Význam penetračních testů při budování Wi-Fi sítí

The importance of penetration testing in building Wi-Fi networks

Bc. Libor Jasný

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. Libor JASNÝ**
Osobní číslo:	**A09365**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Význam penetračních testů při budování Wi-Fi sítí**

Zásady pro vypracování:

1. **Popište význam penetračních testů Wi-Fi sítí**
2. **Uveďte standardy Wi-Fi sítí a v současnosti používaná zabezpečení**
3. **Popište metody útoků na Wi-Fi sítě**
4. **Navrhněte pracovní scénáře zabezpeční Wi-Fi sítí používaných v praxi**
5. **Proveďte penetrační testy na jednotlivé pracovní scénáře**
6. **Analyzujte slabá místa a proveďte návrh zabezpečení**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ZANDL, Patrick. Bezdrátové sítě WiFi – Praktický průvodce. Brno : Computer Press, 2003. 204 s. ISBN 80-722-6632.**
2. **BARKEN, Lee. Jak zabezpečit bezdrátovou síť Wi-Fi. [s.l.] : Computer Press, 2004. 176 s. ISBN 80-251-0346-3**
3. **SOSINSKY, Barrie. Mistrovství ? počítačové sítě. Brno : Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7**
4. **LAMMLE, Todd. CCNA. [s.l.] : Computer Press, 2010. 928 s. ISBN 978-80-251-2359-1.**
5. **OREBAUGH, Angela, et al. Wireshark a Ethereal. Brno : Computer Press, 2008. 448 s. ISBN 978-80-251-2048-4**
6. **HORÁK, Jaroslav; KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. [s.l.] : Computer Press, 2011. 304 s. ISBN 978-80-251-3176-3**
7. **PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace. Brno : Computer Press, 2005. 184 s. ISBN 80-251-0791-4**
8. **KLEVINSKY, T. J.; LALIBERTE , Scott; GUPTA , Ajay. Hack I.T.: Security Through Penetration Testing. [s.l.] : Addison-Wesley, 2002. 544 s. ISBN 0-201-71956-8**

Vedoucí diplomové práce: **Ing. David Malaník**
Ústav informatiky a umělé inteligence

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

Tato diplomová práce se zabývá penetračními testy bezdrátových WLAN sítí. V teoretické části je popsán význam penetračních testů, nejvíce používané Wi-Fi standardy a zabezpečení. V praktické části jsou uvedeny zranitelnosti jednotlivých zabezpečení a na tyto zranitelnosti jsou provedeny útoky. V závěru jsou popsány výsledky a navrhnuty možná protiopatření.

Klíčová slova: IEEE 802.11, Wi-Fi, WLAN, WEP, WPA, WPA2, MAC, SSID, ARP, Penetrační test, Přístupový bod, KoreK ChopChop, Slovníkový útok

ABSTRACT

This thesis deals with penetration tests of WLAN networks. In theoretical part is described the importance of penetration testing, the most widely used Wi-Fi standards and security methods. In practical part are introduced vulnerabilities of each security methods and performed attacks on these vulnerabilities. In conclusion are described results and proposed possible countermeasures.

Keywords: IEEE 802.11, Wi-Fi, WLAN, WEP, WPA, WPA2, MAC, SSID, ARP, Penetration test, Access point, KoreK ChopChop, Dictionary attack

Děkuji Ing. Davidu Malaníkovi za odborné vedení, poskytnutí informací a praktických rad v konzultacích při realizaci této diplomové práce.

Motto:

Problémy neexistují, existují pouze výzvy.

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

Informační technologie ovlivňují náš svět stále větší měrou. Ať už se jedná o desktopové počítače, notebooky, tablety či smartphony, stávají se čím dál více součástmi našeho každodenního života. Spolu s nimi jdou ruku v ruce služby, které nám usnadňují práci, přinášejí zábavu nebo pomáhají v osobním životě. Nejedná se však jen o poskytování služeb formou dnes tak moderního cloud computingu, ale také potřeba konsolidovat hardware z důvodu např. dosažení vyššího výpočetního výkonu, lepší možnosti zálohování nebo sdílení dat. Ve všech případech je však potřeba realizovat kanál sloužící k přenosu informací mezi těmito koncovými body, síť.

Stále více zařízení je dnes vybaveno možností připojit se k síti, zasílat informace, umožňovat vzdálenou správu, či informace ze sítě získávat. Naopak zařízení, která touto možností nedisponují, pak ve velké míře ztrácí svou užitnou hodnotu. Proto v dnešní době spolu s rozvojem sítí a dostupností konektivity, roste i potřeba se k nim připojovat.

Ať už se jedná o síť kabelovou či bezdrátovou, jedná se o základní stavební prvek umožňující přenášení dat a informací. Informací, které je potřeba chránit. Proto je dnes neodmyslitelnou součástí každé sítě její zabezpečení, realizované jak softwarovou tak i hardwarou formou. K prověření zabezpečení dnes slouží penetrační testy, které mají za úkol otestovat odolnost všech prvků sestávající se sítě proti útokům zvenčí i zevnitř.

Tato diplomová práce si nebere za úkol popsat všechna potenciální rizika spojená s útoky na bezdrátové sítě, ale snaží se nastínit situace, které se objevují v prostředích současné domácí i korporátní sféry. Bere si za cíl zmapovat a statisticky vyhodnotit nejvíce nasazované metody zabezpečení. Ty dále podrobit penetračním testům, z daných výsledků vyvodit závěr a navrhnout možná protiopatření.

I. TEORETICKÁ ČÁST

1 PENETRAČNÍ TESTY

Penetrační testování (pentesting) slouží k ověření a posouzení současné úrovně odolnosti testovaného systému metodou pokusu o průnik. Jedná se tedy o formu bezpečnostního auditu vyžádaného na zakázku a řadí se tak do oblasti etického hackingu.

Penetrační testy mohou mít mnoho variant (včetně jejich kombinací) a mohou být použity na různé části informačních systémů. Metody a nástroje používané k penetračnímu testování mohou být manuálního i automatického charakteru, přičemž se vždy snaží simulovat formu reálného útoku a rizika s ním spojená.

1.1 Důsledky reálných utoků

Nedostupnost služby – DoS / DDoS útoky (Denial of Service / Distributed Denial of Service) – způsobují, že dotazovaná služba či server, který byl cílem útoku, přestane odpovídat a bude nucen k restartu. Útok často cílený na online služby, potřebující stálou dostupnost (e-shopy, e-banking, obecně servery poskytující obsah za úplatu).[1]

Neoprávněný přístup (unauthorized access) – výsledek vede k situaci, kdy útočník získá neoprávněný přístup k hardwaru, softwaru či datům, které mu následně umožní provádět změny v konfiguraci HW nebo SW prostředků a modifikaci souborů. S tím je spojena ztráta důvěrných informací (hesel, loginů, pinů, důležitých dokumentů, know how), které mohou být stěžejní pro budoucnost subjektu. Takto napadený server může být také využíván jako zdroj dalších útoků.[1]

Stupňování práv (Privilege Escalation) – jedná se o změnu oprávnění uživatelských účtů za účelem dosažení vyšší úrovně kontroly. Důsledkem tohoto útoku může standartní uživatelský účet získat práva administrátora a provádět pod jeho kontrolou další změny v systému (instalace malwaru, manipulace se soubory atd.).

1.2 Zaměření pentestů

Pentesty se nejčastěji zaměřují na zranitelnosti firewallů, antivirových a jiných bezpečnostních softwarů, nastavení aktivních síťových prvků, analýzu konfigurace a zranitelnosti operačních systémů na serverech a pracovních stanicích, analýzu databází a zálohovacích úložišť, zranitelnosti informačních systémů a služeb, nastavení a dodržování stanovených bezpečnostních politik zaměstnanci.

Při penetračních testech jsou kontrole podrobeny především [1]:

- Firewally – DoS/DDoS útoky, změny směrování, zranitelnost
- Backdoory (popř. jiný malware) - programy umožňující získání kontroly
- CGI scripty - získání plné kontroly www nad serverem
- DNS systémy - předstíráním identity síťového zařízení
- emailové systémy – spam
- FTP systémy - neautorizovaný přístup k souborovému systému a převzetí kontroly nad serverem
- LDAP systémy - zneužití adresářové služby LDAP
- síťové odposlouchávání - špatná konfigurace aktivních síťových prvků či nevhodný návrh infrastruktury
- NFS systémy - neautorizovaný přístup k souborovému systému a převzetí kontroly nad serverem
- systémy založené na RPC - vzdálené volání procedur
- systémy se sdílením zdrojů - získání neautorizovaného přístupu (Samba, SMB)
- SNMP systémy - bezpečnostní díry v implementaci Simple Network Management Protocolu v aktivních prvcích sítě
- IPMI – získání vzdáleného přístupu a administrace serveru
- Web management interface aktivních síťových prvků – neautorizovaný přístup

1.3 Formy penetračních testů

ohlášený penetrační test – jeho účelem je otestovat odolnost informačního systému a bezpečnostních politik vůči provedeným útokům, jak po stránce technické, tak po stránce personální

neohlášený penetrační test – stejně jako u ohlášeného penetračního testu je jeho cílem prověřit jak zabezpečení a konfigurace technických prvků nasazených ve firemní infrastruktuře, tak i dodržování bezpečnostních politik zaměstnanci, avšak latentní formou, kdy se pracovníci nemohou předem připravit a změnit tak své pracovní návyky (v praxi účinnější než první varianta). O konání pentestu bývá uvědomen pouze vrcholový management společnosti.

externí penetrační test – simulován potenciálním útočníkem z vnějšího prostředí (nejčastěji z Internetu), na interní systémy zadavatele. Útočník čerpá informace zpravidla z veřejně dostupných zdrojů (Internet – oficiální webové stránky společnosti popř. jiné

reference, WHOIS - databáze sloužící k evidenci údajů o majitelích internetových domén a IP adres, výpis z Obchodního rejstříku atp.)

interní penetrační test – prováděn z vnitřního prostředí společnosti, kdy je útočník fyzicky přítomen a připojen do firemní počítačové sítě pomocí svého počítače či firemního, ke kterému získal přístup. Tento test má za úkol ověřit možnosti spojené s manipulací s privátními daty společnosti neoprávněnou osobou (přístup, kopírování, odstranění).

sociální inženýrství (sociotechnika) – jedná se o netechnickou metodu spočívající v přesvědčování a ovlivňování osob, s cílem oklamat uživatele tak, aby uvěřil, že útočník je ten, za koho se vydává. Dokázal ho zmanipulovat k vyzrazení důležitých informací (např. autentizačních údajů) nebo přimět k provedení určitých úkonů v jeho prospěch (povolení přístupu do sítě, zapůjčení PC, spuštění/instalace malwaru). Velkou měrou vyplývá z psychologie a je založeno zpravidla na důvěřivosti, strachu, soucitu nebo nátlaku. Úspěch sociotechnika, jak se útočník nazývá, závisí především na jeho znalostech o konkrétním subjektu. Ve všech případech však využívá člověka, jako nejslabšího článku, protože právě přes něj vede nejjednodušší cesta, jak se ke kýženému cíli dostat, aniž by musel překonávat složité hardwarové a softwarové bezpečnostní prvky.[2]

Penetrační testy tvoří důležitou součást bezpečnostní analýzy a jejich výsledky tvoří výčet slabých míst, která mohou přinášet potenciální rizika pro testovanou společnost. Závěrečný report sebou obvykle nese důkazy o proniknutí do informačního systému a může obsahovat i návrhy nezbytných protiopatření. Stejně jako u jiných bezpečnostních analýz platí i zde, že celý systém je bezpečný tak, jak je zabezpečeno jeho nejslabší místo.

2 BEZDRÁTOVÉ SÍTĚ

Bezdrátové sítě se stávají samozřejmostí našeho každodenního života. Ať už jsou to telefonní sítě mobilního operátorů, televizní příjem satelitního vysílání nebo největší datová síť na světě – Internet, poskytovaná skrze přístupové body providerů, jsou všude kolem nás a poskytují nám své služby kdykoli a kdekoli.

S rozvojem bezdrátových sítí v 90. letech a jejich masivnějším rozvojem o deset let později, již nikdo nepochyboval o jejich výhodách. S rozvojem dalších standardů, zvyšování přenosových rychlostí a vyřešení otázky elektromagnetické interference a susceptibility, pronikaly bezdrátové sítě postupně do všech oblastí lidské činnosti. Od průmyslu a služeb, až po dopravu a odvětví zábavní a spotřební elektroniky.

Jednou z mnoha výhod bezdrátových sítí je jejich snadné použití. Uživatel již není fixován na konkrétní místo s datovou zásuvkou a prostor kde může vykonávat svou práci, se tak razantně zvyšuje. S tím je spojena i produktivita práce, kdy pracovník vyžadující přístup k informacím a prostředkům již není nucen svou práci odkládat, ale je schopen zareagovat okamžitě. Není to však jen mobilita, kterou nám bezdrátové sítě nabízejí. Dalším přínosem je snadná instalace. Vzhledem k tomu, že bezdrátové sítě nepotřebují kabeláž propojující jednotlivá zařízení, mohou zajišťovat konektivitu i v obtížněji dostupných místech a jejich instalace se stává rychlejší a snáze rentabilní.

Další nespornou předností je jejich škálovatelnost. S růstem společnosti a zvyšujícím se počtem zaměstnanců, bude kabelová síť vyžadovat zásah do její infrastruktury, zatímco u bezdrátového řešení tato nutnost odpadá a většinou lze využít stávajícího hardwaru. Stinnou stránkou bezdrátových sítí se může zdát jejich zabezpečení. Jelikož u kabelových sítí je nutná fyzická přítomnost uživatele, tvoří tato podmínka již první formu zabezpečení, neboť útočník tak zpravidla musí překonat jiné bezpečnostní systémy vedoucí do objektu (ACS, EZS, CCTV, MZS).

U bezdrátových sítí se tato možnost nenabízí, neboť jejich dostupnost (rozsah pokrytí) může zasahovat i mimo objekt společnosti. Útočník má tak možnost provést útok bez své fyzické přítomnosti v daném objektu (např. ze sousední budovy nebo parkoviště). Nicméně lze v dnešní době nalézt mnohá řešení, ať už softwarová či hardwarová, která dokáží tyto útoky účinně eliminovat (šifrování, firewall, IDS, detekce pomocí triangulace).

