Analýza zabezpečení firemních bezdrátových sítí

Analysis of Corporate Wireless Networks Security

Bc. Vítězslav Jílek

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Vítězslav JÍLEK**
Osobní číslo:	**A09733**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Analýza zabezpečení firemních bezdrátových sítí**

Zásady pro vypracování:

1. **Prostudujte a popište druhy zabezpečení firemních bezdrátových sítí**
2. **Diskutujte varianty možných útoků na firemní bezdrátové sítě**
3. **Analyzujte a popište kroky útočníka po průniku zabezpečením bezdrátové sítě**
4. **Simulujte a popište kontrolní proniknutí do firemní bezdrátové sítě**
5. **Zpracujte plošný přehled a vyhodnocení úrovně zabezpečení firem ve městech České Budějovice a Český Krumlov**
6. **Navrhněte odpovídající zabezpečení pro firemní bezdrátové sítě**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **[1] BARKEN, Lee. Jak zabezpečit bezdrátovou síť Wi-Fi. Praha : Computer Press, 2004. 176 s. ISBN 80-251-0346-3.**
2. **[2] DOSTÁLEK, Libor, a kol. Velký průvodce protokoly TCP/IP – bezpečnost. Praha : Computer Press, 2003. 571 s. ISBN 80-7226-849-X.**
3. **[3] EDNEY, John; ARBAUGH, William A. Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Boston : Addison-Wesley Professional, 2003. 480 s. ISBN 0-321-13620-9.**
4. **[4] MILLER, Stewart S. WiFi Security. Columbus : McGraw Hill Higher Education, 2003. 309 s. ISBN 0-071-41073-2.**
5. **[5] PECHAČ, Pavel. Šíření vln v zástavbě : modely pro plánování mobilních rádiových systémů. Praha : BEN – technická literatura, 2006. 108 s. ISBN 80-7300-186-1.**
6. **[6] PUŽMANOVÁ, Rita. Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. Praha : Computer Press, 2005. 184 s. ISBN 80-251-0791-4.**
7. **[7] PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z. Praha : Computer Press, 2006. 184 s. ISBN 80-251-1278-0.**
8. **[8] OHARA, Bob; PETRICK, Al. The IEEE 802.11 Handbook: A Designers Companion. Boston : Inst Elect & Electronic Engineers, 1999. 188 s. ISBN 0-738-11855-9.**

Vedoucí diplomové práce: **Ing. Petr Neumann, Ph.D.**
Ústav elektroniky a měření

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této diplomové práce je zmapovat úroveň zabezpečení firemních bezdrátových sítí a ukázat možnosti úniku firemních dat. V první části jsou shrnuty jednotlivé úrovně zabezpečení. Dále práce popisuje nedostatky zabezpečení bezdrátových sítí a známé útoky na tyto sítě. V následujících kapitolách jsou uvedeny kroky útočníka, které mohou následovat po proniknutí zabezpečením bezdrátové sítě. V praktické části práce je uveden reálný příklad varianty možného proniknutí do firemní sítě prolomením šifrování WEP. Následuje přehled úrovně zabezpečení bezdrátových sítí firem ve městech České Budějovice a Český Krumlov. Závěrem práce jsou stanovena doporučení pro nastavení zabezpečení firemních bezdrátových sítí.

Klíčová slova:

WEP, WPA, WPA2, šifrování, útoky, bezpečnost, firemní, 802.11, síť

ABSTRACT

The aim of this thesis is to research the security level of corporate wireless networks and describe the possible occurrence of corporate data leakage. The first section summarizes various levels of security. Further, it focuses on the lack of security of wireless networks and already known network attacks. The following chapters describe the steps hackers can take after they penetrate computer wireless network security systems. The practical section of the thesis presents the case study, which describes the likely corporate network hacking attacks through breaking WEP encryption. The last chapter summarizes corporate wireless networks security systems used in companies České Budějovice and Český Krumlov. In the conclusion of the thesis, the recommendations for corporate wireless networks security systems set up are specified.

Keywords:

WEP, WPA, WPA2, Encryption, Attacks, Security, Corporate, 802.11, Network

Poděkování:

Na tomto místě bych rád poděkoval vedoucímu mé diplomové práce panu Ing. Petru Neumannovi, Ph.D. za možnost zpracování tohoto tématu, dále za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce. Dále děkuji vedení soukromé firmy, které mi umožnilo na svém zařízení realizaci praktické části této práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 METODY ZABEZPEČENÍ BEZDRÁTOVÝCH SÍTÍ **11**
1.1 FYZICKÁ VRSTVA 11
1.2 LINKOVÁ VRSTVA 12
1.3 SÍŤOVÁ VRSTVA 14
1.4 APLIKAČNÍ VRSTVA 17
1.5 BLIŽŠÍ POHLED NA VYBRANÉ METODY 19
1.5.1 Potlačení vysílání SSID 19
1.5.2 Filtrace MAC adres 20
1.5.3 WEP 20
1.5.4 Pokusy o vylepšení WEP 22
1.5.5 WPA/WPA2 23
2 VARIANTY ÚTOKŮ NA BEZDRÁTOVÉ SÍTĚ **28**
2.1 PASIVNÍ ÚTOKY 30
2.1.1 Skenování sítí - Wardriving a Warchalking 30
2.1.2 Odposlech a identifikace dat 31
2.2 AKTIVNÍ ÚTOKY 31
2.2.1 Zneužití cizí MAC adresy 31
2.2.2 Útok na WEP 33
2.2.3 Útok na WPA 37
2.2.4 Zamítnutí služby (DoS, Denial of Service) 40
2.2.5 Man-in-the-middle 43
3 KROKY ÚTOČNÍKA PO PRŮNIKU ZABEZPEČENÍM BEZDRÁTOVÉ SÍTĚ **45**
3.1 ZÍSKÁVÁNÍ INFORMACÍ 46
3.2 SKENOVÁNÍ SÍTĚ 47
3.3 ZÍSKÁNÍ PŘÍSTUPU 48
3.4 UDRŽENÍ PŘÍSTUPU 49
3.5 ZAMETÁNÍ STOP 50
II PRAKTICKÁ ČÁST **51**
4 UKÁZKA PRONIKNUTÍ DO FIREMNÍ BEZDRÁTOVÉ SÍTĚ **52**
4.1 VYBAVENÍ 52
4.2 ZJIŠTĚNÍ WEP KLÍČE 54
5 PŘEHLED ÚROVNĚ ZABEZPEČENÍ FIREM V REGIONU **61**
5.1 PŘEDPOKLADY PRO MĚŘENÍ A ANALÝZU 61
5.2 POSTUP MĚŘENÍ 61
5.3 ZPRACOVÁNÍ ZÍSKANÝCH DAT 64
5.4 VYHODNOCENÍ 64
5.5 ZÁVĚREČNÉ POROVNÁNÍ 71
6 BEZPEČNOST NENÍ PRODUKT, ALE PROCES **72**

6.1 BEZPEČNOSTNÍ DESATERO 72
6.2 VLIV LIDSKÉHO FAKTORU NA BEZPEČNOST SÍTĚ 73
6.3 IDEÁLNÍ ŘEŠENÍ – KOMPLEXNÍ PŘÍSTUP 73
ZÁVĚR 75
ZÁVĚR V ANGLIČTINĚ 76
SEZNAM POUŽITÉ LITERATURY 78
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 81
SEZNAM OBRÁZKŮ 86
SEZNAM TABULEK 87
SEZNAM GRAFŮ 88
SEZNAM PŘÍLOH 89

ÚVOD

Během mého studia oboru Bezpečnostní technologie, jsem se setkal s mnoha způsoby zabezpečení hmotného a nehmotného majetku firem. Možnost krádeže nehmotného majetku přes metalické nebo bezdrátové připojení byla však zmíněna jen okrajově. Proto jsem si zvolil tuto problematiku jako téma mé diplomové práce, která snad přispěje dalším studentům k rozšíření znalostí o tomto tématu.

Bezdrátové sítě založené na standardu IEEE 802.11 jsou v dnešní době celosvětově nejrozšířenější bezdrátové sítě. Cenová dostupnost, mobilita, jednoduchá instalace těchto síťových prvků sebou přinesla rozšíření i mezi běžné uživatele. Dalšímu rozšíření pomohlo masové rozšíření notebooků s bezdrátovými síťovými kartami, a to hlavně u firemních uživatelů. Z mé každodenní praxe vyplývá, že většina těchto uživatelů nemá ani základní znalost zabezpečení těchto síťových prvků. Určitá jejich část je sice informována o možnosti různých úrovní zabezpečení, ovšem riziko napadení jejich dat přes bezdrátovou síť podceňují. A navíc s bezpečností jde ruku v ruce složitost nastavení, která není řešitelná uživatelsky příjemným nastavením.

Střední a velké firmy ročně investují desítky tisíc korun do zabezpečení svých firemních sítí, najímají si specializované firmy na provedení bezpečnostních auditů, zadávají pravidelné kontroly a testy specialistům. Stačí ovšem jeden pracovník, který nainstaluje do vnitřní sítě, nezabezpečený bezdrátový prvek a všechna předchozí zabezpečení, jsou proti tomuto ohrožení neúčinná.

Tento bezpečnostní problém se vyskytuje jak u soukromých firem, tak i státních institucí. Pro názornost rozsahu popisované situace uvádím bezpečnostní incident, kdy Správa určitého historického objektu, dokonce vědomě umožnila svému zaměstnanci nainstalovat nezabezpečený bezdrátový prvek do vnitřní počítačové sítě. Přes existenci kvalitního firewallu a mnohamilionové investice do fyzické ostrahy a zabezpečovacího systému, mohla přes tuto „bezpečnostní díru“ uniknout data právě o režimu fyzické ostrahy, nastavení bezpečnostního a požárního systému, dokumenty a fotografie z mobiliářů. V této diplomové práci se pokusím ukázat, jak snadné může být pro útočníka získání dat z interní sítě, pokud se dostane k vůbec nebo slabě zabezpečené bezdrátové síti. Z takto ucelených informací pak vyplynou doporučení pro nastavení zabezpečení bezdrátových sítí, která útočníka zásadně zpomalí nebo ho zcela odradí od pokusu o průnik.

I. TEORETICKÁ ČÁST

1 METODY ZABEZPEČENÍ BEZDRÁTOVÝCH SÍTÍ

V této kapitole budou uvedeny nejrozšířenější metody zabezpečení bezdrátových sítí. Některé velké firmy jako např. Cisco implementovaly do již existujících metod zabezpečení vlastní funkce a vylepšení. Protože však nedošlo k rozšíření těchto implementací mezi výrobci prvků bezdrátových sítí, tak tyto metody nejsou uvedeny.

Základní přehled metod zabezpečení si ukážeme v následující kapitole. Pro přehlednost jsou zařazeny do vrstev síťového modelu.

1.1 Fyzická vrstva

1) Potlačení vysílání SSID

Potlačení vysílání SSID (Service Set Identifier, název sítě) omezuje možnost detekce bezdrátové sítě náhodnými uživateli v dosahu signálu vaší sítě. Vypnutí vysílání SSID v přístupovém bodu zapříčiní, že AP ignoruje zprávy vysílaný klientem a klient je přinucen použít aktivní skenování sítě (vyhledávání s „napevno“ zadaným specifickým SSID). Každý uživatel sítě tedy musí znát svoje SSID, ale tento způsob zabezpečení odradí náhodné a málo znalé útočníky (kapitola 2.1.1).

2) Změna výchozího SSID, přihlašovacích údajů a kanálu přístupového bodu

Výchozí hodnoty SSID všech výrobců bezdrátových zařízení jsou publikovány v dokumentaci k zařízením a jsou tak známy potenciálním útočníkům. Vybrané příklady jsou uvedeny v příloze P I. Útočník tak je schopen zachytit tento identifikátor prostřednictvím bezdrátového rozhraní. Výchozí hodnota by měla být změněna i jako prevence před snadným přidružením do WLAN i nesofistikovaným útočníkem.

Změna výchozích přihlašovacích údajů zabrání útočníkovi, který pomocí odposlechu zjistí výrobce zařízení, podle toho vyhledá patřičné identifikační údaje, aby jejich aplikaci změnil nastavení AP a tím nám k němu zamezil přístup [28].

Analogicky je to i s výchozím nastavením kanálu. Pokud se vyskytují v jedné lokalitě dva nebo více přístupových bodů pracujících v různých sítích, může díky interferenci mezi těmito přístupovými body dojít k DoS (kapitola 2.2.4), tedy dojde k přehlcení sítě požadavky, pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele.

3) Vhodné umístění antény, mechanická ochrana přístupového bodu

Směrovost antény je velice důležitá pro zvýšení bezpečnosti. Útočník se tak musí pro přístup do WLAN dostat do oblasti obsloužené jejím signálem. Pokud je to možné, je výhodné používat směrové, nikoli všesměrové antény [23]

Přístupové body bývají často umístěny ve veřejných částech budov, jako jsou střechy, chodby, haly, kanceláře typu OpenAIRE. Je nutné zamezit fyzický zásah neoprávněné osoby. Útočník by mohl přístupový bod např. fyzicky resetovat a změnit nastavené údaje.

4) Snížení vysílacího výkonu přístupového bodu, omezení úniku signálu

Některé přístupové body umožňují funkci snížení vysílacího výkonu. Snížením vysílacího výkonu dojde k omezení prostoru pokrytého signálem. Toto je zejména výhodné, pokud potřebujeme provozovat bezdrátové připojení např. pouze ve firemní zasedací místnosti.

Jedním z poněkud nestandardních řešení je použít stavební materiály budovy nebo místnosti s minimalizací průniku signálu (kovové prvky uzemnit), okna s termální izolací prostřednictvím kovové folie, metalické zástěny do oken místo rolet či závěsů, nátěr na bázi kovu pro vnitřní i venkovní stěny (tyto kroky fyzicky lépe zabezpečí interní WLAN, ale omezí používání dalších bezdrátových technologií, které komunikují směrem ven, např. mobilní telefony) [12].

1.2 Linková vrstva

1) Filtrování MAC adres

Službu je možné charakterizovat jako doplňkovou. Každý přístupový bod obsahuje tzv. filtr MAC adres. Standardně je tato funkce vypnuta. Je vhodná pro menší firmy maximálně do 20 uživatelů. Pro správce sítě, je při větším počtu uživatelů a jejich určité fluktuaci, náročné udržovat aktuální seznam MAC adres. Nicméně, filtr MAC adres není sama o sobě silná ochrana, neboť se dá MAC adresa poměrně snadno získat odposlechem a poté ji duplikovat (kapitola 2.2.1). Představuje však pro útočníka alespoň jakousi komplikaci [7].

2) Autentizace a šifrování: WEP, WPA, WPA2

WEP (Wired Equivalent Privacy) byl výchozím šifrovacím protokolem, jenž byl poprvé uveden v roce 1999 ve standardu IEEE 802.11. Protokol je založen na principu šifrovacího algoritmu RC4 s tajným klíčem o velikosti 40 nebo 104 bitů kombinovaným s 24bitovým inicializačním vektorem (dále jen IV) pro šifrování textové zprávy M a jejího kontrolního součtu - ICV (Integrity Check Value) [29].

Klíčem k bezpečnosti WEP je samozřejmě inicializační vektor, takže k udržení přiměřené úrovně zabezpečení a zmenšení možnosti odhalení by měl být IV zvětšen pro každý paket tak, aby se následné pakety šifrovaly odlišnými klíči. IV se bohužel pro bezpečnost protokolu WEP přenáší jako nešifrovaný text a standard 802.11 nenařizuje zvyšování IV, čímž ponechává toto bezpečnostní opatření na návrhářích výrobců jednotlivých bezdrátových terminálů (přístupových bodech nebo bezdrátových kartách) [14].

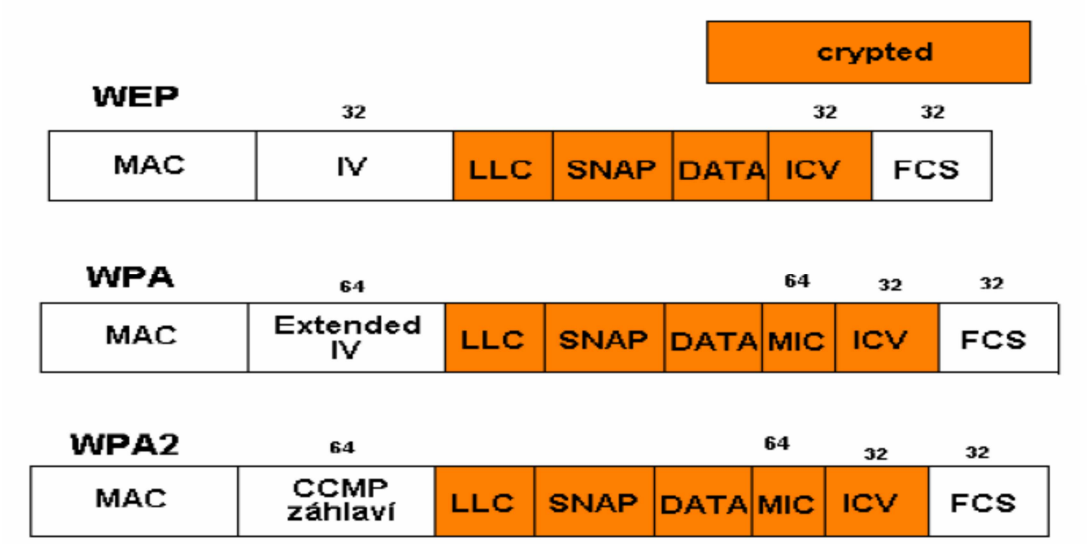
Metoda	**Autentizace**	**Šifra**
WEP	není	WEP
WPA (PSK) osobní	PSK	TKIP
WPA 2 (PSK) osobní	PSK	AES&CCMP
WPA (RADIUS) firemní	802.1x	TKIP
WPA 2 (RADIUS) firemní	802.1x	AES&CCMP

Tab. 1 Porovnání šifrovacích mechanismů [25]

WPA používá 128bitový šifrovací klíč a 48bitový IV. Zásadní vylepšení oproti WEP zabezpečení spočívá v použití TKIP (Temporal Key Integrity Protocol), což je protokol dynamicky měnící klíče. Společně s mnohem delšími inicializačními vektory tak odolává útokům, jimiž je napadán WEP. WPA (Tab. 1) zlepšuje kontrolu integrity dat (pro snadnou možnost vyřazení poškozených rámců). WEP používá algoritmus CRC-32, který je poměrně jednoduchý a navíc není kontrolní součet součástí zašifrovaných dat, takže je možné pozměnit zprávu a kontrolní součet bez znalosti WEP klíče. Dále používá lepší MAC (Message Authentication Code,

konkrétně algoritmus nazvaný Michael), který je zde nazýván MIC (Message Integrity Code). MIC metoda použitá ve WPA zahrnuje počítadlo rámců, které chrání před útoky snažícími se zopakovat předchozí odposlouchanou komunikaci [29].

WPA2 implementuje všechny povinné prvky IEEE 802.11i. Konkrétně přidává k TKIP a algoritmu Michael, nový algoritmus CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) založený na AES (Advanced Encryption Standard), který je považován za zcela bezpečný. Od 13. března 2006 je certifikace WPA2 povinná pro všechna nová zařízení, jež chtějí být certifikována jako Wi-Fi [25].



Obr. 1 Srovnání šifrování WEP, WPA, WPA2 [25]

1.3 Síťová vrstva

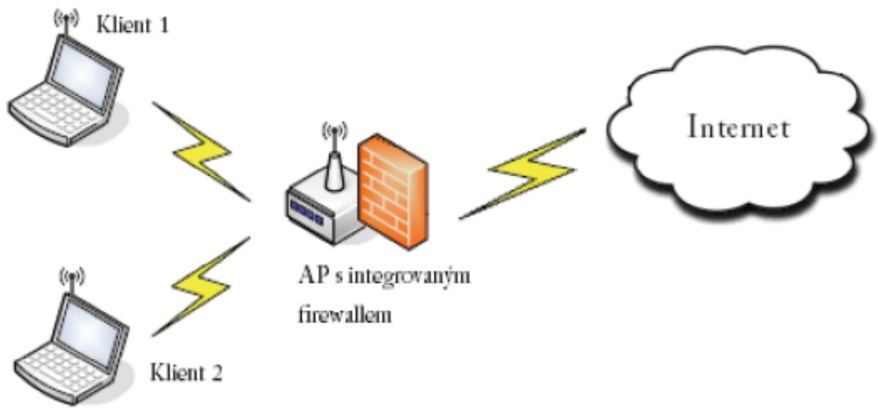
1) Vypnutí DHCP

Automatická síťová připojení zahrnují použití DHCP serveru. Server DHCP slouží k automatickému přidělování IP adres připojeným klientům. Hrozba nastane, pokud útočník získá neautorizovaný přístup do sítě (např. získá odposlechem MAC adresu jiného klienta) a DHCP server přidělí útočníkovi automaticky platnou IP adresu. Zmírnění rizika zahrnuje vypnutí DHCP serveru a použití statického přidělování adres, pokud je to možné. Tato alternativa, stejně jako v případě filtrování MAC adres, může

být praktická pouze pro relativně malé sítě, jejichž velikost je daná správní režií zahrnující přidělování statických IP adres a možností nedostatku adres. Statické přidělování IP adres může také potlačovat některé výhody bezdrátových sítí, jako roaming nebo vytváření ad hoc sítí. Jiným možným řešením je implementace DHCP serveru do firewallu pevné sítě, který uděluje přístup do bezdrátové sítě nacházející se mimo firewall pevné sítě. Dalším možným řešením je použití AP s integrovaným firewallem. Tato možnost přidá další ochrannou vrstvu do celé sítě. Uživatel by měl zhodnotit použití DHCP serveru na základě velikosti zabezpečované sítě [5].

2) Firewall

Dnes už všechny bezdrátové přístupové body a směrovače umožňují blokovat síťový provoz, typicky z internetu do WLAN, popř. naopak. Proto je nutné při konfiguraci AP zkontrolovat zapnutí firewallu. U většiny zařízení je firewall vypnutý v továrním nastavení. Pro začátek se vyplatí povolit pouze port 80 pro připojení uživatelů k internetu. Případné požadavky uživatelů na povolení dalších portů je dobré řešit individuálně.



Obr. 2 Přístupový bod s integrovaným firewallem [12]

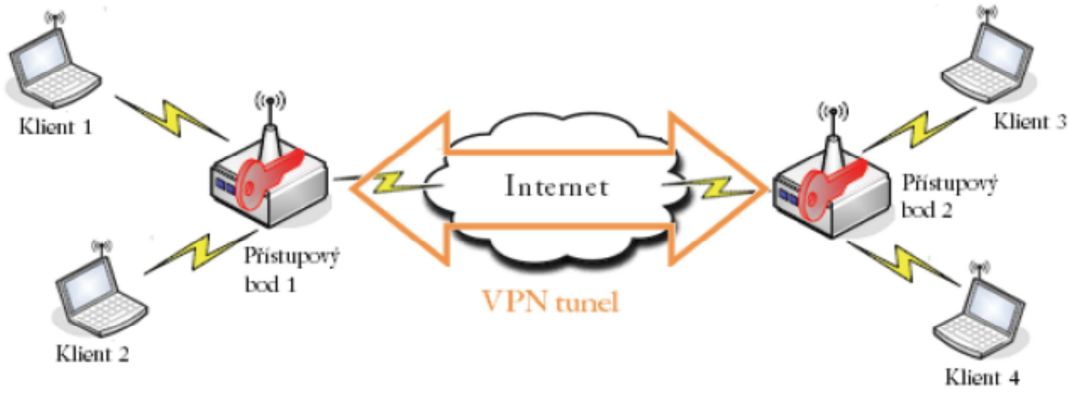
Při povolování portů je potřeba důsledně dodržovat vyplnění IP adresy partnera, s kterým přes tento port komunikujeme např. off-line bankovnictví nebo bankovní platební brána. Pokud totiž útočník sleduje datový tok, ztížíme mu tím případný pokus o prolomení do vnitřní sítě přes námi povolený port [12].

3) Filtrace IP adres

Některé bezdrátové směrovače umožňují řídit provoz v bezdrátové síti na základě seznamu povolených IP adres, které mohou do této sítě přistupovat (za předpokladu vypnutého DHCP serveru). Jedná se o obdobu filtrace MAC adres.

4) VPN

Použití VPN (Virtual Private Network) v bezdrátových sítích poskytuje další úroveň zabezpečení. Mezi dvěma koncovými body ve VPN se vytvoří bezpečný IP tunel. Koncovým zařízením může být klientská stanice, VPN brána, přístupový bod nebo firewall. Komunikace ve VPN plní jak úlohu autentizace, tak i utajení přenášených dat. Šifrování se provádí pomocí protokolu IPSec a tunelování např. pomocí protokolů L2TP nebo PPTP. VPN je ideální pro komunikaci jednoho klienta s jedním serverem (klientem), protože pro každý další server se musí ustavit nový tunel [4].



