-FI sítě). V neposlední řadě jsou zde uvedeny statistiky z projektu Wifileaks, který se zabývá zaměřováním bezdrátových sítí v české republice pomocí

jednoduché mobilní aplikace pro mobilní telefony se systémem Android. Jedná se především o přehled nejčastěji používaných typů zabezpečení a názvů bezdrátových sítí.

V praktické části této bakalářské jsou popsány provedené typu útoků. Tyto útoky jsou založeny na znalostech získaných během vypracování teoretické části a využívají právě zmíněných bezpečnostních nedostatků jednotlivých zabezpečovacích mechanismů.

Celá práce byla zpracována po nastudování zdrojů uvedených v seznamu literatury, který je k nalezení na konci dokumentu.

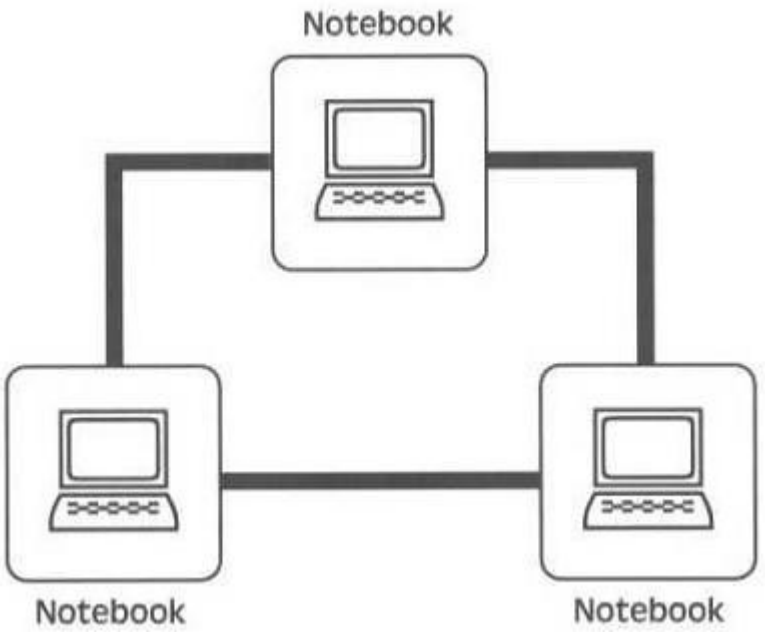
1 Úvod do problému wifi sítí

1.1 Jak funguje wifi

WiFi zařízení spolu komunikují na základě vysílání a přijímání signálu ve stejném frekvenčním pásmu. Rozlišujeme dva druhy komunikace. Buď mohou být spojené přímo (peer-to-peer), nebo pomocí přístupového bodu (access point).

1.2 Ad - hoc

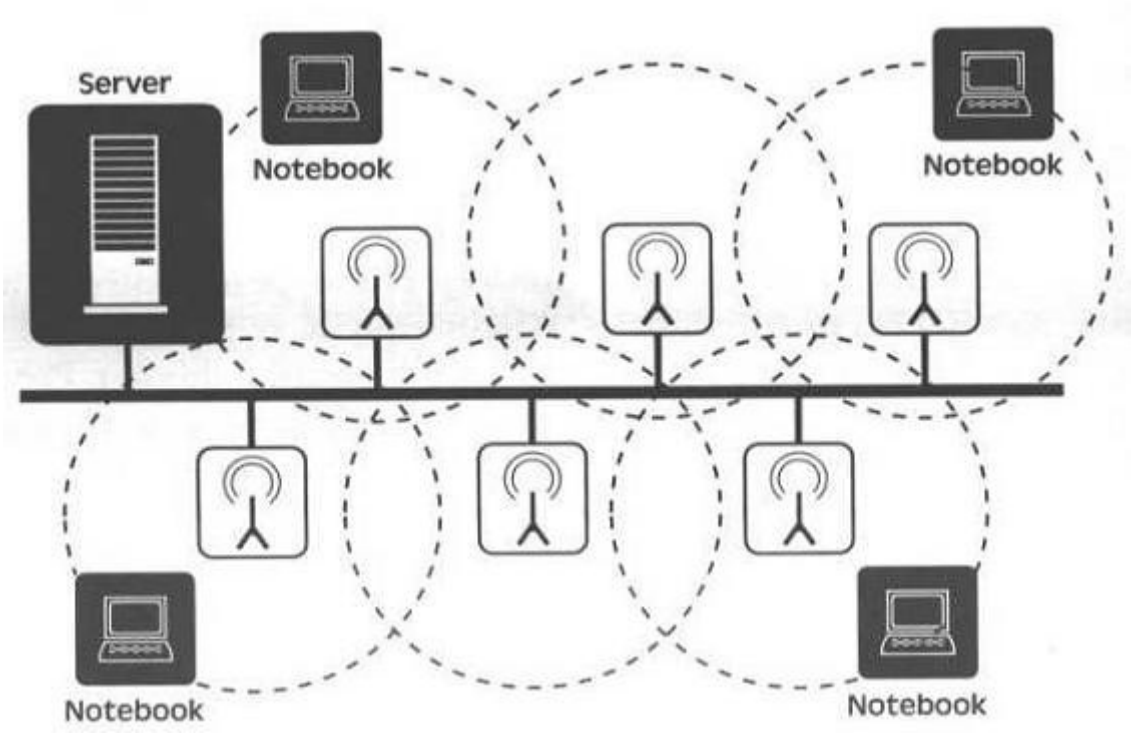
Jedná se o bezdrátové sítě, kde jednotlivé stanice komunikují přímo mezi sebou. Komunikace probíhá bez použití přístupového bodu. Tzv. Imaginární přístupový bod vytváří první připojená stanice, která se stará o řízení komunikace v síti. Při jakémkoliv výpadku této stanice se řízení ujímá jiná, náhodně zvolená, stanice v síti. Komunikující stanice musí být ve vzájemném rádiovém rozsahu. Toto řešení je vhodné pro menší sítě, čítající malé množství stanic a pro komunikaci na menší vzdálenosti. Přístup k internetu lze v Ad - hoc síti sdílet pokud je jedna ze stanic nakonfigurována tak, aby fungovala jako brána (gateway) pro přístup k internetu. Pro domácí použití je vhodné například k hraní síťových multiplayer her, nebo pro přenos dat.



Obrázek 1 - Ad - hoc struktura bezdrátové sítě [1]

1.3 Infrastrukturní sítě

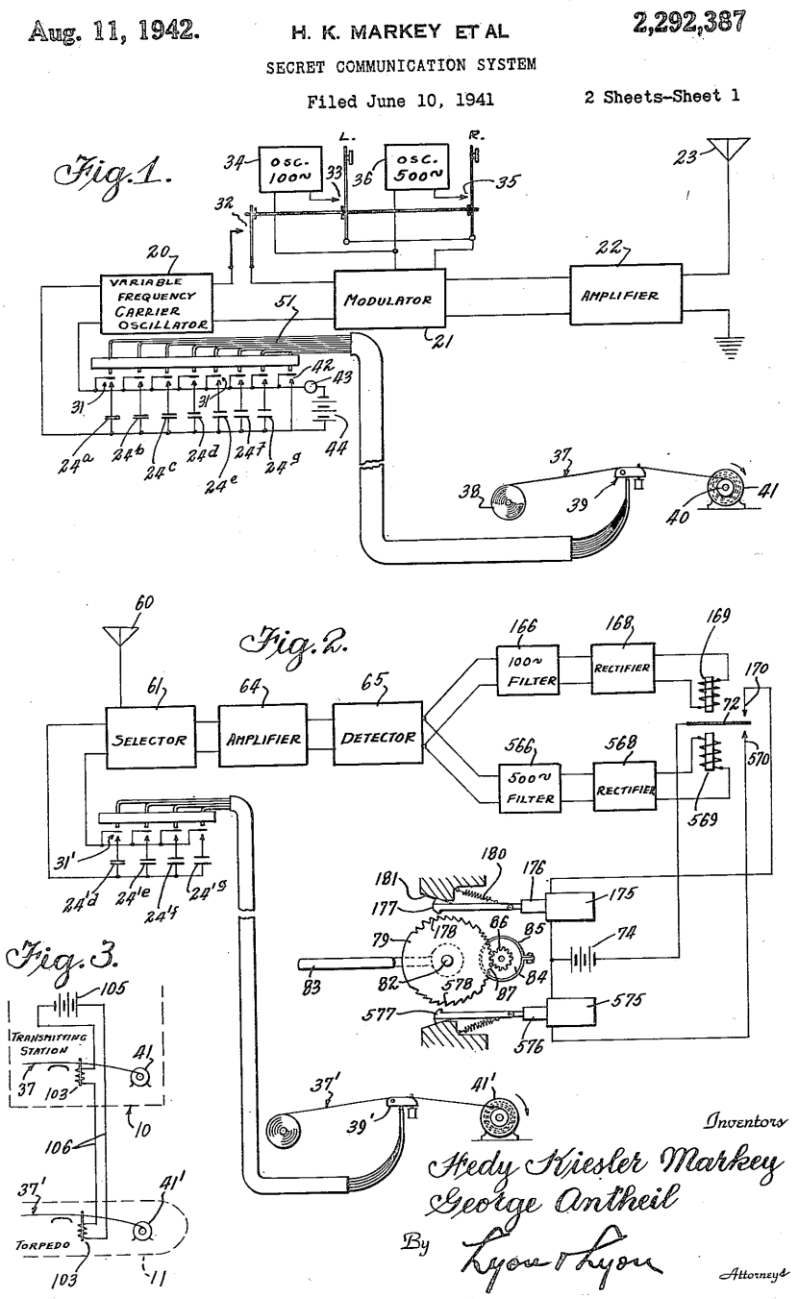
Na rozdíl od Ad - hoc jednotlivé stanice komunikují prostřednictvím jednoho či více přístupových bodů. Tyto sítě mají svou pevně danou infrastrukturu. Klient může být připojen bezdrátově, pokud je v dosahu signálu přístupového bodu, nebo může být připojen drátově. Přístupový bod je potom rozhraním mezi drátovou a bezdrátovou sítí. Je schopný zapojit do komunikace více stanic najednou.



Obrázek 2 - Struktura infrastrukturní bezdrátové sítě [2]

1.4 Historie

Počátky bezdrátových technologií se datují kolem roku 1940, kdy probíhala Druhá světová válka. Hudební skladatel a vynálezce George Antheil společně s herečkou, vynálezkyní a matematičkou Hedy Lamarr objevili princip přenosu dat pomocí rozprostřeného spektra. Tento princip využívají i dnešní bezdrátové sítě. Lamarr a Antheil nabídli práva k používání této technologie americkému námořnictvu. To však technologii začalo používat až v šedesátých letech dvacátého století za doby kubánské krize pro vzájemnou komunikaci lodí na otevřeném moři. Tento předchůdce technologie FHSS (Frequency Hopping Spread Spectrum) byl nadále používán především pro vojenské účely. V osmdesátých letech bylo rozhodnuto, že tato technologie bude využívána i pro civilní účely. Tím začíná příběh bezdrátových sítí takových, jaké známe dnes. V roce 1997 byl vydán organizací IEEE první standard bezdrátových sítí 802.11, který využíval modulační principy FHSS a DSSS (Direct Sequence Spread Spectrum, Rozprostřené spektrum v přímé posloupnosti). Jako další byla možnost komunikace pomocí infračervených signálů. Rychlost byla 1 MB/s, nebo dokonce 2 MB/s, což v porovnání s tehdejší drátovou sítí nemohlo být rychlostí konkurence schopné. Tento standard obsahoval zabezpečení WEP.



Obrázek 3 - Secret communication systém [3]

2 Standard 802.11

Jedná se o původní standard vyvinutý společností IEEE (Institute of Electrical and Electronics Engineers), který byl přijat roku 1997. Umožňoval přenosovou rychlost 1 až 2 MB/s. Využíval tři možnosti řešení fyzické vrstvy:

- FHSS (Frequency Hopping Spread Spectrum),
- DSSS (Direct Sequence Spread Spectrum),
- Infračervený přenos.

Linková vrstva poskytovala následující služby:

- autentizace,
- asociace,
- WEP (Wired Equivalent Privacy).

Velkou nevýhodou byla určitě již zmiňovaná přenosová rychlost, která nedosahovala přenosových rychlostí klasických metalických sítí.

Tabulka 1 - 802.11 - parametry

Přenosová rychlost	Frekvenční pásmo	Kódování
1 až 2 MB/s	2,4 GHz	FHSS/DSSS/IrDA

2.1 IEEE 802.11b

Tento standard vznikl v roce 1999 jako vylepšená verze původního standardu 802.11. Cílem bylo odstranit problém nízké přenosové rychlosti. Standardu 802.11b se přezdívalo Wi-Fi (Wireless Fidelity) což v překladu znamená bezdrátovou věrnost. Při stejném frekvenčním pásmu (2,4 GHz) dosahuje vyšších přenosových rychlostí. Rychlost až 11 Mb za sekundu je dosažena pomocí nového způsobu kódování, tzv. doplňkové klíčové kódování (Complementary Code Keying) na fyzické vrstvě pracující v rámci DSSS.

V závislosti na zarušení prostředí se přenosová rychlost dynamicky mění. Dochází ke snižování a zvyšování rychlosti v řadě 1, 2, 5,5 až 11 Mb/s. Maximální teoretická rychlost na fyzické vrstvě je 11 Mb za sekundu. Uživatelská rychlost se však pohybuje pouze okolo 6 Mb za sekundu. To je způsobeno vlivem rušení, vzdáleností od přístupového bodu a v neposlední řadě potřebnou režií, která zabere přibližně 30% kapacity. Dosah sítě, který je ovlivněn hustotou zástavby, se pohybuje kolem 100 metrů.

2.2 IEEE 802.11a

Norma IEEE 802.11a byla schválena brzy po tom co byla schválena norma 802.11b. Dosahuje teoretických přenosových rychlostí až 54 Mb za sekundu, které jsou díky režii zhruba poloviční. Pracuje ve frekvenčním pásmu 5 GHz z důvodu velkého rušení původního frekvenčního pásma (2,4 GHz). Tuto frekvenci začalo využívat mnoho dalších zařízení jako například mikrovlnné trouby nebo mobilní telefony s technologií Bluetooth.

V porovnání s 2,4 GHz pásmem poskytuje větší šířku pásma a více kanálů. Definováno je osm nezávislých, nepřekrývajících se kanálů. Je zde použita metoda rozprostřeného spektra OFDM (Orthogonal Frequency - Division Multiplexing).

Nevýhodou je, že právě rozdílná frekvence znemožňuje vzájemnou kompatibilitu obou typů WLAN. Naopak výhoda spočívá ve vyšších rychlostech a využití více kanálů bez vzájemného rušení. Počet kompatibilních zařízení s 802.11a je mnohem nižší než počet zařízení kompatibilních se standardy využívajících frekvenční pásmo 2,4 GHz.