2.1 Rozdělení bezdrátových sítí podle rozsahu

2.1.1 WPAN – Wireless Personal Area Network

Síť komunikující na krátkou vzdálenost (řádově jednotky metrů). Příkladem může být dnes velmi populární Bluetooth (IEEE 802.15.1), umožňující komunikovat podle vyzářeného výkonu v rozsahu jednotek až desítek metrů, s přenosovými rychlostmi pohybujícími se v jednotkách Mb/s (standard Bluetooth 3.0;4.0 až 24Mb/s). Zařízení komunikující v této síti jsou např. dálkové ovladače, headsety, repro soustavy nebo počítačové periferie jako klávesnice a myši. Samozřejmostí je dnes podpora této technologie u notebooků a mobilních telefonů.

2.1.2 WLAN – Wireless Local Area Network

Síť pracující v dosahu řádově desítek až stovek metrů (v závislosti na použité anténě a vyzářeném výkonu). Příkladem této sítě je Wi-Fi, jejíž přenosové rychlosti se v závislosti na použitém standardu pohybují v rámci desítek až stovek Mb/s (IEEE 802.11n až 600Mb/s). Tyto sítě nalezneme nejčastěji v interních korporátních prostředích, školách, restauracích, domácnostech ale i v dopravních prostředcích. Podporu těchto zařízení obsahují mobilní telefony, notebooky, tablety, televize, herní konzole a jiné spotřebiče.

2.1.3 WMAN – Wireless Metropolitan Area Network

Síť s metropolitním pokrytím. Typickým zástupcem této sítě je dnes postupně rozšiřující se technologie WiMAX (IEEE 802.16). Tato síť je zaměřena na bezdrátovou komunikaci ve venkovním prostředí a dálkové přenosy na vzdálenosti desítek kilometrů (až 50km), s teoretickou přenosovou rychlostí až 70Mb/s (v praxi však mnohem méně).

2.1.4 WWAN – Wireless Wide Area Network

Síť s velkoplošným pokrytím (celý stát). Příkladem jsou sítě jako GSM nebo 3G (fungující jako soustava vzájemně komunikujících buněk). Sítě tohoto typu jsou nejčastěji provozovány telekomunikačními společnostmi a poskytují hlasové a datové služby. Přenosové rychlosti se dnes pohybují řádově v jednotkách Mb/s.

2.2 Základní rozdělení topologií bezdrátových WLAN sítí

Základním stavebním blokem všech WLAN sítí je BSS neboli Basic Service Set. Standard IEEE 802.11 definuje BSS jako skupinu stanic, které navzájem komunikují. Tyto skupiny stanic mohou být rozděleny do dvou typů.

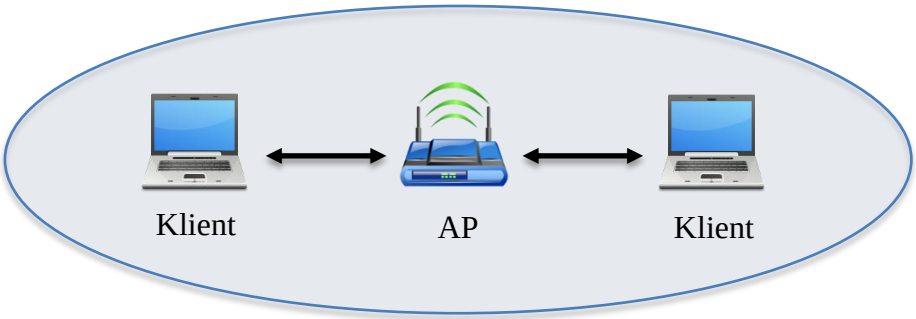
2.2.1 IBSS - Ad Hoc topologie

Pod názvem Ad Hoc se skrývají bezdrátové sítě, jejichž komunikace probíhá bez přítomnosti AP. Všechny stanice v takto vytvořené síti spolu komunikují jako rovný s rovným (Peer to Peerr, P2P) a celá topologie se tak označuje jako IBSS (Independent BSS). Rozsah Ad Hoc sítě je poté dán vysílacím výkonem zúčastněných stanic (řádově jednotky metrů) a je vhodný spíše jenom pro příležitostně vytvořenou síť. Rozsah pokrytí nese název BSA.

Obrázek 1. Topologie Ad Hoc WLAN sítě

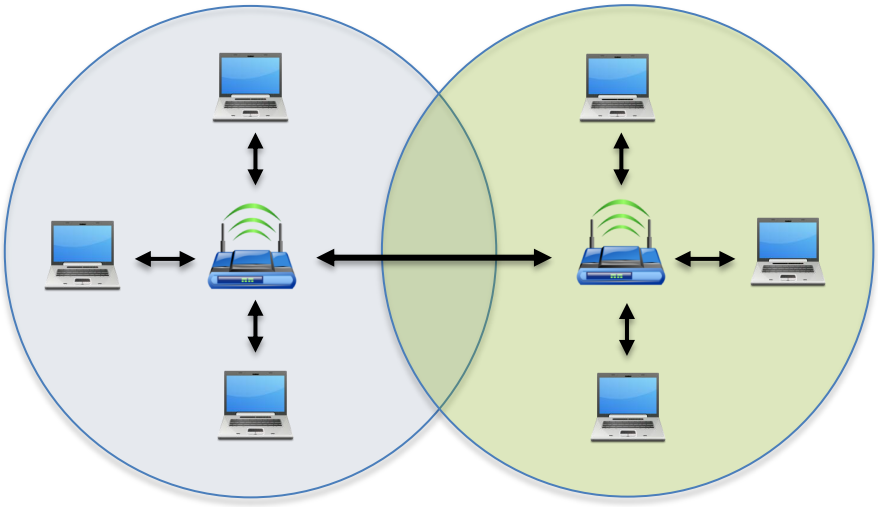
2.2.2 BSS - Infrastrukturální topologie

Druhý typ WLAN topologie se označuje jako BSS (infrastrukturální, někdy také jako Managed). Tato topologie je tvořena jedním přístupovým bodem, který řídí veškerou komunikaci mezi stanicemi. Spojení je tedy nejdříve navázáno s AP a teprve přes něj je traffic směrován k dalším stanicím. Oblast pokrytí je v tomto případě několikanásobně větší (řádově desítky metrů) a nese stejně jako u Ad Hoc sítí název BSA.



Obrázek 2. Infrastrukturální topologie WLAN sítě - BSS

V případě nedostatečného pokrytí požadované oblasti signálem, je možno BSA doplnit dalším přístupovým bodem skrze společný distribuční systém. Ten bude sdílet stejné SSID, avšak komunikovat na jiném kanálu, aby bylo zabráněno vzájemné interferenci (překrývání Wi-Fi sítí se v tomto případě doporučuje v rozmezí od 10 – 15%). Takto sestavená topologie se označuje jako ESS (Extended Service Set) a pokrytí nese název ESA (Extended Service Area)



Obrázek 3. Infrastrukturální topologie WLAN sítě - ESS

2.3 Pásmo ISM

Protože bezdrátově komunikujících zařízení stále přibývá a rádiových frekvencí je omezené množství, bylo zavedeno licencování jednotlivých pásem. Z tohoto důvodu vzniklo také pásmo nazvané ISM (Industrial, Scientific and Medical), které bylo vyhrazeno jak americkým regulátorem FCC, tak i evropskou standardizační organizací ETSI, pro průmyslové, vědecké a lékařské účely. Jelikož se jedná o pásmo, ve kterém komunikují mnohá zařízení jako např. Bluetooth, mikrovlnné trouby, bezdrátové telefony, vysílačky RC modelů aj., bylo toto pásmo ustanoveno jako volné, čili bez licenčních poplatků. Z toho také vyplývá jeho velká nevýhoda, spočívající ve vzájemné interferenci takto komunikujících zařízení.[8]

Z dostupných frekvencí se pro bezdrátové technologie požívá ISM pásmo 2,4GHz a UNII pásmo 5GHz.

2.4 Používané rádiové frekvence

V současnosti bezesporu nejpoužívanějším frekvenčním pásmem pro koncové uživatele (tzv. poslední míli), je pásmo 2,4GHz. Toto pásmo bylo dříve navrženo výhradně pro vnitřní použití, dnes jej ale můžeme nalézt i v prostředích vnějších.

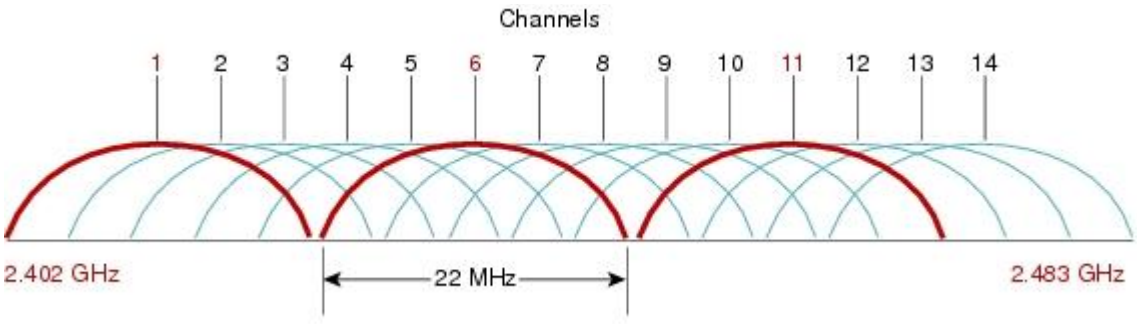
Vzhledem k vysoké hustotě zařízení pracujících na této frekvenci a tudíž vysokému zarušení tohoto spektra, se pomalu začínají prosazovat přístroje pracující na 5GHz.

Z důvodu mnohonásobně vyššího počtu zařízení komunikujících v pásmu 2,4GHz, budou i penetrační testy v praktické části této diplomové práce zaměřeny na toto pásmo.

2.4.1 Bezlicenční pásmo 2,4GHz

Bezlicenční pásmo 2,4GHz pracuje v rozsahu 2,400 – 2,4835GHz což činní jeho šířku 83,5MHz. Toto pásmo je rozděleno, v závislosti na různých částech světa, na určitý počet frekvenčních kanálů. Pro USA (FCC) je to 11, pro Evropu (ESTI) 13 a pro Japonsko (TELEC) 14. Z toho vyplývá, že pro Českou republiku je k dispozici 13 kanálů. Jelikož však některé bezdrátové technologie (IEEE 802.11b/g) využívající toto pásmo používají ke své funkci frekvenční kanál o šířce 22MHz s odstupem 5MHz, poskytuje toto pásmo jenom 3 frekvenční kanály, které se nebudou vzájemně překrývat. Jedná se o kanály 1 – 7 – 13. Všechna zařízení komunikující mezi těmito kanály, budou vždy alespoň z části interferovat.[9]

Dalším důležitým parametrem, který je třeba zmínit v souvislosti s provozem bezdrátových sítí, je vyzářený výkon EIRP. Ten je dán všeobecným oprávněním, které stanovuje příslušný správce frekvenčního spektra. V České republice tuto pozici zastává ČTÚ (Český Telekomunikační Úřad) a pro frekvenční pásmo 2,4GHz nesmí tato hodnota překročit 100mW. (VO-R/12/08.2005-6)[10]



Obrázek 4. Zobrazení překrývajících se kanálů v 2,4GHz pásmu [21]

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.
2412	2417	2422	2427	2432	2437	2442	2447	2452	2457	2462	2467	2472	2484
USA (FCC)													
Evropa (ESTI)													
Japonsko (TELEC)													

Tabulka 1. Čísla kanálů a jejich středové frekvence v MHz pro určité části světa

2.4.2 Bezlicenční pásmo 5GHz

Bezlicenční pásmo pracující na frekvenci 5GHz bylo v České republice schváleno místním regulátorem (ČTÚ) až v roce 2005, proto není zatím tolik používané a do širšího podvědomí se teprve dostává. Dalším faktorem, který také bránil rychlejšímu nasazení zařízení komunikující v tomto pásmu, byla jeho cena, která byla dříve vyšší než u 2,4GHz přístrojů.

5GHz pásmo pracuje v rozsahu od 5,150 – 5,725GHz a je rozděleno do tří dílčích pásem. (VO-R/12/08.2005-6)[10]

- 5,150 – 5,250MHz se středním EIRP výkonem do max. 200mW, určené pouze pro použití uvnitř jedné budovy
- 5,250 – 5,350MHz se středním EIRP výkonem do max. 200mW, určené pouze pro použití uvnitř jedné budovy
- 5,470 – 5,725MHz se středním EIRP výkonem do max. 1W a maximální střední spektrální hustotou EIRP 50 mW/MHz v libovolném 1 MHz úseku

Toto frekvenční pásmo má tedy širší rozsah 455MHz. A protože bezdrátové technologie (IEEE 802.11a) které v něm pracují, používají užší šířku kanálu 20MHz a zároveň větší odstup 20MHz, nabízejí oproti 2,4GHz pásmu výhodu v podobě 11 nepřekrývajících se kanálů.

2.5 Standardy IEEE 802.11

S postupným rozvojem bezdrátových sítí bylo nutné i v tomto oboru lidské činnosti zavést standardy, které měly ustanovit jistá pravidla. O to se postarala mezinárodní organizace IEEE (The Institute of Electrical and Electronics Engineers), vydávající do té doby mimo jiné i standardy týkající se Ethernetových sítí. Za tímto účelem tak byla vytvořena skupina

s označením IEEE 802.11, která měla na starost vývoj a úpravu standardů v oblasti WLAN.

První standard definovaný touto pracovní skupinou byl zveřejněn v roce 1997 a nesl stejné označení jako skupina samotná, tedy IEEE 802.11. Tento standard popisoval tři způsoby přenosu bezdrátového signálu. Metodou přímo rozprostřeného spektra (DSSS) pracující v bezlicenčním pásmu 2,4GHz, dosahující rychlosti 1 nebo 2Mb/s. Metodou rozprostřeného spektra s přeskakováním kmitočtů (FHSS) pracující v téže pásmu a přenosovými rychlostmi 1 nebo 2Mb/s. A metodou infračerveného přenosu (DFIR) vysílající v rozsahu 300 - 428GHz, a rychlostí taktéž 1 nebo 2Mb/s.

2.6 Nejpoužívanější standardy

2.6.1 IEEE 802.11a

Standard uveden v roce 1999, který přinesl výrazný nárůst rychlosti až na teoretických 54Mb/s. Komunikuje v pásmu 5GHz a využívá přitom metodu frekvenční modulace OFDM.

2.6.2 IEEE 802.11b

Tento standard byl publikován v roce 1999 a přinesl určité zvýšení přenosové rychlosti i do 2,4GHz pásma. Jednalo se o maximální rychlost 11Mb/s, která byla dosažena pomocí nového způsobu kódování (CCK) s modulací DSSS.