Obr. 3 Zabezpečení komunikace pomocí VPN [12]

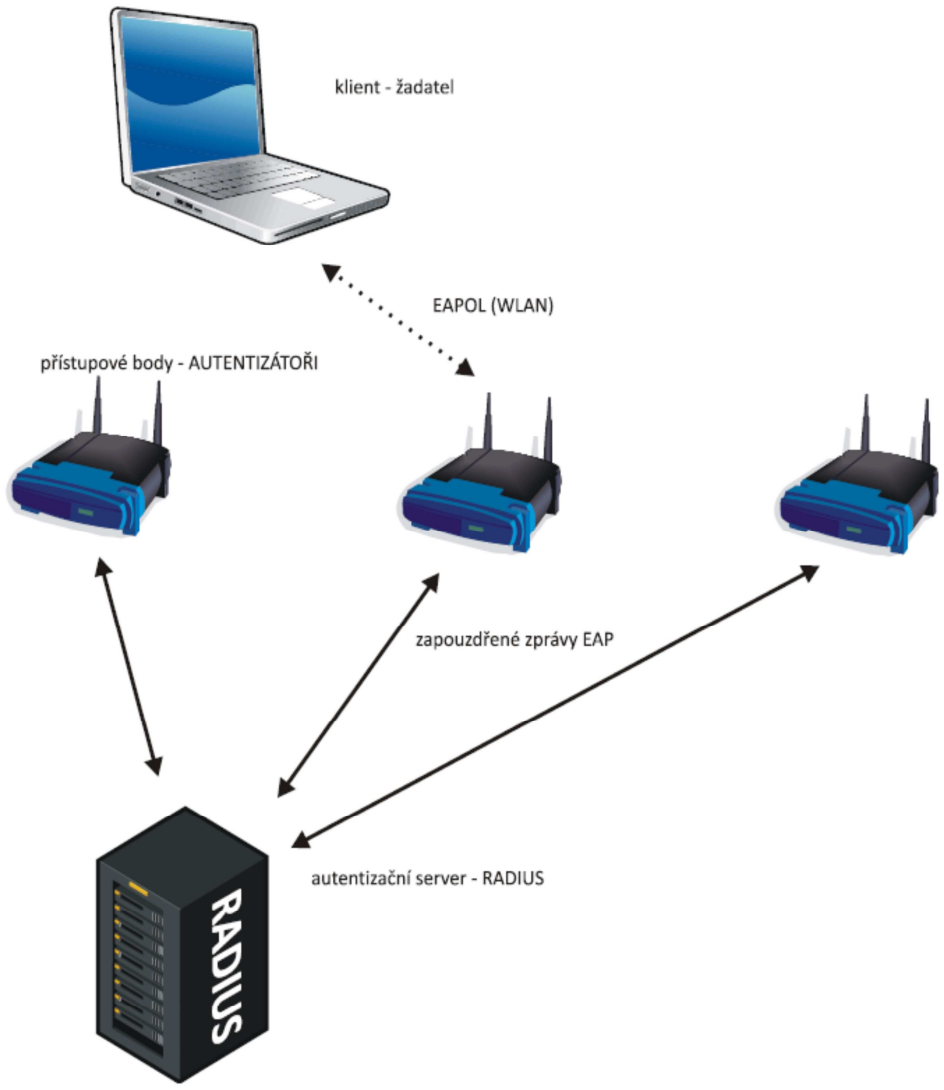
5) Detekce odposlechu

Možnost, jak útočníka odhalit, pokud máme podezření na útok na naše AP. Zjištění, zda někdo odposlouchává WLAN, je velmi obtížné, ale se znalostí odlišností různých běžně dostupných prostředků pro odposlouchávání (např. program NetStumbler), lze útočníka, podle jejich vzorku testování sítě při dostatečném počtu vysílaných paketů, odhalit, alespoň co do existence [3].

1.4 Aplikační vrstva

1) RADIUS (Remote Authentication Dial In User Service)

je AAA (Authentication, Authorization and Accounting - autentizace, autorizace a evidence) protokol pracující na principu klient-server. Klientem je v tomto případě přístupový server NAS (Network Access Server). Uživatel musí před připojením do sítě zadat přihlašovací údaje NAS serveru (v případě bezdrátové sítě plní funkci NAS serveru přístupový bod). NAS server na základě těchto údajů vyšle požadavek (RADIUS Access Request) autentizačnímu RADIUS serveru. RADIUS server přistoupí do databáze uživatelů a porovná přijaté údaje s údaji v databázi. Pro ověření údajů využívá autentizační schémata jako EAP (obr. 4) [3].



Obr. 4 Komunikace mezi přístupovým bodem a klientem [3]

Alternativní server je využit v případě, pokud primární RADIUS server není dostupný nebo neodpovídá. Pokud autentizační údaje souhlasí s údaji v databázi, RADIUS server vyšle informaci Radius Access Accept a klientovi je umožněn přístup k internetu. RADIUS také umožňuje přidělovat IP adresu (nebo rozsah adres) uživateli a další možnosti jako omezení doby připojení uživatele a rychlost připojení uživatele. Heslo vysílané mezi NAS a RADIUS serverem není viditelné. Využívá se komplexních operací jako hašování MD5 (Message - Digest algorithm 5 - rozšířená hašovací funkce s kontrolním součtem o velikosti 128 bitů) a sdílené heslo. RADIUS je obvykle používán také pro účely evidence.

NAS může použít evidenční pakety k oznámení skutečností RADIUS serveru jako začátek a konec uživatelova připojení, celkový počet přenesených paketů během připojení, množství přenesených dat nebo i důvod ukončení připojení. Účelem evidence těchto dat je podklad pro zúčtování uživatelů, ale také použití pro statistické účely a pro monitorování sítě. V dnešní době existuje několik komerčních i open-source RADIUS serverů [3].

Autentizační protokol RADIUS zlepšuje standard šifrování WEP kombinací s dalšími bezpečnostními metodami jako AP-PEAP. Komunikuje na transportní vrstvě prostřednictvím protokolu UDP. Oficiálně přidělené čísla UDP portů pro RADIUS protokol jsou pro autentizaci 1812 a pro evidenci 1813. Přesto některé implementace používají jako výchozí UDP porty 1645 resp. 1646 (např. Cisco) [2].

2) Použití aplikačního software

Aplikace jako je například linuxová aplikace FakeAP je schopna generovat tisíce falešných přístupových bodů. To může útočníkovi zabránit, popř. velmi ztížit útok na bezdrátovou síť. Pokud „uvidí“ stovky nebo tisíce sítí se stejným SSID, nebude vědět, na kterou z nich se připojit [12].

1.5 Bližší pohled na vybrané metody

1.5.1 Potlačení vysílání SSID

Potlačení vysílání SSID, pro které se také používá název „uzavřená síť“, není v pravém slova smyslu zabezpečení. Potlačení vysílání SSID není součástí standardu 802.11 a tedy ne všechna zařízení ho umí aktivovat. Proč je ale nutné ho zde uvést, si nyní ukážeme.

Po instalaci Access pointu (dále AP), začne toto AP vysílat pravidelně každých 100 ms administrativní rámce (takzvaný beacon), které veřejně obsahují informace o SSID a některé další technické údaje jako je např. síla signálu nebo maximální podporovaná rychlost. SSID si uživatel zvolí během softwarové instalace dle výrobního manuálu nebo může ponechat název SSID přednastavený výrobcem [16].

Tomuto nastavení říkáme otevřená síť. Klient v dosahu signálu tyto informace zpracuje, a pokud se chce připojit, vyšle požadavek na spojení. AP mu na tuto výzvu odpoví (většinou hodnotou „potvrzeno“ nebo „zamítnuto“). Pokud útočník odposlouchává bezdrátovou komunikaci, vaše AP mu vysláním SSID ihned sdělí svou přítomnost v síti.

V uzavřené síti je situace jiná. Klient musí předem znát hodnotu SSID a AP naslouchá pouze požadavkům na připojení. Klient tedy vyšle testovací požadavek, který obsahuje hodnotu SSID. Tento požadavek musí být veden přes všechny kanály, protože sice známe hodnotu SSID, ale na jakém kanále AP vysílá, není většinou známo. Pokud AP tento požadavek zaslechne a hodnota SSID se shoduje s hodnotou AP, pak vyšle odpověď. Pokud se hodnota neshoduje, AP požadavek ignoruje. SSID se přenáší nešifrovaný, a proto ho nelze v uzavřené síti chápat jako nějakou formu skrytého hesla.

Pokud útočník hledá přímo konkrétní síť, může hodnotu SSID zjistit i v uzavřené síti, například zachycením asociační výměny mezi AP a oprávněným uživatelem (kapitola 2.1.2). Většina útočníků ale přítomnost vaší sítě nezjistí a vybere si jiný cíl.

Potlačení vysílání SSID sebou přináší i nevýhody. Uživatelé například nemají možnost roamingu mezi AP nebo nedokáží zjistit, jak silný signál mají AP v okolí a podle toho se připojit na AP s nejsilnějším signálem [2].

1.5.2 Filtrace MAC adres

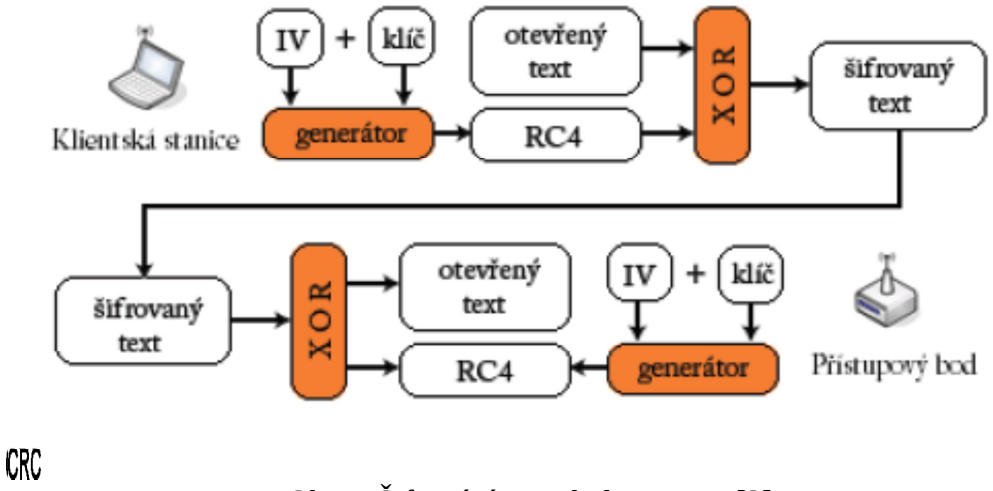
Stejně jako u ethernetových karet je výrobcem stanovena MAC adresa (Media Access Control, označovaná též jako hardwarová adresa), mají stanovenu svou MAC adresu i bezdrátové karty. Princip filtrace MAC adres spočívá v tom, že AP udržuje seznam autentizovaných MAC adres a povoluje přístup a provoz výhradně kartám s těmito adresami. Tento princip se může na první pohled zdát jako dostatečný, kdyby velká řada bezdrátových karet neumožňovala měnit svoji MAC adresu. Právě toto nastavení umožňuje útočníkovi proniknout do takto zabezpečené bezdrátové sítě. Protože zdrojová a cílová MAC adresa se posílají jako nešifrované, může útočník snadno odposlechnout hodnoty povolených MAC adres a svoji bezdrátovou kartu si nakonfigurovat tak, aby se používala tuto autentizovanou adresu (kapitola 2.2.1) [2],[8].

Kromě možnosti zneužití adresy útočníkem, se jeví jako velmi složité udržovat v rozsáhlých sítích aktuální seznam autentizovaných MAC adres. Proto je tento způsob zabezpečení vhodný pouze pro síť s velmi malým počtem konstantních uživatelů. Tato ochrana stejně jako u potlačení vysílání SSID slouží pouze k prvotnímu odrazení útočníka, který si hledá snadný cíl. Nelze ho považovat za dostatečné zabezpečení bezdrátové sítě.

1.5.3 WEP

1) Šifrování protokolem WEP

Šifrování vždy začíná nešifrovaným textovým řetězcem (obr. 5), který chceme chránit. Nejprve WEP z tohoto textového řetězce vypočítá 32bitový cyklický redundantní součet (CRC), tedy kontrolní součet pro ověření integrity dat.



Obr. 5 Šifrování protokolem WEP [3]

Tento kontrolní součet se následně připojí za přenášenou zprávu. Dále vezmeme tajný klíč a připojíme jej k IV. Kombinaci IV a tajného klíče předáme do generátoru pseudonáhodných čísel RC4 (PRNG) a výstupem bude šifrovací klíč. Následně mezi textem spojeným s kontrolním součtem a šifrovacím klíčem provedeme logický výhradní součet (XOR). Výsledkem je šifrovaný textový řetězec. Před něj připojíme hodnotu inicializačního vektoru a tento výsledek pak přenášíme [29].

Po provedení operace XOR před výsledný zašifrovaný text přidáme inicializační vektor. Jeho hodnota se přenáší nešifrovaná, protože její znalost potřebujeme k dešifrování textu.

2) Dešifrování protokolem WEP

Dešifrování probíhá stejně jako šifrování, ovšem obráceně. Vezmeme IV (který je součástí přijaté zprávy), připojíme k němu tajný klíč a výsledek předáme generátoru RC4, který znovu vytvoří sekvenci šifrovacího klíče. Mezi tímto klíčem a zašifrovanou zprávou provedeme operaci XOR, čímž dostaneme původní hodnotu. Znovu si pro ni vypočítáme kontrolní součet a porovnáme jej se součtem, který jsme přijali. Pokud by kontrolní součty nesouhlasily, předpokládáme poškození zprávy a zahodíme ji [16].

3) Inicializační vektor

IV je 24bitová hodnota přidávaná před tajný klíč., kde tato kombinace slouží k inicializaci generátoru RC4. Důvodem, proč se IV vůbec používá, je potřeba zajistit, aby byla inicializační hodnota generátoru pokaždé jiná. Proto je zásadním požadavkem šifry RC4, aby se za žádných okolností znovu nepoužila stejná inicializační hodnota. A v tom tkví jeden z hlavních nedostatků protokolu WEP standardu 802.11, a to, že není určeno, jakým způsobem se má generovat IV. Můžeme začít od nuly a přičítat jedničku nebo vybrat náhodnou hodnotu, nebo zvolit jakýkoliv vlastní postup. Protože k odeslání každého paketu potřebujeme generátor RC4 inicializovat jinou hodnotou, vychází nám, že při dnešních vysokých přenosových rychlostech vyčerpáme celý 24bitový prostor IV za několik hodin. V tom okamžiku jsme nuceni znovu použít již jednou přidělenou hodnotu IV a tím porušujeme nejdůležitější pravidlo šifry RC4, zakazující použít klíč opakovaně [2],[10].

4) Správa klíče

Jak jsem se již zmínil, WEP používá šifrovací mechanismus se sdíleným klíčem, což znamená, že pro šifrování i dešifrování se používá stejná tajná hodnota (klíč). Odesílatel i adresát musí hodnotu klíče znát. Jedním z problémů protokolu standardu 802.11 je to, že neřeší problém správy klíče. Každý uživatel musí klíč znát a musí jej udržet v tajnosti. Pokud dojde k prozrazení klíče, odejde zaměstnanec nebo dojde ke ztrátě či krádeži notebooku, je potřeba každému klientovi sdělit nový klíč a ten si ho musí na svém zařízení nastavit. A to celé je zásadní nedostatek celého mechanismu, pokud se útočníkovi podaří odposlechnout nějaký datový tok a z něj zjistit klíč, pak může tímto klíčem rozluštit kterékoliv vysílání v dané síti, protože všichni používají stejný klíč [2].

5) Proudová šifra RC4

Protokol WEP používá proudovou šifru RC4 společnosti RSA. Jde o stejnou šifru, jaká se používá i v jiných kryptografických systémech, například v SSL (Secure Sockets Layer), která je základem protokolu HTTPS. Problém WEPu spočívá v tom, že protokol 802.11 neřeší, jak má být implementováno generování IV. Jak už bylo řečeno, pro inicializaci šifry RC4 se používá kombinace IV a tajného klíče. IV je 24bitové číslo. Řada výrobců říká, že používá 64bitový nebo 128bitový (na některých zařízeních se objevil i 256bitový) WEP. Ale tento údaj je poněkud zavádějící, protože 24 bitů tohoto klíče je inicializační vektor a ten se přenáší nešifrovaný. Přesně vzato je tedy délka tajné části klíče pouze 40 nebo 104 bitů. Proto problém WEPu není v použití šifry RC4, ale v tom, jak je její použití implementováno [2],[21].

1.5.4 Pokusy o vylepšení WEP

Kvůli prolomení WEPu byla na trh uvedena různá řešení, jejichž úkolem bylo umožnit bezpečnou komunikaci v bezdrátové síti. Oficiálním nástupcem bylo WPA a v současné době pak WPA2.

1) WEPplus

WEPplus (někdy označován jako WEP+) je vylepšení původního WEP zabezpečení od Agere Systems, které se snaží odstranit takzvané slabé IV, pomocí kterých může útočník velmi rychle spočítat použitý šifrovací klíč, použité proudové

šifry RC4 a může tak nejen bezdrátový provoz odposlouchávat, ale může se i do bezdrátové sítě zabezpečené pomocí WEP připojit. Pokud však není WEPplus na všech komunikujících stranách v bezdrátové síti, nemá toto zabezpečení výhody oproti běžnému WEP. Toto řešení se nepodařilo rozšířit mezi výrobci a v dnešní době se s ním téměř nesetkáme [24].

2) WEP2

WEP2 rozšiřuje IV a zesiluje 128bitové šifrování. Používal se na zařízeních, na kterých nebylo možné provozovat novější WPA nebo WPA2 zabezpečení. WEP2 má však stejné bezpečnostní problémy jako WEP, jen útočníkovi zabere více času. V dnešních zařízeních se také již tato verze WEPu nevyskytuje [2].

1.5.5 WPA/WPA2

1) Specifikace

Používá se tato hierarchie klíčů:

- Pairwise Master Key (PMK) – (hlavní párový klíč) tajný klíč mezi AP a každou STA (v případě „personal“ verze je to společný Pre-Shared Key), jeho poznání se dokazuje pro autentifikaci pomocí 4cestného EAPOL (802.1x);
- Pairwise Transient Key (PTK) – (přechodný párový klíč) klíč derivovaný z PMK a hodnot Nonce použitých při autentifikaci, použije se v daném procesu na vytváření klíčů pro šifrování a autentifikaci;
- Group Transient Key (GTK) – (přechodný skupinový klíč) určený pro všechny stanice na dešifrování broadcast komunikace;
- EAPOL-Key Encryption Key (KEK) a EAPOL-Key Confirmation Key (KCK) - klíče pro přenos klíčů přes EAPOL (klíč na šifrování klíče; klíč na potvrzování klíče) – derivované z PTK;
- Temporal Key (TK) – (dočasný klíč) klíč (klíče) pro šifrování a zabezpečení integrity jednoho datového rámce – derivované z PTK a počítadel rámců [29].

2) IEEE 802.1x/EAP

Na autentifikaci a výměnu klíčů je v IEEE 802.11i určený handshake pomocí EAPOL - EAP over LAN zpráv (Extensible Authentication Protocol over LAN,

rozšířitelný autentifikační protokol přes lokální síť), které definuje standard IEEE 802.1x, založený na EAP (Extensible Authentication Protocol, rozšířitelný autentifikační protokol). Výměna klíčů se tvoří spolu s autentifikací ihned po asociaci stanice, a též při požadavku stanice o STA-to-STA (stanice stanici) komunikaci s jinou stanicí. Samotnou autentifikaci nemusí vytvářet AP, ale může pro tento účel použít centralizovaný RADIUS server a s ním komunikuje též pomocí IEEE 802.1x [2].

Typy EAP pod WPA a WPA2 jsou:

- EAP-TLS – Extensible Authentication Protocol Transport Layer Security (bezpečnost transportní vrstvy);
- EAP-TTLS/MSCHAPv2 – EAP-Tunneled TLS/Microsoft Challenge Authentication Handshake Protocol (bezpečnost na transportní vrstvě, protokol pro navázání komunikace pomocí výzvové autentifikace od firmy Microsoft);
- PEAPv0/EAP-MSCHAPv2 – Protected EAP/Microsoft Challenge Authentication Handshake Protocol (zabezpečený EAP);
- PEAPv1/EAP-GTC – Protected EAP/Generic Token Card (všeobecná karta);
- EAP-SIM – vzájemné ověřování a výměna klíčů pomocí SIM karet používaných v GSM sítích [29].

Mimo certifikaci je možné používat i jiné typy EAP, mezi které patří:

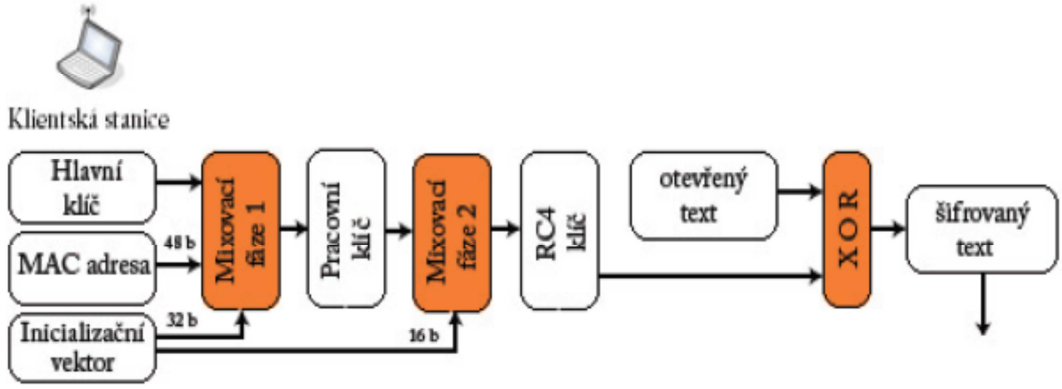
- EAP-MD5;
- LEAP – Cisco Lightweight EAP.

3) TKIP

V zásadě představuje TKIP pouze dočasnou opravu protokolu WEP. Kvůli zachování zpětné kompatibility s velkým počtem stávajících instalovaných hardwarových zařízení byly při jeho návrhu učiněny různé kompromisy. Pokud víme, momentálně ovšem představuje řešení všech známých problémů protokolu WEP.

Mechanismus TKIP zlepšuje šifrování prostřednictvím tří hlavních prvků:

- Funkce mixování klíče pro každý paket
- Vylepšená funkce kontroly integrity (MIC), pojmenovaná Michael
- Vylepšená pravidla generování IV včetně sekvenčních pravidel



Obr. 6 Generování klíče pomocí TKIP a šifrování ve WPA

Nyní si popíšeme fungování TKIP v praxi (obr. 6). Klient začíná se dvěma klíči - 128bitovým šifrovaným klíčem a 64bitovým klíčem pro zajištění integrity, které získá bezpečnými mechanismy v průběhu iniciální komunikace protokolem 802.1x. Šifrovací klíč se značí TK, Temporal Key. Klíč pro zajištění integrity se označuje jako klíč MIC, Message Integrity Code. V první fázi se provede XOR mezi MAC adresou odesílatele a hodnotou TK, čímž vzniká klíč označovaný jako Fáze 1 (někdy též „mezilehlý klíč“). Klíč Fáze 1 se mixuje se sekvenčním číslem a vzniká tak klíč Fáze 2, pro přenos jediného paketu. Výstup druhé fáze se předává mechanismu WEP jako standardní 128bitový WEPový klíč (tedy IV + tajný klíč). Zbytek procesu už probíhá stejně jako klasická transakce protokolem WEP. Rozdíly spočívají v tom, že v důsledku první fáze už nepoužívají všichni klienti stejný WEPový klíč, a ve druhé fázi už neexistuje korelace mezi hodnotou IV (v tomto přípravě sekvenčním číslem) a samotnou klíčovací sekvencí [2].

4) Mixování paketového klíče

Funkce mixování paketového klíče efektivně znemožňuje útok FMS (kapitola 2.2.2), protože díky ní neexistuje přímý vztah mezi IV a šifrovací sekvencí pro daný rámec. Kontrola integrity neprobíhá jednoduchým 32bitovým CRC součtem, ale pomocí jednocestné hashovací funkce Michael. Vstupem této funkce je otevřený text, zdrojová i cílová MAC adresa a klíč. Výstupem je 32bitová hash. Lze tedy ověřit i integritu MAC adres[2].

5) Funkce kontroly integrity

Namísto jednoduché 32bitové hodnoty CRC se v TKIP ke kontrole integrity používá funkce pojmenovaná Michael, jednocestná hashovaní funkce. Nejde o lineární funkci a pro útočníka je tak velmi obtížné při přenosu paket modifikovat. Michael vyžaduje následující vstupy: klíč MIC, zdrojovou adresu, cílovou adresu a nešifrovaný text. Tím, že pracuje i se zdrojovou a cílovou adresou, je možné ověřit integritu MAC adres. Výstup algoritmu Michael je dlouhý 8 bajtů a připojuje se k přenášeným datům [12].

6) Větší prostor inicializačního vektoru

Problém s kolizemi IV řeší TKIP pomocí dvou jednoduchých pravidel. Prostor inicializačního vektoru se zvětšil z 24 bitů na 48 bitů. Při rychlosti 54 Mbps to znamená, že vyčerpání stavového prostoru bude trvat přes 1000 let. A druhé pravidlo TKIP nařizuje, aby hodnota IV rostla inkrementálně od nuly, hodnoty mimo pořadí se ignorují. Z pohledu bezpečnosti znamená rozšíření prostoru IV (respektive sekvenčního čísla) to, že se eliminují kolize IV a na nich založené útoky [2].

7) AES - CCMP

Jak už bylo řečeno, WPA je dočasné opatření, které v polovině roku 2003 umožnilo v praxi nasadit část výsledků práce skupiny 802.11i. WPA je tedy podmnožinou standardu 802.11i. Primární komponenta protokolu 802.11i, která v té době ještě nebyla úplně hotova, byla šifra AES. Ve specifikaci 802.11i je AES povinné, zatímco TKIP je volitelné [10].

AES je šifra odpovídající americkému federálnímu standardu FIPS (Federal Information Processing Standards), která byla navržena jako náhrada RC4. Samotnému přijetí šifry AES americkou vládou předcházel rozsáhlý průzkum a revize šifry.

AES nabízí různé režimy činnosti, ve specifikaci 802.11i se používá čítačový režim s protokolem CBC-MAC (CCM), obvykle označovaný jako AES-CCMP. Čítačový režim zajišťuje šifrování, CBC – MAC pak zajišťuje autentizaci a integritu dat [8].

Stejně jako RC4 je i AES šifra se symetrickým klíčem, což znamená, že se text šifruje i dešifruje stejným sdíleným tajným klíčem. Na rozdíl od šifry RC4, která šifruje

lineárně každý bajt XORováním s náhodnou sekvencí, AES pracuje s bloky o velikosti 128 bitů, a proto se označuje jako bloková šifra.

CCMP i TKIP mají řadu společných vlastností. Oba používají 128bitový dočasný klíč, odvozený od „master“ klíče, který se získává v průběhu negociace protokolem 802.1x. V terminologii CCMP se 48bitová hodnota IV označuje jako „číslo paketu“ (PN) [2],[7].

8) Funkce kontroly integrity

Stejně jako TKIP i CCMP obsahuje algoritmus MIC zajišťující, že nedošlo k modifikaci přenášených dat. Nicméně mechanismus MIC v AES funguje jinak než algoritmus Michael v TKIP. Výpočet MIC je založen na inicializačních hodnotách vycházejících z IV a z dalších hlavičkových informací. Pracuje v 128bitových blocích a počítá se přes jednotlivé bloky až na konec originální zprávy, kdy se vypočte konečná hodnota.

9) Nový šifrovací mechanismus

Čítačový režim šifrování šifrou AES se výrazně liší od WEP/TKIP a RC4. Výstupem šifry AES je po inicializaci (založené na IV a dalších hlavičkových informacích) jen 128bitový blok. Celý vstupní text se rozdělí na 128bitové bloky a ty se postupně XORují se 128bitovým pokaždé nově generovaným výstupem AES tak dlouho, dokud nedojde k zašifrování celé původní zprávy. Nakonec se čítač vynuluje, XORuje se hodnota MIC, která se přidává na konec rámce.