2.3 IEEE 802.11g

Standard 802.11g byl schválen roku 2003. Je navržen pro frekvenční pásmo 2,4 GHz stejně jako jeho předchůdce 802.11b. Maximální přenosová rychlost na fyzické vrstvě je stejná jako rychlost standardu 802.11a a dosahuje 54 Mb za sekundu. Využívá modulace OFMD (Orthogonal Frequency – Division Multiplexing), ale obsahuje i modulaci DSSS (Direct Sequence Spread Spectrum). Je to z důvodu zpětné kompatibility se zařízeními pracujícími na standardu 802.11b. To znamená, že pokud se do sítě 802.11g připojí zařízení pracující na 802.11b dojde ke změně komunikace všech zařízení v síti na 802.11b. Rychlost se v takovém případě sníží ze zmiňovaných 54 na 11 Mb za sekundu.

Dosah sítě se při maximální rychlosti pohybuje okolo 30 metrů. Při rychlostech nižších, stejných jako u 802.11b, je dosah vyšší.

2.4 IEEE 802.11n

Norma 802.11n byla schválena v září roku 2009. Upravuje fyzickou vrstvu a podčást linkové vrstvy tak, aby bylo možno dosáhnout vyšších přenosových rychlostí. Rychlost namísto původního maxima v podobě 54 Mb za sekundu dosahuje až 600 Mb za sekundu. Využívá technologií předchozích norem, které rozšiřuje především o technologii MIMO (Multiple - Input Multiple - Output). To zlepšuje odolnost proti rušení. MIMO pracuje na fyzické vrstvě a lze ji proto využívat bez ohledu na protokoly vyšších vrstev. Maximální propustnost sítě a rychlost dokážeme jednoduše zvýšit právě přidáním antén. Standard dokáže pracovat jak v 2,4 GHz, tak i v 5 GHz frekvenčním pásmu. Pro dosažení maximální propustnosti sítě je však doporučováno použití frekvenčního pásma 5 GHz.

2.5 Přehled parametrů

V následující tabulce je uveden přehled technických parametrů všech výše zmíněných standardů.

Tabulka 2 - Přehled parametrů standardů [1]

Standard	Rok vydání	Frekvence [GHz]	Max. teoretická přenosová rychlost [Mb/s]	Průměrná skutečná rychlost [Mb/s]	Kódování
802.11	1997	2,4	2	0,9	FHSS/DSSS/IrDA
802.11a	1999	5	54	23	OFMD
802.11b	1999	2,4	11	4,3	DSSS
802.11g	2003	2,4	54	19	OFMD/DSSS
802.11n	2009	2,4 / 5	600	-	MIMO-OFDM

3 Bezdrátový přenos dat

Pro bezdrátový přenos dat se využívá technologie rozprostřeného spektra (SS - Spread Spectrum). Cílem je dosažení rychlých datových přenosů v pásmu ISM. Využívá matematické funkce pro rozptýlení signálů s nižším výkonem do širokého rozsahu kmitočtů. To snižuje náchylnost na úzkopásmové rušení a takovéto signály se hůře detekují, protože se chovají jako šum. Přijímač provede opačnou operaci, která spočívá ve zpětném složení rozprostřeného signálu do klasického úzkopásmového signálu. V pásmu ISM nelze používat jiný způsob přenosu signálu než je právě pomocí rozprostřeného spektra.

V České republice se frekvenční pásmo 2,4 GHz rozděluje na 13 kanálů. Technologie rozprostřeného spektra znamená vysílání do frekvenčního rozsahu 22 MHz, ale odstup mezi jednotlivými kanály je pouze 5 MHz. To znamená, že se použitelné kanály překrývají, což z nich nedělá plnohodnotné kanály. Při provozování více přístupových bodů je vhodné volit kanály tak, aby se vzájemně nerušily.

Tabulka 3 - Frekvenční pásmo 2,4 GHz - rozdělení kanálů [2]

Kanál	Frekvence [GHz]
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,477
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

Metody, které slouží pro realizaci rozprostření spektra, jsou:

- Frequency Hopping Spread Spectrum,
- Direct Sequence Spread Spectrum,
- Orthogonal Frequency Division Multiplex.

3.1 DSSS - Direct Sequence Spread Spectrum

Metoda přímé sekvence využívá toho, že každý jednotlivý bit je před přenosem nahrazen celou sekvencí bitů. Tyto sekvence jsou vytvořeny pseudonáhodně za pomocí Barker code nebo Gold code. Pro úspěšný přenos je nutné znát tento mechanismus na obou stranách. Jak na straně vysílací, tak na straně přijímací. Signál je rozprostřen do větší části radiového spektra. Menší náchylnost vůči rušení zvyšuje spolehlivost přenosu. Signál se ostatním uživatelům jeví jako šum.

3.2 FHSS - Frequency Hopping Spread Spectrum

FHSS je technika využívající pro rozprostření spektra frekvenčních poskoků. Vysílač skáče v pseudonáhodném pořadí po frekvenčních pásmech a na každém vysílá krátký datový proud. Frekvenční šířka pásma je 83,5 MHz. Toto pásmo je rozděleno na 79 kanálů o šířce 1 MHz. Zbytek pásma slouží jako tzv. ochranné pásmo proti interferencím. Po odvysílání přeskočí kmitočet nosného signálu na jiný kmitočet. Každých 30 sekund vystřídá alespoň 75 kmitočtů (kanálů). Na každém z nich vysílá maximálně 400 milisekund. Pokud se vysílací strana nachází na některém z kanálů, měla by strana přijímací vědět, který kanál to je. To je zajištěno generátory pseudonáhodných čísel na obou stranách. Jak na straně vysílací, tak na straně přijímací. Teoreticky je možný provoz 26 přístupových bodů. Ve skutečnosti je však počet možných přístupových bodů nižší (okolo 15).

3.3 OFDM - Orthogonal Frequency Division Multiplexing

Technologie OFDM (Orthogonal Frequency Division Multiplexing) je použita u standardů 802.11g a 802.11a. Jedná se o přenosovou techniku využívající rozprostřené spektrum. Vyznačuje se větší propustností a vyšší teoretickou přenosovou rychlostí, která dosahuje až 54 Mb za sekundu. Na rozdíl od DSSS, kde dochází k vytvoření jednoho velkého kanálu, se přenos rozdělí do několika subkanálů. Tyto subkanály pracují paralelně na několika nezávislých frekvencích. Tím je zaručena vyšší odolnost vůči interferencím.

4 Metody zabezpečení Wi-Fi sítě

V dnešní době existuje spousta metod jak zabezpečit bezdrátovou síť. Na rozdíl od kabelových sítí nelze přesně určit prostor, kde bude možno zachytit signál. Při útoku na kabelovou síť je nejprve potřeba se k ní dostat fyzicky. To znamená, že počítač musí být připojen pomocí kabelu. To zlepšuje možnost zabezpečení, protože útočník musí mít přístup k datové zásuvce nebo přímo ke switchi. U kabelových sítí lze proto použít zabezpečení formou odepření fyzického přístupu k síťovým prvkům. Toho lze dosáhnout například pouhým zamknutím místnosti, ve které se datová zásuvka nebo switch nachází. U bezdrátové sítě stačí být pouze v blízkosti přístupového bodu, respektive v dosahu signálu. Zamezení fyzického přístupu proto není zcela možné, ale je možné omezit dosah sítě a zmenšit tak prostor odkud je možné vysílaný signál zachytit. To lze provést omezením výstupního výkonu přístupového bodu na nejnižší, avšak stále vyhovující, možnou míru. Například pokud máme doma bezdrátovou síť, stačí nám šířit signál pouze v rámci domu, nikoliv však do okolních zahrad. V kabelových sítích se data směrují pomocí přepínače pouze na stanici, které patří. Zachycení komunikace je tak o něco složitější. Komunikaci mezi jednotlivými stanicemi v bezdrátové síti je možné zachytit jakoukoliv jinou stanicí v dosahu této sítě. Následně pak můžeme tuto komunikaci ukládat, pomocí k tomu určených programů, a dostat se pak přes tato přenášená data k citlivým informacím.

Bezdrátové sítě zabezpečujeme proti neoprávněnému připojování uživatelů a proti nechtěnému odposlechu přenášených dat. Z hlediska zabezpečení bezdrátových sítí proto rozlišujeme následující dvě skupiny:

- Šifrování - zabezpečení přenášených dat
- Autorizace - přístup oprávněných uživatelů

V této kapitole budou popsány a zhodnoceny z hlediska bezpečnosti právě jednotlivé metody zabezpečení bezdrátových sítí.

4.1 AUTENTIZACE, AUTENTIFIKACE

Ještě před tím, než může dojít k autentizaci, musí proběhnout autentifikace. Ta probíhá následujícím způsobem. Stanice, která se chce připojit k přístupovému bodu, rozešle broadcast (všesměrové vysílání), kterým se dotazuje na existenci přístupového bodu. Tento dotaz se nazývá Probe Request. Obsahuje stanicí podporované přenosové rychlosti a SSID sítě, ke které se chce stanice připojit. Odpověď na takovýto dotaz zasílají přístupové body, které jsou v dosahu a zároveň mají požadované SSID. To zasílají společně s dalšími parametry (podporované přenosové rychlosti, četnost beacons a další) pomocí Probe Responce. Přístupové body, které nemají SSID shodné s požadovaným od stanice Probe Request ignorují a neodesílají žádnou odpověď. Stanice tedy naváže spojení se správným přístupovým bodem a může začít proces samotné autentizace.

Autentizace je proces ověření identity subjektu (uživatele). Jedná se o ověření, zda je uživatel oprávněný pro vstup do bezdrátové sítě. Tento proces je jednosměrný. Což znamená, že autentizovat se musí pouze stanice k přístupovému bodu. Naopak autentizace přístupového bodu ke stanici není nutná. Toho lze využít při útocích man-in-the-middle využívajících podvržení přístupového bodu.

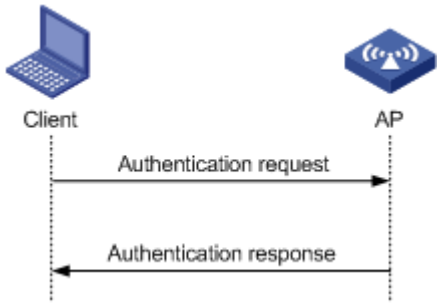
Standard 802.11 rozlišuje dvě metody autentizace:

- Open-system autentizace (otevřený systém)
- Shared-key autentizace (sdílený klíč)

Při budování bezdrátové sítě záleží jen na správci, jakou metodu autentizace zvolí. Důležité je aby tuto metodu podporoval jak přístupový bod, tak stanice, které se budou do sítě připojovat.

4.1.1 Open-system autentizace

Princip fungování je velice jednoduchý, a proto není vhodný pro zabezpečení. Jediné co je třeba pro připojení do bezdrátové sítě, která využívá Open-systém autentizace, je mít nastavené stejné SSID jako vysílá přístupový bod. Není tedy nutná jakákoliv znalost přístupového hesla. Pokud stanice zašle přístupové bodu správné SSID, je připojena a může začít komunikovat v rámci sítě. Při vypnutém vysílání SSID do okolí by se dalo říci, že se bezpečnost sítě zlepšila. Uživatel, který SSID nezná, se nemůže připojit. Částečně tomu tak je. Síť nebude viditelná v seznamu dostupných sítí, ale existují speciální nástroje, které dovedou zjistit SSID i když není vysíláno.



Obrázek 4 - Open-system autentizace [4]

4.1.2 Shared-key autentizace

Shared-key autentizace je o poznání lepší než výše zmiňovaná open-systém autentizace. Standardem 802.11 je dáno, že každé zařízení používající protokol WEP, musí podporovat Shared-key autentizaci. Každý uživatel, který žádá o přístup do sítě, by měl znát sdílený klíč. Proces autentizace začíná tím, že stanice zašle authentication request přístupovému bodu. Ten jej přijme a jako odpověď zašle náhodně vygenerovaný text. Stanice zašifruje tento text RC4 algoritmem pomocí svého klíče a zakódovaný text odešle zpět přístupovému bodu. Dojde k dešifrování zašifrovaného textu pomocí klíče přístupového bodu a následnému porovnání s původním textem. Pokud je tento text shodný s prvotně vygenerovaným, znamená to, že byl zašifrován pomocí stejného klíče. O správnosti klíče

a tedy o rozhodnutí o přijetí nebo odmítnutí se stanice dozví pomocí authentication response. Při zadání správného klíče je stanice následně úspěšně autentizována.

Obrázek 5 - Shared-key autentizace [4]

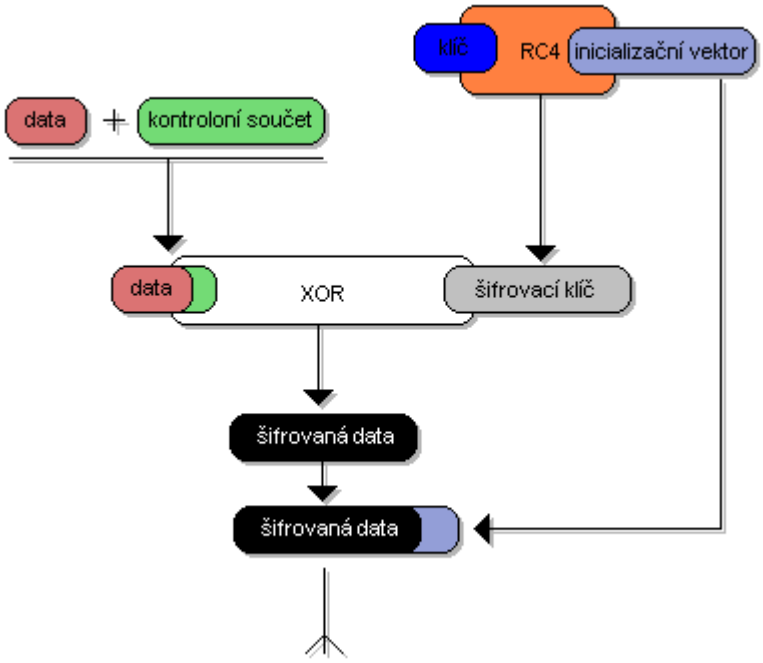
4.2 FILTRACE MAC ADRES

Princip filtrace MAC adres spočívá v omezení přístupu do sítě jen určitým klientům. Každý přístupový bod obsahuje tabulku povolených nebo zakázaných MAC adres. Seznam povolených adres obsahuje MAC adresy stanic, které mají oprávnění přistupovat do sítě. Naopak seznam zakázaných adres obsahuje adresy, kterým je přístup odepřen. Více používané jsou seznamy povolených adres. To z důvodu složitějšího zfalšování MAC adresy útočníkem zvenčí. Je přeci jen o něco složitější trefit adresu z mála povolených, než adresu z velkého množství nedefinovaných. Klient, který žádá o připojení do sítě je identifikován svoji jedinečnou MAC adresou. Ta se porovná s adresou uloženou v tabulce a na základě toho dojde k vyhodnocení přístupu. Přestože je přístup povolen pouze některým stanicím, hrozí odposlechnutí platných (povolených) MAC adres z komunikace v síti. Vzhledem k tomu, že se vysílají v nezabezpečené podobě, není to nijak zvlášť složité. Zařízení bez povolení přístupu změní svoji MAC adresu na některou z odposlechnutých platných. Přístupový bod si bude myslet, že se jedná o povolené zařízení a získá tak plnohodnotný přístup do sítě. Z tohoto důvodu je zabezpečení pomocí filtrování MAC adres samostatně nevyhovující. Hodí se jako doplněk k některému dalšímu zabezpečení.