2.6.3 IEEE 802.11g

Standard uveden v roce 2003, který povýšil rychlost v 2,4GHz pásmu až na max. 54Mb/s. Používá modulaci OFDM a podporuje CCK, což ho činí zpětně kompatibilním se standardem IEEE 802.11b. Další klíčovou technologií, kterou tento standard disponuje je Kvalita Služeb/Quality of Service (QoS), která umožňuje nastavit priority využívaných služeb (např. VoIP) a zajistit tak plynulost jejich datových streamů.

2.6.4 IEEE 802.11n

Standard zveřejněn v roce 2009 přinesl komunikaci v obou výše zmiňovaných pásmech. Zařízení tak může pracovat buď v pásmu 2,4GHz nebo 5GHz. Další změnu, kterou tento standard přinesl, bylo podstatné navýšení přenosové rychlosti a to až na nominálních 600Mbit/s, přičemž minimální dosahovaná rychlost by neměla klesnout pod 100Mbit/s.

Této rychlosti je dosahováno použitím technologie MIMO-OFDM, která pro přenos signálu používá více antén. Standard je také zpětně plně kompatibilní se standardy IEEE 802.11a/b/g.

2.7 Reálné přenosové rychlosti

Všechny uvedené rychlosti výše zmíněných standardů jsou však nominální, nikoliv efektivní. Nominální rychlost považujeme spíše za teoretickou, která nepočítá s režijními informacemi poslanými za účelem navázání spojení, potvrzení příjmu dat apod. Z těchto důvodů je pak reálná efektivní přenosová rychlost o 30 - 40% nižší. Další skutečnost, která snižuje efektivní rychlost je, že bezdrátová zařízení pracují v tzv. Half-Duplex módu, což znamená, že v jednom okamžiku může vysílat pouze jedna strana.

Standard IEEE	802.11a	820.11b	802.11g	802.11n
Rok ratifikace	1999	1999	2003	2009
RF pásmo	5GHz	2,4GHz	2,4GHz	2,4 nebo 5GHz
Modulace	OFDM	DSSS	OFDM	OFDM - MIMO
Přenosová rychlost	54Mbps	11Mbps	54Mbps	600Mbps
Dosah	35m	35m	35m	75m

Tabulka 2. Přehled standardů IEEE 802.11

2.8 Wi-Fi

Wi-Fi – Wireless-Fidelity (Bezdrátová-Věrnost) je dnes v podstatě synonymem pro bezdrátové sítě standardu IEEE 802.11.

Označení Wi-Fi v současnosti vydává certifikační autorita nazvaná Wi-Fi Alliance (dříve WECA), která se stará o dodržování standardů a vzájemnou kompatibilitu takto označený zařízení.

Obrázek 5. Logo Wi-Fil Alliance [12]

3 ZABEZPEČENÍ WI-FI SÍTÍ

3.1 Zabezpečení přístupového bodu – AP

Bezdrátová síť je nejčastěji vytvářena přístupovým bodem - Access Pointem. (nepočítáme-li Ad Hoc sítě). Ten ve svém dosahu v závislosti na daném vyzářeném výkonu EIRP a konstrukčním provedení antén, komunikuje s klienty přítomnými v síti pomocí rádiových vln a bývá obvykle spojovacím bodem s kabelovou sítí. Proto je nutno zabezpečit jeho přístup. Z hlediska sítě se jedná o přístup na základě jména a hesla. To je ve výchozím (defaultním) stavu nastaveno výrobcem a uvedeno v servisním manuálu. Při provádění počáteční konfigurace přístupového bodu, by se tak nemělo zapomenout na jeho změnu.

3.2 Skrytí SSID

Service Set Identifier neboli SSID je unikátní identifikátor označující bezdrátovou síť, v níž se dané zařízení nachází. SSID je řetězec až 32 alfanumerických znaků udávající název sítě. Aby mohli jednotliví klienti přistupovat do sítě, musí se prokázat stejným SSID identifikátorem. Jedná se tak o formu autentizace. SSID je vysílán přístupovým bodem jako broadcast a je tedy dostupný všem zařízením v jeho dosahu. Není-li toto vysílání skryto, může se libovolný klient do dané sítě připojit. V opačném případě bude nutno SSID identifikátor znát. Skrytí SSID vysílání tak můžeme považovat za formu zabezpečení, protože tímto můžeme zamezit, aby se do chráněné sítě nepřipojil neoprávněný uživatel, který SSID nezná. Protože je však SSID vysíláno v otevřené podobě, lze ho pomocí softwarových nástrojů zobrazit, i když je skryto.

3.3 Filtrování MAC adres

Jak už samotný název napovídá, jedná se o kontrolu přístupu na základě MAC adresy. Administrátor sítě je schopen na základě seznamu těchto adres nakonfigurovat síťový hardware. To může být realizováno dvěma způsoby, formou blacklistu nebo whitelistu. V prvním případě bude filtr blokovat klienty, kteří k síti nemají přístup. Nezabrání však přístupu neznámým klientům (MAC adresám), kteří na seznamu uvedeni nejsou. Jelikož však dnes lze snadno dostupnými nástroji MAC adresu změnit, útočník se tak může do sítě připojit znovu, pod alternativní MAC adresou. To činí tuto metodu filtrování méně efektivní. Druhá možnost je opakem první. Filtr umožní přístup pouze těm klientům, kteří jsou na tomto seznamu uvedeni, a zbytku přístup odepře. Útočník by tak v tomto případě

musel konkrétní MAC adresu znát. Tato metoda je bezpečnější, avšak náročnější na správu aktuálního seznamu MAC adres.

3.4 WEP

WEP – Wired Equivalent Privacy je mechanizmus zabezpečení bezdrátových sítí. Tato součást standardu IEEE 802.11b si klade za cíl zabezpečit autentizaci a komunikaci v bezdrátové síti. K tomu používá symetrickou proudovou šifru RC4. Klíč k této šifře musí znát obě zúčastněné stanice. Vysílací stanice jím tedy přenášená data zašifruje a přijímající je stejným klíčem dešifruje. Šifrování dat se provádí 64 bitovým klíčem, který se skládá z uživatelského klíče - 40 bitů (daný standardem) a dynamicky měnícího se inicializačního vektoru (IV) o délce 24 bitů. V praxi se vyskytují i silnější zabezpečení, zpravidla 128 bitů 104 klíč + 24 inicializační vektor.

3.5 WPA

Zkratka WPA - Wi-Fi Protected Access značí další metodu zabezpečení bezdrátových sítí. Tato technologie byla přijata v roce 2002 Wi-Fi aliancí a vychází z tehdy připravovaného standardu 802.11i zveřejněného o dva roky později. Vznikla za účelem nahradit již nedostačující autentizační a šifrovací mechanismus WEP (prolomen v roce 2001) a odstranit jeho nedostatky. WPA používá pro zabezpečení komunikace protokol TKIP (Temporal Key Integrity Protocol). Tento mechanismus nabízí implicitně 128 bitový klíč se 48 bitovým inicializačním vektorem (IV), při zachování stejného šifrovacího algoritmu RC4, což ho činí zpětně kompatibilní s WEP. Další výhoda, kterou TKIP nabízí, je systém dynamicky měnícího se klíče. Kontrola integrity dat je zde realizována pomocí MIC (Message Integrity Check), která poskytuje lepší ochranu než CRC32.

Vylepšení doznala také autentizace, kterou je zde možno realizovat dvěma způsoby. První z nich je PSK (PreShared Key). Jedná se o řešení určené pro domácnosti nebo společnosti, které nedisponují autentizačním serverem, kde všechny zúčastněné stanice přistupují k AP pomocí stejného klíče. Druhá varianta pak nabízí ověřování klienta pomocí standardu 802.1X vůči autentizačnímu serveru nebo službě.

3.6 WPA2

V roce 2004 byl publikován standard IEEE 802.11i nesoucí označení RSN (Robust Security Network), který pozvedl zabezpečení bezdrátových sítí na další úroveň. Wi-Fi

aliancí byl certifikován jako WPA2. Protože WPA bylo vyvíjeno z IEEE 802.11i, logicky tak sdílí některé jeho vlastnosti. Kromě již zavedeného TKIP podporuje také technologii CCMP, která proudovou symetrickou šifru RC4, kterou používají dvě předešle uvedená řešení, nahradila dosud neprolomená bloková šifra AES (Advanced Encryption Standard). Tato šifra nabízí klíč o délce 128/192/256 bitů. O integritu přenášených dat se opět stará MIC (algoritmus označovaný Michael). Autentizace je stejně jako u WPA řešena dvěma způsoby, přednastaveným sdíleným klíčem (PSK) a 802.1X. Samotný proces ověřování je prováděn skrze čtyřcestný handshake.

3.7 802.1X

IEEE 802.1X (známý také jako Port Based Network Access Control) je standard poskytující metodu autentizace ve všech typech LAN/WLAN. Byl vydán v roce 2001 a představuje obecný bezpečnostní rámec zahrnující autentizaci klientů, integritu dat a distribuci klíčů. K tomu využívá protokol EAP (Extensible Authentication Protocol). Hlavní body architektury IEEE 802.1X tvoří tři entity. První z nich je supplicant (klient) žádající o přístup do sítě. Druhou zastává přístupový bod, který plní funkci autentizační autority. Ten se dotazuje na třetí poslední entitu v tom procesu, kterou je obvykle autentizační server (např.: Kerberos, RADIUS). Na základě jeho rozhodnutí, poté AP povolí nebo odepře žadateli přístup. Autentizaci lze provádět prostřednictvím mnoha metod s různým stupněm bezpečnosti. Nejznámější jsou např.: TLS, TTLS nebo PEAP. K ověření se používají hesla i digitální certifikáty. Po autentizaci jsou přístupovým bodem ověřeným klientům distribuovány dynamicky měnící se klíče, které jsou známy pouze danému klientu, mají omezenou životnost a jsou platné, dokud se klient neodhlásí nebo neodpojí. Autentizace pomocí IEEE 802.1X je využívána především v korporátní sféře.

3.8 RADIUS

RADIUS (Remote Authentication Dial In User Service) je autentizační služba běžící na pozadí operačního systému (Windows, UNIX) a spadající do rodiny protokolů AAA. RADIUS server je často používán ve spojení s výše zmíněným standardem IEEE 802.1X pro přístup k bezdrátovým sítím.

3.9 Firewall

Jedno ze základních ochranných opatření serverů či pracovních stanic tvoří firewall. Tento bezpečnostní nástroj může být realizován buď softwarovým programem, nebo hardwarovým zařízením. Firewall monitoruje datový provoz mezi sítěmi (nejčastěji interní síť vs Internet) a na základě nakonfigurovaných pravidel řídí přístup. Může tak sloužit jako ochrana před škodlivým kódem (malwarem) nebo útočníkem, který se pokouší získat vzdálený přístup do sítě, nebo naopak blokovat odesílání dat z interní sítě bez oprávnění. Příchozí a odchozí komunikace může být filtrována v závislosti na bezpečnostní politice stanovené společností. Může se jednat o kontrolu zdrojových a cílových IP adres a portů, ověřování protokolů na jednotlivých vrstvách modelu OSI, správa přístupu aplikací k jednotlivým službám a prostředkům, prověřování emailových domén, sledování množství odeslaných emailů za určitý čas a aj. Další činností firewallů je také zaznamenávání veškeré síťové aktivity do logů, ve kterých lze uložené informace zpětně dohledat a určit tak příčinu problému. Firewally mají nejčastěji podobu packetových filtrů, aplikačních bran (proxy gateways) nebo stavových packetových filtrů. Softwarové firewally jsou obvykle dodávány jako ucelená řešení spolu s antivirovým programem pro komplexní zabezpečení operačních systémů. Správná implementace firewallu je stěžejní při zabezpečování sítí.

3.10 IDS/IPS

IDS a IPS jsou hardwarové bezpečnostní prvky sloužící k filtrování síťové komunikace. Zatímco IDS systémy (Intrusion Detection Systems) pouze monitorují síťový provoz, detekují kompromitující kód a zaznamenávají jej do logů, IPS systémy (Intrusion Prevention Systems) se kromě analýzy také podílí na jejich odstranění/blokování a poskytují tak aktivní ochranu. Protože tato zařízení dokáží filtrovat síťový provoz na nižších OSI vrstvách, uvádí v celkovém důsledku jen zanedbatelnou latenci (řádově desítky mikrosekund).

IDS a IPS zařízení posilují a doplňují bezpečnost síťové infrastruktury, nejsou tudíž náhradou za jiné bezpečnostní prvky jako např. firewall.

II. PRAKTICKÁ ČÁST

4 ZABEZPEČENÍ POUŽÍVANÁ V PRAXI

Pro účely této diplomové práce byla provedena měření, jejichž cílem bylo zjistit a statisticky vyhodnotit dnes nejčastěji používaná zabezpečení Wi-Fi sítí.