Výsledkem je mnohem silnější šifra. Zvýšené šifrovací nároky by ovšem přetížily procesory stávajících zařízení založených na WEP/RC4. Z toho důvodu vyžaduje AES nový hardware, a je tedy nekompatibilní s nynější první generací bezdrátových zařízení [17].

2 VARIANTY ÚTOKŮ NA BEZDRÁTOVÉ SÍTĚ

Útoky do WLAN můžeme rozdělit na pasivní a aktivní. V případě pasivního útoku, na rozdíl od aktivního, útočník zachycená data nemodifikuje. Pasivní útoky jsou bohužel ve většině případů nezjistitelné.

Existuje značné množství druhů útoků do WLAN, většina je však pouze modifikací několika základních druhů a ty si zde uvedeme:

Pasivní útoky:

- Skenování sítí, Wardriving, Warwalking a Warchalking

  Jedná se o techniku zjišťování dostupných sítí a identifikaci zabezpečovacích mechanismů. Identifikace se provádí za jízdy autem - Wardriwing nebo za chůze - Warwalking, Zjištěná data mohou být následně veřejně prezentována - Warchalking.

- Odposlech a identifikace dat

  Umožňuje útočníkovi zjistit činnost odposlouchávané sítě, jejíž znalost potom využije např. pro realizaci některého z aktivních útoků.

Aktivní útoky:

- Zneužití cizí MAC adresy

  Získání legitimní MAC adresy, pokud jde o jedinou ochranu sítě, umožnuje útočníkovi stát se důvěryhodným a získat tak přístup ke všem prostředkům sítě.

- Útok na WEP
  - Útok na WEP hrubou silou

    Postup spočívá v zachycení nejméně jednoho šifrovaného paketu, na kterém budeme provádět dešifrování. Následně útočník zkouší všechny kombinace klíče. Tento útok je velice neelegantní a neefektivní.

  - Injekce rámce

    Tento druh útoku je možný díky tomu, že standard 802.11 nevyžaduje změnu IV u každého rámce. Pokud tedy známe nešifrovaný text nějakého šifrovaného rámce, můžeme odvodit šifrovací sekvenci. Pomocí této šifrovací sekvence zašifrujeme náš text, který poté bude dešifrován jako platný.

- FMS útok

  Tento útok počítá s tím, že existují IV, které vedou k odhalení vlastností privátní části klíče. Pro úspěšné uskutečnění tohoto útoku musíme znát také alespoň několik počátečních bajtů šifrovaného textu, což ale není neřešitelný problém, neboť všechny IP a ARP pakety začínají hodnotou 0xAA .

- KoreK

  Tento útok umožňuje dešifrovat libovolný rámec zašifrovaný pomocí WEP. Útočník musí být v dosahu AP. Ten se použije k dešifrování. Funguje i proti dynamickému WEP, jestliže se během útoku nezmění. Dešifrování 1 rámce trvá desítky sekund až několik minut. Tato doba závisí na ztrátovosti rámce a je přímo úměrná délce rámce [15].

- Útok na WPA a WPA2

  Nejrozšířenější je útok na klíč PSK WPA/ WPA2. Zatímco u WEP bylo možné použít k urychlení dešifrování statistické metody, u WPA/ WPA 2 lze použít pouze techniku lámání hesla slovníkovou metodou a hrubou silou. To proto, že klíč není statický a proto shromažďování IV (jako tomu je u WEP šifrování) nijak neurychlí vlastní útok.

- Zamítnutí služby (DoS, Denial of Service)

  Útoky zaměřené na zamítnutí služby jsou na použitém médiu (vzduch) lehko realizovatelné a dosahují okamžitý účinek. Nejsou však zaměřeny na přístup do sítě a na zneužití systému, ale na znemožnění práce uživatele na cílovém (napadeném) systému (případně celé síti), resp. paralýze jím poskytovaných služeb. Nejčastěji se tak děje zahlcením nebo vyčerpáním některých síťových zdrojů, případně složitými výpočetními úlohami jako šifrování nebo dešifrování [11].

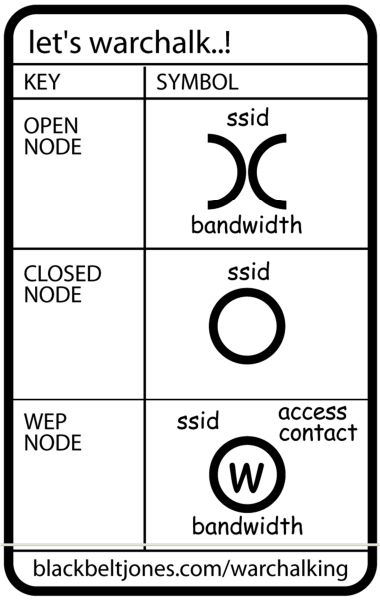
- Man-in-the-middle

  Jde o to získat důvěru uživatele a nechat ho se připojit na podvržené AP. Následně si uživatel bude číst emaily, nakupovat kreditní kartou v e-shopu atp. a my v roli prostředníka mezitím můžeme odposlechnout jeho veškeré soukromé informace.

2.1 Pasivní útoky

2.1.1 Skenování sítí - Wardriving a Warchalking

Slovem „Wardriving“ se jednoduše označuje pasivní hledání bezdrátových sítí za pomoci přenosného počítače nebo PDA, člověkem jedoucím v autě. Pokud se jedná o bezpečnostní průzkum nebo skenování pásma za účelem zjištění vytížení pásem bezdrátové sítě, není tento akt sám o sobě závadný. Situace se ovšem mění v momentě, kdy dojde k potvrzení vazby TCP/IP protokolu na bezdrátový adaptér a dojde k přidělení IP adresy, protože se již dostáváme do neveřejné části komunikace, kde nemáme svolení majitele s užíváním prostředků sítě.



Obr. 7 Symboly užívané při Warchalkingu

- OPEN NODE - otevřený přístup, je uvedeno SSID a rychlost;
- CLOSED NODE - uzavřený přístup, je opět uvedeno SSID;
- WEP NODE - přístup omezený WEP (WPA), je uvedeno SSID, adresa a rychlost.

Termínem „Warchalking“ můžeme označit činnost, kdy se kreslením piktogramů (obr. 7) na viditelná místa upozorňuje na aktivní přítomnost AP. Tyto značky upozorňují na typ přístupu, SSID, zabezpečení, rychlost atd. Celosvětově existuje mnoho stoupenců této metody napojení na cizí bezdrátovou síť. Tito mimo jiné aktivně vyhledávají nová přípojná

místa, která obratem zaznamenávají do sdílených databází. Z velké části není cílem poškození prostředků majitele bezdrátové sítě nebo krádež jeho dat, ale bezplatné připojení na internet [12].

V operačním systému Windows je nejpoužívanějším programem pro odposlech dostupných sítí NetStumler. Tyto aplikace běží ve většině případů na notebooku nebo PDA, který buď nadšenci nosí po okolí, nebo detekují volně přístupné sítě při jízdě autem. Takto získané informace poté poskytující veřejně, pomocí sdílených databází s adresou bodu a GPS pozicí nebo prostými značkami.

2.1.2 Odposlech a identifikace dat

Je to proces ve většině případů pro běžného uživatele nezjistitelný. Existují sice hardwarové sondy, tzv. IDS systémy (Intrussion Detection System), které reagují na rámce Probe Request a Probe Response. Ve spojení s odposloucháváním se často setkáváme s pojmy „monitorovací režim“ a „promiskuitní režim“ bezdrátového adaptéru. Monitorovací režim je mód, ve kterém lze odchytávat pakety bez nutnosti asociace, bez znalosti SSID. Stačí zadat kanál, na kterém běží komunikace. Je jen málo karet, které lze do monitorovacího módu přepnout. Promiskuitní režim je takový, kdy síťová karta zpracovává pakety v celém síťovém segmentu. V normálním režimu zpracovává pakety určené jen pro ni. Díky tomu útočník, který odposlouchává, může stahovat data v daném segmentu, ale nemůže zachytávat data, která jsou mimo segment, tedy za směrovačem, přepínačem sítě apod. Pro Windows se nabízí řada programů pro odposlouchávání sítí. Jedním z nejznámějších je bezesporu WireShark, který je navíc volně šiřitelný, ale neumožňuje práci v monitorovacím režimu. Naproti tomu WildPacket OmniPeek prostřednictvím svých speciálně upravených ovladačů kartu do monitorovacího módu přepnout umí (pokud to karta podporuje) [12].

2.2 Aktivní útoky

2.2.1 Zneužití cizí MAC adresy

Tento způsob útoku patří mezi aktivní a využívá toho, že do bezdrátové sítě se může připojit pouze klient, jehož MAC adresa zařízení je obsažena v seznamu povolených MAC adres nadefinovaných v přístupovém bodu. Často se stává, že „uzamčení sítě na MAC adresy“ je jedinou ochranou sítě. MAC adresa je sice unikátní, na zařízení je obvykle napájená v flash paměti, většinou je však softwarově změnitelná. Paradoxně

někdy za pomoci původního ovladače dodávaného výrobcem. Pasivním monitorováním je možné jednoduše zjistit platné MAC adresy, které ve sledované bezdrátové síti komunikují. Útočník takto získané informace může použít k následujícím účelům:

- posílání falešných technických rámců;
- zneužití MAC adresy pro „legitimní“ využívání služby – po odpojení určitého zařízení ze sítě, resp. po jeho vypnutí, softwarově změníme MAC adresu našeho zařízení na adresu používanou předchozím zařízením, následně můžeme využívat stejné služby sítě jako toto zařízení. Jde o takzvané falšování identity zdroje, kdy útok prostřednictvím falešné adresace mění skutečnou zdrojovou adresu datagramu z adresy zakázané pro vstup do sítě na adresu povolenou (důvěryhodnou adresu z množiny vnitřních podnikových IP adres nebo vnější adresu povolenou pro přístup k některým vnitřním zdrojům);
- krádež MAC adresy – vytipovaného uživatele odstavíme pomocí DoS (kapitola 2.2.4) a použijeme jeho adresu. DoS útok však musíme úzce nasměrovat, abychom odstavili jen vytipovaného uživatele a třeba ne i AP;
- současné používání MAC adresy ve stejném čase – tento způsob lze využít bez větších problémů, pokud se omezíme na UDP (User Datagram Protokol, protokol transportní vrstvy nezaručující doručení zprávy, používaný v rozlehlých sítích) a ICMP (Internet Control Message Protocol, protokol který používají operační systémy pro posílání chybových zpráv, například pro oznámení že cílový počítač není dostupný)[2].

Mezi nebezpečí, které spočívá v získání falešné adresace, patří možnost zjištění informací o oprávněných uživatelích, jejich účtech i heslech, přidání nebo změna konfigurace vnitřního serveru (včetně neoprávněných uživatelských jmen a hesel).
Na síti, kde je pravidelný neřízený provoz, prakticky nemožné zabránit „odchycení“ legitimní MAC adresy. Napříč tomu je tento způsob ochrany často využívaný, protože chrání před neúmyslným zneužitím, resp. zneužitím laikem. Pokud chceme ztížit, resp. zabránit úmyslnému zneužití legitimní MAC adresy, je nutné na bezdrátové síti použít šifrování – WEP, WPA nebo WPA2.

2.2.2 Útok na WEP

1) Útok hrubou silou

je většinou pokus o rozluštění šifry bez znalosti jejího klíče k dešifrování. Jedná se o systematické testování všech možných kombinací nebo omezené podmnožiny všech kombinací.

Útok hrubou silou se často používá pro uhádnutí dvojice uživatel a heslo. Je možné používat náhodná (resp. generická) přihlašovací jména a hesla při pokusech o autentizaci, případně možné varianty omezit – například získat seznam uživatelských jmen a zkoušet pomocí předem připraveného slovníku (seznamu) různá hesla. Protože si uživatelé často volí málo bezpečné heslo, je tento jednoduchý a snadno automatizovatelný útok poměrně úspěšný a široce rozšířený.

- **Slovníkový útok**

  Je modifikací útoku hrubou silou. Tímto postupem se omezí počet prohledávaných klíčů. Nejznámější je v této oblasti program crack. Program má k dispozici několik slovníků a soubor pravidel. Na každé slovo jsou použita pravidla, která dané slovo modifikují. Slovníky jsou stále aktualizovány a rozšiřovány. Pak jsou všechny modifikace zašifrovány a porovnány se souborem hesel. Ve slovnících jsou obsažena jak běžná slova, tak některá hesla jako 123456, qwerty nebo slova počítačového žargonu. Program také zkouší použít další informace, které může získat z uživatelových souborů [14].

- **Útok na generátor klíče**

  Další z variant útoku hrubou silou. Mnoho ovladačů síťových karet umožňuje namísto alfanumerického klíče zadat tzv. „passphrase“, z které se generátorem vytvoří čtyři klíče. Tento generátor je běžně používaný, ale není nijak standardizovaný. 64bitová verze využívá XORování (exclusive OR) jednotlivých znaků passphrase navzájem a RC4 PRNG (Pseudo-Random Number Generator, generátor pseudonáhodné posloupnosti čísel) takovým způsobem, že výsledný 40bitový klíč, bez ohledu na délku původního passphrase, má entropii jen 21 bitů. Detailně je tento generátor a útok na něj popsaný v [15]. Většina volně stažitelných utilit umí s pomocí 2 odchytnutých rámců takovýto WEP klíč prolomit, na stroji s procesorem P4 2.6 GHz a vyšším, do několika minut[29].

2) Injekce rámce

Ochranu před zdvojenými rámci poskytuje obvykle firmware WLAN zařízení, a to pomocí pole Sequence number v hlavičce. WEP šifruje a zabezpečuje pomocí ICV jen datovou část rámců. Specifikace WEP umožňuje opakování IV a klíč je statický, proto je teda možné libovolný zachycený rámec znovu vysílat. Aby následně nebyl identifikovaný jako zdvojený, postačuje změnit Sequence number.

Injekcí rámců můžeme dosáhnout různé cíle:

- poškozování toku dat;
- celkové zvýšení provozu na síti za účelem zachytit co nejvíc různých IV pro FMS/KoreK útoky (kapitola 2.2.2);
- zvýšení ARP (protokol pro zjišťování adres) [18].

3) ARP injekce

Pro její uskutečnění je nutné mít alespoň jednoho asociovaného klienta na přístupový bod. Využívá faktu, že ARP rámce jsou v provozu snadno rozeznatelné i v zašifrovaných datech. K rozeznání od ostatních dat nám napomůže jejich délka, a také ARP request, který má cílovou adresu FF:FF:FF:FF:FF:FF (broadcast). Opětovné vysílání ARP request je velmi efektivní způsob jak generovat nové inicializační hodnoty. Použitý program čeká na přijetí ARP rámce, který následně odešle zpět na přístupový bod. To způsobí, že přístupový bod zopakuje APR rámec, ale s novým IV. Tento ARP rámec je znovu zaslán na přístupový bod, který jej zpracuje stejným způsobem. Každý zopakovaný ARP rámec přístupovým bodem dá novou hodnotu IV. ARP injekce je implementovaná v programovém balíku pro Linux aircrack-ng, konkrétně ji využívá utilita aireplay-ng [29].

4) Podvržená autentizace

Jinou variantou útoku na šifrovací sekvenci je podvržená autentizace. Abychom mohli tento typ útoku pochopit, připomeneme si, jak probíhá autentizace se sdíleným klíčem:

- První krok: klient pošle na AP autentizační požadavek;
- Druhý krok: AP pošle klientovi 128 bajtů dlouhou výzvu;

- Třetí krok: Klient zašifruje výzvu svým WEPovým klíčem a zašifrovaný text pošle zpátky na AP;
- Čtvrtý krok: AP využije svou znalost WEPového klíče a ověří, zda klient zná sdílený klíč;
- Pátý krok: AP klientovi oznámí úspěšnou či neúspěšnou autentizaci;

Problém tohoto mechanismu spočívá ve skutečnosti, že pokud se útočníkovi podaří zachytit tuto autentizační sekvenci, zjistí jak přímý text (výzvu), tak odpovídající zašifrovaný text (odpověď). Stejným postupem jako u injekce paketů, pak útočník může zjistit šifrovací sekvenci, vyžádat si autentizaci a k zašifrování výzvy, kterou od AP obdrží, použije zjištěnou šifrovací sekvenci a vytvoří tak platnou odpověď. Útočníkovi se tak může podařit platná autentizace, přestože WEPový klíč nezná. Útok je možný díky tomu, že výzva je vždy dlouhá 128 bajtů a protože IV lze používat opakovaně [29].

5) Fragmentační útok

V roce 2005 se objevil na internetu návod na praktický fragmentační útok. Jeho princip spočívá právě v defragmentaci. Pokud vyšleme *K* fragmentovaných rámců (*K=N+1*) do distribučního systému, AP tyto fragmenty pospojuje a pošle v jednom rámci.

Když je na síti použitý WEP, jednotlivé rámce zašifrujeme pomocí známé dvojice (IV, RC4 proud) do distribučního systému. AP je defragmentuje, zašifruje pomocí IV, a pokud cílová MAC adresa není určená pro jinou síť, pošle zpět do vzduchu pro známého anebo neznámého adresáta. Plaintext zašifrovaného defragmentovaného rámce jsme však zvolili my, a tedy umíme ihned určit nově získanou dvojici (IV, delší jiný RC4 proud).

Tento útok je o hodně efektivnější než jiné útoky, protože nepotřebuje posílat zkusmo neplatné rámce. Teoreticky umožňuje už s 5 známými bajty PRGA (1 bajt pro data a 4 pro ICV) poslat libovolně dlouhý rámec. V běžném provozu umíme poměrně spolehlivě odhadnout 7-16 bajtů plaintextu, a zároveň i PRGA – podle velikosti rámce určíme protokol vyšší vrstvy a podle MAC adres z hlavičky rámce můžeme odhadnout některé z polí hlavičky protokolu vyšší vrstvy (ARP, ICMP, IP, ...). Získané pseudonáhodné sekvence můžeme potom použít na injekci rámců (kapitola 2.2.2), případně sestavení kompletního PRGA slovníku [29].

6) KoreK

V roce 2004 publikoval programátor s pseudonymem KoreK nový způsob lámání RC4 algoritmu, a to zaměřením se ne na konkrétní hodnoty IV, ale na to, jakým způsobem je ovlivněný Key Scheduling algoritmus (KSA). V [15] jsou detailně popsány KoreK útoky na KSA. Hodně z nich dává falešná pozitiva (víc jak FMS), proto je nutné větší ověřování dešifrováním rámců.

Postupně od zveřejnění byl KoreK útok (to je vlastně více KoreK útoků, které „hlasují“ o výsledku pro jednotlivé stavy KSA) implementovaný do všech programů, které lámou WEP pomocí FMS.

Při všech realizovaných pokusech se úspěšně podařilo najít šifrovací klíč. Simulovaný provoz byl zaměřený na maximalizaci počtu paketů a teda nasbíraných IV, pomocí flood ping-u, který na 11Mbit/s síti (ad-hoc) generuje okolo 100 000 paketů za minutu (obousměrně), na 54Mbit/s okolo 125 000 paketů za minutu.

KoreK útok je stejně jako FMS pasivní, určený jen pro zjištění tajného klíče. Pokud by byl provoz na skutečné síti nízký, můžeme ho zvýšit aktívním útokem – injekcí anebo fragmentačním útokem.

Díky silnému provozu se podařilo klíč zjistit vždy maximálně do 6 minut. Při slabém provozu na síti by tento útok trval několik hodin, pokud bychom však použili ARP reinjekci (viz. 2.3.3) s rychlostí okolo 500 paketů/sek, umíme pak potřebných 500 tisíc rámců nasbírat do 17 minut. Výjimečně postačí na prolomení i 250 tisíc rámců. [29].

7) FMS útok

Útok byl popsán již v roce 2001. Útok počítá s tím, že se vyskytují inicializační vektory, podle kterých se dá určit privátní část klíče. Útočník pro uskutečnění musí znát několik počátečních bajtů šifrovaného textu, ale díky tomu, že všechny IP a ARP pakety začínají hodnotou 0xAA není toto problém. První verzí byl BF-FMS (útok hrubou silou FMS), který se liší s klasickým BF v potřebě výkonu a počtu paketů. Pro klasický BF stačí jeden paket, ale je potřeba velký výpočetní výkon, oproti tomu BF-FMS potřebuje velké množství paketů, ale stačí menší výpočetní výkon. V roce 2002 byl představen optimalizovaný FMS. Ten pomocí ARP dotazů generuje síťový provoz. Dnes je tento způsob útoku již přežitý [14].

2.2.3 Útok na WPA

1) Útok na klíč PSK WPA/ WPA2

Nejznámější zranitelností WPA/ WPA2 zabezpečení je útok na klíč PSK WPA/ WPA2. Zatímco u WEP bylo možné použít k urychlení dešifrování statistické metody, u WPA/ WPA2 lze použít pouze techniku lámání hesla slovníkovou metodou a hrubou silou. To proto, že klíč není statický a proto shromažďování IV nijak neurychlí vlastní útok. Jedinou možností, která se naskýtá, je zachycení tzv. 4cestného handshake mezi klientem a přístupovým bodem. Handshake proběhne, jakmile se bezdrátový klient úspěšně připojí k přístupovému bodu. PSK (Pre-shared key) je řetězec o délce 256 bitů nebo heslo skládající se z 8 až 63 znaků. Pokud je PSK generováno na základě fráze o délce méně než 20 znaků, je náchylné ke slovníkovým útokům [8],[12].

Klíč PMK, který se stará o 4cestný handshake se vypočítá z PSK podle vzorcePMK = PBKDF2 (heslo, SSID, délka SSID, 4096, 256), kde PBKDF2 je metoda z PKCS #5 v2.0 (Password-based Cryptography Standard). Spojení řetězce hesla, SSID a hodnoty délky SSID je 4 096krát hašováno, z čehož se vygeneruje 256bitová hodnota PMK.

PTK je odvozen z PMK pomocí 4cestného handshake a všechny informace, které slouží k výpočtu jeho hodnoty, se přenáší jako nešifrovaný text. Síla PTK závisí tedy pouze na hodnotě PMK, která v podstatě pro PSK znamená sílu hesla. Druhá zpráva 4cestného handshake se stala předmětem jak slovníkových, tak offline útoků hrubou silou. Ke zneužití této trhliny v bezpečnosti byla vytvořena utilita cowpatty, jejíž zdrojový kód použil a zlepšil Christophe Devine v nástroji Aircrack, aby umožnil slovníkové útoky a útoky typu brute-force (útoky hrubou silou) na WPA/ WPA 2.

Návrh protokolu (4096 hašů na každý pokus hesla) znamená, že útoky hrubou silou jsou velmi pomalé (pouze několik stovek hesel za sekundu pomocí nejnovějšího samostatného procesoru). PMK nelze vypočítat dopředu, jelikož heslo je na základě ESSID dodatečně zakódováno. Jediná možnost, jak prolomit Pre-shared Key nástává, pokud jde o relativně krátké slovníkové slovo.

K získání neprolomitelné bezdrátové sítě tedy stačí použít WPA/ WPA2 a heslo o délce 63 znaků skládající se z náhodných znaků a navíc obsahující speciální symboly. K provedení útoku na WPA/ WPA2 musí útočník pasivním sledováním bezdrátové sítě nebo pomocí deautentizačního útoku zachytit zprávy 4cestného handshake, aby proces

zrychlil. Počítač je schopen otestovat pouze 50 až 500 možných klíčů za 1 s dle svého výkonu. Projít obsáhlý slovník tak může trvat hodiny, dny, někdy i déle.

Délka hesla [znaků]	Počet strojů	Rychlost [Heslo/s]	Pouze číslice	Pouze malá písmena	Pouze velká písmena	Doba trvání
8	**1**	**300**	×			**4 dny**
8	**1**	**300**		×		**5 let**
8	**2**	**300**		×	×	**2865 let**

Tab. 2 Doba rozluštění PSK - WPA podle různých kritérií [12]

Rozdíly mezi lámáním šifrování se zabezpečením WPA-PSK a WPA 2-PSK v podstatě nejsou. Autentizační metodologie je prakticky stejná. Proto také použitá technika je identická [12],[13].

2) Útok na MIC v TKIP

Navrhovatelé algoritmu Michael použitého na výpočet MIC v TKIP si byli vědomi, že je kryptograficky slabý, a proto je v něm zaimplementovaná ochrana vůči útoku na MIC. Pokud je v přijatém rámci správné FCS i ICV, ale MIC ne, je pravděpodobné, že se jedná o útok. Standard [10] určuje, že počet selhání MIC může být nejvíc jedno za minutu. Pokud jsou v intervale 60 sekund přijaté 2 rámce, v kterých MIC takto selhalo, musí se příjem rámců na minutu zastavit a následně vyměnit šifrovací klíče pomocí EAPOL. Každé selhané MIC má být zaznamenáno a ohlášené administrátorovi. Tento přístup zabrání útokům na obsah přenášené zprávy, ale může vést k DoS. Událost má však být zaznamenána a ohlášená, proto je použití na nenápadný DoS útok nevhodné. Účinnou obranou vůči tomuto možnému útoku je použití WPA2 (AES šifrovaní) [2].

3) Slovníkový útok na LEAP

Licenční Cisco autentifikační metoda Lightweight EAP (LEAP), kterou implementovalo více výrobců do svých zařízení, je velmi lehce prolomitelná. LEAP používá přenos jména jako plaintext a na ověření hesla modifikované MSCHAPv2

challenge/response schéma, kde 8bajtový challenge text je 3 krát nezávisle zašifrovaný 56bitovým DES a poslaný jako 24bajtová odpověď. Na vygenerování tří klíčů pro DES je použitý 16bajtový MD4 hash (tzv. NT hash, používaný ve Windows) hesla. Použitý způsob zarovnání je hlavní slabinou LEAP:

- klíč: H1 H2 H3 H4 H5 H6 H7
- klíč: H9 H10 H11 H12 H13 H14
- klíč: H15 H16 0 0 0 0 0 – pět nulových bajtů

Třetí klíč má tak jen 216 možností – po dešifrování response umíme určit 2 poslední bajty MD4 hashe, což umožní jednoduché vyhledávání v předpřipravených slovnících – ověřit dešifrováním DES stačí jen malou část slovníku. Výpočet MD4 hashů je navíc rychlý a díky popularitě prolamování Windows hesel existují rozsáhlé slovníky [2].