4.3 WEP

Protokol WEP (Wired Equivalent Privacy) měl dokázat zabezpečit bezdrátové sítě na úrovni tehdejšího zabezpečení kabelových LAN sítí. Na rozdíl od kabelových sítí s pevně danou strukturou se signál bezdrátových sítí síří všemožně do okolí. Cílem bylo zamezit možným odposlechům. Tento zabezpečovací standard byl uveden v roce 1999. Byl navržen tak, aby mohl být implementován do stávajících síťových karet. Kvůli dodržení těchto kompromisů je v dnešní době jako zabezpečení nevyhovující avšak stále používaný. Používání tohoto protokolu není standardem vyžadováno, ale je doporučováno. Přestože je zabezpečení pomocí WEP poměrně snadno prolomitelné, je stále hojně využívané například v domácích sítích. Je to stále lepší varianta nežli naprosto

nezabezpečená síť a pro běžného uživatele vystavuje nepřekonatelnou překážku proti připojení do sítě. V dnešní době však existují vhodnější metody zabezpečení (např. WPA nebo WPA2). Základem protokolu WEP je šifrování za pomoci algoritmu RC4 s tajným klíčem.



Obrázek 6 - Princip šifrování WEP [5]

4.3.1 Šifrování RC4

O tom, zda se bude přenášená zpráva šifrovat, rozhoduje bit Protected frame, který je součástí MAC rámce. Šifrování může být realizováno buď 64 bitovým, nebo 128 bitovým klíčem. Klíč se skládá z tajného klíče a inicializačního vektoru (Initialization Vector). Inicializační vektor má konstantní délku, která je 24 bitů pro obě varianty. Inicializační vektor se přenáší nešifrovaný, takže na šifrovanou část připadá z celkového počtu bitů pouze 40 bitů, respektive 104 bitů. Problém protokolu WEP spočívá v tom, že standard 802.11 neřeší způsob jak implementovat generování inicializačního vektoru, který se používá společně s tajným klíčem při vytváření RC4 šifry.

Jak již bylo zmíněno, protokol WEP používá k šifrování symetrickou proudovou šifru RC4 (Rivest Cipher 4) společnosti RSA Security. Pro šifrování proudovou šifrou RC4 je důležité používat jedinečné šifrovací klíče. Tento klíč je kombinace tajného klíče a inicializačního vektoru. Když by byl každý paket šifrován stejným klíčem, byl by tento klíč snadno rozluštitelný. Proto je inicializační vektor pseudonáhodně generovaný a to v délce 24 bitů. To nám však zaručuje maximálně 2^24 = 16777216 hodnot. Takovýto počet by se mohl zdát jako dostačující, ale není tomu tak. Při běžném síťovém provozu dojde poměrně brzy k vyčerpání všech možných kombinací. Po vyčerpání všech jedinečných možností se začnou generované klíče opakovat. S tím roste šance na rozluštění hesla útočníkem. Právě toto se ukázalo jako největší nedostatek.

Algoritmus RC4 vygeneruje pomocí klíče pseudonáhodnou posloupnost. Ta se následně slučuje s daty pomocí operace XOR. Tím se získávají šifrovaná data ve stejné délce jako data původní.

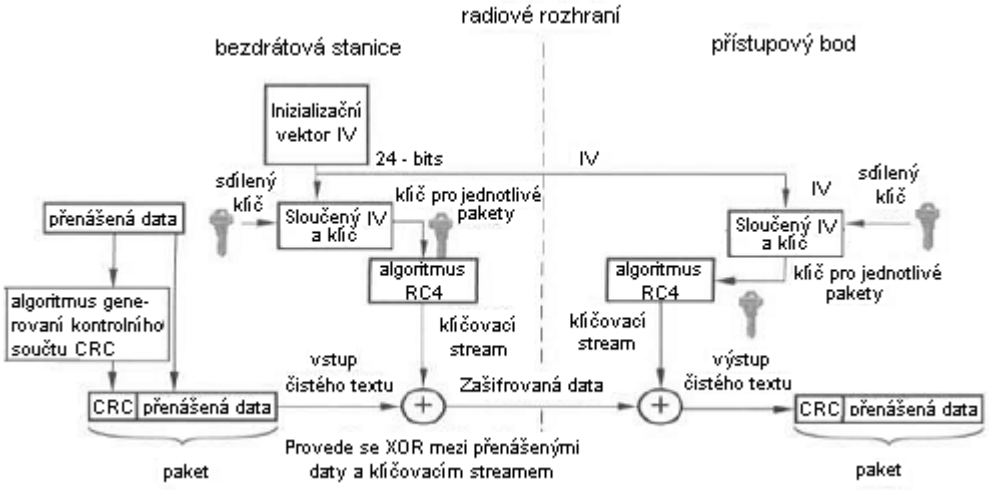
Bezpečnost RC4 šifry je dána následujícími parametry:

- délkou klíče,
- četností obměny klíče.

Shrnutí jednotlivých bitových délek klíčů lze vidět v následující tabulce.

Tabulka 4 - Parametry WEP64 a WEP128

Délka šifrovacího klíče	64 bitů	128 bitů
Délka tajného klíče	40 bitů	104 bitů
Délka inicializačního vektoru	24 bitů	24 bitů



Obrázek 7 - WEP zabezpečení pomocí algoritmu RC4 [6]

4.3.2 Integrita dat

U protokolu WEP je integrita přenášených dat zajištěna pomocí kontrolního součtu datové části přenášeného rámce. To je provedeno pomocí cyklického redundantního součtu CRC (Cyclic Redundancy Check). Výsledek toho součtu je označován jako ICV (Integrity Check Value), což je hodnota, která se připojuje na konec rámce. Celý rámec se poté šifruje včetně tohoto ICV na konci. Na přijímací straně dojde k dešifrování rámce a provede se kontrola správnosti ICV. Pokud tato hodnota nesouhlasí s hodnotou uvedenou v rámci, je jasné, že během přenosu došlo ke změně daného rámce. Tento rámec je považován za neplatný a dojde k jeho zahození.

4.3.3 Bezpečnostní slabiny

Protokol WEP je hojně využíván pro zabezpečení především domácích sítí i přes všechna známá bezpečnostní rizika. Je to hlavně z důvodu snadné konfigurace. Ve firemním

prostředí se dnes téměř nepoužívá a to právě z důvodu snadného prolomení zabezpečení i méně zdatným útočníkem.

Při útoku na bezdrátovou síť zabezpečenou pomocí protokolu WEP se využívá následujících bezpečnostních slabin tohoto protokolu.

- **Jednostranná autentizace** - uživatel neví, zda se opravdu připojuje ke správnému přístupovému bodu.
- **Autentizace uživatele** - je autentizována pouze stanice. Při odcizení počítače, notebooku nebo jiného zařízení s povolením vstupu do sítě, má pak toto zařízení stále přístup. Útočník má tak k dispozici aktuální přihlašovací údaje, proto je třeba provést změnu tajného klíče.
- **Proces autentizace** - Při autentizaci je útočník schopen zachytit proces autentizace, který se provádí nešifrovaný. Z toho lze získat tajný klíč.
- **Statický klíč** - protokol WEP nedokáže dynamicky měnit klíče. Změnu klíče je nutné provádět ručně a nastává tak problém s distribucí klíčů uživatelům. Každé zařízení připojující se do bezdrátové sítě zabezpečené protokolem WEP využívá stejný sdílený klíč. Při změně klíče je proto velmi problematické, především v rozsáhlých sítích tento klíč doručit všem klientům.
- **Generování IV** - není pevně dáno jak přesně se má měnit hodnota inicializačního vektoru. Nelze tedy vyloučit opakovaného použití stejné hodnoty, čehož může útočník využít k prolomení klíče.

4.4 802.1X

Standard 802.1x byl schválen roku 2001 jako nová bezpečnostní norma. Jejím úkolem je zabezpečit jak bezdrátové sítě, tak i sítě kabelové. Řízení přístupu spočívá v tom, že port na switchi je otevřen až poté, co je stanice úspěšně autentizována. V případě bezdrátových sítí je autentizace prováděna na úrovni logických portů přístupového bodu. Přístupový bod zprostředkovává ověřování. Stará se o spojení uživatele s autentizačním serverem (běžně se používá Kerberos nebo RADIUS). Autentizace je realizována protokolem EAP (Extensible Authentication Protokol), který se stará o přenos EAP paketů prostřednictvím spojové vrstvy LAN. Ty jsou zapouzdřeny do rámců 802.1x, proto se označují jako EAPOL (Extensible Authentication Protokol over LANs).

Během procesu autentizace spolu komunikují následující tři entity:

- **Klient** - Klient žádající o přístup do bezdrátové sítě. Zasílá své identifikační údaje přístupovému bodu.
- **Přístupový bod** - Stará se o zprostředkování ověřování identity klienta. Zajišťuje komunikaci klienta s autentizačním serverem. Na základě ověření blokuje nebo povoluje provoz na daném portu.
- **Autentizační server** - Jedná se o autentizační server, který na základě svých autentizačních informací ověří identitu klienta. Rozhodnutí o úspěšné nebo neúspěšné autentizaci zasílá přístupovému bodu.

Průběh autentizace:

1) Odeslání počáteční zprávy od klienta přístupovému bodu. Ten odpovídá zprávou EAP REQUEST-ID, kterou se snaží zjistit identitu klienta.

2) Klient odešle svoji identifikační údaje prostřednictvím zprávy EAP RESPONSE-ID. Tato zpráva je zapouzdřena do paketu RADIUS ACCESS_REQUEST a přístupový bod ji odesílá autorizačnímu serveru RADIUS.

3) RADIUS server odpovídá přístupovému bodu zprávou RADIUS ACCESS_ACCEPT/DENY. Tato zpráva obsahuje rozhodnutí o povolení/zakázání přístupu. V případě RADIUS ACCESS_ACCEPT je přístup povolen. V případě RADIUS ACCESS_DENY je přístup zakázán. Přístupový bod poté přepošle rozhodnutí klientovi zprávou EAP SUCCESS/FAILURE. Zpráva EAP SUCCESS znamená povolený přístup. Zpráva EAP FAILURE naopak zakázaný.

4) Pokud je autentizace úspěšná, byla přijata zpráva EAP SUCCESS, je otevřen právě ten port, přes který autentizace probíhala. Uživatel komunikující na tomto portu je považován za autentizovaného.

EAP

EAP je protokol, který se využívá ke zprostředkování výměny autentizačních zpráv mezi klientem, přístupovým bodem a autentizačním serverem. Tyto zprávy jsou zabaleny do linkových rámců. Existují metody EAP, které řeší pouze autentizaci klienta vůči autentizačnímu serveru RADIUS. Potřeba je však provádět vzájemnou autentizaci. To zabraňuje podvržení přístupového bodu útočníkem. Proto celý proces autentizace probíhá ve dvou základních fázích. V první fázi ověří klient, pomocí certifikátu, identitu serveru. Následně vytvoří šifrovaný tunel, po kterém bude probíhat komunikace. V druhé fázi dochází k autentizaci klienta vůči autentizačnímu serveru. Výše uvedeným způsobem funguje například metoda EAP-TTLS (Tunneled Transport Layer Security) nebo PEAP (Protected EAP).

Mezi nejčastěji používané autentizační mechanismy patří:

- EAP-MD5
- EAP-TLS
- EAP-TTLS
- LEAP
- PEAP

4.5 WPA

Zkratka WPA znamená Wi-Fi Protected Access. Jedná se o metodu zabezpečení bezdrátové sítě, která vznikla v roce 2001, kdy došlo k prolomení sítě zabezpečené pomocí protokolu WEP. Při zjištění těchto nedostatků byl započat vývoj nového zabezpečení

s označením 802.11i. Tato bezpečnostní norma byla schválena až v roce 2004. Mezitím uvedlo sdružení výrobců Wi-Fi Alliance dočasné řešení v podobě WPA, které bylo vyvinuto s ohledem na technické vybavení. Cílem bylo ponechat stávající hardware. Pomoci měla pouhá aktualizace softwaru. Bezpečnostní mechanismy WPA slouží k potlačení známých nedostatků protokolu WEP. Mezi ně patří šifrování statickým klíčem a slabá autentizace.

4.5.1 Šifrování

Data jsou opět šifrována pomocí proudové šifry RC4. Nově je však použit větší inicializační vektor. Jeho délka je 48 bitů. Délka tajného klíče je nově 128 bitů. Vylepšené šifrování bylo dosaženo protokolem TKIP (Temporal Key Integrity Protocol), který využívá dočasné klíče. Pro každý paket je generován jiný klíč. Při vytváření klíče dochází ke sloučení MAC adresy přijímací stanice, pořadového čísla rámce a základního klíče. Základní klíč je vygenerován hashovacím algoritmem při každé asociaci klienta k přístupovému bodu. Chrání proti útoku hrubou silou.

4.5.2 Kontrola integrity

WPA nevyužívá 32bitový kontrolní součet (CRC-32) jako předchozí protokol WEP. Využívá MIC (Message Integrity Check), který je součástí standardu IEEE 802.11i. Jedná se o vylepšenou kontrolu integrity dat nahrazující klasický kontrolní součet (CRC) u WEP. Zabraňuje v přijetí falešných paketů. Jestliže přístupový bod přijme dva nesprávné MIC kódy během minuty, provede příslušná opatření. Což znamená, že dojde k vygenerování nového TKIP klíče dané relace.

Při návrhu WPA byl brán ohled na dva možné způsoby implementace. Může být použit jak ve firemním, tak v domácím prostředí. V domácím prostředí (většinou malé sítě) není příliš vhodné používat na autentizaci uživatelů autentizační server. Naopak ve firemním prostředí je využití autentizačního serveru vhodné.

4.5.3 WPA - Pre Shared Key (PSK)

WPA-PSK je řešení pro domácí sítě nebo podnikové sítě menších rozměrů. Pro připojení klienta do sítě je nutné znát sdílený klíč. Na základě zadaného klíče rozhodne přístupový bod o autentizaci klienta. Pokud je klíč zadaný klientem shodný s klíčem uloženým v AP, je klient úspěšně autentizován. Z používání sdíleného klíče plyne bezpečnostní riziko, proto se doporučuje využívat tento způsob pro malé (domácí) sítě, čítající několik málo uživatelů.