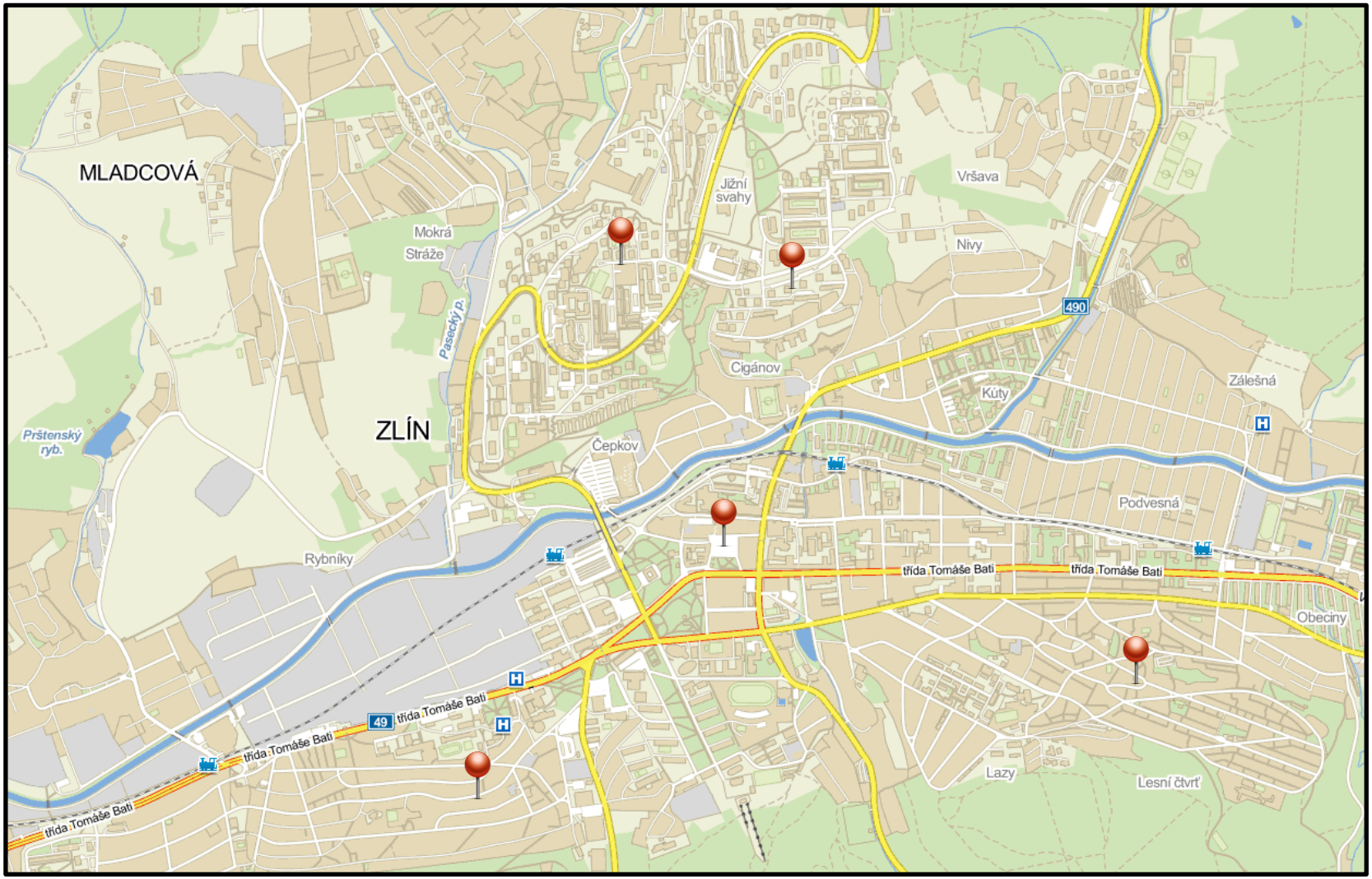
Tato měření probíhala ve Zlíně v následujících pěti lokalitách:

- ulice Budovatelská - 49°14'6.327"N, 17°40'17.121"E
- ulice Luční - 49°14'12.266"N, 17°39'42.967"E
- náměstí Míru - 49°13'35.495"N, 17°40'0.943"E
- ulice Prostřední - 49°13'22.503"N, 17°41'4.724"E
- ulice Na Vyhlídce - 49°13'5.949"N, 17°39'20.54"E

Hodnoty byly zaměřeny pomocí bezdrátového adaptéru Alfa AWUS036H s 5dB anténou a zaznamenány programem KisMAC 0.3.3. Tyto lokality byly vybrány s ohledem na pokrytí panelákových sídlišť, rodinné zástavby i centra města, kde lze očekávat větší zastoupení firem a tudíž i nasazení silnějších forem zabezpečení. Měření v každé lokalitě probíhalo ve venkovním prostředí po dobu 15 minut.

#	Ch	SSID	BSSID	Enc	Signal	Avg	MaxSignal	Packets	Data
0	1	c3111ea	[redacted]	WEP	0	28	35	163	15.71KiB
1	1	VOIP	[redacted]	WEP	30	27	38	257	24.09KiB
2	1	wmpet1	[redacted]	WPA2	47	47	66	700	189.09KiB
3	3	Pippen	[redacted]	WPA2	72	69	87	906	186.17KiB
4	1	davenove	[redacted]	WPA	0	27	33	286	52.90KiB
5	1	-WiFi-	[redacted]	WEP	32	29	40	446	51.46KiB
6	1	Kristina	[redacted]	WEP	0	29	36	154	10.65KiB
7	1	Andree	[redacted]	WPA2	26	30	38	119	13.83KiB
8	3	<hidden ssid>	[redacted]	NO	23	23	36	215	22.91KiB
9	3	Doma	[redacted]	WEP	40	41	50	540	155.33KiB
10	3	VOIP	[redacted]	WEP	33	32	41	529	35.32KiB
11	3	AVONET_Zlin_05	[redacted]	NO	23	24	50	330	34.43KiB
12	3	mojeWiFi_Zlin_42	[redacted]	NO	23	24	38	335	36.75KiB
13	4	INET_L	[redacted]	WEP	0	29	38	145	14.59KiB
14	8	<hidden ssid>	[redacted]	WPA	0	28	36	525	55.92KiB
15	6	nivyair	[redacted]	WEP	0	27	41	465	54.31KiB
16	8	Annie	[redacted]	WEP	0	45	67	1368	114.95KiB
17	5	cznet4	[redacted]	NO	0	36	49	409	34.71KiB
18	5	linksys5B92	[redacted]	NO	0	30	41	698	68.94KiB
19	5	dream_01	[redacted]	WEP	0	26	33	187	21.00KiB
20	10	i2net_svahy	[redacted]	WEP	0	78	89	4306	332.07KiB
21	4	vyoralek	[redacted]	WEP	32	30	43	441	31.33KiB
22	8	<hidden ssid>	[redacted]	WPA2	0	32	49	281	68.33KiB
23	6	VOIP	[redacted]	WEP	0	25	35	237	22.21KiB
24	4	Sisi	[redacted]	WPA	43	41	55	772	244.68KiB
25	4	BBB	[redacted]	WPA	0	27	44	678	78.22KiB
26	6	VOIP	[redacted]	WEP	0	32	46	761	70.29KiB
27	9	jika	[redacted]	WPA	0	39	50	673	81.33KiB
28	8	vope	[redacted]	WEP	0	28	33	328	22.80KiB
29	7	linksys8A76	[redacted]	WEP	0	37	49	632	52.45KiB
30	12	Wifi	[redacted]	WPA2	0	54	100	2528	0.76MiB

Obrázek 6. Příklad zaznamenaných Wi-Fi sítí

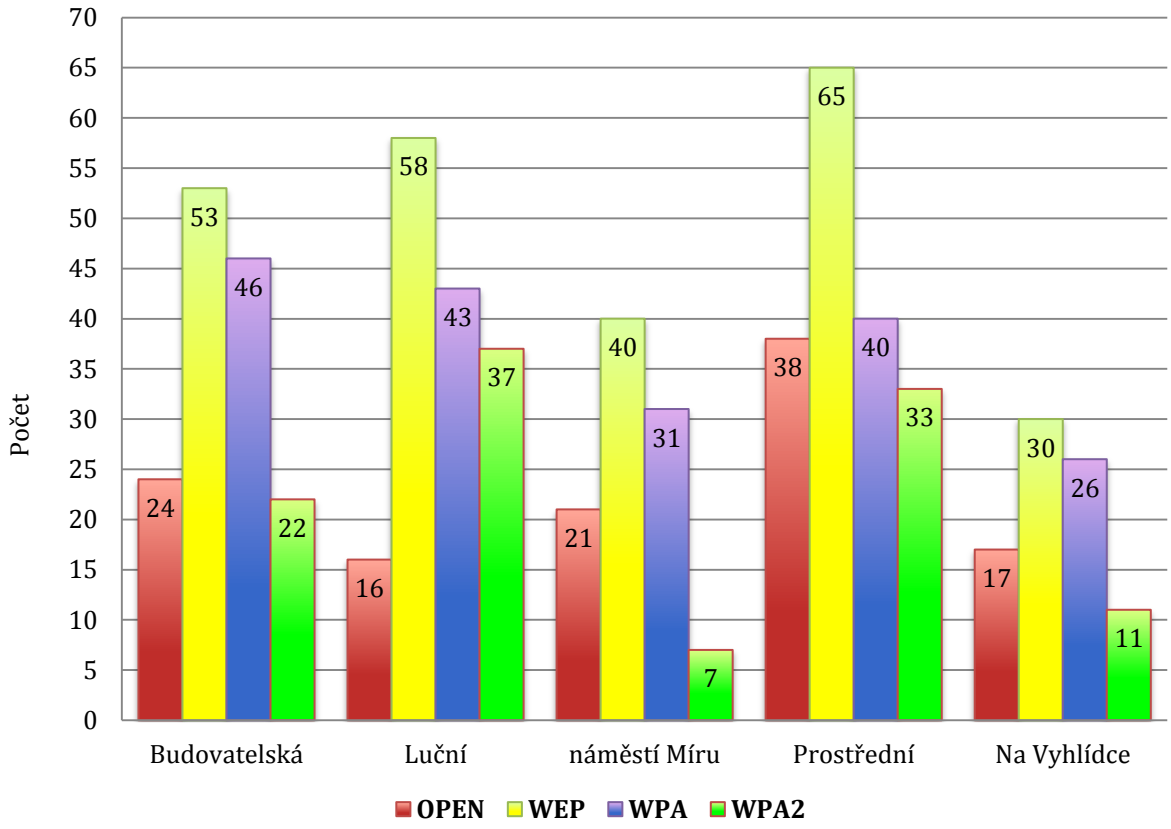


Obrázek 7. Lokality ve kterých probíhala měření

Naměřené hodnoty uvedené v tabulce níže, vypovídají o nejčastěji nasazovaných metodách zabezpečení jak v domácnostech, tak i v korporátní sféře. Lokality, ve kterých měření probíhala, byla ovlivněna několika faktory jako např. nadmořská výška bodu, ve kterém měření probíhalo, okolní objekty a členitost terénu (stínění panelákovým segmentem a jinými výškovými budovami – větší útlum signálu) nebo samotné umístění lokality (okrajová část města x centrum).

Lokalita	Počet sítí	OPEN	WEP	WPA	WPA2
ulice Budovatelská	145	24	53	46	22
ulice Luční	154	16	58	43	37
náměstí Míru	99	21	40	31	7
ulice Prostřední	176	38	65	40	33
ulice Na Vyhlídce	84	17	30	26	11
Celkem	658	116	246	186	110

Tabulka 3. Počet naměřených Wi-Fi sítí a jejich zabezpečení

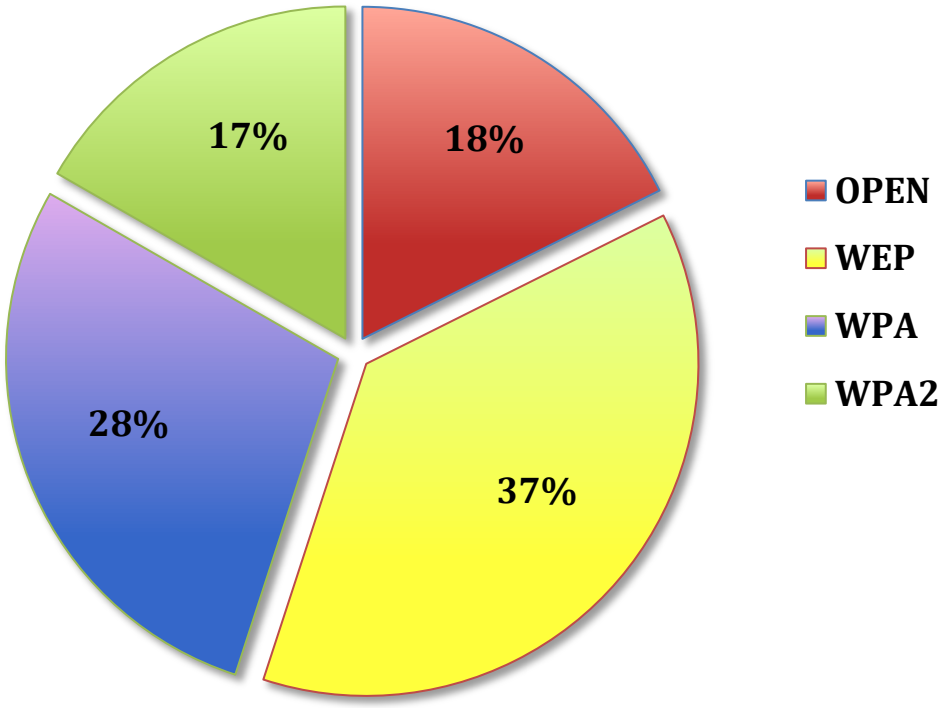


Graf 1. Použitá zabezpečení v jednotlivých měřených lokalitách

V lokalitách panelákových sídlišť (ulice Budovatelská, Luční), tedy s větší aglomerací, se potvrdil předpoklad velké hustoty Wi-Fi sítí. Naopak v prostředí rodinných zástaveb (ulice Prostřední, Na Vyhlídce), kde byl počet naměřených bezdrátových sítí menší, se hodnoty značně lišily, což mohlo být zapříčiněno jak rozdílem nadmořské výšky obou měřených míst (25m), tak prostým faktem, že je v této lokalitě provozováno méně Wi-Fi sítí.

Z celkového počtu 658 zaznamenaných bezdrátových sítí, jasně převažovalo zabezpečení WEP v poměru 37%, na druhém místě se umístilo WPA s 28%, jako třetí, přesto v hojném počtu byly sítě otevřené (OPEN) se zastoupením 18% a až na posledním místě se umístil bezpečnostní mechanismus WPA2 s 17%.

Typy zabezpečení na jednotlivých pozicích byly až na jednu vyjímku shodné ve všech místech, kde měření probíhala, z čehož lze vyvodit současný trend používaných zabezpečení. Počet nezabezpečených (otevřených) sítí, tvořil vždy nezanedbatelné procento v každé lokalitě, přičemž pouze v lokalitě Náměstí Míru bylo toto množství OPEN sítí zdůvodněno větší měrou zastoupených společenských zařízení, jako jsou bary, kavárny apod.



Graf 2. Procentuální znázornění použitých zabezpečení ve všech naměřených sítích (658)

5 NÁVRH PRACOVNÍCH SCÉNÁŘŮ PRO PENETRAČNÍ TESTOVÁNÍ

Na základě analýzy více než 600 Wi-Fi sítí byly sestaveny 3 pracovní scénáře nejčastěji vyskytující se v praxi. Tyto scénáře byly vhodným způsobem doplněny o další možnosti zabezpečení popsaných v teoretické části této práce a následně podrobeny penetračním testům, za účelem odhalit jejich slabá místa.