4) Útok na jiné EAP

Mezi méně bezpečné typy EAP patří MD5 – algoritmus MD5 byl totiž už prolomený v roce 2004 a je jen otázkou času kdy někdo zveřejní aplikaci, která EAP-MD5 zneužije v praxi. Dále EAP, při kterých se používají certifikáty (EAP-TLS, EAP-TTLS), jsou bez ověření autenticity náchylné na man-in-the-middle útoky (kapitola 2.2.5)

2.2.4 Zamítnutí služby (DoS, Denial of Service)

Útoky zaměřené na zamítnutí služby jsou na použitém médiu (vzduch) lehko realizovatelné a dosahují okamžitý účinek. Nejsou však zaměřeny na přístup do sítě a na zneužití systému, ale na znemožnění práce uživatele na cílovém (napadeném) systému (případně celé síti), resp. paralýze jím poskytovaných služeb. Nejčastěji se tak děje zahlcením nebo vyčerpáním některých síťových zdrojů, případně složitými výpočetními úlohami jako šifrování nebo dešifrování [11].

Pro tento typ napadení může mít útočník různé druhy motivace:

- škodolibost / ekonomické cíle;
- dočasné odpojení stanice ze sítě za účelem získaní informací v době připojení;
- odpojení stanice ze sítě za účelem man-in-the-middle útoku (kapitola 2.2.5);
- DoS jen na zabezpečenou síť ve snaze donutit nezkušeného uživatele vypnout bezpečnostní prvky.

Většina z DoS útoků není trvalá, účinky zmizí jakmile útok přestane (vyjma případů pokud se zařízení zasekne nebo zahltí - Zahlcování tabulek, Poškozené rámce v kapitole 2.2.4) a síť se v krátkém čase (nejvíce však několik vteřin) zregeneruje. Jejich využití na získávání informací anebo man-in-the-middle útoky je však významné.

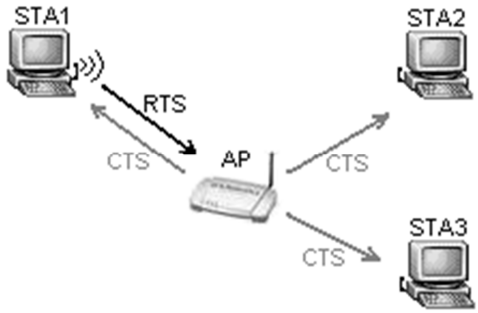
1) Útok na jiné EAP

Pro efektivní rušení pásma je nejlepší použít rušičku na naslouchajících frekvencích. Také je možné upravit na tento účel ovladače WLAN karty tak, aby mohla odesílat rámce bez čekání (nulový backoff time) a zahlcovat kanál náhodnými daty. Většina síťových karet ale neumožňuje konstantní vysílání rámců a firmware nedovolí vysílat v čase, kdy je detekovaná přicházející komunikace, a tak nedokážou kanál zahltit úplně, ale jen zhoršit propustnost a odezvu. Rušení pásma je náročné na sílu vysílaného signálu. Z bezpečnostního pohledu je nejméně obávaným útokem [29].

2) RTS/CTS

Pro přítomnost skrytých uzlů ve WLAN je ve standardu na zamezení kolizí pro posílání delších rámců definovaná technika řídících rámců Request To Send (RTS, požadavek na vysílání) a Clear To Send (CTS, povoleno vysílat). STA1 a STA3 mohou být navzájem mimo rádiového dosahu (obr. 8), teda STA1 neví, zda STA3 vysílá

a naopak. Pokud chce STA1 poslat delší rámec na AP a vyhnout se případné kolizi, pošle nejprve RTS s požadavkem na „rezervování“ kanálu na určitý čas, daným polem Duration v rámci. AP následně odpoví rámcem CTS, který vyhradí kanál na určitý čas (Duration) pro STA1.



Obr. 8 Příklad RTS/CTS komunikace [29]

Tento rámec je poslaný všem stanicím, aby bylo zřejmé, že v dané době může začínat vysílat jen STA1 (identifikovaná pomocí MAC adresy v CTS rámci). Každá stanice si po přijetí RTS anebo CTS rámce podle Duration nastaví Network Allocation Vector (NAV) - časovač, který indikuje obsazenost kanálu [29].

3) Flood RTS rámců

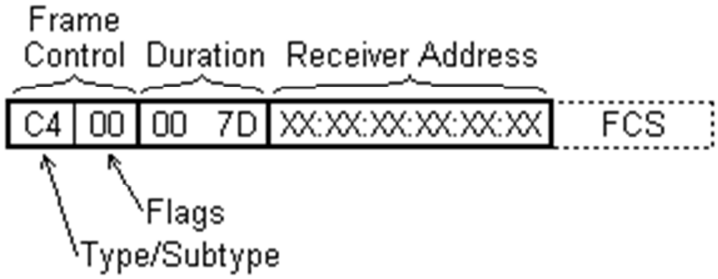
Cílem útoku je bez energeticky náročného zahlcování kanálu zabránit komunikaci. Princip je následující:

- pošleme RTS rámec na AP s velkou hodnotou Duration
- AP pošle všem CTS rámec s velkou hodnotou Duration
- stanice nevysílají (očekávaný efekt)

Standard povoluje stanicím vynulovaní NAV v případě, že byl přijatý RTS rámec a v očekávané době nebyl detekovaný přicházející signál (kanál zůstal volný) - to způsobí ukončení ignorování RTS/CTS a zabráni tak očividnému DoS. To znamená, že NAV budou mít nastavené jen stanice, které prvotní RTS nezachytili. Ostatní stanice včetně AP, mohou vysílat. Útok má teda požadovaný efekt v síti, kde je hodně skrytých uzlů (například městské přístupové sítě se směrovými anténami)[29].

4) Flood CTS rámců

CTS rámec je velmi jednoduchý, určený pro vyhrazení kanálu jen na určitou dobu. Posílá ho stanice anebo AP jako odpověď na RTS rámec. Na obr. 9 je příklad CTS rámce - Frame Control (řídící pole): Type 1 (Control - řídící rámec), Subtype 12 (Clear To Send, podtyp = CTS), volitelné (Flag) bity nastavené na 0 (tady je možných víc přijatelných kombinací).



Obr. 9 Formát CTS rámce [29]

Pole Duration je udávané v milisekundách, platné hodnoty jsou 0 až 32767, udávané v mikrosekundách. V našem případě ho nastavíme na velkou hodnotu 32000, to je v hexadecimálním tvaru 7D00 [29].

5) Deautentizace

Protože rámce nejsou žádným způsobem chráněny, je lehké je zfalšovat. Tak můžeme dosáhnout odpojení stanice od sítě po dobu útoku. Deautentizaci můžeme docílit různými způsoby:

- poslání falešného „Deauthentication“ rámce stanici (od AP);
- poslání poškozeného „Authentication“ rámce AP (od stanice), například se špatným sekvenčním číslem anebo použitým algoritmem – AP následně stanici deautentizuje [29],[14].

6) Smazání ARP cache

Pokud útok trvá déle (3-5 sekund), OS Windows připojení indikuje jako „odpojené“, čehož si uživatel může všimnout. Dosáhneme tím však smazání ARP cache, teda po zastavení útoku a obnovení spojení se pošle ARP request, jakmile stanice bude chtít

komunikovat pomocí IP protokolu (což často bývá na stanici i bez přítomnosti uživatele). Toto můžeme využít při útocích na WEP – zvláště ARP injekce (kapitola 2.2.2) [29].

7) Zahlcování tabulek

Každé zařízení má omezenou paměť. Jednoduché AP, určené pro domácnosti a malé firmy, dokážou autentizovat a asociovat malé množství stanic (většinou 16 až 256). To na legitimní používání postačuje, při útoku se však tabulky určené na udržování informací o stavu autentizace, asociace a vzájemného šifrovacího klíče (v případě WPA/WPA2) jednotlivých stanic mohou zaplnit. AP potom není schopné žádného dalšího klienta – v případě, že během útoku navíc deautentizujeme legitimní stanice, bude síť vyřazená z provozu. Pro některé typy AP není tento typ útoku závažný, po odpojení útočníka se dokáží lehko zregenerovat vyřazením neaktivních stanic [20].

8) Poškozené rámce

Chybně implementovaný firmware a ovladače je možné posláním konkrétně sestaveného rámce zaseknout. Může potom vykazovat různé nepředpokládané stavy - v případě samostatných zařízení „zatuhnutí“ anebo podivné chování; v případě OS GNU/Linux zaseknutí se ovladače jádra; v OS Windows zaseknutí systému. Pokud bychom toto zjednodušili, jsou to rámce, které mají některé z polí delší, jako je maximální velikost podle specifikace. Mohou to být například technické nebo testovací rámce s příliš dlouhým SSID. Sestrojit takový rámec můžeme ručně (například pomocí spolupráce s programem s Wireshark pro referenci jednotlivých polí) a poslat pomocí utility Framespam [29].

2.2.5 Man-in-the-middle

Útok „muže uprostřed“ je možné použít ve skutečnosti vždy, kdy si některá z komunikujících stran nemá možnost ověřit autenticitu té druhé. Typický příklad je autentizace STA vůči AP, přičemž AP svoji autenticitu nijak neprokáže. Man-in-the-middle na druhé vrstvě je nejnebezpečnějším útokem na bezdrátovou síť, protože je možné zneužít protokoly vyšší vrstvy, a to také té „bezpečné“, jako například

SSL. Získávání osobních údajů, hesel, modifikace provozu, jsou možné i přes šifrované spojení [4].

1) Falešné AP

Tento útok spočívá v zamaskování autentizovaného přístupového bodu falešným přístupovým bodem. To znamená, že útočník nakonfiguruje svůj vlastní přístupový bod, přičemž nastaví SSID a číslo kanálu tak, aby tyto údaje odpovídaly autentizovanému přístupovému bodu. Poté ještě na falešném zařízení povolí např. pouze port 80 pro prohlížení webových stránek. K tomuto přístupovému bodu musí být připojena anténa s velkým ziskem, resp. musí být zajištěno, aby falešné AP vykazovalo lepší úroveň signálu než AP autentizované. Tak dojde k zamaskování tím, že při autentizaci klienta k přístupovému bodu klientská NIC upřednostní bezdrátovou síť s lepší úrovní signálu.

Aby stanice použila toto podstrčené AP namísto původního „pravého“, je možné:

- použít stejné SSID – použití jiného SSID je též možné, pokud je klient nakonfigurovaný na připojení se do libovolně dostupné sítě;
- použit síťovou kartu (anebo AP) s velkým výkonem, resp. směrovou anténou - aby bylo stanicí, kterou chceme napadnout, preferované;
- spustit DoS na stanici (pomocí druhé síťové karty) – naší snahou je donutit ji vyhledávat nové AP (kapitola 2.2.2);
- spustit DoS na pravé AP anebo kanál, v kterém pracuje (pomocí druhé síťové karty) – donutíme tak stanice připojit se na další dostupné AP, tím bude to falešné. (kapitola 2.2.4).

Klient se tedy připojí k falešnému AP a má-li povolen pouze port 80, veškeré zabezpečené transakce za normálních okolností spravované portem 443, který se používá k zabezpečenému přístupu na webové stránky pomocí protokolu TLS (Transport Layer Security), budou pro útočníka viditelné. Útočník tak může zachytit prakticky všechny citlivé informace – přístupová hesla do poštovních schránek, při nákupu virtuální platební kartou apod. Falešné AP jsou hrozbou i v prostředí velké firmy, kde např. nezodpovědný zaměstnanec nechal do sítě připojené AP, které slouží jako útočníkovi jako „zadní vrátka“ do (jinak dobře zabezpečené) sítě [2],[12],[20].

3 KROKY ÚTOČNÍKA PO PRŮNIKU ZABEZPEČENÍM BEZDRÁTOVÉ SÍTĚ

Povede-li se útočníkovi proniknout zabezpečením bezdrátové sítě, není ještě u cíle. Pokud se jedná o náhodného útočníka, který testuje svoje schopnosti nebo potřebuje získat přístup k internetu zadarmo, tak se například spokojí jen s přidělením IP adres od DHCP serveru a jeho činnost se nadále projeví jen větší zátěží firemní linky. Pokud však útočník hledá konkrétní cíl např. sdílená firemní data nebo je jeho cílem destrukce firemní sítě, bude potřebovat informace o fungování vnitřní lokální sítě nebo vzdálený přístup na některý z existujících počítačů.

Obr. 9 Kroky útočníka uvnitř firemní sítě [20]

Obecný průnik zabezpečením systému s využitím vzdáleného přístupu se nechá popsat pěti základními kroky:

- Získávání informací
- Skenování sítě
- Získání přístupu
- Udržení přístupu
- Zahlazení stop

3.1 Získávání informací

Prvním krokem je přípravná fáze, která spočívá ve shromažďování co největšího množství relevantních informací o cíli útoku. Má několik částí:

- aktivní průzkum
- pasivní průzkum
- footprinting
- pasivní skenování
- enumerace

Aktivní a pasivní průzkum spočívá ve vyhledávání informací o struktuře sítě. Zejména monitorování síťového provozu, hledání vodítek a analyzování jeho skladby.

Footprinting je fáze, která využívá poznatků aktivního a pasivního průzkumu k vytvoření ucelené představy o fungování a struktuře systému. Používají se např. DNS dotazy, skenování portů, ping a jiné. Nejvíce používanými programy pro Windows jsou: Sam Spade a NeoTrace [20].

Pasivní skenování je souborem technik, kdy se pomocí vnějších projevů zjišťuje, které počítače v síti jsou dostupné z internetu a jaké služby nabízejí. Sem patří např. skenování portů otevřených TCP/UDP portů, identifikace operačních systémů, identifikace architektur (x86, Alpha, Sparc) používaných v rámci sítě. Používané techniky jsou např. ICMP ECHO, TCP Sweep, Stealth skenování k obcházení filtrovacích pravidel, koordinované skenování schopné obejít systémy IDS. Používané nástroje NMAP, ScanRand a jiné [26].

Enumerace je soubor technik, kdy útočník aktivně zkoumá napadaný počítač. Cílem je získat konkrétní údaje o konkrétním stroji, jako jsou pracovní skupina, jméno a heslo přihlášeného uživatele, seznam sdílených prostředků apod. Používané nástroje pro Windows: Enum, Net View, Net Use, pro Unix: Snmpwalk, Muts.

Ukázkový výpis programu NetView může vypadat třeba takto:

C:\net view

\\NOVAK

\\USER

\\INET

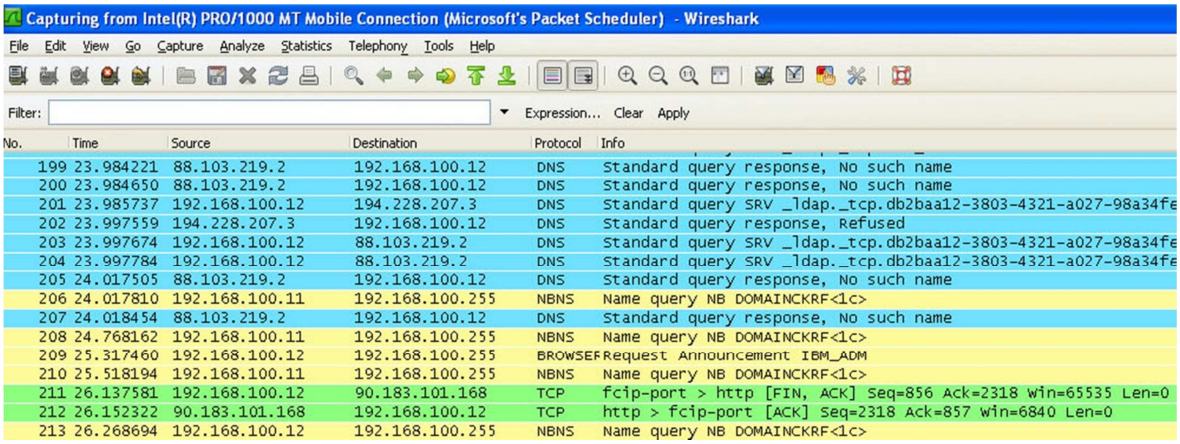
\\SERVER login: user; pass: deny

Příkaz byl úspěšně dokončen.

Na výpisu je vidět seznam počítačů připojených do sítě. Správce serveru, pravděpodobně aby si ušetřil práci, uvedl do poznámky uživatelské jméno i heslo pro připojení [20].

3.2 Skenování sítě

Druhou fází je aktivní skenování. Na rozdíl od pasivního skenování se zaměřuje na konkrétní cíle. Úkolem je opět lokalizovat otevřené porty, zjistit přesnou verzi použitého operačního systému, hledaní slabin v jeho zabezpečení. Výsledkem úspěšného skenování je nalezení výchozího místa průniku.

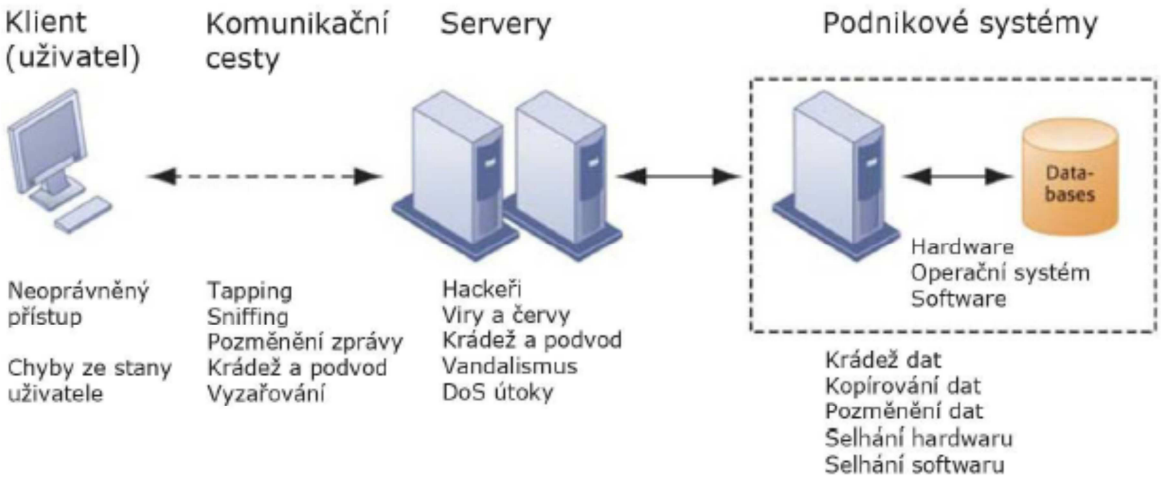


Obr. 10 Výřez protokolového snifferu WireShark (příloha P IV)

Ideálním nástrojem je program Wireshark (příloha P III), protokolový sniffer, který dokáže celý paket dekódovat a ukázat ho celý, jak ho počítač poslal. Program pracuje pasivně - tj. nic z našeho počítače neodesílá, a je proto skoro nezjistitelný. Jeho výhoda je také, že je šířen pod licencí GNU/GPL.

3.3 Získání přístupu

Ve fázi získání přístupu dochází k samotnému útoku na některou z klíčových komponent systému. K útoku může dojít prostřednictvím místní sítě, na dálku přes Internet nebo v místě, kde se fyzicky nachází hardware podnikového systému prostřednictvím krádeže či podvodu. Na každou z těchto komponent lze aplikovat jiné metody útoku. Taxonomie těchto útoků je zobrazena na obr. 11.



Obr. 11 Druhy útoků podle klíčových komponent systému [20]

Typickým příkladem pro získání přístupu je program Nessus – exploit scanner. Pro příklad uvádím některé pluginy pro získání přístupu, které obsahuje:

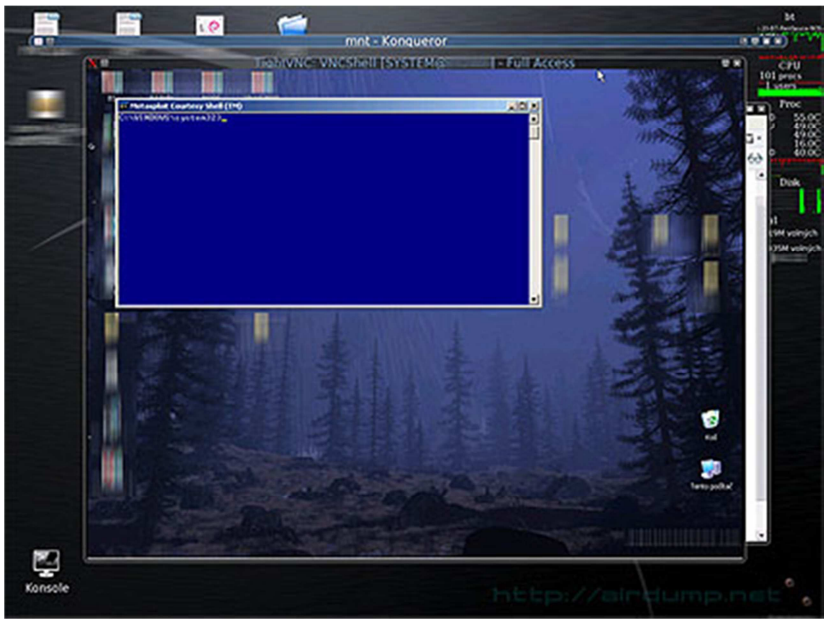
- Backdoors (trojské koně)
- Default Unix Acounts
- Denial od Service
- Zranitelnosti služby Finger

- Vzdálené získání shell
- Vzdálené získání root
- Vzdálený přístup k souborům

Nástroj exploit je speciální program nebo sekvence příkazů, které využívají chybu programátora, která způsobí původně nezamýšlenou činnost software a umožňuje tak získat nějaký prospěch. Obvykle se jedná o ovládnutí počítače nebo nežádoucí instalaci software, která dále provádí činnost, o které uživatel počítače neví (např. nějaký druh malware) [1].

3.4 Udržení přístupu

Jakmile se jednou útočníkovi podaří proniknout do serveru, je v jeho zájmu si tento přístup udržet. V této fázi provádí instalaci rozličných nástrojů, s jejichž pomocí toho lze dosáhnout. Takovými nástroji jsou například rootkity (soubory utilit, které jsou schopny např. zamaskovat běžící proces, zvýšenou síťovou aktivitu nebo změnu v registrech) nebo zadní vrátka. Také je možno pozměnit konfiguraci již existujících, běžících programů, případně si vytvořit záložní uživatelské konto.



Obr. 12 Vzdálení plocha napadeného počítače

po spuštění exploit (příloha P IV)

Příkladem může být program Backtrack 2. Po spuštění toho programu je potřeba pouze nakonfigurovat IP adresu PC v síti a portu kam se má exploit směřovat. Když se kód na vzdáleném PC úspěšně spustí, útočník získá mimo „prohlížení“ vzdálené plochy přes software TightVNC, také kompletní administrátorský přistup, PC může plně ovládat a instalovat další aplikace, pomocí kterých může anonymně přistupovat do sítě Internet [1].

3.5 Zametání stop

K završení úspěšného útoku je potřeba za sebou zamést stopy. Zametání stop je soubor činností, které mají za úkol zničit důkazy o hackerově přítomnosti v systému. Mezi techniky zametání stop patří pozměňování nebo smazání souboru logů, pozměňování datových toků, vypnutí systémového auditu pro prolomená konta. Pokud byl počítač použit jako anonymní terminál pro útočníkovy aktivity na internetu, nezřídka pak použije pro zametení stop destrukci operačního systému [22].

Jako jednoduchý příklad si můžeme ukázat vypnutí logu Prohlížeče událostí přes utilitu REGEDIT:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog, kde výchozí hodnotu Autostart (0x2) změníme na Disable (0x4).

II. PRAKTICKÁ ČÁST

4 UKÁZKA PRONIKNUTÍ DO FIREMNÍ BEZDRÁTOVÉ SÍTĚ

Pro ukázku kontrolního proniknutí do firemní bezdrátové sítě jsem se rozhodl použít reálnou bezdrátovou síť. V laboratorních podmínkách nelze reálně vyzkoušet a popsat všechny kroky útočníka.

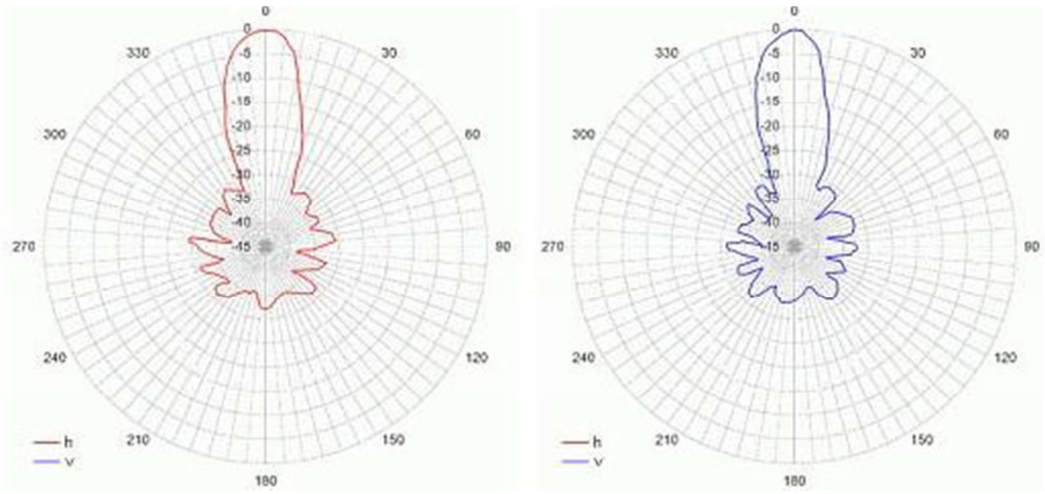
Prvním krokem byl výběr vhodné sítě. Při skenování firemních bezdrátových sítí v Českém Krumlově, mne zaujala síť, která se prezentovala svým SSID jako Parking s šifrováním WEP. Šlo o lokalitu, která je veřejnosti pravidelně prezentována jako centrála kamerového systému pro všechna veřejná parkoviště v Českém Krumlově. Lze tedy předpokládat, že pokud by se podařilo proniknout do této firemní bezdrátové sítě, mohl by útočník získat přístup ke kamerovému systému. Tento systém následně destruovat nebo použít data k majetkové trestné činnosti. Protože vedení společnosti nemělo o této síti žádné informace, získal jsem souhlas pro testovací proniknutí s příslibem předání výstupních informací pro případnou změnu řešení bezdrátového připojení v této lokalitě.