4.5.4 WPA - Enterprise

Vhodné především pro rozsáhle podnikové Wi-Fi sítě. Na rozdíl od předchozí varianty má každý uživatel jiné přihlašovací údaje. Ověření a následné povolení přístupu do sítě provádí autentizační server, což poskytuje rozhodně vyšší zabezpečení. Autentizace se provádí přes EAP-TLS (EAP-Transport Layer Security) který zajišťuje bezpečnou komunikaci klienta s autentizačním serverem. K bezpečnému ověření uživatele a autentizačního serveru se používá systém veřejných klíčů (certifikátů). Klient za pomoci svého veřejného klíče zašifruje a následně dešifruje zprávy mezi ním a serverem. Ke své

zprávě přidá digitální podpis pomocí svého soukromého klíče a server si pomocí veřejného klíče z certifikátu klienta ověří pravost podpisu. Stejný postup použije i klient pro ověření pravosti autentizačního serveru. Toto řešení zabraňuje útokům typu man in the middle.

Tabulka 5 - Pracovní režimy WPA

Režim	Autentizace	Šifrování
Firemní mód	802.1x /EAP	TKIP / MIC
Domácí mód	PSK	TKIP / MIC

4.6 WPA2

Zabezpečovací metoda WPA2 vychází z, nám již známe, metody WPA. Tuto metodu rozšiřuje o protokol CCMP. Na rozdíl od protokolů WEP a WPA nevyužívá k šifrování proudovou šifru RC4, ale novější blokovou šifru AES (Advanced Encryption Standard). Použití této šifrovací metody umožní použití až 256 bitů dlouhého klíče. WPA2 také využívá režim PSK (Pre-Shared Key). Každý klient, připojující se do sítě, musí znát jediné sdílené heslo o 8 až 63 znacích. To je však znatelné bezpečnostní riziko, protože hrozí vyzrazení tohoto klíče. Při použití příliš krátkého hesla je možné toto heslo získat pomocí slovníkového útoku.

Obsahuje stejně jako WPA dva způsoby zabezpečení:

- Enterprise
- Pre Shared Key

Oba pracovní režimy jsou v rámci kompatibility naprosto shodné s WPA. Není proto nutné je nadále rozepisovat. Všechny potřebné informace je možno najít v předchozí kapitole (pro Enterprise kapitola 4.5.3 a pro PSK kapitola 4.5.4).

4.6.1 CCMP

Jedná se o protokol používaný v zabezpečovacím algoritmu WPA2. Byl vytvořen, aby nahradil stávající protokol TKIP (Temporal Key Integrity Protocol), používaný u WPA. Namísto proudové šifry RC4 využívá blokovou šifru AES. Díky 128 bitovému klíči je šifra považována za neprolomitelnou. I to má ale své nevýhody. Kvůli své výpočetní náročnosti není podporována staršími zařízeními.

5 Typy útoku na bezdrátovou síť

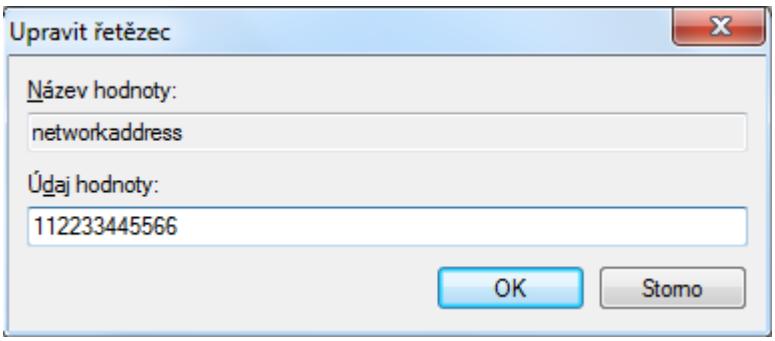
5.1 MAC SPOOFING

Jedná se o typ útoku, kdy jedinou bezpečnostní překážkou je filtrování MAC adres, kterou lze překonat během několika málo sekund. V první fázi útočník odposlouchává komunikaci v síti a snaží se o zachycení MAC adresy zařízení, které má do této sítě přístup. Druhá fáze spočívá ve změně MAC adresy své síťové karty na adresu, která byla odposlechnuta. Na první pohled by se mohlo zdát, že MAC adresa každého zařízení je pevně daná jeho výrobcem. Pravda je ale taková, že MAC adresa je součástí firmwaru síťové karty. Za pomoci speciálního softwaru na změnu MAC adresy (například MAC MakeUp nebo SMAC) nemá ani méně zkušený uživatel problém realizovat takovýto útok. Při použití tohoto způsobu musíme zajistit, aby stanice, jejíž adresu jsme si nastavili jako svoji, nevysílala. Nejjednodušší způsob je počkat až se odpojí, nebo ji odstavit jiným způsobem (DoS útok). Více v kapitole 5.5 Denail of Service.

- **Změna MAC v OS Windows**

Změnu v OS Windows je možno provést v systémových registrech. Postup je následující:

1) V příkazovém řádku spustíme editor registrů „*regedit*“
2) Vyhledáme klíč [HKEY_LOCAL_MACHINE – SYSTEM – CurrentControlSet –Control - Class {4D36E972-E325-11CE-BFC1-08002BE10318}, který obsahuje další podklíče síťových adaptérů ve tvaru 0001, 0002, 0003, atd.
3) Vyhledáme adaptér, jehož MAC adresu chceme změnit. V tom nám pomůže položka „*DriverDesc*“
4) Vytvoříme novou řetězcovou hodnotu REG_SZ, která bude mít název "networkaddress" a její hodnota bude požadovaná MAC adresa.



Obrázek 8 - Změna MAC adresy

Poznámka: Pokud chceme MAC adresu 11-22-33-44-55-66, hodnota, kterou budeme zapisovat do pole "Údaj hodnoty" bude v tomto tvaru 112233445566.

- **Změna MAC v OS Linux**

Změnu v OS Linux lze provést jednoduše z příkazového řádku za pomoci nástroje ifconfig a probíhá v následujících krocích:

1) Vypnutí zařízení
   ifconfig <interface> down
2) Vlastní změna adresy
   ifconfig <interface> hw ether <MAC_adresa>
3) Zapnutí zařízení
   ifconfig <interface> up

V příkazech za <interface> dosadíme identifikátor rozhraní (např. eth0, eth1, atd.), za <MAC_adresa> adresu ve tvaru 00:00:00:00:00:00.

Změnu ověříme pomocí následujícího příkazu:

ifconfig <interface>

Poznámka: Změna MAC adresy může ovlivnit provoz některých síťových služeb, které nemusí být poté funkční.

5.2 WEP CRACKING

Možností prolomení bezdrátové sítě zabezpečené pomocí protokolu WEP existuje velké množství. Již v roce 2000, vydán byl v roce 1999, byla publikována práce o bezpečnostních nedostatcích protokolu WEP. Od roku 2004 se síť zabezpečena pomocí protokolu WEP považuje za soukromou, ne však zcela bezpečnou. Klíče lze získat pasivním útokem zaměřeným na dešifrování zachycených přenosů. Odposloucháváním komunikace mezi připojenou stanicí a přístupovým bodem, ke kterému je stanice připojena, lze získat tajný klíč. Čím větší provoz na síti je, tím rychleji dojde k vyčerpání pseudonáhodných inicializačních vektorů. Ty se poté začnou opakovat a usnadní prolomení klíče.

5.2.1 Brutal-force attack

Jedná se o útok hrubou silou. Tento typ útoků spočívá v postupném testování všech možných hodnot šifrovacího klíče. Pro WEP64 má šifrovací klíč délku 40 bitů, pro WEP128 je pak délka klíče 104 bitů. Za pomoci výkonného počítače lze v přijatelném čase provádět útok hrubou silou pouze na 64 bitovou variantu WEP. Takový útok může trvat několik hodin, až dní. Útok na 128 bitovou variantu je často realizován v kombinaci se slovníkovým útokem. To z důvodu, že se jedná o časově poměrně náročnou činnost. Obrana proti takovému útoku spočívá v časté změně šifrovacího klíče, což zabraňuje jeho prolomení. Pokud je přesto prolomen, je po změně klíče původní klíč neplatný. Útočník tak nemůže zneužít získané údaje k připojení do sítě. Další možností jak se bránit je omezení počtu pokusů o autentizaci. To však může způsobovat problémy i při autentizaci oprávněného uživatele.

5.2.2 Injekce paketu

Při tomto útoku dochází ke změně hlavičky paketu nebo se zcela nahradí datový blok. Lze provádět díky tomu, že se inicializační vektor nemusí měnit pro každý paket. Pokud se

nám podaří získat nešifrovaný text nějakého zachyceného šifrovaného paketu, lze z něj odvodit šifrovací sekvenci. Následně zašifrujeme námi zvolený text pomocí této šifrovací sekvence. Tento podvrhnutý text bude dešifrován jako platný.

5.2.3 FMS

Název tohoto útoku je odvozen od jmen svých autorů. Těmi jsou Fluhrer, Mantin a Shamir, kteří útok popsali již v roce 2001. Tento útok využívá zranitelnosti proudové šifry RC4, kdy některé IV inicializují pseudonáhodný generátor následujícím způsobem. První bajt šifry je vygenerován za využití bajtu z klíče. To částečně odhaluje informaci o privátním klíči. Také se zde využívá znalosti, že první bity IP a ARP paketů jsou hexadecimální hodnotou 0xAA. S využitím těchto znalostí stačí útočníkovi zachytit dostatečné množství paketů, respektive inicializačních vektorů. Z nich lze pak odvodit tajný klíč.

Obrana

Vhodnou obranou je:

- používat nejdelší možný klíč (raději WEP128, než WEP64).
- nepoužívat příliš jednoduchá hesla (např. 12345, heslo, dlink, atd) Taková hesla jsou často součástí slovníku a jejich prolomení je o to jednodušší.
- používat bezpečná hesla. Kombinace velkých a malých písmen obsahují interpunkční znaménka nebo číslice. Více v kapitole 6.2 Problematika hesel.
- provádět změnu klíče.

5.3 PSK CRACKING

Bezpečnost WPA-PSK je založena na jednom sdíleném hesle, které je třeba k připojení do sítě. Pokud je toto heslo odhaleno, útočníkovi nic nebrání v přístupu. Útočníkovi stačí odposlechnout jednu jedinou výměnu paketů při autentizaci klienta, kterou není problém vynutit zasláním deautentizační ho rámce. V takovém případě se stanice musí odpojit a při následném připojení znovu autentizovat. Deautentizační rámce jsou identifikovány MAC adresou přístupového bodu, ta lze ale také podvrhnout. Na základě odposlechnuté autentizace (WPA handshake) může zkoušet hesla ze slovníku i mimo dosah sítě.

Obrana

Jelikož je bezpečnost bezdrátové sítě založena na jednom sdíleném hesle, tak vhodnou obranou proti útoku na WPA-PSK je použití dostatečně silného hesla. Více v kapitole 6.2 Problematika hesel.

5.4 ANALÝZA PROVOZU

Analýza provozu je důležitá především ve firemním prostředí při zjišťování maximální dostupnosti sítě. Je důležité, aby síť byla provozována bez jakýchkoliv výpadků, které mohou mít vliv na dostupnost důležitých informací. Mezi nejznámější analyzátory provozu patří určitě analyzátor paketů Wireshark. Ten je vyvíjen jako open source, což znamená, že

jeho zdrojové kódy jsou volně k dispozici. Po spuštění programu vybereme rozhraní, které bude zachytávat komunikaci v promiskuitním módu (jinak řečeno monitorovacím módu) a spustíme zachytávání provozu. Jednotlivé parametry zachytávaných paketů (například zdrojové adresy a porty) mohou být pomoci filtru skryty. Neznamená to však, že o zachycená data přicházíme. Jsou pouze skryta z důvodu přehlednosti výpisu a mohou být kdykoliv opět zobrazena. Pokud známe tajný klíč, je možné dešifrovat zachycenou šifrovanou komunikaci. Každé provedené zachytávání může být uloženo do speciálních souborových formátů.

5.5 DENIAL OF SERVICE

Cílem většiny popsaných útoků je získání přihlašovacích údajů za účelem přístupu do bezdrátové sítě. Z názvu DoS (Denial of Service) lze odvodit, že tomu tak není. Cílem útoku typu DoS je vyřazení nějaké služby (většinou sítového připojení), počítače nebo dokonce celé sítě z provozu. Podstatou útoku je generování provozu a zahlcení systému velkým množstvím dotazů, které nestíhá zpracovávat. Při útoku na bezdrátovou sít se velmi často využívá v kombinaci s útokem MITM popsaným v následující kapitole. Útok je směrován proti přístupovému bodu za účelem vyřazení jeho činnosti z provozu. Existují dva způsoby jak přístupový bod vyřadit. Jedním z nich je způsob využívající protokol TCP/IP, který je realizován následujícím způsobem. Útočník se snaží generovat co nejvíce dotazů na jedno konkrétní zařízení. Toto zařízení přestává po nějaké době stíhat na tyto dotazy odpovídat a tím je vyřazeno z provozu. V dnešní době se však velká část výrobců snaží implementovat obranné mechanismy, aby zabránili možných zahlcením zařízení. Při detekci DoS útoku se zařízení snaží zablokovat IP adresu počítače, ze které dotazy přicházejí. Při distribuované variantě DDoS (Distributed Denial of Service) útoku dochází k zaplavování z více míst. Zařízení tak nestačí blokovat pouze jednu adresu útočníka. Druhou možností jak vyřadit přístupový bod z provozu je zarušení frekvence na které vysílá. To se provádí tak, že do blízkosti přístupového bodu útočník přidá další přístupový bod. Tento přidaný přístupový bod je nastaven tak, aby vysílal na stejné frekvenci. Tím dochází k tomu, že se signál stává spatně detekovatelným pro koncová zařízení. Výhodou pro útočníka je, že při provádění tohoto útoku, není třeba získávat přístup do sítě.

Obrana

Jelikož se DoS často využívá v kombinaci s MITM útokem je důležité zamezit právě možnost útoku MITM. Vhodnou obranou je také filtrování MAC adres nebo používání firewallu s dobrou analýzou příchozích paketů.

5.6 DICTIONARY ATTACK

Každý slovníkový útok je založen na postupném zkoušení, pomocí speciální aplikace, všech předem uložených hesel ve slovníku. Při nalezení správného hesla dojde k přihlášení a tím útok končí. Základem takové útoku je dostatečně kvalitní slovník. Na internetu lze

stáhnout již vytvořené slovníky[1], nebo si lze pomocí speciálního nástroje vytvořit slovník vlastní.