Na jednotlivé scénáře byly aplikovány postupy, jejichž cílem bylo:

- detekovat testovanou bezdrátovou síť
- zjistit potřebné informace – SSID, BSSID, zabezpečení, datový traffic aj.
- překonat dané zabezpečení – WEP, WPA, WPA2, MAC filtering
- získat kompletní kontrolu nad sítí

Všechny penetrační testy byly provedeny na MacBooku Pro 13“ s procesorem Intel Core 2 Duo 2,26GHz, 4GB 1066 MHz DDR3 RAM, NVIDIA GeForce 9400M, v aplikaci Gerix Wifi Cracker, součásti Linuxové distribuce Backtrack 4 R2, spouštěné virtualizovaně pomocí softwaru Parallels Desktop 6.0 a bezdrátovým adaptérem Alfa AWUS036H s 5dB anténou.

Další softwarové aplikace použité při penetračních testech byly KissMAC 0.3.3 a Brutus. Testovanými přístupovými body byly Air Live WL-5460AP a Cisco Linksys WRT320N.

5.1 Scénář A

Z naměřených dat vyplynulo, že WEP, ačkoliv nejméně přijatelné zabezpečení, je stále nejvíce využíváno. Broadcast SSID byl u tohoto typu zabezpečení vždy zapnut a bezdrátové sítě tak byly vždy viditelné. Jelikož takto zabezpečenou síť provozují především domácí uživatelé, nepředpokládá se použití žádných dalších nastavení pro zvýšení bezpečnosti jako např. filtrování MAC adres. Jednou z častých chyb konfigurace AP je, že autentizační údaje pro administraci přístupového bodu zůstávají nezměněny z jeho výchozích hodnot. Zná-li pak útočník tyto defaultní údaje, je schopen vstoupit do administrace přístupového bodu a plně nad ním převzít kontrolu. Přihlašovací údaje přístupového bodu zůstaly v tomto scénáři nezměněné, aby mohl být demonstrován postup, jak snadno lze získat kontrolu nad primárním zařízením celé bezdrátové sítě. Z těchto poznatků lze vyvodit následující situaci:

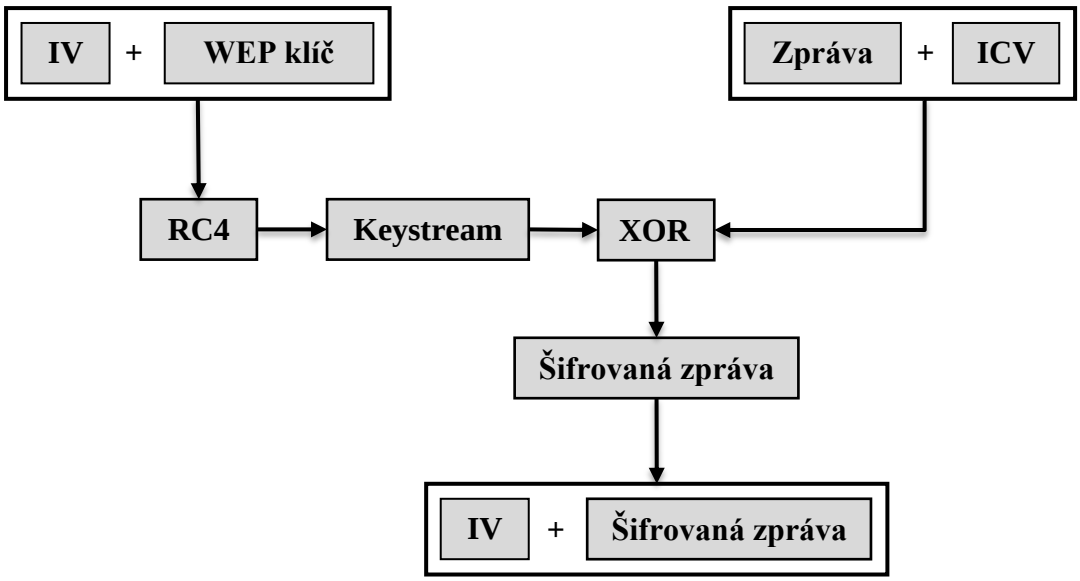
- SSID broadcast povolen
- zabezpečení WEP 128bit
- výchozí autentizační údaje přístupového bodu

5.1.1 Zranitelnosti WEP

Abychom mohli zaútočit na bezdrátovou síť zabezpečenou pomocí WEP, je potřeba znát její vnitřní strukturu a z ní vyplývající zranitelnosti.

Proudová šifra RC4 vytvoří z inicializačního vektoru a tajného klíče tzv. Keystream, kde WEP klíč je vždy stejná hodnota, ale IV se dynamicky mění. Jak již bylo zmíněno v teoretické části, inicializační vektor má délku 24 bitů a může tak nabývat 2^{24} hodnot, což je celkem 16777216 kombinací. Při dlouhodobějším přenosu nebo vyšší rychlosti dojde k situaci, kdy již jednou zvolený inicializační vektor bude opětovně použit a takto vyslaný packet již nebude jedinečný.

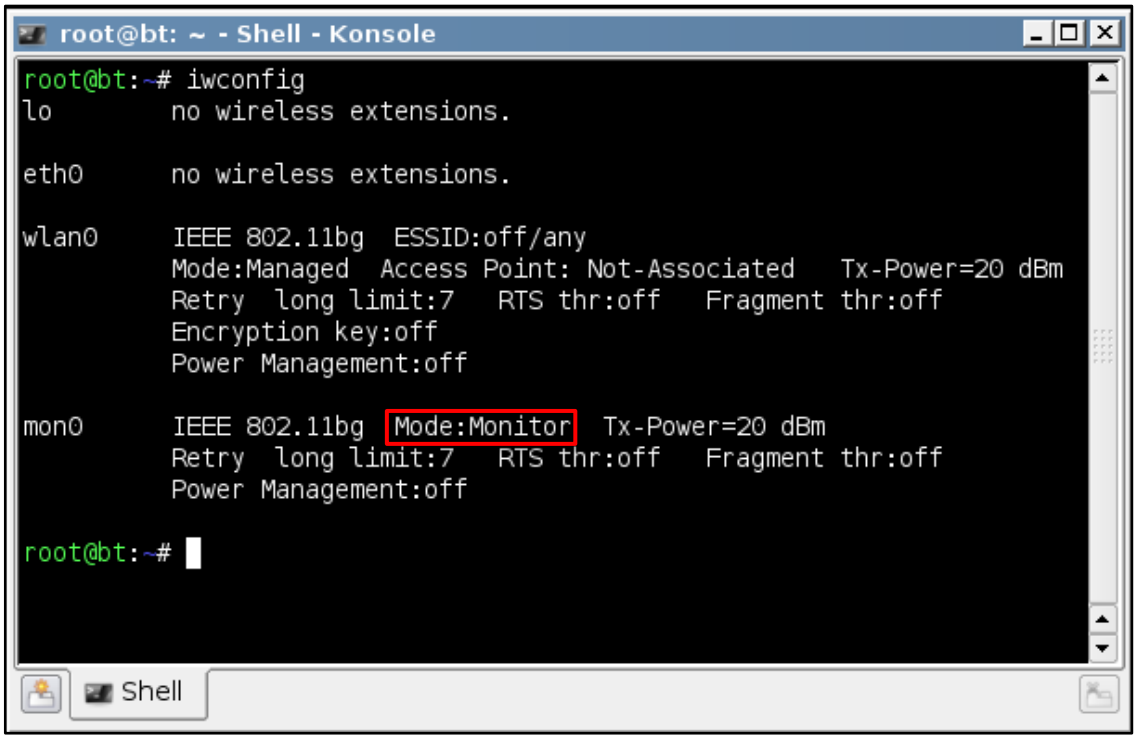
Keystream poté dále vstupuje do logické funkce XOR, kde je zpracován spolu s nešifrovanou zprávou (plaintext) a jejím kontrolním součtem ICV (Integrity Check Value). Tyto hodnoty tvoří na výstupu logického výhradního součtu šifrovanou zprávu, která je nakonec doplněna o použitý inicializační vektor a odeslána. Předsazený IV je použit pro zpětné dešifrování.



Obrázek 8. Blokové schéma bezpečnostního mechanizmu WEP

5.1.2 Penetrační test scénáře A

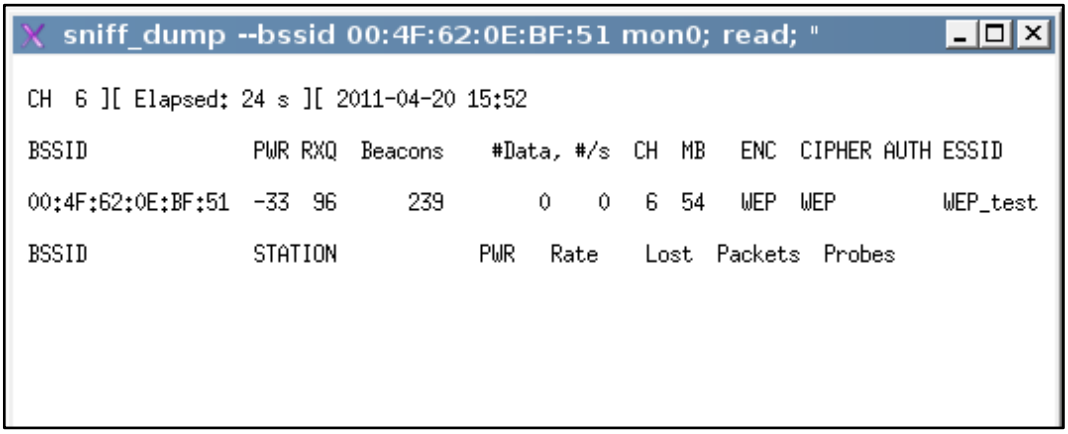
Provoz v bezdrátových sítích probíhá na druhé vrstvě modelu OSI. Chtějí-li dvě bezdrátové stanice navzájem komunikovat, musí znát své hardwarové adresy. Vysílající stanice zadá MAC adresu do Destination pole v hlavičce Datalinkového rámce a pouze ta stanice, s níž se tato adresa shoduje, rámec zpracuje. Všechny ostatní stanice v bezdrátové síti tento rámec zahodí a budou jej ignorovat. Aby však bylo možné provést sniffing – odposlouchávání/monitorování sítě, bylo nutné daný bezdrátový adaptér přepnout do tzv. monitor módu (RFMON), ve kterém je schopen síťový traffic přijímat i v případě, že mu není určen. (Monitor mód není možné zapnout na všech bezdrátových adaptérech. Jedná se většinou o bezdrátové síťové karty určené pro tento typ činnosti a je potřebná podpora ze strany ovladačů pro konkrétní operační systém). Bezdrátový adaptér byl v tomto případě přepnut do monitor módu v aplikaci Gerix Wifi Cracker.



Obrázek 9. Bezdrátový adaptér přepnut do monitor módu

Po provedení sniffingu sítě, byl zachycen nepřetržitý proud beacon packetů, který signalizoval, že se v dosahu klienta nachází bezdrátové zařízení. Po bližším ohledání zaznamenaných informací bylo z SSID identifikátoru zjištěno, že se nalezená síť jmenuje WEP_test, vysílá na kanálu 6(CH) a MAC adresa jejího přístupového bodu, čili BSSID je 00:4F:62:0E:BF:51. Informace o útlumu -33dB(PWR) naznačovala, že vysílající AP se nachází v blízkosti bodu, ze kterého byla detekce provedena. Dále bylo vypozorováno, že

pro zabezpečení této sítě je použit bezpečnostní mechanismus WEP(ENC) a na sítí nikdo nevysílá, neboť v době monitorování síťového provozu nebyla zjištěna žádná aktivita klientů (0 #/s).



Obrázek 10. Výstup z aplikace Gerix Wifi Cracker – sniffing

5.1.3 Prolomení WEP útokem KoreK Chopchop attack

Aby mohl být tento útok proveden, je potřeba zachytit packet, který budeme dešifrovat.

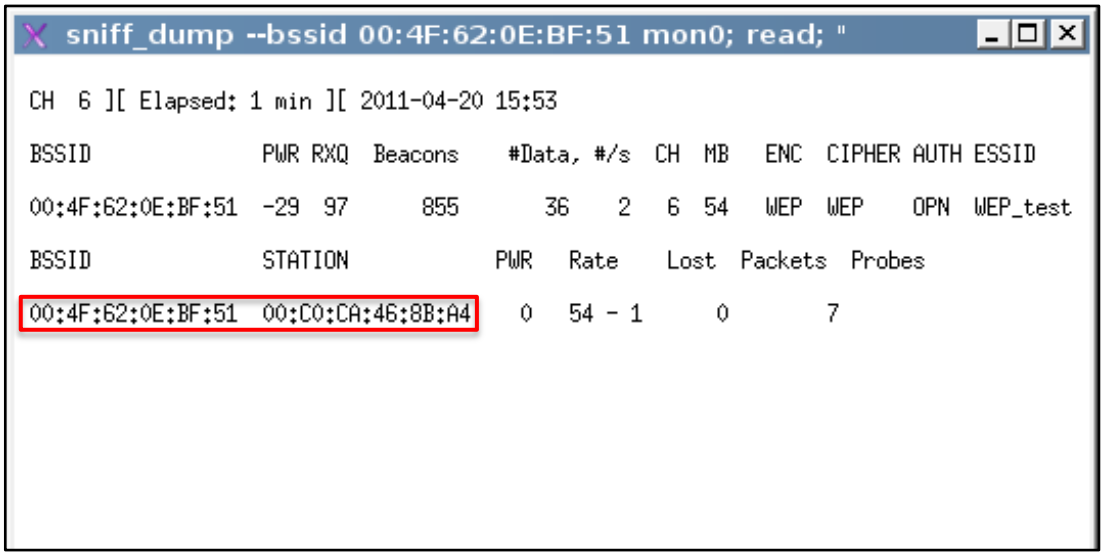
KoreK ChopChop útok využívá slabého zabezpečení integrity posílaných dat. Ta je realizována pouze metodou kontrolního součtu CRC-32, který slouží k detekci chyb v přenosu. Ten kvůli své lineárnosti není kryptograficky bezpečný a umožňuje útok typu Man-In-The-Middle.