4.1 Vybavení

K ukázce proniknutí byla použita směrová anténa (obr. 13) Buffalo Yagi XP 16dB (tab. 3). Síťová karta Buffalo AirStation WLI-PCM.L11GP s chipsetem Orinoco, notebook IBM T42p s operačním systémem Windows 7 Professional. Jako software pro proniknutí sítí jsem vybral balíček Windows Wifi Collection – aircrack. Většina programů byla vyvinuta pro operační systém Linux. Instalace a práce s tímto systémem ovšem vyžaduje určitou uživatelskou úroveň a této v práci si ukážeme, že je snadné použít i programy pro systémy typu MS Windows.

Zisk	16dBi
V pásmu	2400-2500MHz
Svislá paprsková šíře	18°
Horizontální paprsková šíře	20°
Impedance	50ohm
Váha	0,9kg
Rozměry	600/80mm
Obrácené záření	-20dBi
Konektor	RSMA-male

Tab. 3 Technická data Orinoco Yagi XP



Obr. 13 Vyzařovací charakteristika antény Orinoco Yagi XP [23]

Kompletní vybavení pro průniky do bezdrátových sítí včetně předinstalovaného software si může kdokoli zakoupit na specializovaných internetových obchodech jako je např. HTTP://WWW.SECPOINT.COM/PORTABLE-PENETRATOR.HTM za cenu 15.000 Kč včetně DPH a dopravy. Případně lze zakoupit vše v internetovém bazaru za cenu 3000 s DPH ovšem bez potřebného programového vybavení. Tyto částky ukazují, že potřebné vybavení je cenově dostupné široké veřejnosti.

Obr. 14 Použitá sestava pro skenování bezdrátové sítě

4.2 Zjištění WEP klíče

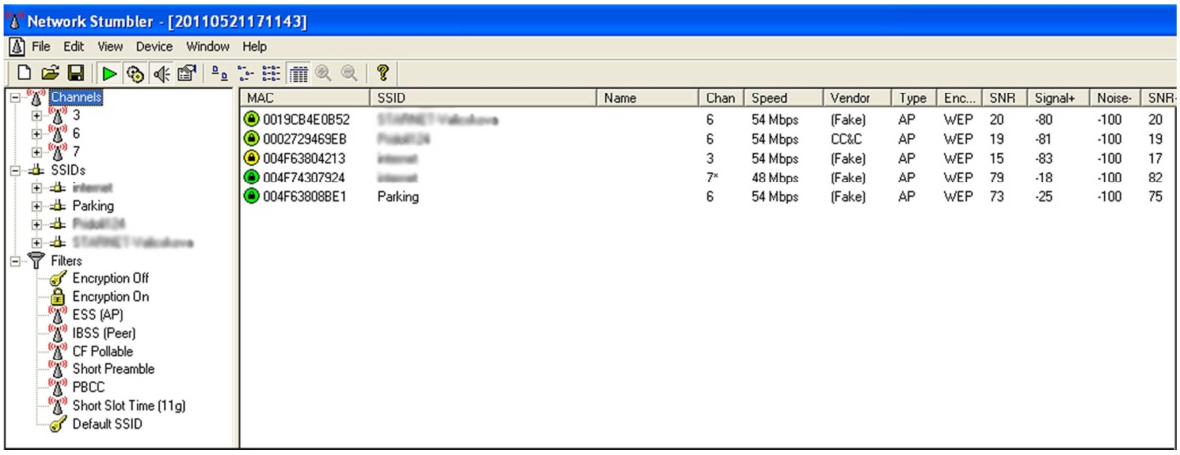
Jak jsem již zmínil, pro získání klíče jsem použil softwarový balíček Windows Wifi Collection – aircrack. Tento program bohužel není universální. Podporuje jen omezený počet bezdrátových karet. Seznam těchto karet je k dispozici jako příloha u instalačního souboru. Optimální karta je s chipsetem od firmy Orinoco.

Aircrack je program pro 802.11a/b/g sítě, který umí po nashromáždění dostatečného počtu paketů vypočítat jejich 40, 104, 256 a 512 bitové WEP klíče. Také umí útočit na sítě používající WPA, a to buď pokročilými metodami jako je třeba KoreK, nebo prostou hrubou silou. Implementuje standardní útok FMS, ovšem s několika optimalizacemi, takže je rychlejší, než ostatní nástroje pro prolamování klíče WEP [27].

Prvním krokem bylo stažení softwarového balíčku ze stránek výrobce, a to ve verzi Portable, protože instalace nezatěžuje operační systém. Po prvním spuštění programu je uživatel vyzván k nahrazení standartního ovladače od výrobce, ovladačem speciálně upraveným pro práci s aircrack 2.1. Není potřeba mít obavy z následné nestability systému při běžné práci s bezdrátovou kartou, žádné problémy se po instalaci neobjevily.

Obr. 15 Odposlouchávání komunikace v bezdrátové síti ve sledované lokalitě

Jako první krok pro zjištění WEP klíče je potřeba získat velké množství paketů a k tomu odpovídající množství IV. Čas potřebný pro získání toho potřebného množství je dán provozem na bezdrátové síti.

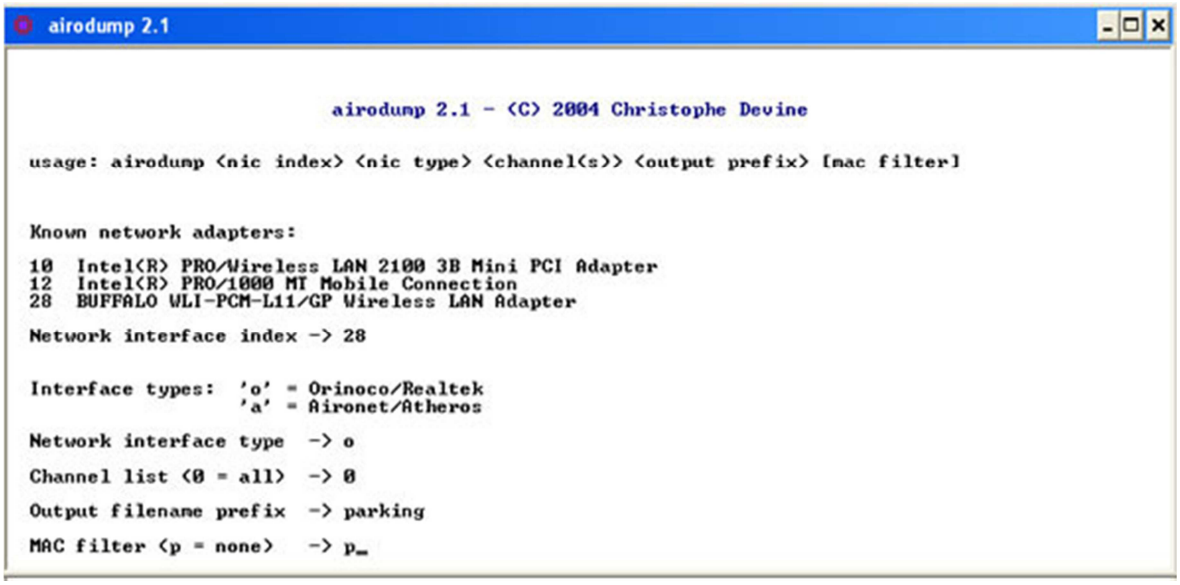


Obr. 16 Výřez okna z programu Netstumler (příloha P V)

Pomocí programu Netstumbler (obr. 16), který umí měřit i sílu signálu, jsem si našel optimální místo (obrázek 15) pro sběr potřebných dat, bez ztráty paketů způsobenou slabým signálem.

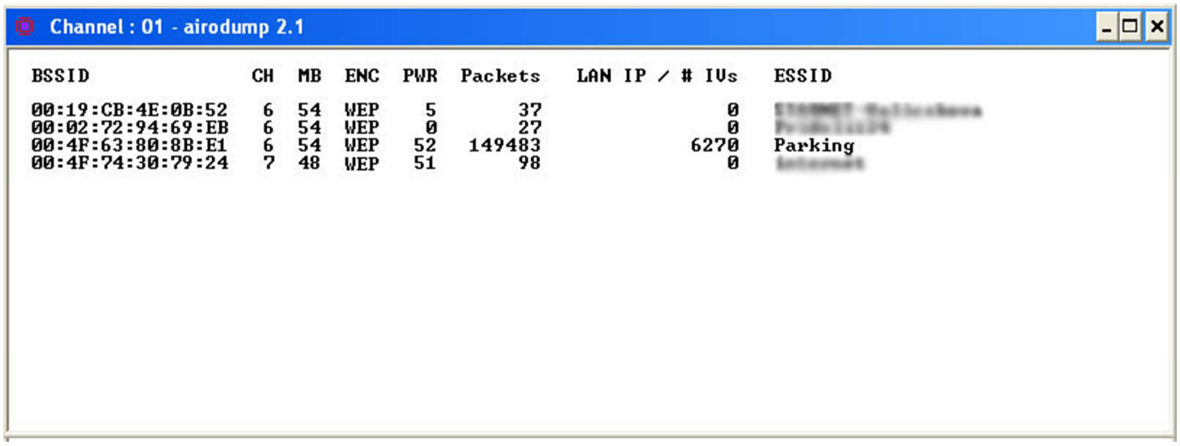
Pro sběr potřebným paketů jsem použil utilitu airodump 2.1. Po spuštění této utility je uživatel vyzván k výběru podporované bezdrátové karty, pokud je v zařízení přítomno více karet (obr. 17). Dalším krokem je výběr chipsetu bezdrátové karty. Pokud se uživatel chce věnovat sledování pouze jednoho kanálu, v našem případě již víme z programu NetStumler že chceme sledovat kanál číslo 6, má možnost si tento kanál vybrat a tím urychlit požadovaný sběr dat. Posledním krokem je zvolit název souboru, kam se budou naskenovaná data ukládat, případně zvolit MAC filter, pokud je známa MAC adresa sledovaného zařízení, a to opět pro urychlení sběru dat na společném kanále.

Po vyplnění základní obrazovky se spustí sběr paketů na sledované síti. Pokud je na sledované síti slabý provoz je potřeba pomocí utility airplay, ze stejného programového balíčku, spustit paket injection, abychom si potřebný provoz dodali sami. Může se stát, že po spuštění paket injection se žádný datový tok neobjeví. Pak jsme buď daleko od AP a nebo data jsou v G módu zatímco my je chytáme v B módu.

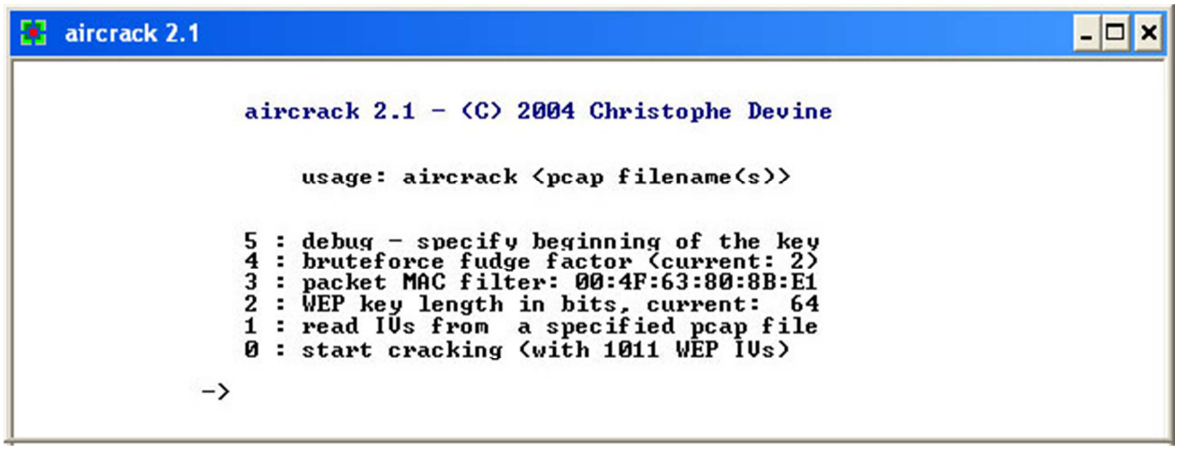


Obr. 17 Okno programu airodump 2.1, konfigurace před spuštěním sběru paketů

Po hodině sledování jsem měl nasbíráno 149483 paketů a 6270 IV (obr. 18). Prolomení WEP není exaktní věda. Počet IV potřebných pro prolomení WEP klíče záleží na délce WEP klíče a mnohdy i štěstí. Obvykle, lze 40-bit WEP (64 bit klíč, 5-místné heslo) prolomit s počtem zachycených IV 30 až 300 000 a 104-bit WEP (128 bit klíč, 13-místné heslo) s 100 000 až 1,500,000 IV. Klidně to ale může být číslo vyšší, třeba 2 miliony IV a víc [1].



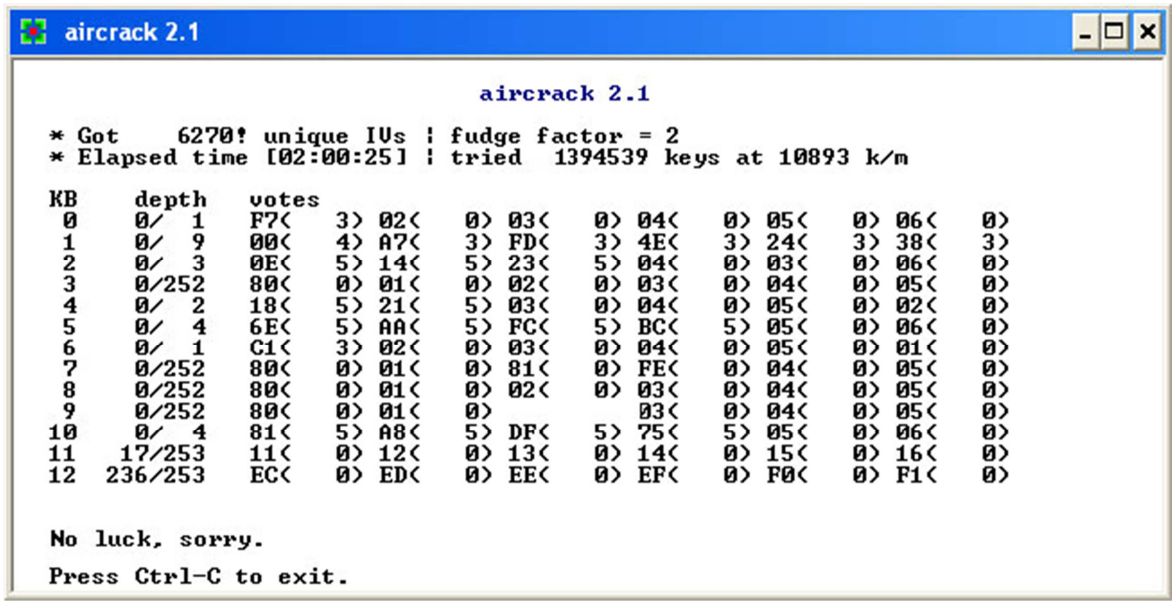
Obr. 18 Okno programu airodump 2.1, sběr paketů a IV



Obr. 19 Okno utility aicrack 2.1, konfigurace

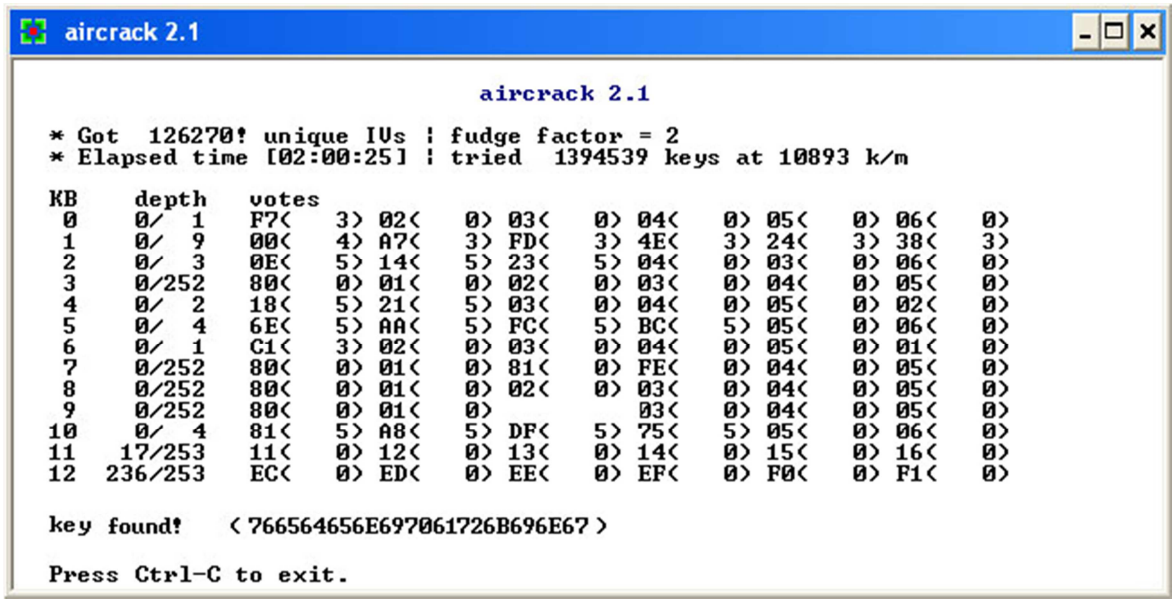
Pokud máme vytvořený soubor s nasbíranými pakety, můžeme se pokusit o dešifrování WEP klíče. Pro tento účel použijeme utilitu aircrack 2.1, která má implementovány KoreK algoritmy. Najdeme si v adresáři s programem airdump námi vytvořený soubor parking.pcap, který stylem plug and play vložíme do okna programu aircrack 2.1 (obr. 19).

Vidíme, že se našimi daty vyplnily řádky 3: Mac filter a 0: Start cracking. Hodnotu 2: Fudge factor (rozmezí 1 – 10), která nám udává, jak hluboko v datech má WEP klíč hledat, neměníme. Výrobcem je doporučeno tuto hodnotu měnit až při neúspěchu v hledání nad 4 milióny IV. Poslední hodnota, kterou nastavíme je 2: WEP key length (výchozí hodnota 64). Délku klíče ovšem nemáme odkud zjistit. Tato informace je ukryta a není nikdy přítomna v management nebo data paketech. Není tedy žádná možnost, jak to zjistit před tím, než se klíč povede prolomit. Následkem toho utilita airodump není schopna reportovat délku WEP klíče. Právě proto je doporučeno testovat všechny délky klíče. Když máme 2500 IV, spustíme aircrack s hodnotou délky klíče "64" pro prolomení 40bitového WEP klíče. Pokud klíč nebude nalezen, restartujeme aircrackg s hodnotou délky klíče "64" pro prolomení 104bitového WEP klíče.



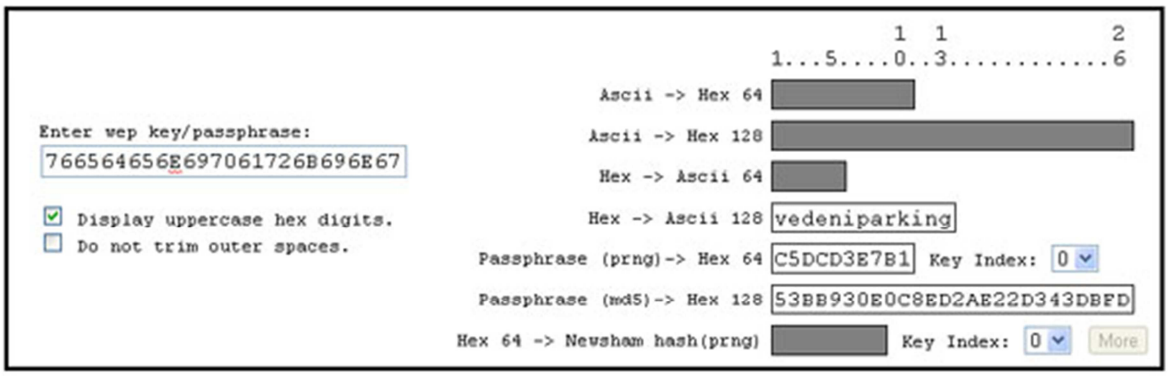
Obr. 20 Okno programu aircrack 2.1, výsledek pokusu o prolomení WEP

Po 25 minutách testování jsme dospěli k neúspěšnému výsledku (obr. 20). Klíč nebyl nalezen. Je potřeba tedy nasbírat více paketů. Proto bylo potřeba se vrátit a odposlechnout další data. Naštěstí byl provoz na síti tentokrát větší a během 3 hodin se povedlo nasbírat 2098734 paketů a z toho 126270 IV.



Obr. 21 Okno programu aircrack 2.1, získání WEP klíče

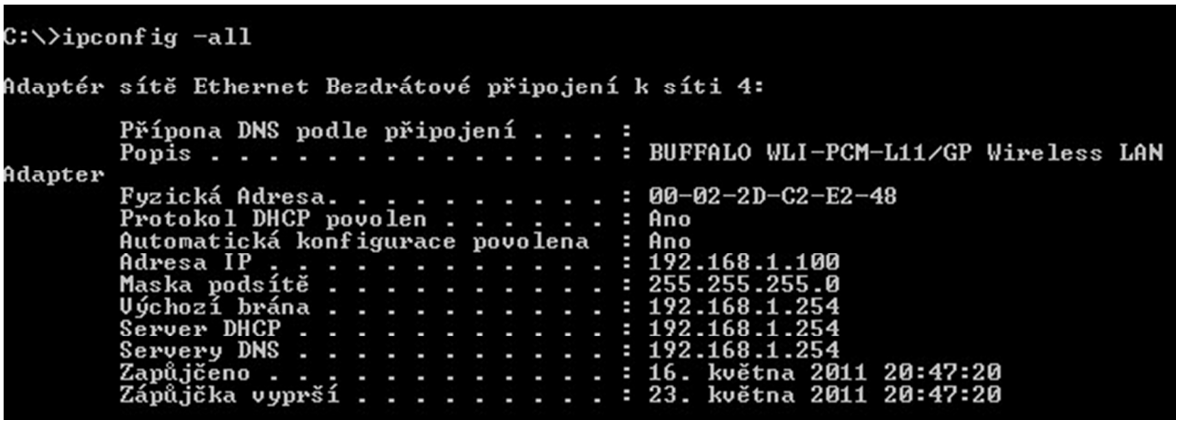
Po následném dešifrování se za 2 hodiny povedlo najít požadovaný klíč. Ten se objevil v hexadecimální formě (obr. 21). Pokud si toto číslo nedokážeme převést sami, můžeme použít programy. V našem případě jsme zvolili on-line převodník dostupný na HTTP://WWW.LATINSUD.COM/WEPCONV.HTML



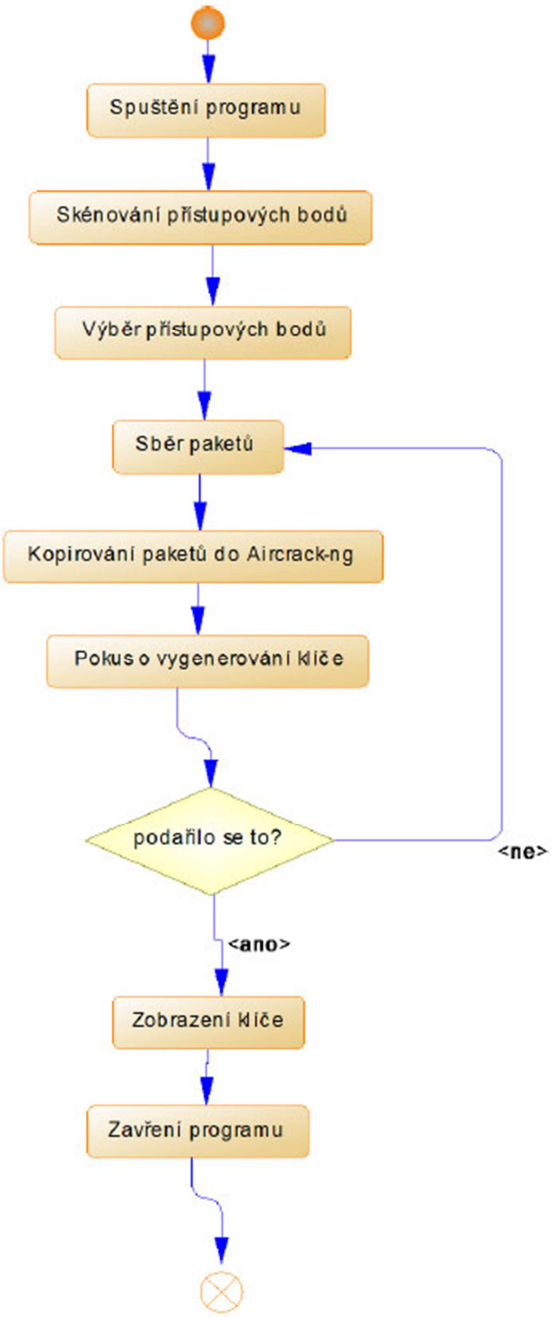
Obr. 22 Převod hexadecimálního řetězce na Ascii řetězec

Po zadání hexadecimálního řetězce se nám objevilo v pravé části heslo (obr. 22). Pro názornost jsem toto heslo zobrazil, protože v současné době na základě výsledků této práce, byla bezdrátová síť ve sledované lokalitě překonfigurována včetně výměny zařízení.

Nyní se naposledy můžeme vrátit k odposlouchávané síti a heslo vyzkoušet. Po asociaci s AP nám byla přidělena IP adresa a DNS (obr. 23). Další kroky jak postupovat jsou v kapitole 3 této diplomové práce.



Obr. 23 Přiřazení IP adresy interním DHCP serverem pro prolomení WEP klíče



Obr. 24 Diagram aktivit

- utilita Aircrack

5 PŘEHLED ÚROVNĚ ZABEZPEČENÍ FIREM V REGIONU

V následující části se budeme zabývat praktickým porovnáním zabezpečení firemních bezdrátových sítí. Lokality pro měření byly vybrány s ohledem na koncentraci firem. Lokalitou pro první měření bylo zvoleno krajské město Jihočeského kraje České Budějovice (dále jen: ČB) a to z toho důvodu, že je zde registrováno nejvíce firem v kraji. Lokalitou druhého měření bylo zvoleno okresní město Český Krumlov (dále jen: ČK) vzdálený cca 25km jižně od Českých Budějovic, a to z toho důvodu, že zde mám sídlo podnikání. V ČK bylo měření hlavně zaměřeno na průmyslovou zónu Tovární ulice, kde sídlí všechny velké firmy z ČK. Měření v obou zmíněných lokalitách bylo provedeno v květnu 2011 a bylo zaměřeno na bezlicenční frekvenční pásmo 2,4GHz.