5.6.1 Pomocí grafické karty

Pro realizaci slovníkového útoku pomocí grafické karty je nutné mít grafickou kartu Nvidia s podporou technologie CUDA. Vyšší rychlost výpočtů spočívá v dělení složitějších výpočtů na jednodušší, které následně paralelně rozděluje mezi jednotlivé stream procesory. Více o této technologii v následujícím odkaze[2]. Vzhledem k tomu, že výkon grafické karty je několikanásobně vyšší, než je výkon procesorů, je vhodné její použití k útoku. Toho lze využít pro slovníkový útok na WPA klíč, kde počet vyzkoušených slov je během sekundy mnohonásobně vyšší.

Obrana

Největším bezpečnostním rizikem v předcházení tomuto útoku je lidský faktor. Uživatelé si často neprávně volí příliš jednoduchá hesla. Více o tom jak zvolit bezpečné heslo je možné zjistit v kapitole 6 Zásady zabezpečení.

5.7 MAN-IN-THE-MIDDLE

Podle názvu (muž uprostřed) lze odvodit, že se jedná o typ útoku, kdy se útočník dostává do pozice mezi přístupový bod a připojující se stanici. Cílem útočníka je přesměrování datového toku tak, aby mohl pohodlně odposlouchávat. Útočník je schopen zachytit a modifikovat přenášené zprávy bez vědomí komunikujících stanic. MITM útoky je možné využít například při útoku na bezdrátovou síť využívající ověřování uživatelů pomocí veřejných klíčů. Ze zachycené komunikace dokáže útočník zjistit IP adresy a vysílané SSID přístupového bodu. Za pomoci těchto informací může útočník vytvořit falešný přístupový bod se stejným SSID a použitým zabezpečením jako má originál. Aby na takto vytvořený přístupový bod nalákal uživatele, musí originál vyřadit z činnosti, což lze provést pomocí DoS útoku. Tím donutí uživatele, aby se připojovali místo k originálnímu přístupovému bodu k útočníkem podvrženému. Při zadání platných přihlašovacích údajů nedojde k přihlášení, ale útočník tak získá právě tyto platné přihlašovací údaje. Následně se může pomocí takto získaných údajů přihlásit přes originální přístupový bod.

Obrana

Obranou proti útokům typu MITM je použití vhodných autentizačních metod nebo využití VPN (Virtual Private Network). Možností jak odhalit takový útok je monitorování přístupových bodů. Více v kapitole 7 Bezpečnost v praxi.

[1] Například na adrese http://www.aircrack-ng.org/doku.php?id=faq#where_can_i_find_good_wordlists

[2] Nvidia CUDA http://developer.nvidia.com/what-cuda

6 Zásady zabezpečení

6.1 Jak zvolit

Neexistuje způsob jak zabezpečit svoji bezdrátovou síť proti neoprávněnému přístupu na 100%. V domácím prostředí většinou záleží na schopnostech uživatele. Konkrétně na tom, jak dobře dokáže nakonfigurovat přístupový bod. Ve firemním prostředí předpokládáme, že konfigurace bude provedena odborně. Vše pak záleží především na technickém vybavení. Více v kapitole 7 Bezpečnost v praxi.

6.2 Problematika hesel

Používání hesel je jedna z nejjednodušších a nejlevnějších metod zabezpečení. Existuje však mnoho způsobů jak heslo zjistit. Heslo může být odposlechnuto, zachyceno speciálním programem pro logování stisknutých kláves, vyzrazeno samotným uživatelem nebo prolomeno slovníkovým útokem. Lze tedy rozlišovat hesla, která jsou pro zabezpečení nejen bezdrátové sítě vhodná či nevhodná.

Heslo je nevhodné pokud:

- je možné ho najít ve slovnících.
- je kratší než osm znaků.
- použijeme například jméno, značku auta nebo název oblíbené hudební skupiny.
- použijeme pouze kombinaci čísel (datum narození).

Vhodná hesla:

- obsahují interpunkční znaménka nebo číslice (například 0-9, !@#$%^&*()_+|~-).
- jsou složená z kombinací velkých i malých písmen.
- jsou delší než osm znaků.

Po vytvoření hesla se lze přesvědčit o jeho kvalitě na webu projektu The Password Meter[3].

Pokud máme problém s vymyšlením dostatečně silného hesla, můžeme použít generátor hesel[4].

[3] Projekt The Pasword Meter na adrese http://www.passwordmeter.com/

[4] Generátor hesel na adrese http://darkvoice.dyndns.org/wlankeygen/

7 Bezpečnost v praxi

Shrnutí výhod a nevýhod jednotlivých typů zabezpečení. Všechny technické parametry jsou uvedeny v následujících tabulkách.

Tabulka 6 - Specifikace použitých zabezpečovacích metod [3]

	WEP	**WPA**	**802.11i (WPA2)**
Autentizace	Otevřená	EAP-TLS / PEAP	EAP-TLS / PEAP
Šifrování	Statický WEP	TKIP / CKIP	AES

Tabulka 7 - Odolnost proti jednotlivým útokům [3]

Typ útoku	**Míra odolnosti**		
Na integritu, důvěrnost dat, man in the middle	dobrá	lepší	nejlepší
falešná autentizace	nic moc	nejlepší	nejlepší
na slabý klíč	nic moc	nejlepší	nejlepší
falšované pakety	minimální	nejlepší	nejlepší
falešný přístupový bod	minimální	lepší	lepší
úroveň šifrování	pro domácí síť (40 – nebo 104bitový klíč; 24bitový vektor IV)	pro podnikovou síť (128bitový klíč; 48bitový vektor IV)	pro podniky i vládu (128+bitový klíč; 48bitový vektor IV)

Tabulka 8 - Uplatnění WEP, WPA a WPA2 [3]

	autentizace	**šifrování**	**použitelnost pro podnikové sítě**	**použitelnost pro domácí a malé sítě**
WEP	nulová	WEP	nic moc	dobrá
WPA (PSK)	PSK	TKIP	nic moc	nejlepší
WPA2 (PSK)	PSK	AES-CCMP	nic moc	nejlepší
WPA (plná)	802.1×	TKIP	lepší	dobrá
WPA2 (plná)	802.1×	AES-CCMP	nejlepší	dobrá

7.1 Domácí síť

Míra zabezpečení domácí sítě je často dána schopnostmi uživatele. Domácí sítě však nepředstavují příliš atraktivní cíle pro útočníky. Získat přístup do takové sítě je často mnohem náročnější než by se předpokládalo a vynaložené úsilí je neúměrné ceně získaných dat. Často se u takových sítí útočník zaměřuje hlavně na získání přihlašovacích údajů za účelem připojení se do sítě Internet. Vyšší požadavky na zabezpečení než u domácích sítí jsou kladeny u firemních sítí.

Při návrhu zabezpečení domácí sítě je nutné vycházet z požadavků uživatelů využívajících tuto síť. Existují uživatelé, kteří se domnívají, že nikdo nemá důvod útočit na jejich špatně nebo vůbec zabezpečenou sít. Na druhé straně se můžeme setkat s uživateli, kteří požadují i v domácím prostředí vysokou míru zabezpečení.

- **Změna továrního nastavení AP** - Toto je věc, kterou spousta lidí zanedbává. Pro přístup do konfigurace je nutné být do sítě připojen. To izoluju klienty, kteří nemají do sítě přístup. Avšak při prolomení zabezpečení bezdrátové sítě, neexistuje při nezměněných přihlašovacích údajích do konfigurace žádná překážka k připojení. Předem nastavená jména a hesla od výrobce zařízení, jsou všeobecně známá a není problém je dohledat v dokumentaci na Internetu. Například jméno admin, heslo admin nebo jméno admin, heslo 1234 jsou často používaná jako výchozí nastavení přímo od výrobce přístupových bodů.

- **Volba vhodných hesel** – Důležité je zvolit dostatečně silné heslo. Ideální je volba kombinace velkých a malých písmen obsahují interpunkční znaménka nebo číslice. Více v kapitole 9.2 Problematika hesel.

- **Zrušení vysílání SSID** - Tím, že zakážeme vysílání SSID, uděláme síť neviditelnou pro okolí. Existují však speciální nástroje, které dovedou zjistit SSID i když není vysíláno. Dále není vhodné požívat přístupové heslo do sítě shodné s SSID. Vypnutí SSID není povinnou součástí standardu 802.11, ale většina zařízení tuto možnost podporuje.

- **Filtrace MAC adres** - Hodí se pro zabezpečení domácích sítí nebo malých firemních sítí a to především jako doplněk k WEP nebo WPA (WPA2). Při útoku na síť využívající filtrování MAC adres není problém ověřit platnost použitých MAC adres a takovou adresu podvrhnout. To však útočníkovi zabere čas navíc a dělá tak pro něj útok o něco namáhavější.

- **Fyzická bezpečnost AP** - Fyzickou bezpečností je myšleno umístění síťových prvků na, neoprávněným osobám, nedostupná místa. V domácím prostředí to nebývá velký problém. V podstatě stačí mít přístupový bod uvnitř domu. Ve firemním prostředí pak například v zamčené technické místnosti.

- **Omezení dosahu** - Omezení dosahu přístupového bodu se používá, aby se signál nešířil zbytečně daleko. Například do okolních bytů v panelácích nebo do okolních domů a zahrad. Existují tři možnosti jak šíření signálu ovlivnit.

    - Použití směrové antény - Nahrazení klasické všesměrové antény směrovou anténou. Je nutné zakoupit nový hardware a je vhodné nejdříve ověřit, zda se tento nákup vyplatí.
    - Omezení výkonu - Jedná se o metodu, kdy lze omezit výkon stávající všesměrové antény na minimální avšak stále dostačující hodnotu. Některé levnější modelu tuto možnost nepodporují.
    - Strategické umístění - Je vhodné umístit přístupový bod do středu bytu tak, aby se minimum signálu šířilo mimo tento byt.

- **Aktivace bezpečnostních mechanismů** - Používání zabezpečovacích protokolů je jednou z nejdůležitějších části zabezpečení nejen domácí sítě. I přes všechny známé nedostatky protokolu WEP platí, že je lepší využívat právě jej, nežli nic. Dává to síti alespoň status, že se jedná o privátní síť nikoliv o veřejnou. Mnohem lepší je využít zabezpečení pomocí WPA (v domácím prostředí většinou WPA-PSK). Nejlepší možnou variantou je využití WPA2 také většinou v režimu PSK.

7.2 Firemní síť

Na zabezpečení firemních bezdrátových sítí jsou kladeny mnohem vyšší nároky, než je tomu u domácích bezdrátových sítí. Ve většině případů je požadována stejná míra zabezpečení jako u kabelové sítě. Výhody, které přináší používání bezdrátové sítě, jsou zřejmé. V první řadě je to lepší mobilita stanic. Druhou výhodou je snadnější instalace oproti kabelovým strukturovaným sítím. Na druhé straně je však velkou nevýhodou horší zabezpečení a nižší spolehlivost. Při rozhodování o instalaci takové sítě je proto nutné zvážit všechny výhody a nevýhody. Ve firmách je také často nutné připojovat se do interní sítě pomocí vzdáleného připojení přes veřejnou síť (Internet). Takové připojení je nutné zabezpečit. Nejhodnějším řešením je využití virtuální privátní sítě VPN (Virtual Private Network).

- **Monitorování přístupových bodů** - V rozsáhlých firemních sítích je nutné mít přehled o počtu a rozmístění přístupových bodů. Existují speciální programy, analyzátory sítě, které dovedou odhalit falešný přístupový bod. Jedním z nich je například NetStumbler. Problém spočívá v tom, že některý ze zaměstnanců může do sítě připojit nový nezabezpečený přístupový bod. V rámci bezpečnosti sítě by měli být o tomto problému zaměstnanci proškoleni.

- **Autentizační server** - Pokud navrhujeme zabezpečení pro firemní bezdrátovou síť, rozhodně bychom neměli volit zabezpečení WEP. Minimální vhodnou míru zabezpečení poskytuje až WPA-EAP. Využití autentizačního serveru, kdy ověření a následné povolení přístupu do sítě provádí právě autentizační server, je více než

vhodné. Autentizace při přihlašování do sítě by měla být vzájemná. To z důvodu, aby nemohl útočním podvrhnout falešný přístupový bod, čímž se zabraňuje útokům typu man in the middle.

- **Pokrytá oblast** - Je důležité minimalizovat přesah signálu do míst, kde je jeho výskyt zbytečný, mnohdy až nebezpečný. Obvykle firma nechce, aby signál její interní sítě byl zachytitelný mimo areál firmy. Například firemní parkoviště nemusí být pokryto signálem bezdrátové sítě. Vhodným řešením je omezení dosahu přístupového bodu nebo využití sektorové a směrové antény.

- **Bezdrátová zóna** - Oddělení bezdrátové sítě od kabelové sítě pomocí firewallu, který je nakonfigurován tak, aby povolil přístup pouze předem určeným MAC adresám.

- **DHCP** - Pro domácí síť je používání DHCP ideální volbou vzhledem k snadné konfiguraci. DHCP server přiděluje automaticky IP adresy z daného rozsahu. Není však schopen ověřit zda uživatel má potřebná oprávnění pro získání IP adresy. Při nastavení IP adres staticky (ručně) a vypnutém DHCP serveru jsme schopni minimalizovat bezpečnostní riziko v podobě neoprávněného získání platné IP adresy útočníkem.

  Vyhrazené rozsahy IP adres pro vnitřní sítě:
  - 10.0.0.0. až 10.255.255.255
  - 172.16.0.0 až 172.31.255.255
  - 192.168.0.0 až 192.168.255.255

  Většina přístupových bodů má od výrobce přednastavenou IP adresu 192.168.0.1. Útočník proto využívá této znalosti a zkouší tento rozsah jako první. V rámci zvýšení bezpečnosti je proto vhodné tento výchozí rozsah IP adres změnit na jiný.

- **VPN** - Pro zabezpečení domácí sítě je využití VPN zbytečně složitým řešením. Ve firemní síti je VPN vhodné především pro zaměstnance pracující z domova, připojující se do interní firemní sítě prostřednictvím veřejné sítě.

7.3 Veřejná síť

V případě veřejných bezdrátových sítí nejde ani tak o problém zabezpečení přístupu do bezdrátové sítě. Větším problémem je jak zabezpečit připojované stanice tak, aby nebylo možné zneužít osobní data uživatele. Důležitou věcí je určitě nainstalovaný firewall. Pro zabezpečení komunikace například do firemní sítě je vhodné používat VPN. Další možností je vypnutí sdílení souborů. Doporučuje se nezadávat čísla kreditních karet nebo hesla k účtům. Dále je vhodné odpojit se od bezdrátové sítě, pokud ji zrovna nepožíváte.