Tato zranitelnost umožňuje útočníkovi upravit jak šifrovaný paket, tak jeho odpovídající algoritmus CRC. Mimoto použití operátoru XOR v protokolu WEP znamená, že vybraný bajt v šifrované zprávě, vždy závisí na tomtéž bajtu nešifrované zprávy. Pokud se tedy poslední bajt šifrované zprávy oddělí, zpráva se sice poruší, ale rovněž tím lze uhodnout hodnotu odpovídajícího nešifrovaného bajtu a podle toho šifrovanou zprávu opravit.[18]

Je-li poté opravený packet znovu zaveden na síť, přístupový bod ho odstraní, když se domnívá, že byl chybný (v tomto případě je třeba provést nový odhad), ale správný odhad bude jako obvykle přenesen. Opakováním útoku pro všechny bajty zprávy lze dešifrovat packet WEP a obnovit proud klíčů.[18]

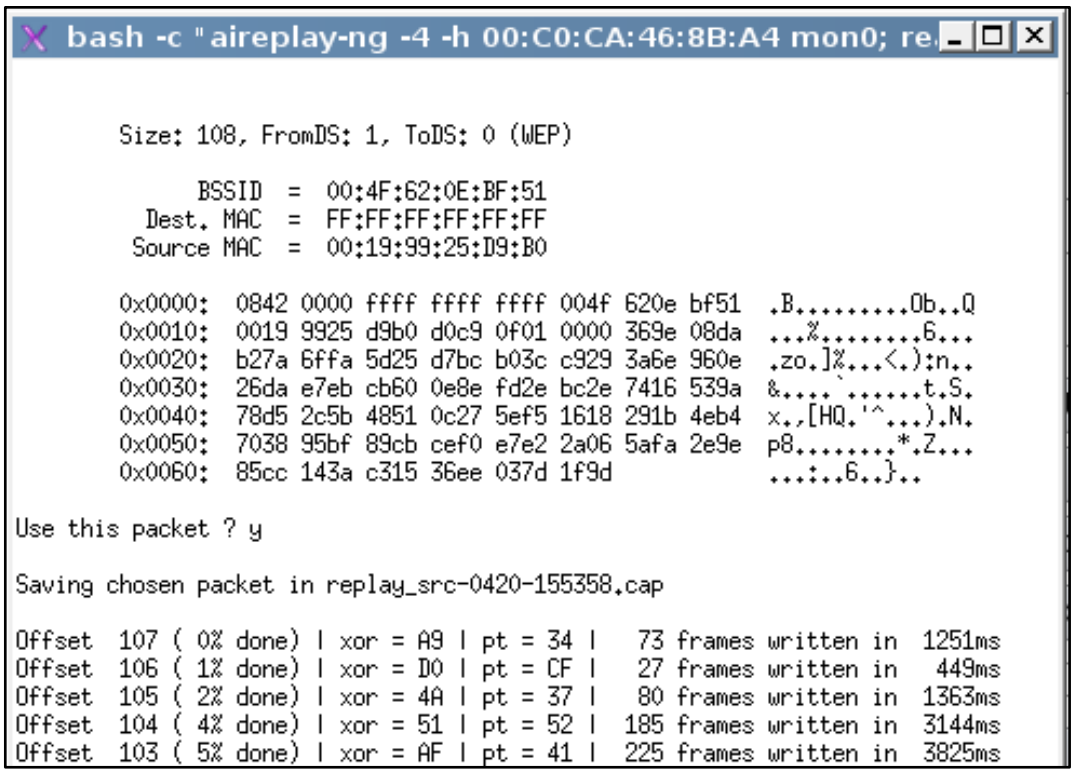
Aby mohl být útok proveden, bylo nejprve nutné bezdrátový adaptér asociovat s přístupovým bodem. Jelikož však zatím nebyl znám tajný WEP klíč, bylo nejdříve nutno provést falešnou autentizaci. Ta byla provedena volbou **Start false access point**

Authentication on Victim. Po jejím úspěšném vykonání, byla MAC adresa útočníka zobrazena v seznamu dostupných stanic přístupového bodu.

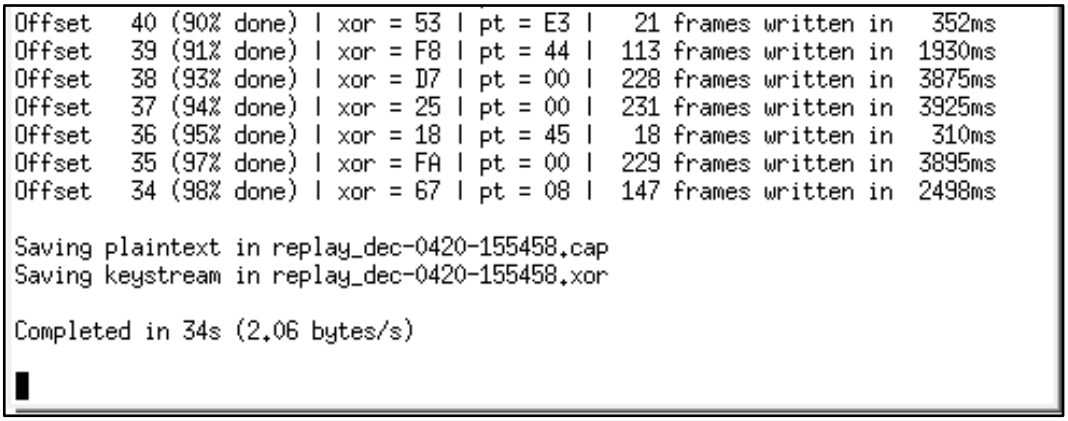


Obrázek 11. Přidaná MAC adresa útočníka po falešné autentizaci

Poté již mohl být proveden KoreK Chopchop útok. Obrázek uvedený níže zobrazuje zachycení packetu a následné provádění opakujícího se výhradního logického součtu, dokud nebyl sestaven keystrem i plaintext.

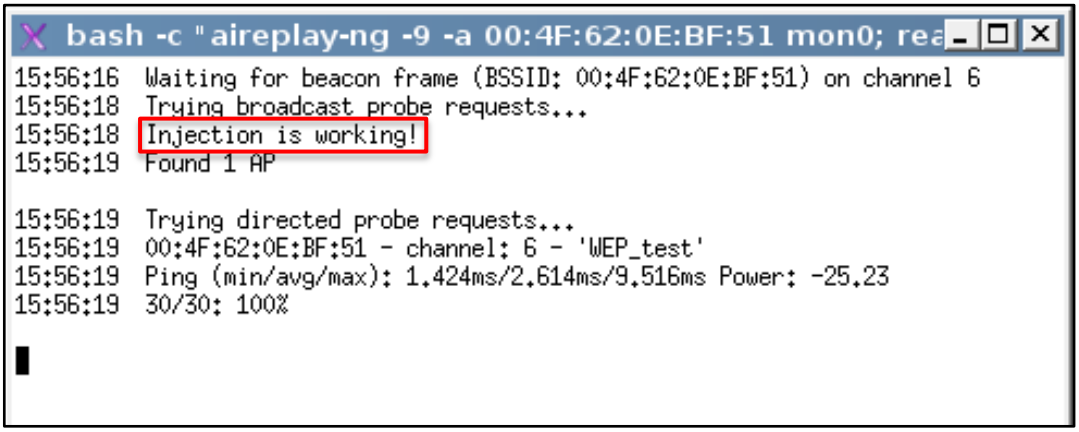


Obrázek 12. Začátek KoreK ChopChop útoku



Obrázek 13. Ukončení KoreK ChopChop útoku

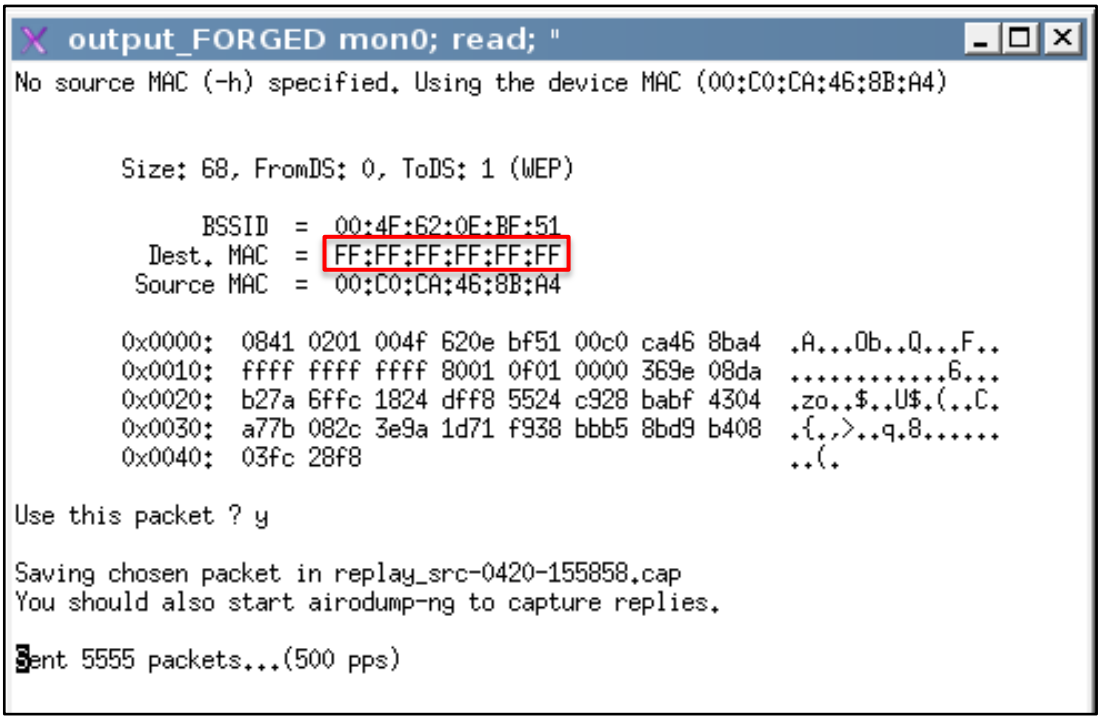
Hlavním cílem tohoto útoku bylo vygenerovat datový traffic a následně zachytit dostatečné množství jedinečných inicializačních vektorů. Je sice možné datové packety obsahující IV zachytávat pasivně pouhým sniffováním, nicméně se jedná o zdlouhavý proces, který je závislý na aktivitě klientů komunikujících v dané síti. V bezdrátové síti, kde se žádné vysílající stanice nenacházejí, se doba potřebná k nasbírání požadovaného množství IV může pohybovat řádově v hodinách i dnech. Aby bylo možné docílit vysokého množství datových packetů v krátkém čase, byla do sítě implementována packetová injekce. Zda-li je tuto techniku možné provést na konkrétní přístupový bod, ověřila volba **Performs a test of injection AP**.



Obrázek 14. Výstup potvrzující, že je packetová injekce funkční

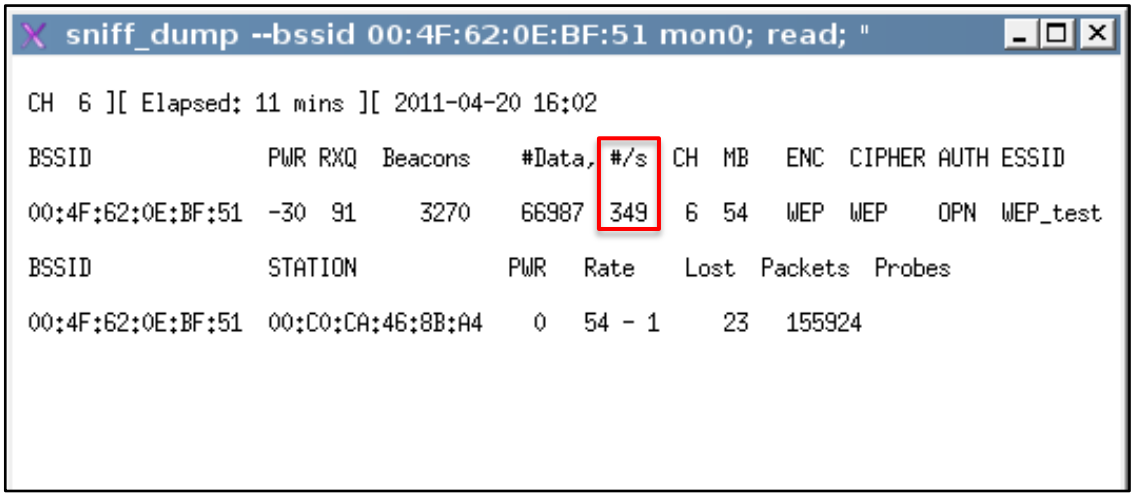
Poté co byl keystream (proud klíčů) zachycen, bylo možné vytvořit falešný packet. K tomuto účelu byl vytvořen ARP packet pomocí možnosti **Create the ARP packet to be Injected on the victim access point**, který byl následně injektován do testované sítě. Ten má za následek, že na stejné dotazy od útočníka (ARP Request) přístupový bod odpoví

zprávami (ARP Reply), zašifrovanými vždy pomocí nových inicializačních vektorů. ARP packet byl zaslán na adresu FF:FF:FF:FF:FF:FF.



Obrázek 15. Injektování podvrženého ARP packetu

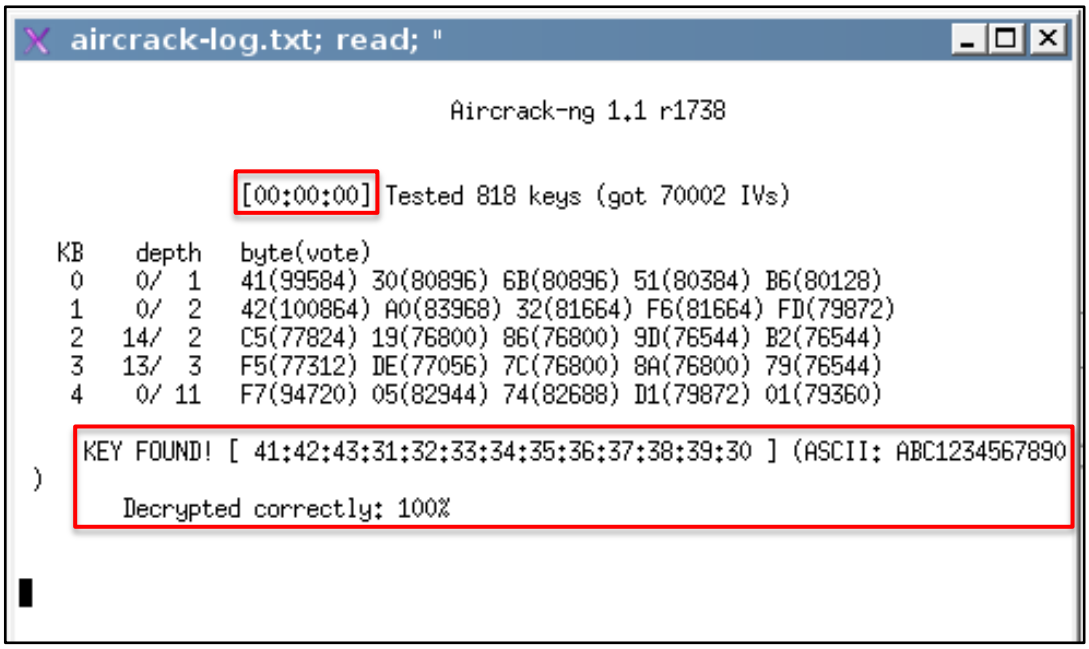
Po provedení injektace packetů byl zaznamenán rapidní nárůst datového trafficu (#/s) na síti, což dokládá obrázek uvedený níže. Injektace byla provedena průměrnou rychlostí 350 packetů za sekundu a nasbírání potřebného množství datových packetů obsahující jedinečné inicializační vektory, tak byla otázkou desítek sekund až jednotek minut.