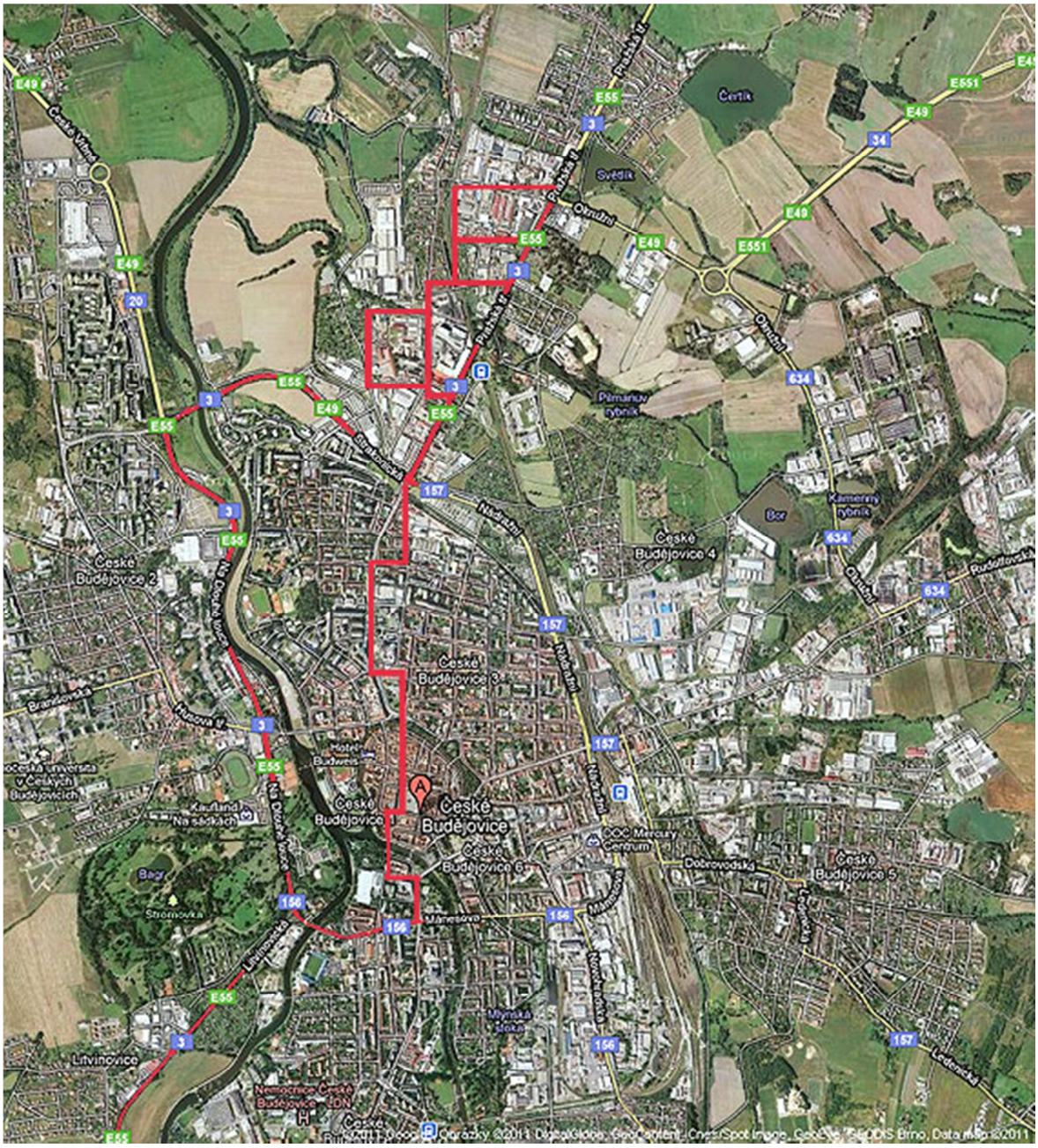
5.1 Předpoklady pro měření a analýzu

Pro stanovení předpokladů v rámci této práce jsem vycházel z dostupných zdrojů [6] a [9], které se již problematice věnovaly v jiných lokalitách. Tyto zdroje ovšem neposkytují aktuální data. Proto jsem ve stanovení předpokladů zohlednil i vývoj v oblasti bezdrátových technologií. Hlavními předpoklady pro porovnání zabezpečení sítí jsou:

- Více jak 80% dostupných přístupových bodů bude používat zabezpečení
- polovina a více zabezpečených přístupových bodů bude zabezpečena šifrováním WPA nebo WPA2
- v četnosti kanálů frekvenčního pásma bude použito celé pásmo – snaha o změnu výchozího nastavení přístupového bodu

5.2 Postup měření

Měření probíhalo pomocí osobního automobilu projíždějícího lokalitami rychlostí do 50 km/h. V případě upřesňujícího měření v průmyslové zóně ČK bylo měření prováděno ze stojícího vozidla v těsné blízkosti firemních budov. K získání dat byla použita měrová anténa Yagi XP 16dB umístěna v interiéru vozidla v blízkosti čelního skla, notebook IBM T42p se systémem Windows 7 Professional 32bit. Jako softwarové vybavení pro sběr a export dat bylo použito programu ViStumbler.



Obr. 25 Trasa měření v Českých Budějovicích

Trasa v Českých Budějovicích vedla okrajovými částmi s objekty pro drobné podnikání až do průmyslové zóny. Následně přes centrum, kolem objektů s nájemnými kancelářemi. Trasa měření je znázorněna na obr. 25.

V Českém Krumlově byla preferována již zmíněná Tovární ulice a následně trasa vedla přes centrum Českého Krumlova, kde jsou v dnešní době pouze kanceláře, hotely a penziony. Trasa měření je zobrazená na obr. 26.

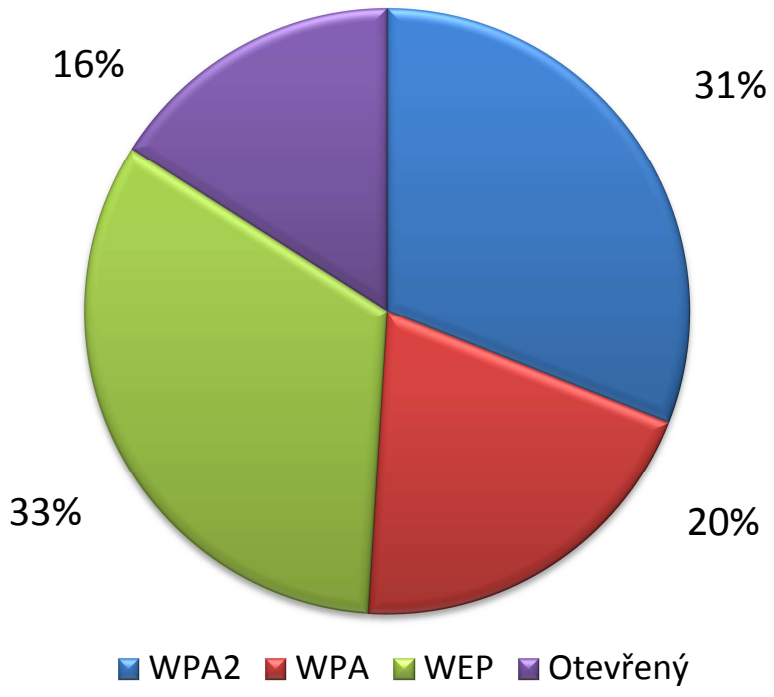
Obr. 26 Trasa měření v Českém Krumlově

5.3 Zpracování získaných dat

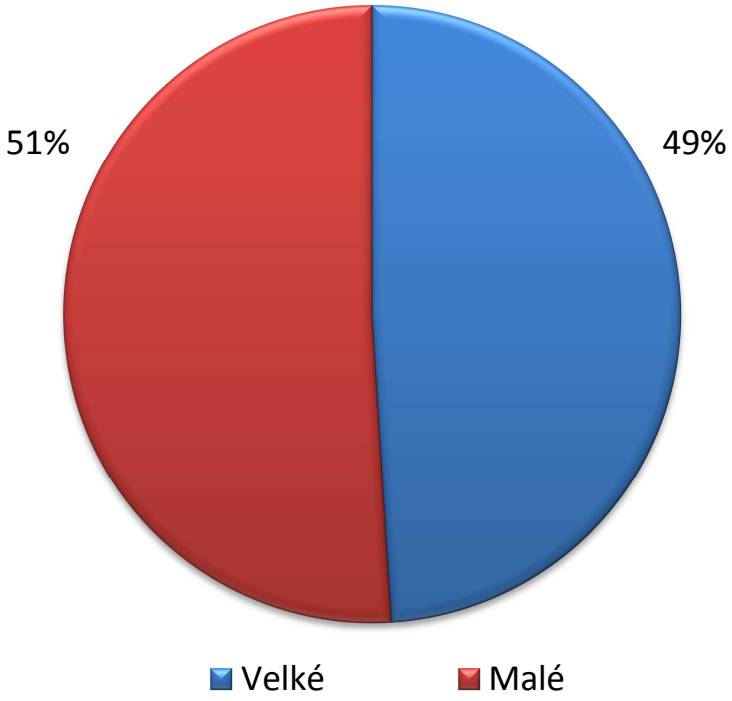
Naměřená data byla postupně zpracována do tabulek pomocí tabulkového procesoru a za využití filtrů byly získány detailní informace o zaznamenaných bezdrátových sítích. Tyto informace byly rozděleny podle posuzovaných kritérií a následně porovnány s výsledky měření na druhé trase. Protože cílem této kapitoly je vyhodnocení zabezpečení firemních bezdrátových sítí, bylo nutné provést oddělení SSID soukromých osob, jejichž signál se překrýval se signálem firemních bezdrátových sítí.

5.4 Vyhodnocení

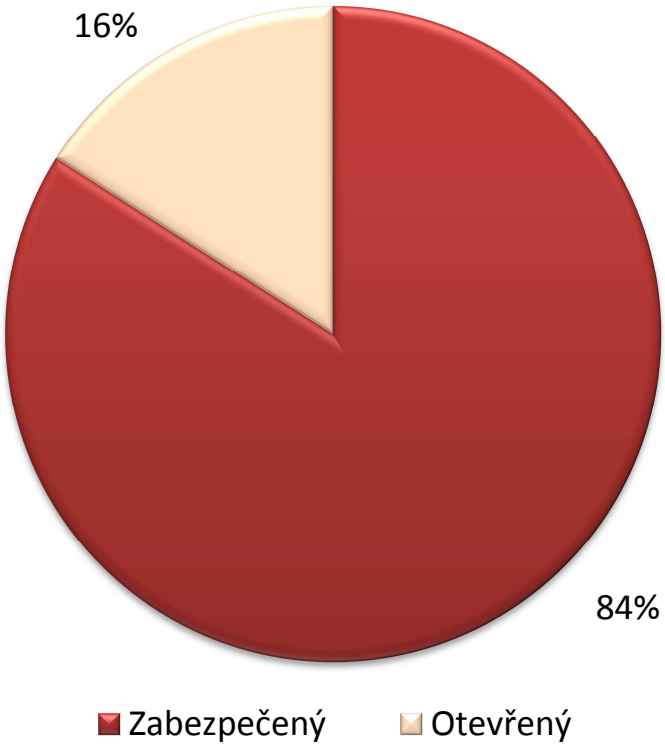
Celkově během měření v lokalitě Českých Budějovic bylo zaznamenáno 751 jedinečných bezdrátových sítí. Z toho 235 bylo jednoznačně určeno jako firemní sítě. Z toho 74 (31 %) používalo silné zabezpečení WPA2, zabezpečení typu WPA bylo u 46 (20%) sítí. Zastaralé zabezpečení technologií WEP používalo 78 (33 %) sítí. U 37 (16%) nebylo nastaveno žádné zabezpečení šifrováním. Sečteme-li nezabezpečené sítě a sítě používající slabé WEP zabezpečení vychází orientační údaj o počtu sítí s vysokým rizikem napadení. V případě Českých Budějovic je až 49 % naměřených sítí potenciálně velmi snadno napadnutelných.



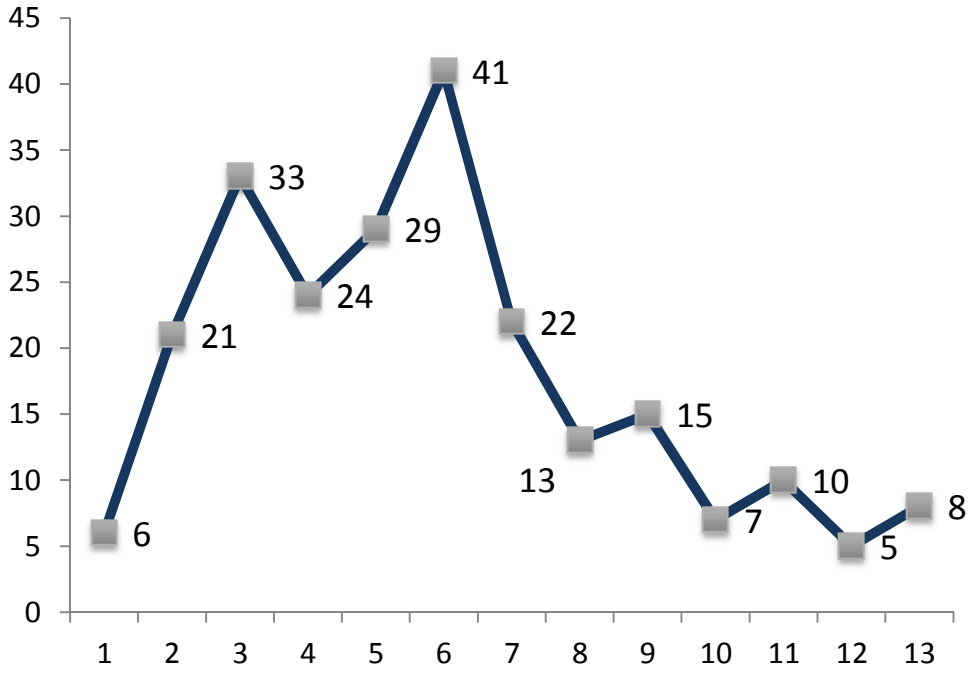
Graf 1 Zabezpečení AP – České Budějovice



Graf 2 Podíl rizika napadení AP – České Budějovice

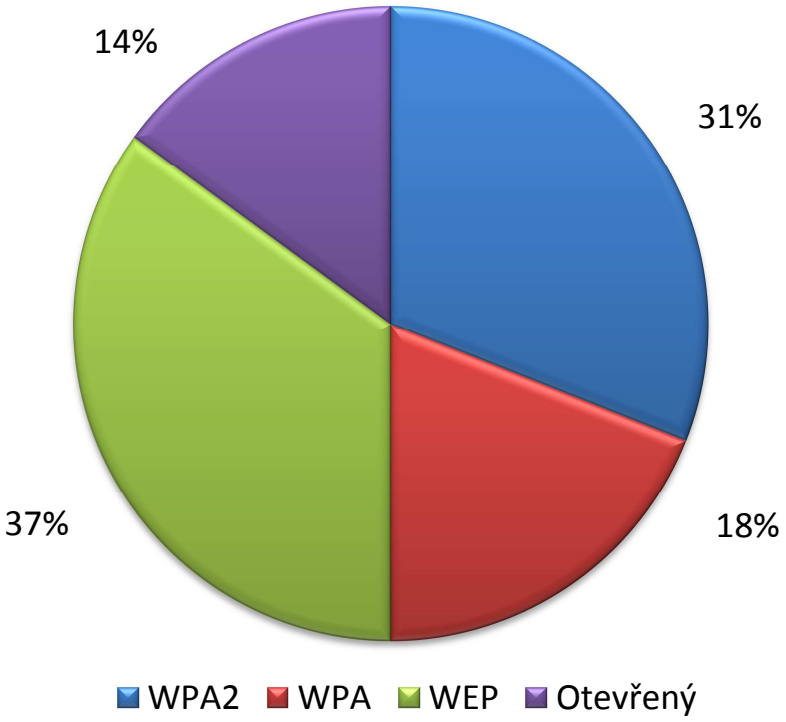


Graf 3 Podíl nezabezpečených AP – České Budějovice

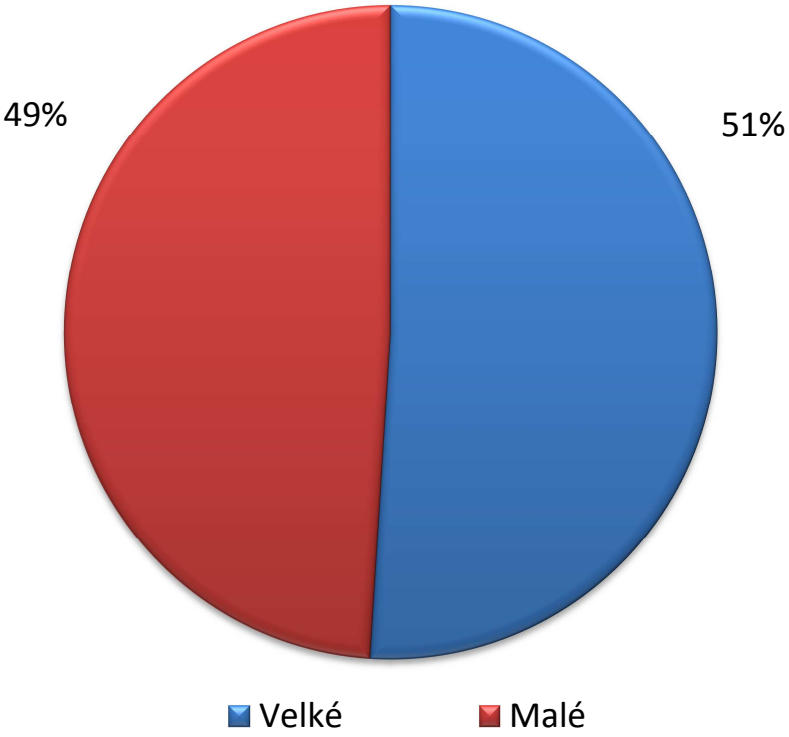


Graf 4 Podíl AP na kanál pásma – České Budějovice

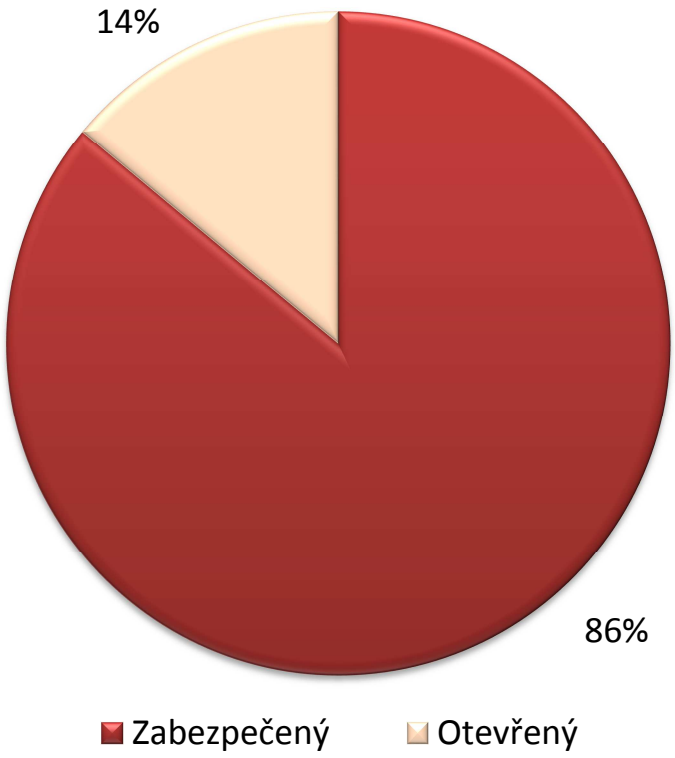
Během měření v lokalitě Českého Krumlova bylo zaznamenáno 353 jedinečných bezdrátových sítí. Firemních sítí bylo jednoznačně určeno 150. Z toho 46 (31 %) používalo silné zabezpečení WPA2, zabezpečení typu WPA bylo u 27 (18%) sítí. Zastaralé zabezpečení technologií WEP používalo 56 (37 %) sítí. U 21 (14%) nebylo nastaveno žádné zabezpečení šifrováním. Sečteme-li nezabezpečené sítě a sítě používající slabé WEP zabezpečení vychází orientační údaj o počtu sítí s vysokým rizikem napadení. V případě Českého Krumlova je až 51 % naměřených sítí potenciálně velmi snadno napadnutelných.



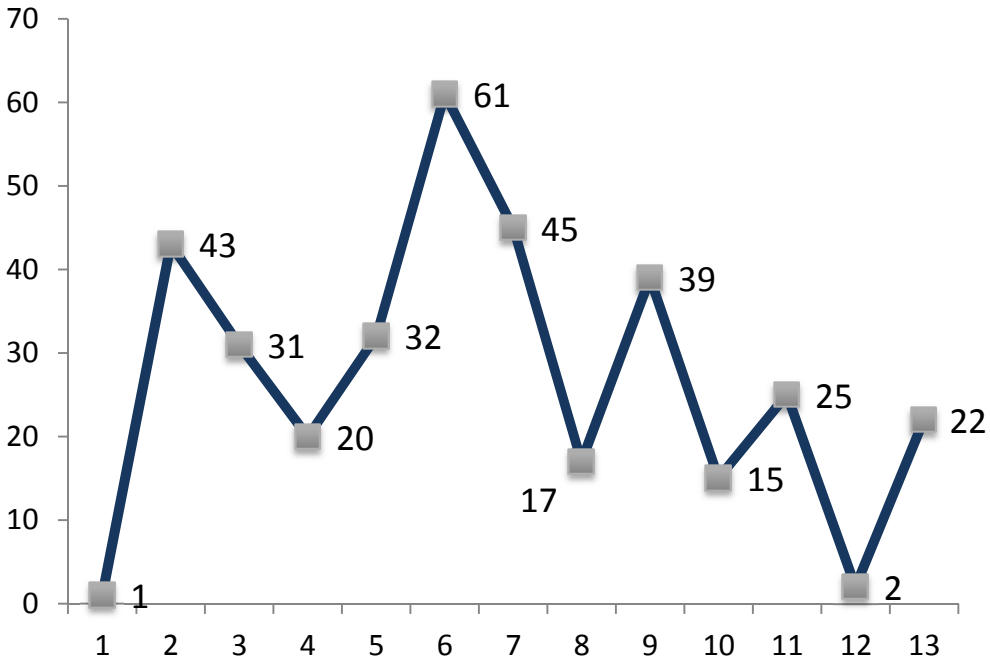
Graf 5 Zabezpečení AP – Český Krumlov



Graf 6 Podíl rizika napadení AP – Český Krumlov

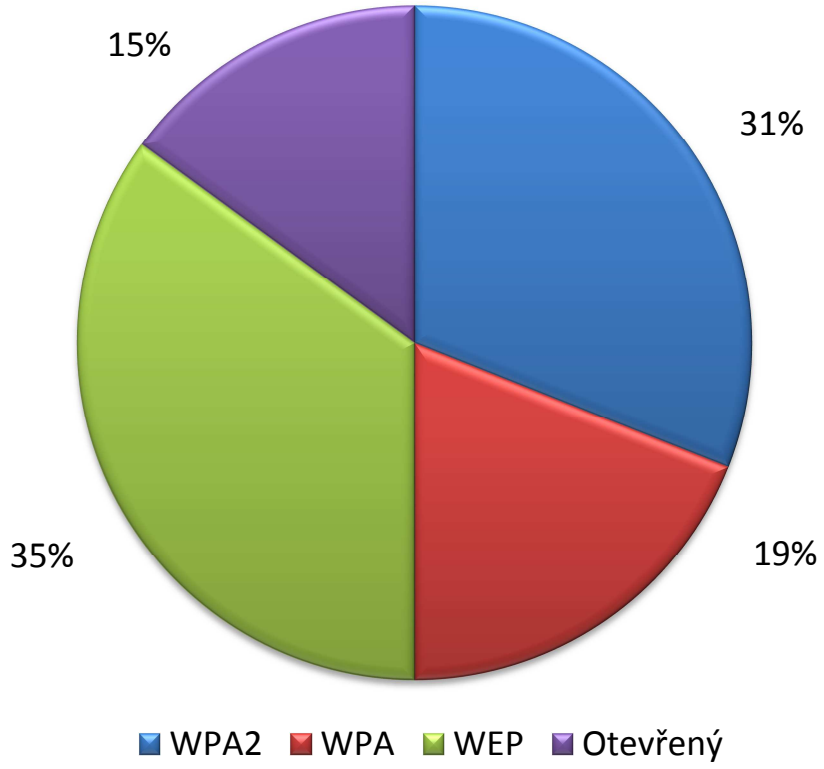


Graf 7 Podíl nezabezpečených AP – Český Krumlov

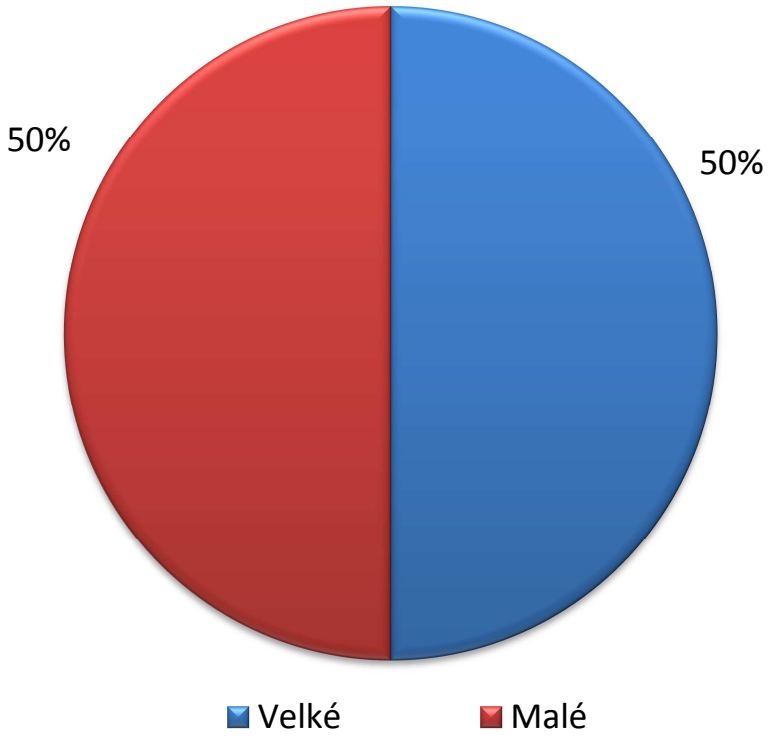


Graf 8 Podíl AP na kanál pásma – Český Krumlov

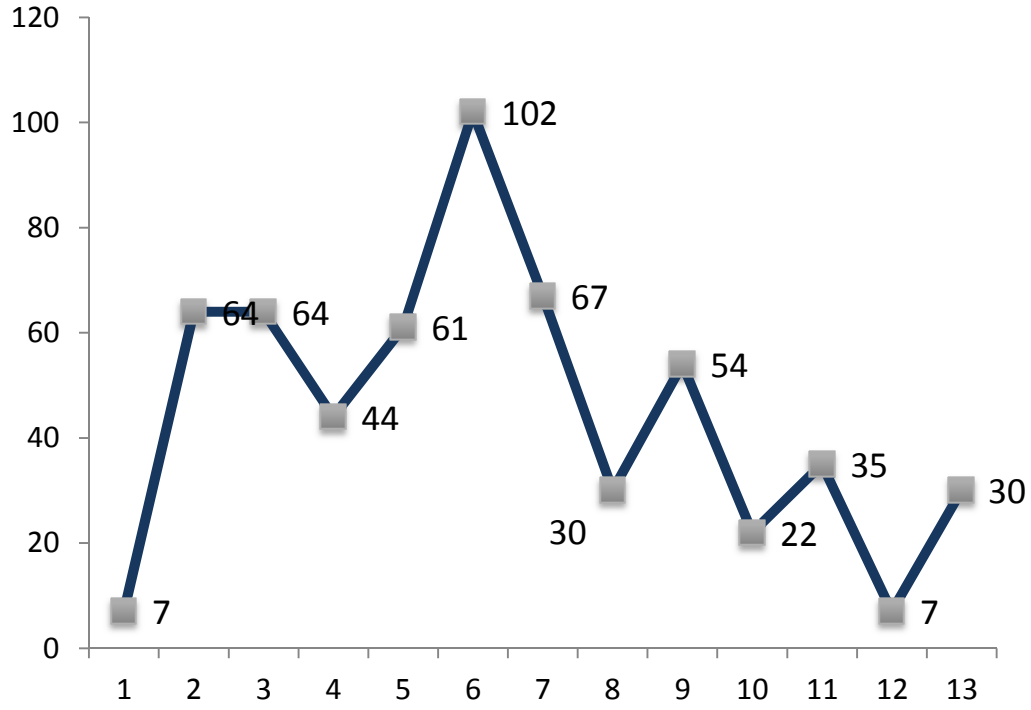
Celkem v obou lokalitách bylo zaznamenáno 385 firemních sítí. Z toho 120 (31 %) používalo silné zabezpečení WPA2, zabezpečení typu WPA bylo u 73 (19%) sítí. Zastaralé zabezpečení technologií WEP používalo 134 (35 %) sítí. U 58 (15%) nebylo nastaveno žádné zabezpečení šifrováním. Sečteme-li opět nezabezpečené sítě a sítě používající slabé WEP zabezpečení vychází údaj o počtu sítí s vysokým rizikem napadení. V případě obou lokalit jde o 50%. Toto číslo vypovídá o tom, že v obou lokalitách je 50% lehce napadnutelných sítí. Podíváme-li se na celkové vytížení kanálů spektra, vychází nám, že v obou lokalitách je nejvytíženější kanál číslo 6.