8 Wifileaks

Jedná se o projekt komunitního zaměřování bezdrátových sítí Wi-Fi. V České republice jsou stovky tisíc, možná i miliony, bezdrátových sítí Wi-Fi standardu 802.11 bgn (2,4 GHz). Pojďme je zaměřit s pomocí jednoduché mobilní aplikace pro Android a vytvořme kompletní mapu pokrytí. Zjistíme, jaké nejtypičtější zabezpečení Wi-Fi používáme, kde je podobných sítí nejvíce, jak se zpravidla jmenují. [20]

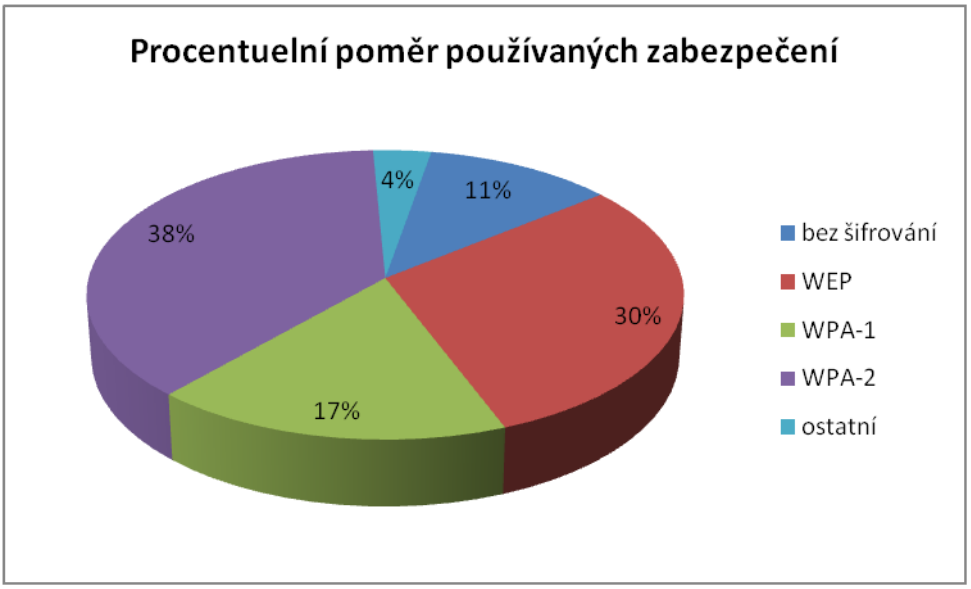
8.1 Nejčastější zabezpečení

V následující tabulce jsou uvedeny nejčastější typy zabezpečení bezdrátových sítí a jejich četnosti. Všechna data jsou uvedena z celkového počtu 678 592 dosud zaměřených sítí.

Tabulka 9 - Nejčastější zabezpečení [4]

bez šifrování	77 676×
WEP	203 008×
WPA-1	118 563×
WPA-2	255 489×
Ostatní	23 856×

Následující graf udává poměr mezi jednotlivými typy zabezpečení.



Obrázek 9 - Procentuelní poměr používaných zabezpečení

8.2 Nejčastější názvy sítí

V následující tabulce jsou uvedeny nejčastější názvy bezdrátových sítí a jejich četnosti. Všechna data jsou uvedena z celkového počtu 678 592 dosud zaměřených sítí. V tabulce je uvedeno celkem 120 880 zaměřených sítí, jejichž název patří mezi nejvíce používané. Zbytek tvoří sítě s méně rozšířeními názvy (například křestní jména nebo příjmení rodin).

Tabulka 10 - Nejčastější názvy sítí (SSID) [4]

VOIP	53 386×
Internet	21 684×
dlink	5 969×
doma	4 820×
default	4 744×
ZyXEL	3 131×
Airlive	2 608×
Eduroam	2 601×
TP-LINK	2 448×
FreeWifi	2 291×
Tenda	2 171×
ASUS	2 114×
Linksys	2 069×
NETGEAR	1 858×
Wifi	1 833×
MyWLAN	1 583×
T-Com	1 575×
Hpsetup	1 380×
home	1 320×
SFR WiFi Public	1 295×

Data z projektu Wifileaks byla aktualizována: 22:23:05, 24. dubna 2012

9 Praktická část

9.1 Použitý hardware

Zde popíšu hardware, který byl použit pro realizaci praktické části bakalářské práce.

Přístupový bod

Jako bezdrátový přístupový bod byl použit **D-Link DSL-2641B**

Rozhraní: 1 x RJ-11 ADSL port, 4 x RJ-45 10/100BASE-TX
Standard: IEEE 802.11g
Frekvenční pásmo: 2,4 GHz
Přenosová rychlost: až 54 Mbit/s
64/128bitové WEP šifrování dat
WPA/WPA2 zabezpečení s TKIP, podpora AES

Uživatelské PC

Jako uživatelské PC byl použit Notebook HP ProBook 4525s.

- AMD Turion II P540 Dual-Core Processor 2,40 GHz
- 4,00 GB RAM

Integrovaná sítová karta Broadcom 4313 sloužila k připojování k přístupovému bodu. Druhá síťová karta, miniaturní WiFi USB adaptér, byla použita v monitorovacím módu k zachytávání komunikace.

Mac adresa síťové karty - 00:1F:1F:C9:4F:8F

Mac adresa přístupového bodu - 02:AF:F7:AF:FC:6D

Jako připojující se klient byl též využíván mobilní telefon HTC Wildfire s MAC adresou 90:21:55:6D:FA:F2.

9.2 Použitý software

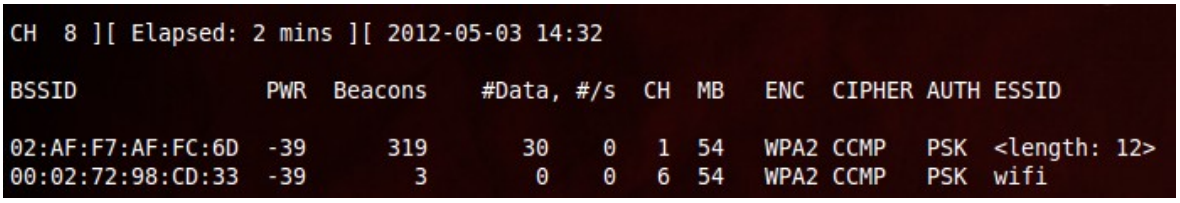
Software, který byl použit pro realizaci praktické části bakalářské práce.

Jako operační systém posloužila dvojice Windows 7 Professional Service Pack 1 a virtualizovaný systém BackTrack 5 R2. Vlastní útoky byly provedeny pomocí programu Aircrack-ng. K analýze paketů posloužil program Wireshark.

9.3 Odhalení skrytého SSID

Bezdrátová síť může být zabezpečena tak, že je vypnuto vysílání SSID. Pokud není SSID vysíláno, je nutné, aby uživatel znal SSID sítě při připojování. Když se chce připojit, pošle svoje SSID pomocí asociačního rámce v nešifrované podobě. Útočníkovi tak stačí zachytit tento rámec. Za pomoci programu Kismet dokáže ze zachyceného rámce zjistit SSID sítě.

Při skenování okolních bezdrátových sítí pomocí aplikace airodump-ng odhalíme i ty přístupové body, které nevysílají své SSID. Zjistíme pouze informace o délce SSID.



Obrázek 10 - Skryté SSID

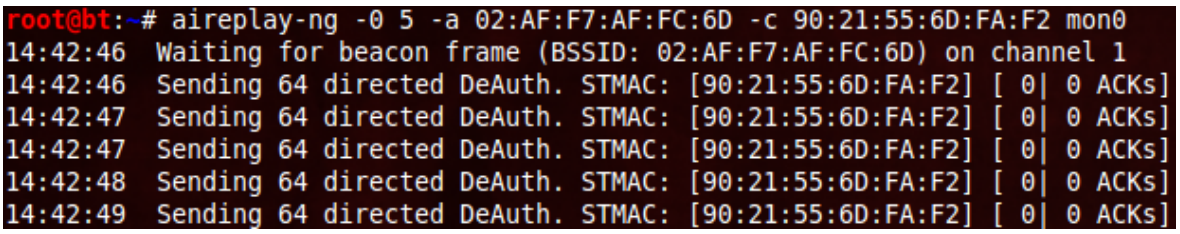
U bezdrátové sítě, která vysílá své SSID je vidět její název (wifi). U sítě, která své SSID nevysílá je zobrazeno místo názvu <lenght: 12>. To udává, že SSID sítě je název o délce dvanáct znaků.

Spustíme následující příkaz:

aireplay-ng -0 5 -a 02:AF:F7:AF:FC:6D -c 90:21:55:6D:FA:F2 mon0

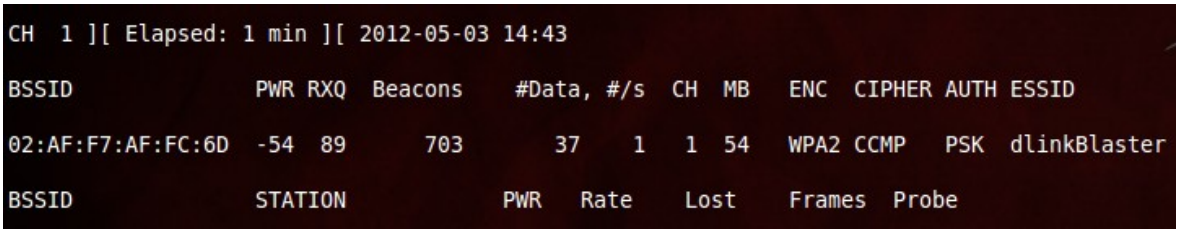
- -0 (--deauth) znamená deautentizační útok
- 5 počet zaslaných deautentizací
- -a 02:AF:F7:AF:FC:6D je MAC adresa přístupového bodu
- -h 90:21:55:6D:FA:F2 je MAC adresa klienta připojeného k síti
- mon0 je rozhraní bezdrátové karty, která bude útočit

Na následujícím obrázku lze vidět, jak probíhá deautentizace klienta od přístupového bodu.



Obrázek 11 - Zasílání deautentizací

Pokud vše proběhlo jak má, klient byl úspěšně deautentizován. Je nucen znovu se připojit k síti. Při následné autentizaci klienta dojde k zachycení procesu autentizace. Z této zachycené autentizace pak aplikace airodump-ng dokáže zjistit SSID sítě, protože je přenášeno v nešifrované podobě. To je poté zobrazeno ve sloupci ESSID. V mém případě se jednalo o síť s názvem dlinkBlaster.



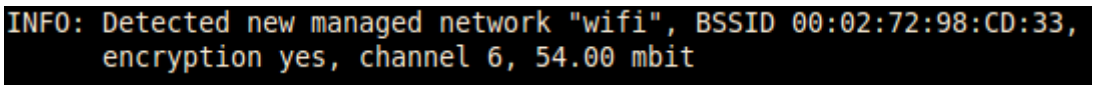
Obrázek 12 - SSID bylo odhaleno

Kismet

Kismet je nástroj pro vyhledávání a odposloucháváni bezdrátových sítí. Dokáže pracovat s jakoukoliv kartou, která podporuje monitorovací mód. Dokáže sledovat provoz 802.11b, 802.11a, 802.11g i 802.11n sítí. Pro operační systém Windows existuje alternativa v podobě programu Netstumbler.

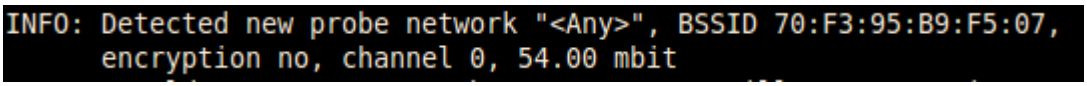
Při výchozím nastavení programu není v přehledu bezdrátových sítí zahrnuta položka udávající sílu signálu. Pokud o tom chceme mít přehled, je nutné upravit konfigurační soubor kismet_ui.conf. Položku „What columns do we display?“ doplnit o „signal“.

Pokud bezdrátová sít vysílá svoje SSID je normálně zachyceno. Na následujícím obrázku můžeme vidět, že byla nalezena síť s názvem wifi. Dále vidíme, že se jedná o zabezpečenou sít, na kterém kanálu vysílá a přenosovou rychlost.



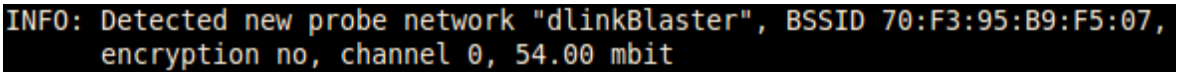
Obrázek 13 - Zachycení vysílaného SSID

Pokud bezdrátová síť nevysílá své SSID, je místo něj zobrazeno <Any>.



Obrázek 14 - Skryté SSID

Při pokusu o připojení uživatele do bezdrátové sítě, která nevysílá své SSID, dojde k zachycení asociačního rámce. Z něj pak program Kismet dokáže získat SSID sítě.



Obrázek 15 - Zachycení skrytého SSID

9.4 WEP cracking

V této kapitole budou provedeny a popsány dva útoky na zabezpečení WEP. První z nich se bude zaměřovat na prolomení bezdrátové sítě zabezpečené pomocí 64 bitové varianty WEP. Druhý útok bude zaměřen na 128 bitovou variantu WEP.

9.4.1 Útok na WEP64

Jako první byl zvolen útok na 64 bitovou variantu WEP. Tento zabezpečovací algoritmus využívá inicializační vektor o velikosti 24 bitů. Více v kapitole 4.3 WEP. To nám zaručuje maximálně 2^24 = 16777216 hodnot. Při běžném sítovém provozu dojde poměrně brzy k vyčerpání všech možných kombinací a generované klíče se tak začnou opakovat.

Před začátkem provádění útoku je třeba nastavit přístupový bod. Nastavení je zachyceno v následující tabulce.

Tabulka 11 - Nastavení AP při útoku na WEP64

IP adresa AP	192.168.1.1
Maska	255.255.255.0
SSID sítě	testWEP64
Kanál	2.437 GHz - CH 6
Šifrování	WEP
Délka klíče	64 bitů

Výpis všech síťových rozhraní a zjištění názvu bezdrátové síťové karty:

iwconfig

Vytvoření virtuálního rozhraní mon0 s podporou monitorovacího módu:

airmon-ng start wlan0

Po úspěšném vytvoření rozhraní mon0 je vypsáno monitor mode enabled on mon0.

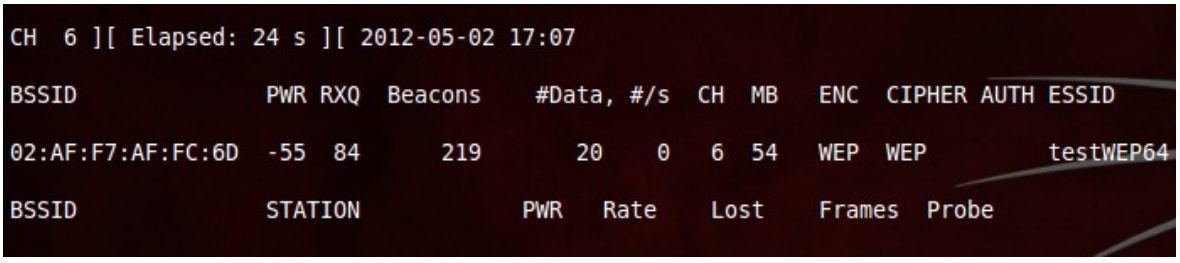
Pro skenování okolních sítí použijeme příkaz:

airodump-ng mon0

Takto zapsaný příkaz skenuje všechny kanály, lze upravit přepínačem tak, aby skenoval jen uživatelem zvolené kanály. Například námi zvolený kanál číslo 6 (2.437 GHz):

airodump-ng --channel 6 mon0

Získané informace o bezdrátové síti:



Obrázek 16 - Skenování sítí

Důležité je si zapamatovat:

- **BSSID** - MAC adresa přístupového bodu
- **CH** - číslo kanálu sítě.