Obrázek 16. Výrazné zvýšení datového provozu po vykonání packetové injekce

Minimální množství datových packetů potřebných pro prolomení hesla je individuální pro každý přístupový bod a liší se také použitým WEP šifrováním – 64/128bitů. Obecně platí, že čím více datových packetů je, tím větší je pravděpodobnost, že bude heslo prolomeno.

V tomto případě bylo za 11 minut nasbíráno přibližně 70 000 datových packetů, z nichž bylo heslo okamžitě prolomeno. Tedy za 0 sekund (00:00:00). Heslo bylo v tomto případě dlouhé 13 znaků a bylo tvořeno velkými písmeny a číslicemi.

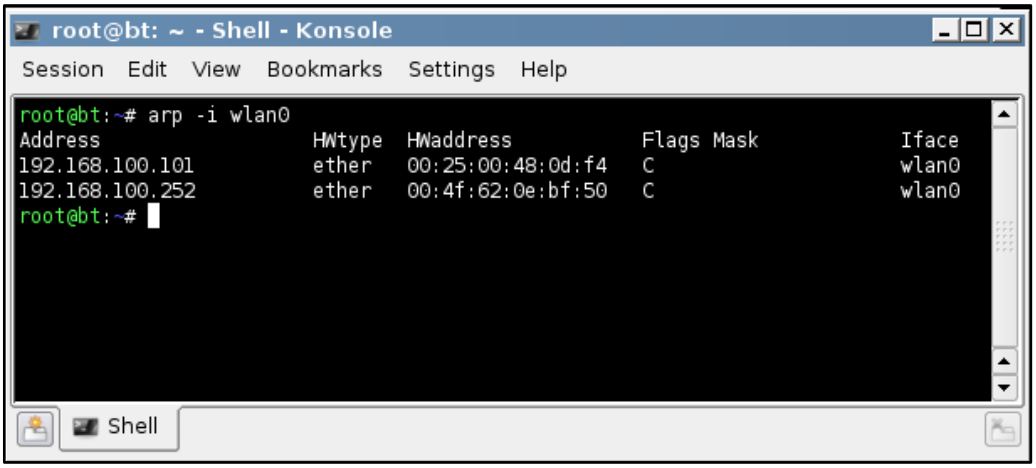


Obrázek 17. Prolomení hesla

Po prolomení hesla do zabezpečené sítě WEP_test, byly získané údaje použity k připojení k této síti a následně otestována Internetová konektivita, zadáním náhodné webové adresy. Tento krok měl také za následek, že mezi klientem a přístupovým bodem došlo k překladu síťových adres a záznamu do ARP tabulky.

5.1.4 Prolomení zabezpečení přístupového bodu

Po prolomení zabezpečení a získání hesla do testované sítě, byl proveden útok na administraci přístupového bodu. Po přihlášení do sítě bylo nutno zjistit IP adresu, na které se AP nachází. K tomuto účelu byl použit ARP protokol, který překládá fyzické hardwarové adresy (MAC) na logické adresy (IP). Pomocí příkazu **arp –i wlan0** v terminálovém řádku linuxové distribuce byl zobrazen obsah ARP tabulky pro bezdrátový adaptér. A protože MAC adresa přístupového bodu byla již známa, jednoznačně tak určila jeho IP adresu.



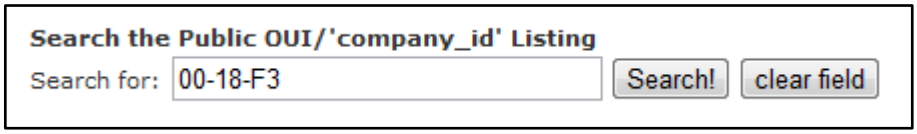
Obrázek 18. Výpis ARP tabulky

Po zadání IP adresy přístupového bodu do adresního řádku webového prohlížeče, byla zobrazena výzva pro zadání přístupových údajů. Tyto údaje jsou vždy uvedeny v servisních manuálech a jsou často shodné v rámci všech přístupových bodů daného výrobce. Za předpokladu, že přihlašovací údaje zůstaly nezměněny, je potřeba určit výrobce přístupového bodu, v jehož servisním manuálu lze přihlašovací údaje nalézt.

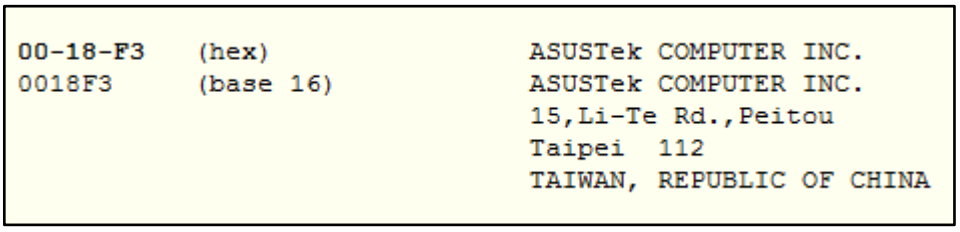
Každý síťový adaptér obsahuje MAC adresu. MAC adresa (Media Access Control), často nazývaná také jako fyzická nebo hardwarová adresa, je 48 bitová adresa NIC adaptéru implementována výrobcem dané komponenty při výrobě. Zapisuje se obvykle jako šest dvojic hexadecimálních znaků oddělených dvojtečkami nebo pomlčkami (např.: 00:0A:CD:11:7E:85). Tato adresa je rozdělena na dvě části po 24 bitech a to na OUI (Organizational Unique Identifier) a NIC (Network Interface Card). OUI kód přiděluje IEEE a jednoznačně tak identifikuje jejího výrobce.

OUI identifikátor tak lze využít na vyhledání výrobce daného přístupového bodu. Tento identifikátor dokáží interpretovat některé snadno dostupné softwarové nástroje, nebo ho lze zpětně zjistit přímo z webu IEEE.

V tomto případě však měl testovaný přístupový bod vyžadování přihlašovacích údajů defaultně vypnuto, proto zde nebyla potřeba vyhledávat jeho výrobce. Avšak v případě, že jsou přihlašovací údaje vyžadovány, prvních 6 hexadecimálních znaků z MAC adresy tvořící OUI, identifikuje výrobce síťového hardwaru.



Obrázek 19. Příklad vyhledání výrobce síťového hardwaru na webu IEEE



Obrázek 20. Nalezení výrobce podle OUI identifikátoru

Autentizační údaje do přístupového bodu je také možné nalézt více způsoby. Samozřejmostí jsou oficiální webové stránky identifikovaného výrobce. Existují však také webové databáze jako např.: http://www.phenoelit-us.org, které dokáží tyto údaje poskytnout včetně informací o modelu a jeho verzi.

Po zjištění přihlašovacích údajů, které jsou vloženy na IP adresu přístupového bodu, může být převzata úplná kontrola nad bezdrátovou sítí.

5.1.5 Zhodnocení útoku

Přibližná doba útoku se pohybovala v rozmezí od 10 do 20 minut a to od počáteční detekce až po převzetí úplné kontroly nad sítí. Čas ovlivňovala zejména rychlost, s jakou mohl být proveden KoreK ChopChop útok a vzdálenost Wi-Fi adaptéru od přístupového bodu, kdy packety u sítě s větším útlumem musely cestovat delší dobu mezi těmito dvěma zařízeními.

5.2 Scénář B

Jako druhé nejčastěji nasazované zabezpečení z provedené statistiky vyplynulo WPA a proto bude vystaveno útoku ve scénáři B. I přesto, že tento bezpečnostní mechanizmus odstranil mnoho nedostatků předchozího zabezpečení, tak i WPA skýtá několik zranitelností, na které bude útok směrován. Další možnost, jak posílit zabezpečení, je skrytí SSID identifikátoru, kdy AP nevysílá tento broadcast a stanice v dosahu přístupového bodu se tak nemohou asociovat. Bude tedy demonstrována metoda, jak tuto informaci odhalit. Posledním rozdílem, kterým se bude tento scénář lišit od předchozího, je zabezpečení administrace přístupového bodu, kdy autentizační údaje byly změněny z jejich výchozích hodnot. Zadání scénáře je tak následující:

- SSID broadcast skryt
- zabezpečení WPA
- autentizační údaje přístupového bodu změněny

5.2.1 Zranitelnosti WPA

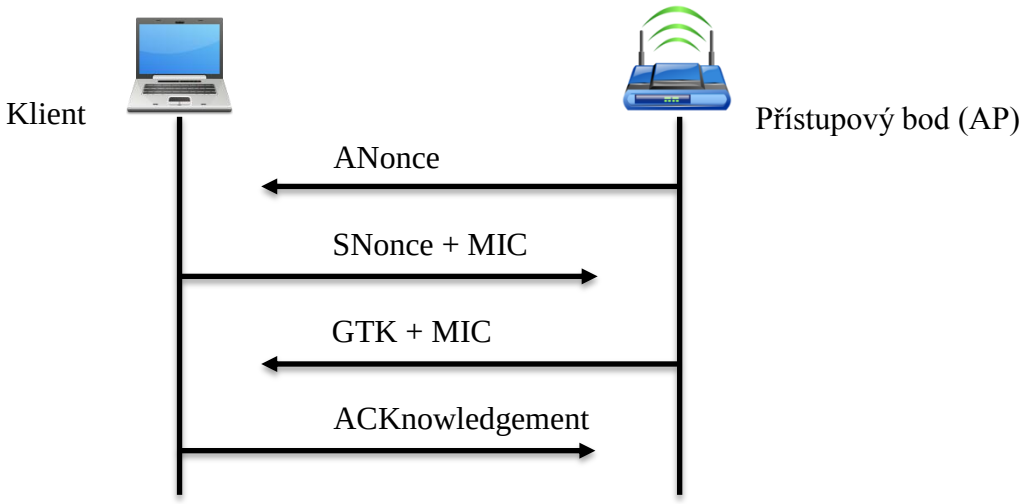
Z důvodu slabého a dále už nedostačujícího zabezpečení, které poskytoval bezpečnostní mechanizmus WEP, byl vyvinut protokol WPA (vycházející z pozdějšího WPA2), který měl zacelit jeho slabiny a poskytnout vyšší úroveň bezpečnosti. Především pak technika dynamické výměnu klíčů již déle neumožnovala využití metod, které byly schopny překonat WEP (KoreK ChopChop, Fragmentation attacks). Avšak i u WPA byly postupem času objeveny zranitelnosti, jež dovolují toto zabezpečení prolomit.

Cílem útoku se v případě WPA stává autentizace přihlašujícího se klienta k bezdrátovému přístupovému bodu a výměna klíčů. Ta je v případě Personal režimu (využívá Pre-Shared Key) realizována metodou zvanou 4 - Way Handshake (doslova: čtyřcestné podání ruky), která umožňuje potvrdit, že klient zná PMK, odvodit PTK, instalovat klíče šifrování a integrity, šifrovat přenos GTK a potvrdit výběr sady šifer.

Výměna klíčů mezi klientem (suplicant/žadatel) a přístupovým bodem (AP) probíhá následovně:

Přístupový bod vyšle nešifrovanou zprávu obsahující pseudonáhodné číslo ANonce žadateli. Ten pomocí svého náhodně vygenerovaného čísla SNonce, PMK, BSSID přístupového bodu, jeho ANonce a MAC adresy žadatele vypočítá PTK klíč (Pairwise Transient Key), který spolu s kontrolou integrity MIC zašle zpět na AP (zpráva je stále nešifrovaná). PTK klíč se skládá z několika přidělených dočasných klíčů a liší se v závislosti na použitém protokolu. Pro TKIP je to 512 bitů, u CCMP se jedná o 384 bitů. Poté co přístupový bod obdrží tuto zprávu, může pomocí hodnoty SNonce vypočítat PTK i MIC a ověřit tak, že žadatel skutečně zná PMK (Pairwise Master Key). PMK je v tomto případě roven PSK, které se generuje z hesla, jež je tvořeno 8 – 63 znaky nebo 256 bitovým řetězcem. Toto heslo spolu s délkou SSID vstupuje do algoritmu PBKDF2, kde jsou vykonány hashovací funkce. Autentizátor – AP zašle žadateli GTK klíč (Group Transient Key), který je již šifrovaný a MIC. Poslední zpráva, která handshake zakončuje je potvrzení žadatele, že klíč byl nainstalován a šifrovaná komunikace může být zahájena.

Handshake a všechny informace, které slouží k výpočtu jeho hodnoty, se přenáší jako nešifrovaný text.[18] Je-li útočník schopen tento handshake zachytit, může ho pak podrobit slovníkovému útoku nebo útoku hrubou silou a získat tak heslo.