Graf 9 Zabezpečení AP – obě lokality



Graf 10 Podíl rizika napadení AP – obě lokality



Graf 11 Podíl AP na kanál pásma – obě lokality

5.5 Závěrečné porovnání

Vyhodnocením byly předpoklady potvrzeny, i když některé velmi hraničně. Předpoklad, že více jak 80% přístupových bodů bude používat zabezpečení šifrováním, se potvrdil. Celkově používá zabezpečení šifrováním 85% zachycených bezdrátových sítí. Tento předpoklad se potvrdil nejen celkově, ale i jednotlivě. V Českých Budějovicích bylo zachyceno 84% sítí se zabezpečením šifrováním a v Českém Krumlově jich bylo 86%.

Abychom si mohli vyhodnotit námi naměřené výsledky, použijeme pro srovnání průzkum společnosti Ernst & Young provedený v roce 2010 v Praze. Tento průzkum uvádí, že pouze 63% firemních sítí je zabezpečeno šifrováním, z toho 50% je šifrováno protokolem WPA, WPA2 a 50% je šifrováno pomocí WEP. Celosvětově je přitom běžně šifrováno více jak 90% sítí, z toho 23% je šifrováno WEP.

Ze srovnání s tímto měřením společnosti Ernst & Young vyplývá, že z námi provedeného měření je o 22 % více sítí zabezpečeno a spíše se blíží světovému průměru. Toto zvýšení lze zdůvodnit meziročním nárůstem zabezpečených sítí nebo větším rozšíření bezdrátových technologií v námi sledovaných lokalitách v posledních dvou letech, kdy výrobci více upozorňují v instalačních manuálech na nutnost nastavení šifrování.

Dalším potvrzeným předpokladem je to, že u poloviny a více zabezpečených sítí bude používáno zabezpečení typu WPA, WPA2. Tento předpoklad, i když hraničně, byl potvrzen výsledky pro celkové měření 50 %. Pro jednotlivé lokality se výsledky lišily. V lokalitě ČB byl tento předpoklad potvrzen zjištěním 51 % sítí a v lokalitě ČK se tento předpoklad nesplnil, bylo zjištěno 49 % sítí. Pokud bychom opět naměřená čísla srovnaly s průzkumem v Praze, ukázalo se, že zjištěná data jsou shodná. Bohužel zjištěné hodnoty ukazují, že proti světovému měřítku zaostáváme o 27% v kvalitě zabezpečení šifrováním.

Posledním předpokladem je rozložení počtu bezdrátových sítí po frekvenčním pásmu. Je jednoznačně patrné z výše uvedených grafů, že se tento předpoklad potvrdil. Zajímavý se jeví rozložení počtu bezdrátových prvků ke konci pásma. Konkrétněji tedy mezi 11 a 13 kanálem. USA a Kanadě se používá pouze 11 kanálů a zařízení určená pro trh v tomto regionu neumí pracovat v jiném rozsahu pásma. Proto někteří správci přístupových bodů nastavují maximálně 11 kanál, aby nedocházelo k problémům u importovaných zařízení z těchto regionů. Ukázalo se také, že nejvytíženější je kanál 6, který výrobci nastavují jako výchozí. Lze tedy předpokládat, že změna nastavení kanálu je při konfiguraci přístupového bodu podceňována.

6 BEZPEČNOST NENÍ PRODUKT, ALE PROCES

Nároky na zabezpečení firemního prostředí se odlišují nejen podle počtu klientů, používaných aplikací, ale i množství informací, které považujeme za nutné ochránit. Dále je nutné si uvědomit, že zaměstnanci mají k firemnímu vybavení a firemní síti jiné chování. Proto je taková síť náchylná na jiné typy útoků a některé formy zabezpečení již v takovéto síti nejsou výhodné. Takovým příkladem může být například omezení přístupu na základě MAC adresy, neboť toto omezení je obvykle doporučováno pro sítě, které mají méně než 20 klientů a současně se tito klienti často nemění. Což je relativně snadné zaručit v malé firemní síti, ale takřka nemožné na rozsáhlejším pracovišti. Jinak je možné použít takřka všechny prvky elementárního zabezpečení, které jsou doporučovány včetně kompletního WPA/WPA2 včetně serveru RADIUS.

6.1 Bezpečnostní desatero

Ve firemním prostředí se může vyskytnout potřeba vzdáleného připojení k síti přes nějakou „veřejnou“ sít (Internet). V takovém případě je nutné pro zachování bezpečnosti využít VPN (Virtual Private Network).

Při návrhu zabezpečení firemní bezdrátové sítě by každý firemní IT pracovník měl vzít v úvahu obecné bezpečnostní desatero, které se za posledních deset let ustálilo jako neoficiální doporučení [14]:

- znemožněte fyzický přístup uživatelů k AP;
- využijte nejlepší možné zabezpečení (WPA2 apod.);
- pravidelně klíče WPA měňte;
- pokud je to udržitelné, v AP zaveďte tabulku povolených MAC adres;
- nepovolujte DHCP a adresy přidělujte ručně;
- zakažte SSID Broadcast;
- pokud je to možné, nastavte také tabulku povolených IP adres;
- pravidelně kontroluje síť i logy z AP;
- omezte výkon tak, aby síť zbytečně nepřesahovala půdu vaší firmy;
- pokud chcete opravdu zajistit bezpečnost, používejte VPN.

6.2 Vliv lidského faktoru na bezpečnost sítě

V každé větší firmě se vyplatí zavést jakousi „pomyslnou normu“ chování zaměstnanců v rámci sítě. V této normě jsou pak uvedeny povinnosti uživatelů a jejich oprávnění. Obvykle v této normě bývají uvedeny také postihy, které vyplývají z porušení těchto pravidel.

V každém případě je nejslabším článkem celého zabezpečení člověk. Může to být administrátor, který udělal chybu v konfiguraci, stejně tak to ale může být zaměstnanec, který si svévolně nainstaloval AP. Velice častým případem je zaměstnanec, který v dobré víře prozradí zdánlivě nedůležité údaje (například nějaké informace o síti). Jedná se o tzv. sociální inženýrství. Proti němu se velice těžko bojuje, jedinou možností je vzdělávání jednotlivých zaměstnanců v této oblasti a stanovení pevně daných pravidel toho, jaké informace je ten který zaměstnanec oprávněn sdělovat dalším osobám.

6.3 Ideální řešení – komplexní přístup

Pokud se firma rozhodne používat bezdrátové připojení svých zaměstnanců do vnitřní sítě, měla pokrýt všechna pracoviště silným signálem. Vypadá to, že si protiřečím v souvislosti s předchozím textem, ale jen tak firma získá větší jistotu, že nebude nikdo instalovat vlastní zařízení, které nebudete mít pod kontrolou.

Všechny přístupové body by měly být ale umístěny (logicky, nikoliv fyzicky) ve vnější části firemní sítě. Jinými slovy, každý jejich uživatel bude přistupovat do firemní sítě stejně, jako kdyby se připojoval přes nezabezpečený Internet. Aby mohli zaměstnanci plnohodnotně pracovat a přitom aby jejich připojení bylo bezpečné, musíte tedy vytvořit privátní virtuální sítě (VPN), kde komunikace probíhá po tzv. virtuálních tunelech a veškerý provoz je šifrovaný.

Zároveň není možné zapomínat na lidskou stránku a měli bychom aplikovat velmi striktní a přísná pravidla (např. Příloha PIII). Každému, kdo naruší firemní bezpečnost, musí hrozit zrušení pracovního poměru, podle §55 – Zvláště hrubé porušení pracovních povinností. Ruku v ruce je nutné proškolení všech zaměstnanců, aby nemohli narušit bezpečnost nevědomky (např. špatným nastavením bezdrátové karty v notebooku) a přitom aby plně využívali nově získané mobility. Důležité je vytvořit přátelské firemní prostředí,

aby se žádný zaměstnanec nebál svěřit se svými potřebami IT oddělení a bylo mu rychle vyhověno, jinak bude hledat potenciálně nebezpečnou cestu.

Následně přichází technická stránka zabezpečení. Zde uvádím metody zabezpečení seřazené podle navazujících kroků při budování bezdrátové sítě a jejich priority.

Nezbytné zabezpečení:

1) Vhodné umístění antény
2) Mechanická ochrana přístupového bodu
3) Zakázání vysílání SSID přístupového bodu
4) Změna výchozího SSID přístupového bodu
5) Změna výchozích přihlašovacích údajů přístupového bodu
6) Autentizace a šifrování WPA2
7) Vypnutí DHCP
8) Firewall
9) VPN

Doplňkové zabezpečení:

1) Filtrování MAC adres
2) Filtrování IP adres
3) RADIUS
4) Změna výchozího kanálu přístupového bodu
5) Snížení vysílacího výkonu přístupového bodu
6) Použití aplikačního software
7) Detekce odposlechu
8) Vymezení prostoru a omezení úniku signálu

IT zaměstnanci by měli také pravidelně kontrolovat výskyt signálu bezdrátových prvků ve firemních prostorách, na to ale není třeba speciálního hardwaru, stačí libovolný notebook / PDA s Wi-Fi, s nabitými bateriemi a spuštěný software typu NetStumbler.

ZÁVĚR

Cílem diplomové práce bylo zmapovat úroveň zabezpečení firemních bezdrátových sítí a ukázat možnosti úniku firemních dat. Byly zde rozebrány jednotlivé možnosti zabezpečení bezdrátových sítí. Tyto jsou pro větší přehlednost strukturované do vrstev síťového modelu. Následně bylo navázáno s popisem možných druhů útoků na tyto sítě, a to jak útoky pasivní jako je odposlouchávání komunikace, tak aktivní jako jsou prolomení WEP, WPA-PSK, falšování identity zdroje, deautentizační a DoS útoky.

Aby byly informace o jednotlivých krocích útočníka úplné, jsou dále uvedeny jeho jednotlivé kroky po průniku zabezpečením bezdrátové sítě. Zde jsou předkládány příklady programů a utilit, které jsou pro tyto účely běžně dostupné na internetu.

V první polovině praktické části je provedena ukázka prolomení WEP klíče v praxi. Pro tento účel se podařilo získat souhlas soukromé firmy, která síť s tímto šifrováním provozuje, k testování prolomení zabezpečení. Tím se podařilo stanovené zadání realizovat nikoli v teoretických laboratorních podmínkách, ale přímo v praxi. Výsledek ukázky byl pozitivní. Heslo získané dešifrováním WEP klíče bylo funkční. Na takto provedenou demonstraci soukromá firma následně reagovala změnou zařízení a kvality zabezpečení.

Za touto kapitolou následuje přehled zabezpečení bezdrátových sítí firem ve městech České Budějovice a Český Krumlov. Celkem bylo skenováno 1151 bezdrátových sítí, z toho bylo jednoznačně identifikováno 385 jako firemní. Předpoklady pro analýzu získaných dat, které jsme si stanovili, se potvrdily. Následně byly výsledky porovnány s výzkumem společností Ernst & Young v Praze a Deloitte ve světovém měřítku. Výsledkem tohoto porovnání bylo zjištění, že námi sledované lokality se spíše blíží světovému průměru než aktuální situaci ve velkoměstě České republiky, Praze. Ovšem co do kvality zabezpečení šifrováním zaostávají sledovaná města včetně Prahy za světovým průměrem o celých 22%. Výsledkem je také zjištění, že 16 % procent firemních sítí v obou městech je nezabezpečeno. Pokud ve výsledku sečteme počet nezabezpečených sítí a počet sítí zabezpečených šifrováním WEP (Deloitte ve svých analýzách dokonce řadí sítě s WEP mezi nezabezpečené), dostáváme se k číslu 50%. Tento výsledek jednoznačně ukazuje na podceňování zabezpečení bezdrátových sítí ze strany firem a jejich zaměstnanců.

Závěrem jsou uvedena nezbytná a doplňková doporučení pro zabezpečení firemní sítě, včetně návrhu omezení vlivu lidského faktoru na bezpečnost sítě.

ZÁVĚR V ANGLIČTINĚ

The aim of this thesis is to research the security level of corporate wireless networks and describe the possible occurrence of corporate data leakage. Particular possibilities of wireless networks security systems were indicated and to give a clearer picture, these were presented through structured network model levels. The next section describes possible types of hacking attacks through breaking into these networks including passive hacking attacks as passive listening to communication as well as active hacking attacks as cracking WEP, WPA-PSK, IP address spoofing, de-authorization and DoS (***denial-of-service)***.

To give a full picture on hackers´ single steps, their step by step actions are described after they penetrate the wireless network security system. The examples of programs and utilities that are available though internet and can be used for hacking network security systems, are described further.

In the first part of the practical section, the example of the WEP key hacking was carried out. In order to be able to do that, the consent to test the security system on this was given by a private business, which operates the network using this particular encryption. This enabled the aim of the thesis to be carried out in practice and not just on a theoretical level. The result of this action was positive. The password obtained by decrypting the WEP key worked out. After the company learned that, the decision was made to change the existing technology and security system used in the company.

The following chapter brings summary of wireless networks security systems used within the companies in České Budějovice and Český Krumlov. In total, 1151 wireless networks were scanned, out of which 385 networks were identified as corporate ones. Determined hypothesis was proved through the obtained data analysis. The next step involved the comparison of the results obtained and the research results presented by Ernst & Young based in Prague and Deloitte worldwide. The result coming out from this comparison showed that the monitored locations are rather closer to the world average than to the actual situation in the Czech city of Prague. As concerns the quality of security systems using encryption, the monitored towns including Prague lagged behind the world average as much as by 22%. The results of this research also showed that 16 % of all assessed corporate networks in both towns had no wireless network security systems. When the number of insecure networks and number of networks secured through WEP

encryption (Deloitte analysis consider networks with WEP to be insecure) were add together, the final number was 50 %. This clearly showed that the security of wireless corporate networks is underestimated by the companies´ management and employees. The conclusion states the necessary and additional recommendations for securing corporate networks, including a proposal how to minimize human factor influence in network security.

SEZNAM POUŽITÉ LITERATURY

[1] *Airdump.cz* [online]. 2011 [cit. 2011-04-19]. Metasploit – exploitace zranitelností windows. Dostupné z WWW: <http://airdump.cz/metasploit-hacking-windows-exploit/>.

[2] BARKEN, Lee. *Jak zabezpečit bezdrátovou síť Wi-Fi* . Praha : Computer Press, 2004. 176 s. ISBN 80-251-0346-3

[3] BRZEK, Tomáš. *Zabezpečení wi-fi sítí*. Most, 2008. 38 s. Bakalářská práce. Česká zemědělská univerzita v Praze. Dostupné z WWW: <http://tombrzek.webnode.cz/news/bakalarska-prace-zabezpeceni-wi-fi/>.

[4] CIBULA, Stanislav. *Aplikace nových technologií do firemní počítačové sítě*. Brno, 2007. 62 s. Bakalářská práce. Vysoké učení technické v Brně. Dostupné z WWW: <http://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=782>.

[5] DOSTÁLEK, Libor; KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP - bezpečnost*. Praha : Computer Press, 2003. 571 s. ISBN 80-7226-849-X.

[6] *Deloitte* [online]. 2011 [cit. 2011-05-16]. Press release: Wifi Security Survey. Dostupné z WWW: < http://www.deloitte.com/view/en_LU/lu/services/consulting/technology/bcffa519df199210VgnVCM200000bb42f00aRCRD.htm >.

[7] DWORKIN, M. USA: *National Institute of Standards and Technology* [online]. 2004 [cit. 2011-04-17]. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. Dostupné z WWW: <http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf>.

[8] EDNEY, Jon; ARBAUGH, William A. *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*. Boston : Addison-Wesley Professional, 2003. 480 s. ISBN 0-321-13620-9.

[9] *Ernst & Young* [online]. 2011 [cit. 2011-05-16]. Přehled zabezpečení Wi-fi v Praze 2010. Dostupné z WWW: <http://www.ey.com/CZ/cs/Newsroom/News-releases/2009_V-bezpecnosti-wifi-pripojeni>.

[10] *IEEE 802 LAN/MAN Standards Committee* [online]. 2004, 2011 [cit. 2011-04-17]. IEEE 802 document archives. Dostupné z WWW: <http://grouper.ieee.org/groups/802/>.

[11] HALLER, Martin. *Lupa.cz* [online]. 2006 [cit. 2011-05-10]. Denial of Service (DoS) útoky: typy využívající chyb a vyčerpání systémových prostředků. Dostupné z WWW: <http://www.lupa.cz/clanky/typy-vyuzivajici-chyb-a-vycerpani-systemovych-prostredku-1/>.

[12] HRÁČEK, Jiří. *Perspektivy zabezpečení bezdrátových komunikačních sítí*. Brno, 2008. 104 s. Diplomová práce. Vysoké učení technické v Brně. Dostupné z WWW: <http://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=6271>.

[13] Intel. *Nástroje pro připojení Intel(R) PROSet/Wireless WiFi* [online]. 2009 [cit. 2011-05-16]. Podnikové zabezpečení. Dostupné z WWW: <http://support.elmark.com.pl/rgd/drivery/S15S/WLAN/INTEL/XP_VISTA/XP/Docs/CSY/securset.htm>.

[14] KAPLER, Tomáš. *Internet pro všechny* [online]. 2006 [cit. 2011-05-19]. 9 z 10 firemních Wi-Fi sítí není dostatečně zabezpečeno. Dostupné z WWW: <http://www.internetprovsechny.cz/9-z-10-firemnich-wi-fi-siti-neni-dostatecne-zabezpeceno/>.

[15] KLEIN, Andreas. *Homepage von Andreas Klein* [online]. 2005 [cit. 2011-04-17]. Angriffe auf RC4. Dostupné z WWW: <http://cage.ugent.be/~klein/RC4/RC4-beamer.pdf >.

[16] KROUPA, Filip. *Analýza zabezpečení WiFi sítě*. Praha, 2006. 63 s. Bakalářská práce. České vysoké učení technické v Praze Fakulta elektrotechnická. Dostupné z WWW: <https://dip.felk.cvut.cz/browse/pdfcache/kroupf1_2006bach.pdf>.

[17] KUCHAŘ, Martin. *Svethardware.cz* [online]. 2004 [cit. 2011-05-19]. Jak zapojíme síť: WiFi bez tajemství. Dostupné z WWW: <http://www.svethardware.cz/art_doc-73940D77C1996925C12570 A6004690C0.html>.

[18] MILLER, Stewart S. *WiFi Security*. Atlanta : McGraw Hill Higher Education, 2003. 309 s. ISBN 978-0071410731.

[19] NEWSHAM, Tim. *Applying known techniques to WEP Keys* [online]. 2001 [cit. 2011-04-17]. Cracking WEP Keys. Dostupné z WWW: <http://www.thenewsh.com/~newsham/wlan/WEP_password_cracker.ppt>.

[20] NIGMATULLIN, Timur. *Realizace a zabezpečení domácí ad hoc Wi-fi sítě*. Praha, 2010. 76 s. Bakalářská práce. Vysoká škola ekonomická v Praze. Dostupné z WWW: <http://info.sks.cz/www/zavprace/soubory/72250.pdf>.

[21] O'HARA, Bob; PETRICK, Al. *The IEEE 802.11 Handbook: A Designer's Companion*. Boston : Inst Elect & Electronic Engineers, 1999. 188 s. ISBN 0-738-11855-9.

[22] PCtuning redakce. *Scritube* [online]. 2006 [cit. 2011-05-16]. WiFi: Průniky do sítí a připojení k Internetu. Dostupné z WWW: <http://www.scritube.com/limba/ceha-slovaca/WiFi-Prniky-do-st-a-pipojen-k-1632491817.php>.

[23] PECHAČ, Pavel. *Šíření vln v zástavbě*. Praha : BEN - technická literatura, 2003. 108 s. ISBN 80-7300-186-1.

[24] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace*. Praha : Computer Press, 2005. 184 s. ISBN 80-251-0791-4.

[25] PUŽMANOVÁ, Rita. *Lupa.cz* [online]. 2004 [cit. 2011-05-17]. WLAN konečně bezpečné. Dostupné z WWW: <http://www.lupa.cz/clanky/wlan-konecne-bezpecne/>.

[26] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. Praha : Computer Press, 2005. 432 s. ISBN 80-251-1278-0.

[27] *Root.cz* [online]. 2008 [cit. 2011-04-22]. Aircrack-ng: napadení WEP sítí. Dostupné z WWW: <http://www.root.cz/clanky/aircrack-ng-napadeni-wep-siti/>.

[28] SIROVÝ, Ladislav. *Použití analyzátoru paketů bezdrátových sítí Wireshark*. České Budějovice, 2009. 71 s. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích. Dostupné z WWW: <http://theses.cz/id/n970c2/downloadPraceContent_adipIdno_12547>.