Další parametry jsou:

- **PWR** - síla signálu
- **Beacons** - počet přijatých beacon rámců
- **#Data** - počet zachycených datových paketů
- **#/s** - počet zachycených datových paketů za posledních 10 sekund
- **MB** - maximální podporovaná rychlost přístupového bodu
- **ENC** - použitý šifrovací algoritmus
- **CIPHER** - detekovaná šifra
- **AUTH** - autentizací metoda
- **ESSID** - název sítě

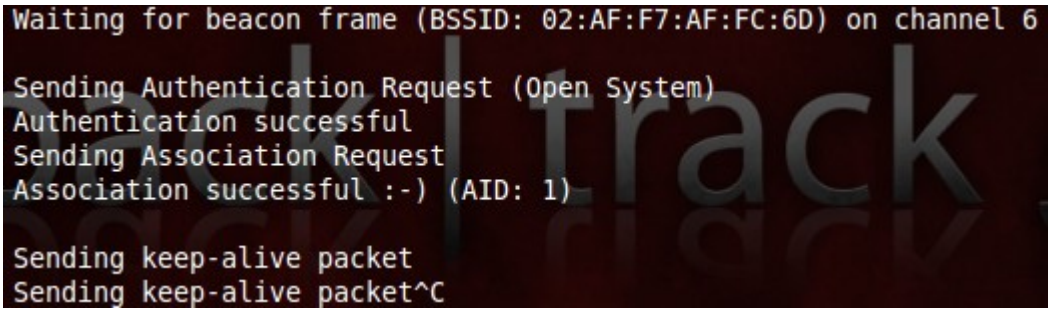
Zachytávání a ukládání komunikace na konkrétním přístupovém bodu a kanálu číslo 6, na kterém tento AP vysílá. Přepínač --ivs udává, že budou zachytávány pouze inicializační vektory:

airodump-ng -w testWEP64 -c 6 --bssid 02:AF:F7:AF:FC:6D --ivs mon0

Provedení falešné autentifikace k přístupovému bodu:

aireplay-ng -1 5000 -q 10 -a 02:AF:F7:AF:FC:6D -h 00:1F:1F:C9:4F:8F mon0

Pokud je pokus úspěšný, vypíše se:



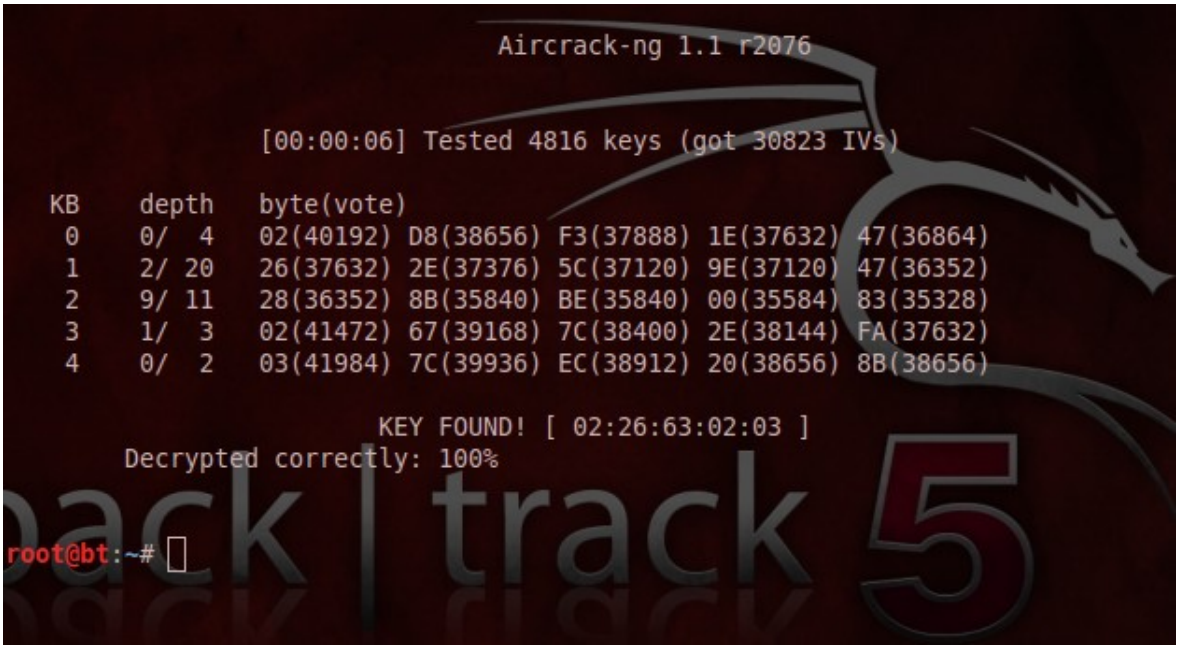
Obrázek 17 - Falešná autentifikace

Generování ARP dotazů pro zachytávání více paketů a rychlejší nalezení klíče:

aireplay-ng -3 -b 02:AF:F7:AF:FC:6D -h 00:1F:1F:C9:4F:8F mon0

Prolomení hesla po získání dostatečného množství paketů:

aircrack-ng testWEP64.ivs



Obrázek 18 - Prolomení WEP64 klíče

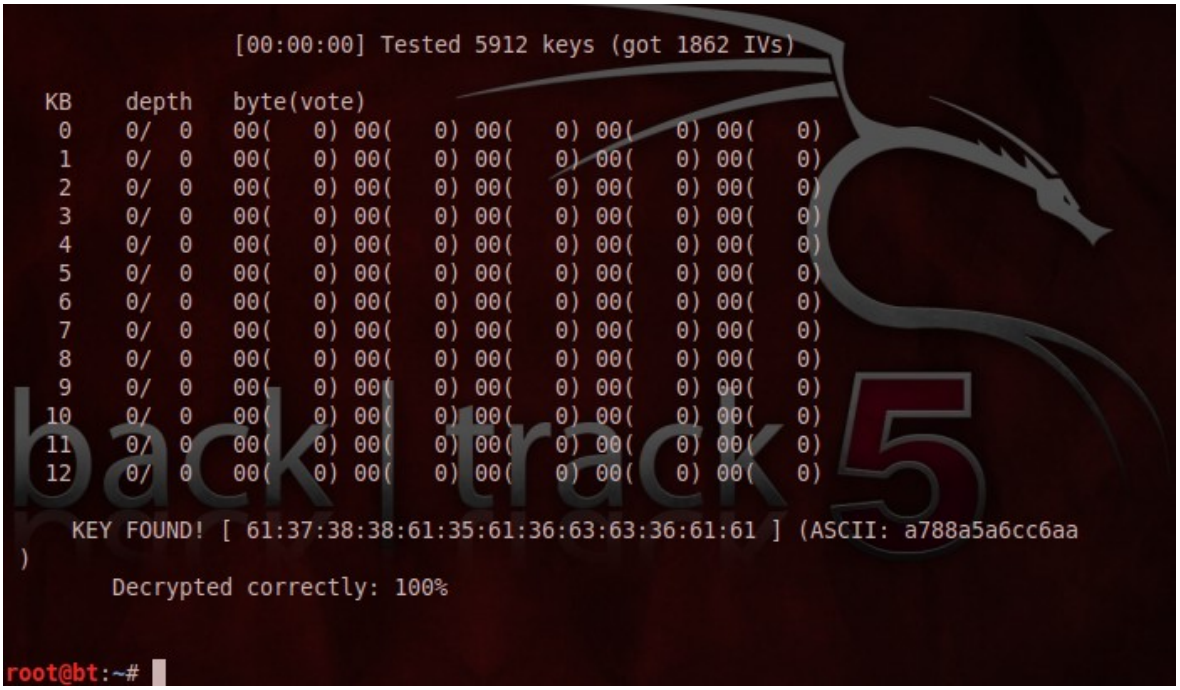
9.4.2 Útok na WEP128

Jako druhý byl realizován útok na 128 bitovou variantu WEP. Rozdíl oproti WEP64 je v délce klíče. WEP64 využívá na šifrovanou část 40 bitů, WEP128 pak 104 bitů. Velikost inicializačního vektoru je pro obě varianty 24 bitů. Jelikož postup je stejný jako u předchozí varianty, rozhodl jsem se pro malou změnu. Útok bude realizován pomocí slovníkového útoku.

Testování hesel zahájíme příkazem:

aircrack-ng -w mujSlovnik.lst testWEP128.cap

kde přepínač -w udává cestu k souboru obsahující slovník a následuje název souboru, ve kterém je zachycena komunikace.



Obrázek 19 - Prolomení WEP128 klíče

9.5 WPA cracking

V této kapitole se budu věnovat prolomení bezdrátové sítě zabezpečené pomoví WPA v režimu PSK. Při zvoleném slovníkovém typu útoku je velice důležité zvolit správný slovník. Jedná se o seznam, čítající spoustu běžně používaných hesel. Více o slovníkovém útoku v kapitole 5.6 Dictionary attack.

Před začátkem provádění útoku je třeba nastavit přístupový bod. Nastavení je zachyceno v následující tabulce.

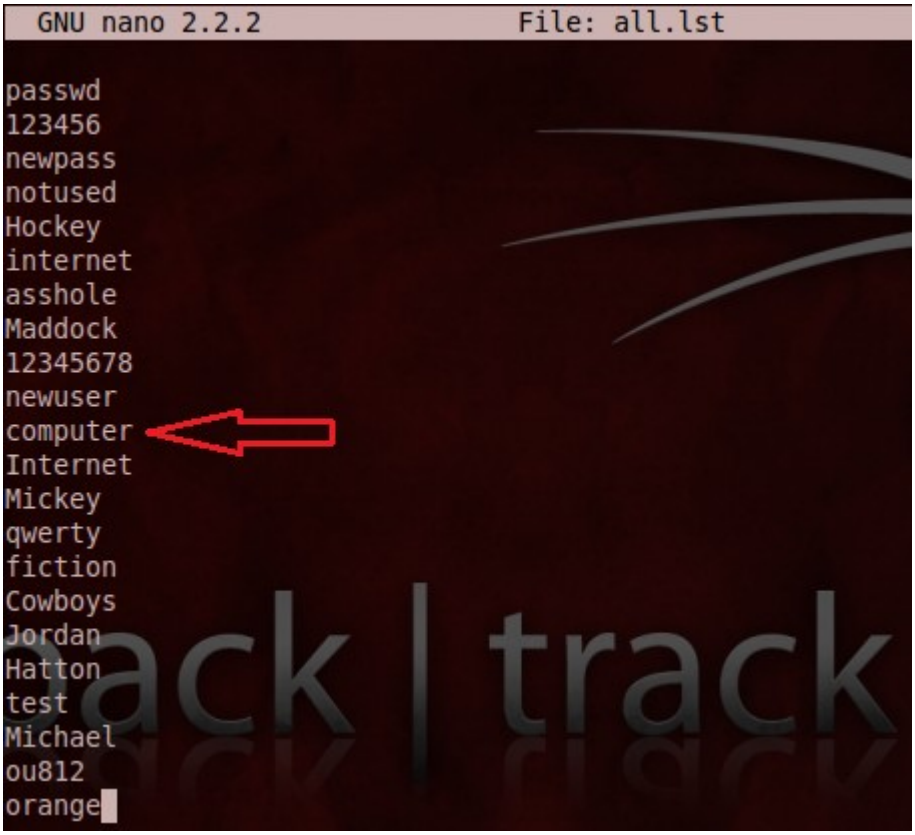
Tabulka 12 - Nastavení AP při útoku na WPA

IP adresa AP	192.168.1.1
Maska	255.255.255.0
SSID sítě	testWPA
Kanál	2.437 GHz - CH 6
Šifrování	WPA
Režim	PSK
Tajný klíč	computer

Přístupové heslo bylo zvoleno tak, aby bylo obsaženo ve mnou zvoleném slovníku. Použil jsem slovník, který je k naleznutí v následujícím odkazu jako zabalený soubor all.gz o velikosti 11,5 MB:

ftp://ftp.openwall.com/pub/wordlists/

O tom, že je heslo obsaženo ve slovníku, jsem se přesvědčil otevřením souboru v některém z textových editorů. Já jsem použil jednoduchý terminálový editor Nano.



Obrázek 20 - Část slovníku all.lst

Podstata útoku spočívá v zachycení procesu autentizace, který je popsán v teoretické části. To lze provést dvěma způsoby:

- **Pasivně** - útočník zachytává komunikaci v síti a vyčkává na připojení nového klienta. Ten musí být nejprve autentizován.
- **Aktivně** - útočník monitoruje síť. Zjišťuje, že k přístupovému bodu je připojen jeden či více klientů. Toho lze využít tak, že zasílá deautentizační rámce a vynutí si tak u připojených klientů novou autentizaci.

Samotné zachytávání je spuštěno příkazem:

airodump-ng --bssid 02:AF:F7:AF:FC:6D -w testWPA --channel 6 mon0

Tentokrát však bez přepínače --ivs, protože potřebuje zachytávat celé pakety a ne jenom inicializační vektory.

Deautentizace připojeného klienta se provádí pomocí aplikace aireplay-ng zadáním příkazu:

aireplay -0 5 -a 02:AF:F7:AF:FC:6D -c 90:21:55:6D:FA:F2 mon0

kde -0 udává typ útoku deauth, číslo 5 znamená počet deautentizačních paketů, přepínač -a upřesňuje MAC adresu přístupového bodu a přepínač -c MAC adresu cílové stanice. Mon0 na konci příkazu udává rozhraní, kterým se bude útočit.

K získání samotného hesla ze zachycené komunikace slouží aplikace aircrack-ng. Testování hesel zahájíme příkazem:

aircrack-ng -w all.lst testWPA.cap

kde přepínač -w udává cestu k souboru obsahující slovník a následuje název souboru, ve kterém je zachycena komunikace (4-Way Handshake).

Při neúspěšném útoku se vypíše hláška „Passphrase not in dictionary“, které oznamuje, že heslo není ve slovníku obsaženo. Je tedy nutné zvolit kvalitnější, obsáhlejší slovník.

Na následujícím obrázku lze vidět výstup aplikace při úspěšném dokončení útoku.

Obrázek 21 - Prolomení WPA klíče

Nás nejvíce zajímá řádek obsahující KEY FOUND! [computer], kde je v hranatých závorkách uvedeno přístupové heslo.

Shrnutí

Jak již bylo zmíněno v teoretické části v kapitole 5.3 PSK Cracking je bezpečnost bezdrátové sítě zabezpečené pomocí WPA v režimu PSK založena na jednom sdíleném hesle. Toto heslo by proto mělo být zvoleno dostatečně silné, aby dokázalo odolat právě výše realizovanému útoku slovníkového typu. Více o tom jak zvolit kvalitní heslo je možné najít v kapitole 6.2 Problematika hesel.

9.6 Nástroj WIFITE

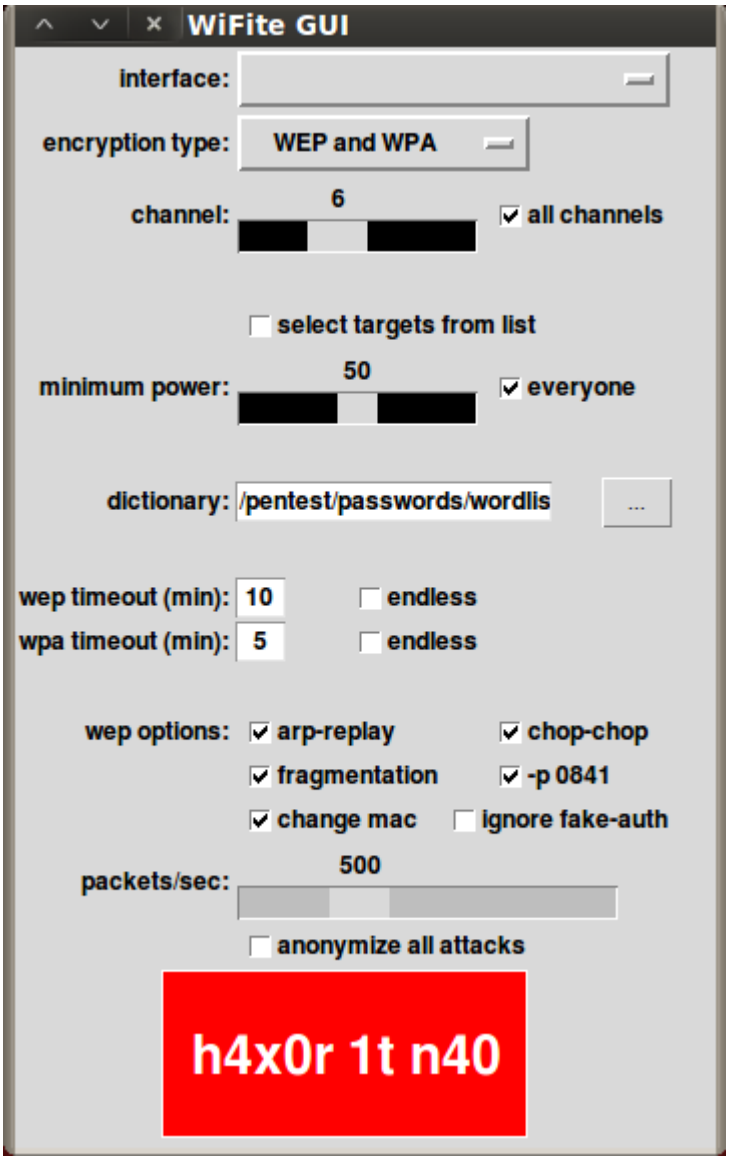
Jedním z používaných nástrojů pro získání přihlašovacích údajů do bezdrátové sítě je WIFITE. Ten je napsaný v jazyce Python. Pro chod aplikace je nutné pracovat v některé

z distribucí Linuxu. Ideálním systémem je BackTrack, kde jsou již všechny potřebné součásti nainstalovány.

Pokud je použita některá jiná distribuce, je nutné nainstalovat:

- macchanger,
- python,
- pyrit,
- aircrack-ng.

WIFITE je možné spouštět jak v textovém tak v grafickém režimu. Pokud aplikace nenalezne žádnou bezdrátovou síťovou kartu, vypíše chybovou hlášku (the program is unable to continue and will now exit) a dojde k jejímu ukončení. Na následujícím obrázku je zachycena úvodní obrazovka grafického režimu.



Obrázek 22 - WIFITE - grafické rozhraní

Význam jednotlivých položek v hlavním oknu aplikace:

- **Interface** - volba síťového rozhraní, které bude prostřednictvím aplikace WiFite útočit (například wlan0).
- **Encryption type** - můžeme zvolit jednu z následujících možností:
    - WEP - při skenování sítí v dosahu se budou zobrazovat pouze ty, které jsou zabezpečené pomocí WEP.
    - WPA - analogicky k první možnosti se zobrazují pouze sítě zabezpečené pomocí WPA.
    - WEP and WPA - zahrnuje obě předchozí možnosti.
- **Channel** - volba kanálu v rozsahu od 1 do 14. zašktrtnutím možnosti "all channels" budou skenovány všechny kanály.
- **Minimum power** - minimální úroveň síly signálu. Výběr hodnoty v rozmezí od 1 do 100. Zaškrtnutím možnosti "everyone" budou zahrnuty všechny hodnoty. Zaškrtnutím možnosti "select targets from list" dostává uživatel možnost vybrat si ze seznamu naskenovaných sítí tu, kterou bude on sám požadovat.
- **Dictionary** - používá se pří slovníkovém útoku na zabezpečení WPA. Je to cesta k souboru obsahující slovník, ze kterého budou zkoušena hesla.
- **WEP/WPA timeout** - hodnota v minutách udává čas, po který se bude program pokoušet zachytávat. Zaškrtnutím možnosti "endless" se čas nastaví na nekonečno.
- **Wep options** - zaškrtnutím jednotlivých možností volíme, které metody útoku budou použity na prolomení zabezpečení WEP.
- **packets/sec** - hodnota od 100 do 1500 udává četnost paketů, které budou zasílány.
- **anonymize all attacks** - touto volbou zajistíme anonymitu všech prováděných útoků.
- **h4x0r 1t n40** - kliknutím na velké červené tlačítko zahájíme útok s požadovaným nastavením.

10 Závěr

Bakalářská práce představila v teoretické části oblast bezdrátových sítí, která je v dnešní době vzhledem k masivnímu rozšíření těchto zařízení podporujících bezdrátové technologie Wi-Fi poměrně široká. Je představována a využívána množstvím běžně používanými zařízeními jako jsou chytré mobilní telefony, tablety nebo notebooky. Zároveň roste i popularita bezdrátových sítí a jsou hojně využívány jak ve firemním, tak v domácím prostředí.

Ve výše uvedených kapitolách byly popsány jednotlivé standardy IEEE 802.11, metody bezdrátového přenosu dat, zabezpečovací mechanismy, typy útoků a zásady zabezpečení bezdrátových sítí.

V praktické části bakalářské práce jsem si ověřil znalosti získané během vypracovávání teoretické části. Provedl a popsal jsem jednotlivé útoky, které využívají známých bezpečnostních mezer jednotlivých zabezpečovacích mechanismů. Při realizaci praktické části jsem si ověřil jak nevhodné je použití zabezpečení WEP. Toto zabezpečení využívá statického klíče a slabé autentiazace. Prolomení takto zabezpečené sítě není obzvláště složitým úkolem. Postačí pouze zachytit dostatečné množství inicializačních vektorů. Přestože je použití WEP mnohem lepší než naprosto nezabezpečená síť, doporučuji používat minimálně WPA v režimu PSK. Kdy je ovšem bezpečnost sítě založena na jednom sdíleném hesle. Toto heslo je třeba zvolit dostatečně silné, aby bylo imunní vůči útoku slovníkového typu. Tomu jak správně zvolit heslo jsem věnoval jednu z kapitol. Další součástí práce je řekněme stručný návod jak ovlivnit míru zabezpečení domácí i firemní sítě.

Tato práce by tak měla být vhodná jak pro běžného uživatele, tak pro správce sítě. Ti by zde měli najít odlišný pohled, pohled potencionálního útočníka, na zabezpečení. Práce poukazuje na mezery v zabezpečení, kterých útočník zneužívá. Cílem by tak mělo být poučit čtenáře v oblasti zabezpečení bezdrátových sítí a doporučit vhodná bezpečnostní opatření tak, aby dokázal předcházet možným útokům na jím spravovanou bezdrátovou síť.

11 Použité zdroje

11.1 Literatura

[1] BIGELOW, Stephen J. *Mistrovství v počítačových sítích*: *správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.

[2] ZANDL, Patrick. *Bezdrátové sítě WiFi*: *praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003, 190 s. ISBN 80-722-6632-2.

[3] PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G. Vyd. 1. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.

[4] CARROLL, Brandon. Bezdrátové sítě Cisco: autorizovaný výukový průvoce. 1. vyd. Brno: Computer Press, 2011, 478 s. Samostudium. ISBN 978-80-251-2884-8.

[5] BOUŠKA, Petr. *Samuraj-cz* [online]. 03.11.2009 [cit. 08.04.2012]. Dostupné z: <http://www.samuraj-cz.com/clanek/cisco-wifi-zakladni-principy-a-protokoly/>.

[6] VALÁŠEK, Michal A. Politika hesel: všechno co víte, je špatně. In: *Secpublica.cz*: *securitas, res publica // bezpečnost, věc veřejná* [online]. 12.3.2012 [cit. 08.04.2012]. Dostupné z: <http://www.secpublica.cz/articles/3-politika-hesel-vsechno-co-vite-je-spatne>.

[7] DARKAUDAX. How to Crack WPA/WPA2. In: *Aircrack-ng* [online]. [cit. 08.04.2012]. Dostupné z: <http://aircrack-ng.org/doku.php?id=cracking_wpa>.

[8] WI-FI ALLIANCE. *Wi-Fi CERTIFIED™*: *makes it Wi-Fi* [online]. 1999 [cit. 08.04.2012]. Dostupné z: <http://www.wi-fi.org/knowledge-center/glossary>.

[9] ŠTRAUCH, Adam. Aircrack-ng: slovníkový útok na WPA-PSK. In: *Root.cz*: *Informace nejen ze světa Linuxu* [online]. 20. 10. 2008 [cit. 08.04.2012]. Dostupné z: <http://www.root.cz/clanky/aircrack-ng-slovnikovy-utok-na-wpa-psk/>.

[10] Aircrack-ng s podporou nVidia CUDA. In: *Airdump.cz*: *security wifi hacking cracking exploity* [online]. [cit. 08.04.2012]. Dostupné z: <http://airdump.cz/aircrack-ng-podporuje-nvidia-cuda/>.

[11] FAQ. *Aircrack-ng* [online]. 19.11.2006, 09.04.2012 [cit. 11.04.2012]. Dostupné z: <http://www.aircrack-ng.org/doku.php?id=faq#where_can_i_find_good_wordlists>.

[12] WRIGHT, Josh. COWPATTY: ATTACKING WPA/WPA2-PSK EXCHANGES. *Willhackforsushi* [online]. [cit. 11.04.2012]. Dostupné z: <http://www.willhackforsushi.com/Cowpatty.html>.

[13] NVIDIA. What is CUDA. *NVIDIA*: *Developer Zone* [online]. [cit. 11.04.2012]. Dostupné z: <http://developer.nvidia.com/what-cuda>.

[14] Wifite: automated wireless auditor. GOOGLE PROJECT HOSTING. *Http://code.google.com* [online]. [cit. 11.04.2012]. Dostupné z: <http://code.google.com/p/wifite/>.

[15] TODNEM, Jeff. *The Password Meter* [online]. v.2.0. [cit. 11.04.2012]. Dostupné z: <http://www.passwordmeter.com/>.

[16] MICHAEL G. *WLAN Key Generator* [online]. 16.03.2006 [cit. 11.04.2012]. Dostupné z: <http://darkvoice.dyndns.org/wlankeygen/>.

[17] Hacking WiFi sítí. In: Wiki.airdump.cz [online]. [cit. 2012-05-03]. Dostupné z: <http://wiki.airdump.cz/Hacking_WiFi_sítí >.

[18] STRÁNSKÝ, Petr. Historie Wi-Fi: od FHSS k bezdrátu. In: Svět hardware: vše ze světa počítačů [online]. 2009 [cit. 2012-05-03]. Dostupné z: <http://www.svethardware.cz/art_doc-E8854472EA5653EBC1257636003B03D0.html>.

[19] PUŽMANOVÁ, Rita. WLAN konečně bezpečné. In: Lupa.cz [online]. 2004 [cit. 2012-05-03]. Dostupné z: <http://www.lupa.cz/clanky/wlan-konecne-bezpecne/>.

[20] Wifileaks: Komunitní zaměřování Wi-Fi [online]. [cit. 2012-05-03]. Dostupné z: <http://www.wifileaks.cz>.

11.2 Zdroje obrázků

[1] ZANDL, Patrick. *Bezdrátové sítě WiFi*: *praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003, 190 s., str. 7, ISBN 80-722-6632-2.

[2] ZANDL, Patrick. *Bezdrátové sítě WiFi*: *praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003, 190 s., str. 8, ISBN 80-722-6632-2.

[3] HEDY KIESLER MARKEY et al. SECRET COMMUNICATION SYSTEM [patent]. 2292387. Dostupné z: <http://www.google.com/patents?vid=USPAT2292387>.

[4] WLAN Security Introduction. In: H3C.com [online]. [cit. 2012-05-03]. Dostupné z: <http://www.h3c.com/portal/Products___Solutions/Technology/WLAN/Technology_Introduction/200812/624019_57_0.htm#_Toc213669064>.

[5] Hacking WiFi sítí. In: Wiki.airdump.cz [online]. [cit. 2012-05-03]. Dostupné z: <http://wiki.airdump.cz/w/images/Wep.png>.

[6] ZANDL, Patrick. *Bezdrátové sítě WiFi*: *praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003, 190 s., str. 128, ISBN 80-722-6632-2.

11.3 Zdroje tabulek

[1] STRÁNSKÝ, Petr. Historie Wi-Fi: od FHSS k bezdrátu. In: Svět hardware: vše ze světa počítačů [online]. 2009 [cit. 2012-05-03]. Dostupné z: <http://www.svethardware.cz/art_doc-E8854472EA5653EBC1257636003B03D0.html>.

[2] ZANDL, Patrick. *Bezdrátové sítě WiFi*: *praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003, 190 s., str. 17, ISBN 80-722-6632-2.

[3] PUŽMANOVÁ, Rita. WLAN konečně bezpečné. In: Lupa.cz [online]. 2004 [cit. 2012-05-03]. Dostupné z: <http://www.lupa.cz/clanky/wlan-konecne-bezpecne/>.

[4] Wifileaks: Komunitní zaměřování Wi-Fi [online]. [cit. 2012-05-03]. Dostupné z: <http://www.wifileaks.cz/statistika/>.