[29] ŠUSTR, Matej. *Analýza bezpečnosti štandardu IEEE 802.11*. Brno, 2007. 69 s. Diplomová práce. Slovenská technická univerzita v Bratislave.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAA *Authentication, Authorization and Accounting* - autentizace, autorizace a evidence

Ad-hoc bezdrátová síť bez AP

AES *Advanced Encryption Standard*, rozšířený šifrovací standard

AP *Access Point*, přístupový bod sítě WLAN, který ji často spojuje s LAN

ARP *Address Resolution Protocol*, protokol na zjišťování adres

ASCII *American Standard Code for Information Interchange*, standardní způsob kódování písmen, číslic a jiných znaků

BSS *Basic Service Set*, základná sada služeb, množina stanic v IEEE 802.11 koordinovaná společně

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

CCA *Clear Channel Assessment*, odhad volného kanálu, funkce fyzické vrstvy

CCM *Counter-Mode/Cipher Block Chaining-Message Authentication Code*, počítadlový mód s autentifikací správy řetězením bloků šifer

CCMP *CCM Protocol*, zkratka zaměňovaná s CCM

CRC *Cyclic Redundancy Code*, cyklický kód určený na detekci chyb CSMA/CA – *Carrier Sense with Multiple Access/Collision Avoidance* – přístup na médium s detekcí signálu, vícenásobným přístupem a předcházením kolizí

CTS *Clear To Send*, povolení vysílání, kontrolní rámec

CVS *Concurrent Version System*, open-source systém na správu verzí programů

DES *Data Encryption Standard*, bloková šifra

DHCP *Dynamic Host Configuration Protocol*, protokol pro dynamickou konfiguraci uživatelů sítě

DoS *Denial of Service*, zamítnutí služby, druh útoku, který vyřazuje software zařízení anebo síť z provozu

DS *Distribution System*, distribuční systém

DSSS *Direct Sequence Spread Spectrum*, modulace rozprostřeným spektrem s přímou sekvencí

EAP *Extensible Authentication Protocol*, rozšířitelný autentifikační protokol

EAPOL *Extensible Authentication Protocol over LAN*, rozšířitelný autentifikační protokol přes lokální síť

ESS *Extended Service Set*, rozšířená sada služeb, množina jedné nebo více propojených BSS, která se LLC podvrstvě jeví jako jedna BSS

ESSID identifikátor ESS, zkratka používaná namísto SSID

FCS *Frame Check Sequence*, kontrolní hodnota rámce, vypočítává se při vysílání a přijímání rámce

FMS *Fluhrer-Mantin-Shamir*, útok na WEP, pojmenovaný po autorech

FPGA *Field-programmable gate array*, programovatelné hradlové pole

GTK *Group Transient Key*, přechodný skupinový klíč

HMAC *Hash Message Authentication Code*, autentifikační kód správy použitím Hashe

Host-AP *Host Access Point*, přístupový bod na počítači

IBSS *Independent BSS*, nezávislá, „ad-hoc“ síť (bez AP)

ICMP *Internet Control Message Protocol*, protokol pro řídící zprávy na internetu - chybové, testovací a informační zprávy v IP

ICV *Integrity Check Value*, kontrolní součet dát použitý pro šifrování pomocí WEP

IDS *Intrusion Detection System*, systém na detekci průniků

IEEE *Institute of Electrical and Electronics Engineers, Inc.*

IP *Internet Protocol*, základní protokol dnešního Internetu

IV *Initialization Vector*, inicializační vektor, tvořící část klíče pro PRNG

KSA *Key Scheduling Algorithm*, algoritmus na rozvržení klíče, 1. fáze RC4

LAN *Local Area Network*, lokální počítačová síť

LEAP *Lightweight EAP*, odlehčený EAP, vyvinutý firmou Cisco

LCC *Logical Link Control*, řízení logické linky, vyšší podvrstva linkové vrstvy referenčního modelu OSI

MAC *Medium Access Control*, řízení přístupu na médium, nižší podvrstva linkové vrstvy referenčního modelu OSI

MAN *Metropolitan Area Network*, počítačová síť městského rozsahu

MIC *Message Integrity Code*, kód správy, zkratka používaná v IEEE 802.11 místo *Message Authentication Code*, kvůli možnosti záměny za Medium Access Control

MTU *Maximum Transmission Unit*, maximální poslatelná velikost jednotky

NAV *Network Allocation Vector*, vektor alokace sítě, časovač, který je na stanici nastavený, v čase kdy nesmí vysílat

NDIS *Network Driver Interface Specification*, specifikace pro ovladače síťových rozhraní, používaná hlavně ve Windows

NIST *National Institute of Standards and Technology*, vládní organizace USA schvalující některé standardy

NT označení operačního systému Windows NT od firmy Microsoft

OFDM *Orthogonal Frequency Division Multiplex*, multiplex s ortogonálním dělením frekvencí

OS *Operating System*, operační systém

OSI *Open Systems Interconnection*, standard v komunikaci počítačových sítí

PAP *Password Authentication Protocol*, protokol na autentifikaci pomocí otevřeného jména a hesla

PCI *Peripheral Component Interconnect*, rozhraní pro připojení periferií

PCMCIA *Personal Computer Memory Card International Association*, standard pro rozhraní mobilních počítačových periferií

PKI *Public Key Infrastructure*, infrastruktura veřejných klíčů

PLME *Physical Layer Management Entity*, entity na management fyzické vrstvy

PMK *Pairwise Master Key*, hlavní párový klíč

PN *Packet Number*, číslo paketu

PPTP *Point-to-Point Tunneling Protocol*, protokol pro vytvoření spojení mezi dvěma body, používaný ve VPN

PRGA *Pseudo-Random Generation Algorithm*, algoritmus generování pseudonáhodné posloupnosti

PRNG *Pseudo-Random Number Generator*, generátor pseudonáhodné posloupnosti čísel

PSK *Pre-Shared Key*, předsdílený tajný klíč používaný v WPA a WPA2

PTR *Pairwise Transient Key*, přechodný párový klíč

RADIUS *Remote Authentication Dial In User Service*, protokol pro autentifikaci uživatelů

RFMON *Radio Frequency Monitor*, režim monitorování rádiových frekvencí

RM OSI referenční model OSI (*Open System Interconnect*)

RSN *Robust Security Network*, síť s robustní bezpečností (podle IEEE 802.11i)

RSNA *Robust Security Network Association*, asociace RSN

RTS *Request To Send*, požadavek na vysílání, kontrolní rámec

RX *Receive*, přijímání

SHA *Secure Hash Algorithm*, bezpečný Hash algoritmus

SNAP *Sub-Network Access Protocol*, často používaný v LLC, pro určení typu vnořeného protokolu ve 3. vrstvě

SSID *Service Set Identifier*, identifikátor sady služeb, tj. identifikátor WLAN sítě

STA *Station*, stanice ve WLAN sítě

TCP *Transmission Control Protocol*, protokol pro řízení vysílání

TK *Temporal Key*, dočasný klíč

TKIP *Temporary Key Integrity Protocol*, protokol s integritou dočasných klíčů, protokol zabezpečující výměnu šifrovacích klíčů v šifrování WPA

TSC *TKIP Sequence Counter*, sekvenční počítadlo pro TKIP

TX	*Transmit*, vysílání
UDP	*User Datagram Protokol*, protokol pro uživatelské datagramy
USB	*Universal Serial Bus*, typ externího počítačového rozhraní
VPN	*Virtual Private Network*, virtuální privátní síť
VPU	*Vector Processing Unit*, vektorová procesní jednotka
WEP	*Wireless Equivalent Privacy*, původní protokol zabezpečující IEEE 802.11
WIDS	*Wireless Intrusion Detection System*, systém na detekci průniků do bezdrátových sítí
Wi-Fi	*Wireless Fidelity*, aliance společností vyrábějících WLAN zařízení
WLAN	*Wireless Local Area Network*, lokální bezdrátová počítačová síť
WPA	*Wi-Fi Protected Access*, zabezpečený přístup Wi-Fi, protokol zabezpečující IEEE 802.11 z roku 2003
WPS	*Wi-Fi Protected Setup*, zabezpečené nastavení Wi-Fi
XOR	*Exclusive OR*, vylučující anebo

SEZNAM OBRÁZKŮ

Obr. 1 Srovnání šifrování WEP, WPA, WPA2 [25] 14
Obr. 2 Přístupový bod s integrovaným firewallem [12] 15
Obr. 3 Zabezpečení komunikace pomocí VPN [12] 16
Obr. 4 Komunikace mezi přístupovým bodem a klientem [3] 17
Obr. 5 Šifrování protokolem WEP [3] 20
Obr. 6 Generování klíče pomocí TKIP a šifrování ve WPA 25
Obr. 7 Symboly užívané 30
Obr. 8 Příklad RTS/CTS komunikace [29] 41
Obr. 9 Kroky útočníka uvnitř 45
Obr. 10 Výřez protokolového snifferu WireShark (příloha P IV) 47
Obr. 11 Druhy útoků podle klíčových komponent systému [20] 48
Obr. 12 Vzdálení plocha napadeného počítače 49
Obr. 13 Vyzařovací charakteristika antény Orinoco Yagi XP [23] 53
Obr. 14 Použitá sestava pro skenování bezdrátové sítě 53
Obr. 15 Odposlouchávání komunikace v bezdrátové síti ve sledované lokalitě 54
Obr. 16 Výřez okna z programu Netstumler (příloha P V) 55
Obr. 17 Okno programu airodump 2.1, konfigurace před spuštěním sběru paketů 56
Obr. 18 Okno programu airodump 2.1, sběr paketů a IV 56
Obr. 19 Okno utility aicrack 2.1, konfigurace 57
Obr. 20 Okno programu aircrack 2.1, výsledek pokusu o prolomení WEP 58
Obr. 21 Okno programu aircrack 2.1, získání WEP klíče 58
Obr. 22 Převod hexadecimálního řetězce na Ascii řetězec 59
Obr. 23 Přiřazení IP adresy interním DHCP serverem pro prolomení WEP klíče 59
Obr. 24 Diagram aktivit 60
Obr. 25 Trasa měření v Českých Budějovicích 62
Obr. 26 Trasa měření v Českém Krumlově 63

SEZNAM TABULEK

Tab. 1 Porovnání šifrovacích mechanismů [25] 13
Tab. 2 Doba rozluštění WPA-PSK podle různých kritérií 38
Tab. 3 Technická data Orinoco Yagi XP 52

SEZNAM GRAFŮ

Graf 1 Zabezpečení AP – České Budějovice 64
Graf 2 Podíl rizika napadení AP – České Budějovice 65
Graf 3 Podíl nezabezpečených AP – České Budějovice 65
Graf 4 Podíl AP na kanál pásma – České Budějovice 66
Graf 5 Zabezpečení AP – Český Krumlov 67
Graf 6 Podíl rizika napadení AP – Český Krumlov 67
Graf 7 Podíl nezabezpečených AP – Český Krumlov 68
Graf 8 Podíl AP na kanál pásma – Český Krumlov 68
Graf 9 Zabezpečení AP – obě lokality 69
Graf 10 Podíl rizika napadení AP – obě lokality 70
Graf 11 Podíl AP na kanál pásma – obě lokality 70

SEZNAM PŘÍLOH

Příloha P I: Výchozí hodnoty SSID vybraných výrobců bezdrátových zařízení [27]

Příloha P II: Porovnání typů autentifikace a šifrování [24]

Příloha P III: Pracovní okno programu Wireshark

Příloha P IV: Vzdálená plocha napadeného počítače po spuštění exploid [1]

Příloha P V: Pracovní okno programu NetStumbler

Příloha P VI: Vnitřní předpis

Příloha P VII: DVD s digitální verzí diplomové práce

PŘÍLOHA P I: VÝCHOZÍ HODNOTY SSID VYBRANÝCH VÝROBCŮ BEZDRÁTOVÝCH ZAŘÍZENÍ [27]

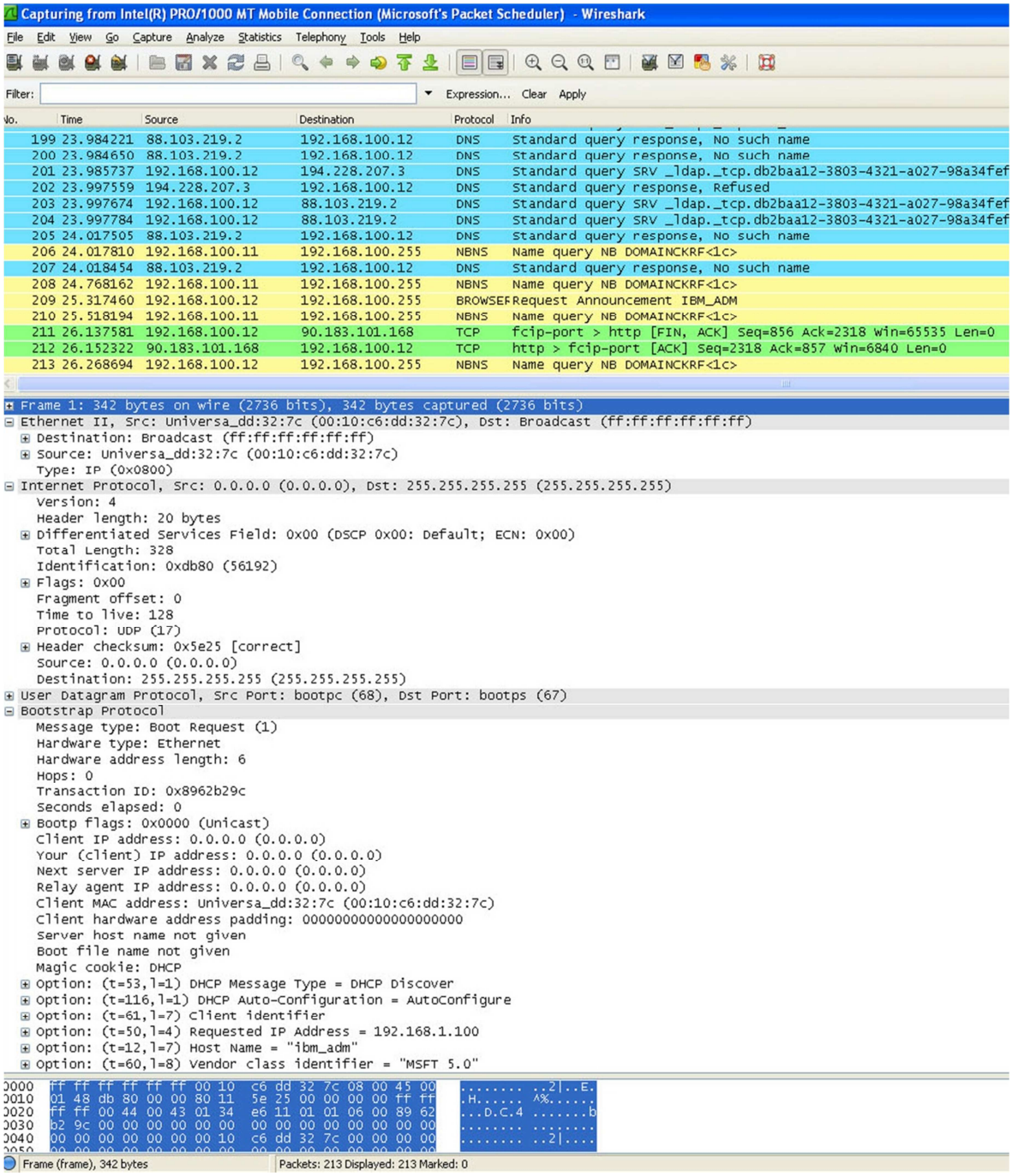
Výrobce	SSID
Com	101, comcomcom
CC&C	MyWlan
Cisco	Tsunami, WaveLAN Network
Compaq	Compaq
Dlink	WLAN
Intel	101, 195, xlan , intel
Linksys	Linksys, wireless
NetGear	Wireless
SMC	WLAN, SMC
Symbol	101
Vigor	default
Ostatní výrobci	Wireless,
Ovislink	Admin
Teletronics	Any
Zcomax	Any
Zyxel	Wireless

PŘÍLOHA P II: POROVNÁNÍ TYPŮ AUTENTIFIKACE A ŠIFROVÁNÍ [24]

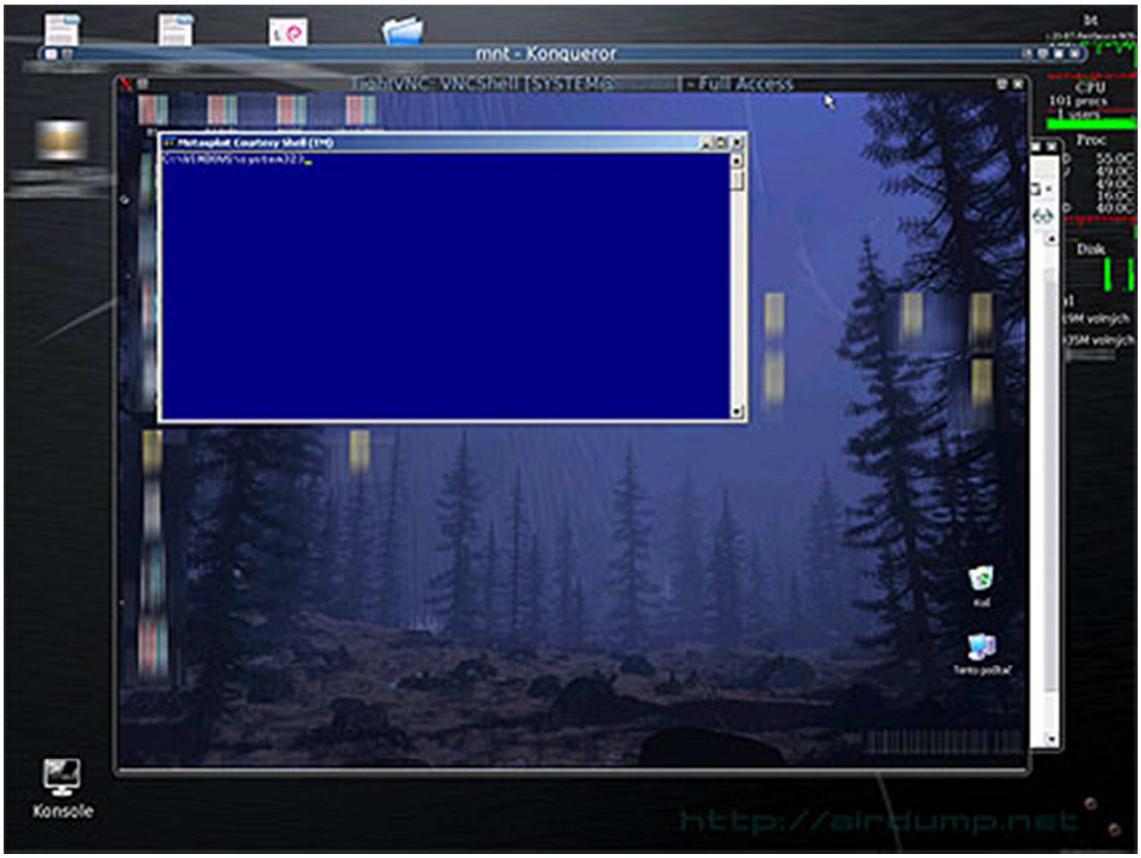
	WEP	**WPA**	**WPA2**
autentizace	Otevřená	EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) nebo PEAP (Protected EAP)	EAP-TLS nebo PEAP
šifrování	statický WEP	WEP TKIP/CKIP (Cisco Key Integrity Protocol)	AES
útok	**odolnost**		
na integritu, důvěrnost dat	Dobrá	lepší	nejlepší
Falešná autentizace	Malá	nejlepší	nejlepší
na slabý klíč	Malá	nejlepší	nejlepší
falšované pakety	Minimální	nejlepší	nejlepší
Falešný přístupový bod	Minimální	lepší	nejlepší
úroveň šifrování	(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)

škálování: minimální, malá, dobrá, lepší, nejlepší

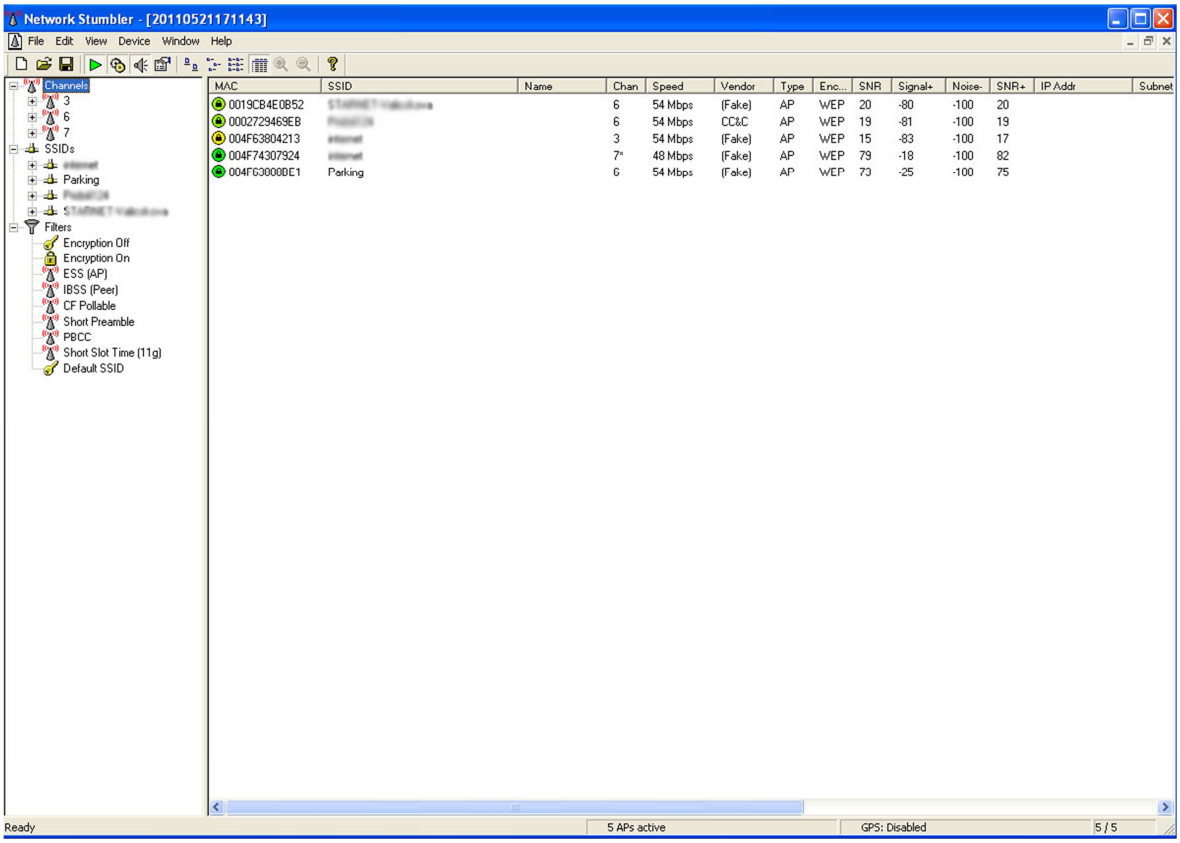
PŘÍLOHA P III: PRACOVNÍ OKNO PROGRAMU WIRESHARK



PŘÍLOHA P IV: VZDÁLENÁ PLOCHA NAPADENÉHO POČÍTAČE PO SPUŠTĚNÍ EXPLOIT [1]



PŘÍLOHA P V: PRACOVNÍ OKNO PROGRAMU NETSTUMBLER



PŘÍLOHA P VI: FIREMNÍ VNITŘNÍ PŘEDPIS

PRAVIDLA POUŽÍVÁNÍ A ZÁSADY BEZPEČNOSTI PRÁCE PŘI PRÁCI NA PC, INTERNETU A S E-MAILEM

Zaměstnavatel, zastoupený ředitelem společnosti vydává následující vnitřní předpis, kterým se upravují pracovně právní nároky zaměstnanců zaměstnavatele.

čl. 1
Působnost vnitřního předpisu

Vnitřní předpis se vztahuje na všechny zaměstnance, pokud jsou se zaměstnavatelem v pracovním poměru, včetně zaměstnanců zaměstnaných na dohody o pracích konaných mimo hlavní pracovní poměr.

čl. 2
Pojmy a vymezení

1. Tento vnitřní předpis upravuje způsob, zásady a pravidla, na základě kterých zaměstnanci společnosti používají osobní počítače ve vlastnictví zaměstnavatele (dále jen PC), veřejné datové sítě (dále jen internet) a elektronickou komunikaci (dále jen e-mail).

2. Předpis se vztahuje na všechny zaměstnance společnosti, kteří při výkonu své činnosti pro zaměstnavatele používají nebo mohou používat PC, internet a email, a to bez ohledu na dobu a čas, kdy tyto věci využívají a používají.

čl. 3
Pravidla užívání, bezpečnostní zásady

1. Každý zaměstnanec je povinen dodržovat následující pravidla užívání PC, internetu a e-mailu:

a) Neinstalovat žádné programy a zařízení bez předchozí konzultace s nadřízeným pracovníkem, případně se správcem počítačové sítě.

b) Nepřihlašovat se na internetové servery určené pro sdílení soukromých informací a souborů jako např. Mybook.com, Facebook.com, Lide.cz, ICQ, SKYPE, CHAT, MESSENGER, MIRANDA atd.

c) Chyby systému a jiné nefunkční programy ohlásit bezodkladně nadřízenému pracovníkovi a nepokoušet se je opravit vlastními silami bez předchozí konzultace s nadřízeným pracovníkem.

d) Nesdílet žádné adresáře, soubory a tiskárny bez předchozí konzultace s nadřízeným pracovníkem

e) Nepoužívat firemní e-mail k internetovým a emailovým registracím, potvrzením a jiným osobním či soukromým aktivitám, pokud nejsou spojeny s výkonem činnosti pracovníka.

f) Nepoužívat firemní e-mail pro jakoukoliv soukromou korespondenci, dále pro korespondenci spojenou se sdílením dat a jiných souborů, zvláště pak s šíření falešných zpráv, upozornění, výstrah (např. e-maily hledající dárce orgánů a jiné textové informace zneužívající důvěry uživatele), dále neodpovídat na dotazy od firem, bank, úřadů které nejsou spojeny s výkonem pracovní činnosti zaměstnance.

g) Nepoužívat na pracovišti vlastní informační technologie, hardware či software, ani jiné prostředky jako např. přenosné paměti flash, přenosné počítače apod.

h) Nevyužívat internet a vyhledávání na něm ani žádné internetové stránky jinak, než v přímé souvislosti s výkonem své práce.

i) Chovat se tak, aby nedocházelo k poškozování majetku zaměstnavatele a nevznikala škoda

2. Používat svěřené firemní PC výhradně pro práci určenou zaměstnavatelem.

3. Není povoleno používat PC ke kopírování dat, filmových a zvukových záznamů,

4. Není povoleno používat PC včetně příslušenství (např. tiskárny, kopírky, vypalovací mechaniky, USB disky, paměťové karty atd.) a síťová úložiště k ukládání a kopírování dat a záznamů, jinak než v souvislosti s výkonem práce a v souladu s právním řádem, zejména s autorským zákonem 121/2000 Sb. a jeho pozdějších znění.

5.Vyjimky se shora specifikovaných zásad a zákazů lze učinit v odůvodněných případech, v souladu s právním řádem a současně po předchozím písemném souhlasu nadřízeného.

čl. 4
Kontrola a sankce

1. Každý zaměstnanec je povinen strpět kontrolu dodržování těchto pravidel nadřízeným či pověřeným zaměstnanec a je povinen poskytnout k této kontrole potřebnou součinnost.

2. Zaměstnavatel je oprávněn provádět kontrolu dodržování těchto pravidel a činit opatření směřující k nápravě.

3. Zjistí-li zaměstnavatel využívání PC, internetu či emailu ze strany zaměstnance v rozporu s tímto nařízením pro účely nespojené s výkonem jeho práce, zaměstnavatel se s obsahem jeho soukromých zpráv seznamovat nebude, je však oprávněn zajistit potřebné podklady prokazující porušení tohoto vnitřního předpisu a zaměstnanec je povinen poskytnout k tomuto zaměstnavateli potřebné vysvětlení.

4. Nerespektování tohoto vnitřního předpisu zakládá na straně zaměstnance odpovědnost dle právních předpisů, zejména zákoníku práce č. 262/2006 Sb. v platném znění autorského zákona č. 121/2000 Sb. a jeho pozdějších znění, občanského zákoníku č. 40/1964 Sb. v platném znění Zaměstnavatel nenese za uvedená překročení ze strany zaměstnance svoji odpovědnost.

5. Nedodržování tohoto vnitřního předpisu ze strany zaměstnance se považuje za porušování povinností vyplývajících z právních předpisů vztahujících se k jím vykonávané práci zvlášť hrubým způsobem.

čl. 5
Účinnost a platnost

1. Zaměstnavatel je oprávněn tento vnitřní předpis kdykoliv jednostranně změnit

2. Tento vnitřní předpis se vydává na dobu neurčitou

3. Tento vnitřní předpis je účinný od okamžiku jeho vyhlášení u zaměstnavatele tj. od …….

Ředitel společnosti podpis: …….

Potvrzuji seznámení se s obsahem tohoto vnitřního předpisu ze dne ……...

Zaměstnanec……. Podpis ……