Obrázek 21. Schéma principu 4 – Way Handshake

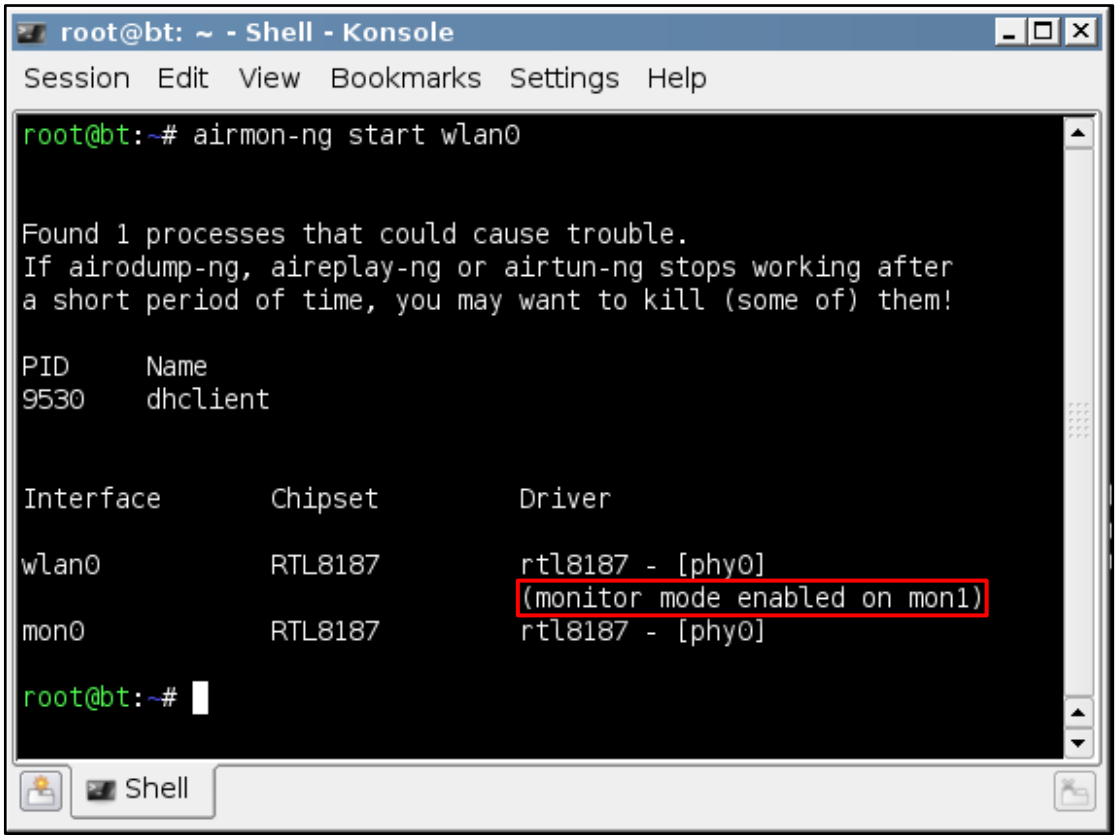
Z výše popsaného tedy vyplývá, že podmínkou, která musí být splněna při útoku na bezdrátovou síť zabezpečenou WPA je, aby se v této síti nacházela alespoň jedna aktivní stanice.

Tento útok může být aplikován na Wi-Fi sítě používající zabezpečení WPA PSK, čili předsdílený klíč, který je znám jak přístupovému bodu, tak přihlašujícímu se klientu. U zabezpečení WPA, používající ověřování pomocí AAA serveru jako např. RADIUS (označovaný jako WPA Enterprise), tuto techniku použít nelze.

Zachycení hesla může být provedeno dvěma způsoby, a to buď pasivním odposlechem, kdy je daná síť neustále monitorována sniffovacím nástrojem, který čeká, až se k ní někdo přihlásí, nebo může být vynucena pomocí vyslaného deautentizačního rámce, který již jednou autentizovaného klienta odpojí a přinutí jej tento proces opakovat. V tomto případě byla využita druhá varianta.

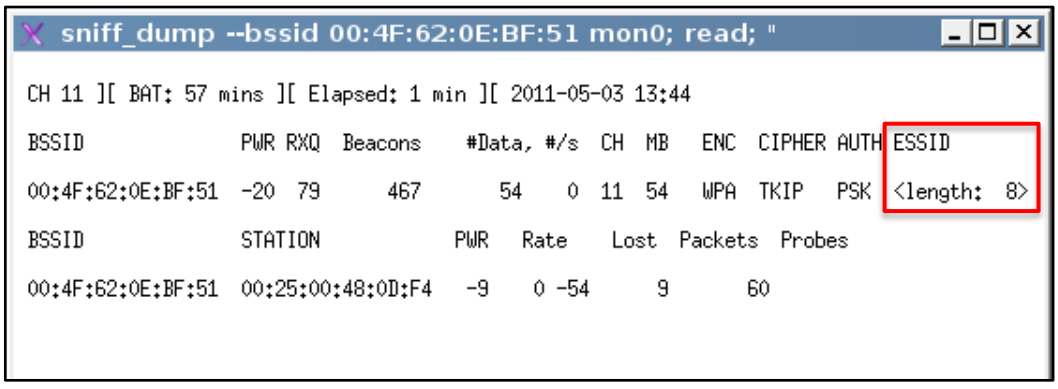
5.2.2 Penetrační test scénáře B

Aby bylo možno provést sniffing sítě, bylo opět nutno přepnout bezdrátový adaptér do monitorovacího režimu. V tomto případě k tomu byl použit příkaz **airmon-ng start wlan0** v terminálovém řádku linuxové distribuce.



Obrázek 22. Přepnutí Wi-Fi adaptéru do RFMON režimu

Po provedení detekce sítí v dosahu bezdrátového adaptéru, která byla nastavena na 10 sekund, byla objevena testovaná Wi-Fi síť a její parametry. Z těchto informací bylo zjištěno, že MAC adresa přístupového bodu je 00:4F:62:0E:BF:51(BSSID). Útlum signálu byl v tomto případě -20dB(PWR), což opět značilo, že se AP nachází v blízkosti adaptéru. Wi-Fi síť vysílala na kanálu 11(CH), byla zabezpečena mechanizmem WPA(ENC) a šifrována protokolem TKIP(CIPHER). Autentizace PSK(AUTH) prozradila, že se jedná o Personal mód a pole ESSID <length: 8>, že vysílání SSID broadcastu je v tomto případě potlačeno. Číslo 8 poté napovědělo, že SSID identifikátor tvoří řetězec o osmi znacích.



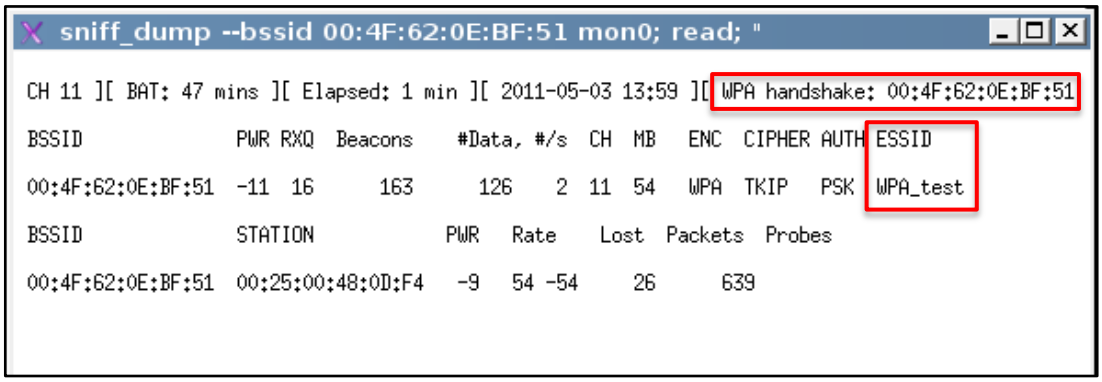
Obrázek 23. Detekce testované sítě scénáře B

5.2.3 Odhalení SSID a zachycení 4 – Way Handshake

V případě, že je přístupový bod nastaven, aby nevysílal Beacon packety nesoucí mimo jiné identifikátor sítě, tedy SSID broadcast byl vypnut, stanice v jeho dosahu jej nebudou znát a nebudou se tak moci asociovat. Jinými slovy, na výzvu Probe Request klient nedostane od AP žádnou odpověď.

Řešení jak SSID identifikátor získat je však velice snadné. Budou-li s přístupovým bodem již asociovány nějaké stanice, je jasné, že tyto stanice SSID musejí znát. Pak tedy stačí jen vyčkat, než se stanice znovu připojí, nebo do sítě vyslat deautentizační rámce, které klienta odpojí a ten se bude muset znovu s přístupovým bodem asociovat. Při tomto procesu je SSID identifikátor vysílán nešifrovaný a je ho tak možno sniffovacím programem zachytit.

Aby bylo možno nasimulovat jak zachycení handshaku, tak i proces odhalení SSID, byla k přístupovému bodu připojena jedna stanice – STATION 00:25:00:48:0D:F4. Emulováním její MAC adresy byly do sítě vyslány deautentizační rámce, které spustily opětovnou asociaci. Odhalené SSID a zachycený handshake je zobrazen na obrázku níže.



Obrázek 24. Zachycení handshaku a odhalení SSID

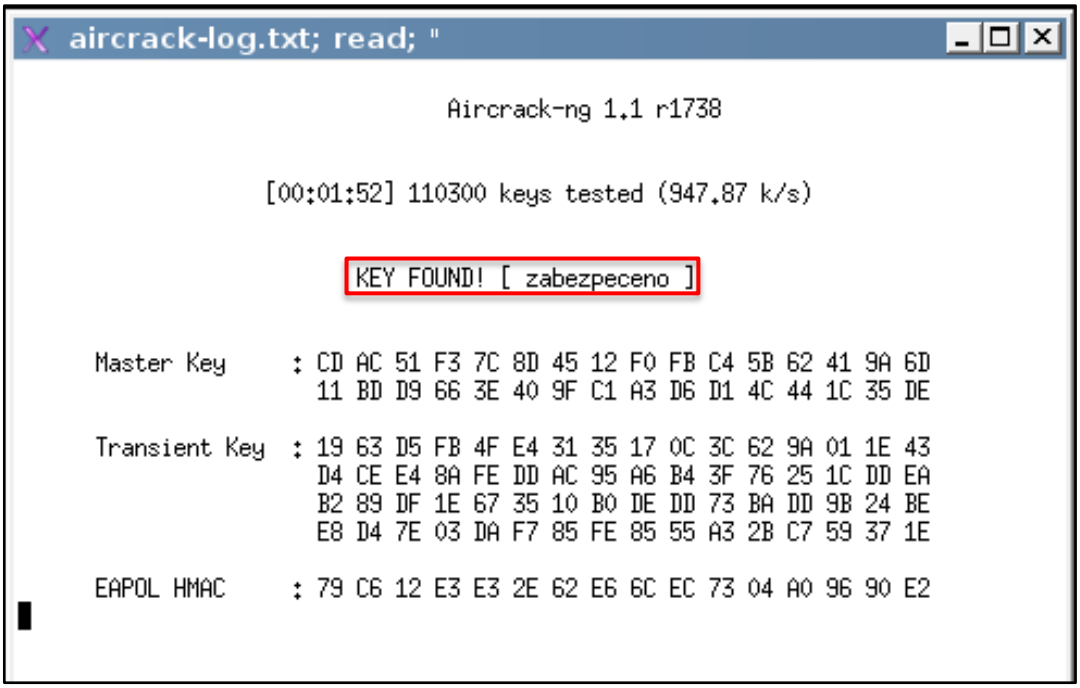
Po zachycení handshaku mohl být proveden jeden z útoků. V případě aplikování útoku hrubou silou (Brute force attack) by se jednalo o sestavení hesla generovaného ze všech možných kombinací znaků (malá/velká písmena, číslice, další speciální znaky sady Unicode jako @, ?, #), přičemž by se složitost hesla zvyšovala exponenciálně s každým přidaným znakem. Takto provedený útok by v závislosti na komplexitě hesla mohl trvat i několik desítek či stovek let, i při použití moderních výkonných více jádrových procesorů.

Protože však většina uživatelů používá hesla, která jsou jednoduchá na zapamatování, opakují se a často zastupují jména, názvy nebo posloupnosti, je možné z nich utvořit seznam – slovník, který bude takto nejčastěji používaná hesla obsahovat (Wordlist). Tyto

slovníky lze nalézt na Internetu v mnoha podobách. Od jednoduchých slovníků, obsahujících základní a nejběžnější výrazy složené pouze z malých písmen, až po slovníky specializované na určité sady hesel, sestavené z různě kombinovaných znaků a délek v jednotlivých světových jazycích. Slovníky je také možno vygenerovat podle předem stanovených kritérií.

Slovníkový útok je procesorově náročná operace, kdy výpočetní výkon CPU, hraje důležitou roli při porovnávání slovníkových kombinací. Tento proces může být urychlen využitím více jádrových procesorů, kdy lze vykonávanou úlohu rozdělit do více vláken a zpracovávat ji tak paralelně nebo využít výpočetní výkon grafické karty. V obou případech je však nutná podpora ze strany softwaru.

K provedení slovníkového útoku byl použit Wordlist (slovník), který obsahoval celkem 162 133 slov různé délky bez diakritiky, především pak slova delší než 8 znaků. Heslo, jímž byla bezdrátová síť zabezpečena, bylo úmyslně vybráno z druhé poloviny slovníku, aby mohla být zaznamenána průměrná rychlost, se kterou bylo možno jednotlivá hesla zkoušet.



Obrázek 25. Prolomení hesla slovníkovým útokem

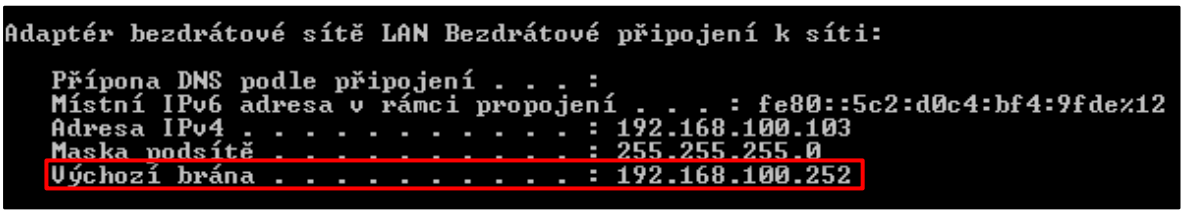
Heslo bylo nalezeno za 1 minutu a 52 vteřin, kdy bylo otestováno 110 300 možností průměrnou rychlostí 1000 slov za sekundu. Pro srovnání, kdyby bylo stejné heslo (11

pouze malých písmen) podrobeno útoku hrubou silou, stejnou rychlostí by to jednomu PC trvalo 118 003 let.

5.2.4 Prolomení zabezpečení přístupového bodu

K získání autentizačních údajů byl v tomto případě použit crackovací software Brutus. Ten dokáže jak formou brute force útoků, tak i slovníkovým útokem (Dictionary attack) prolamovat hesla síťových služeb.

Protože je však tato aplikace pouze pro operační systém Microsoft Windows, byl další průběh proveden na této platformě. IP adresa přístupového bodu byla tentokrát zjištěna pomocí příkazu **ipconfig**, který vypíše informace o konfiguraci síťového hardwaru. Pod označením výchozí brána byla identifkována IP adresa přístupového bodu. Na rozdíl od minulého scénáře, byla pro administraci AP vyžadována autentizace v podobě přihlašovacího jména a hesla.



Obrázek 26. Výpis z příkazu ipconfig

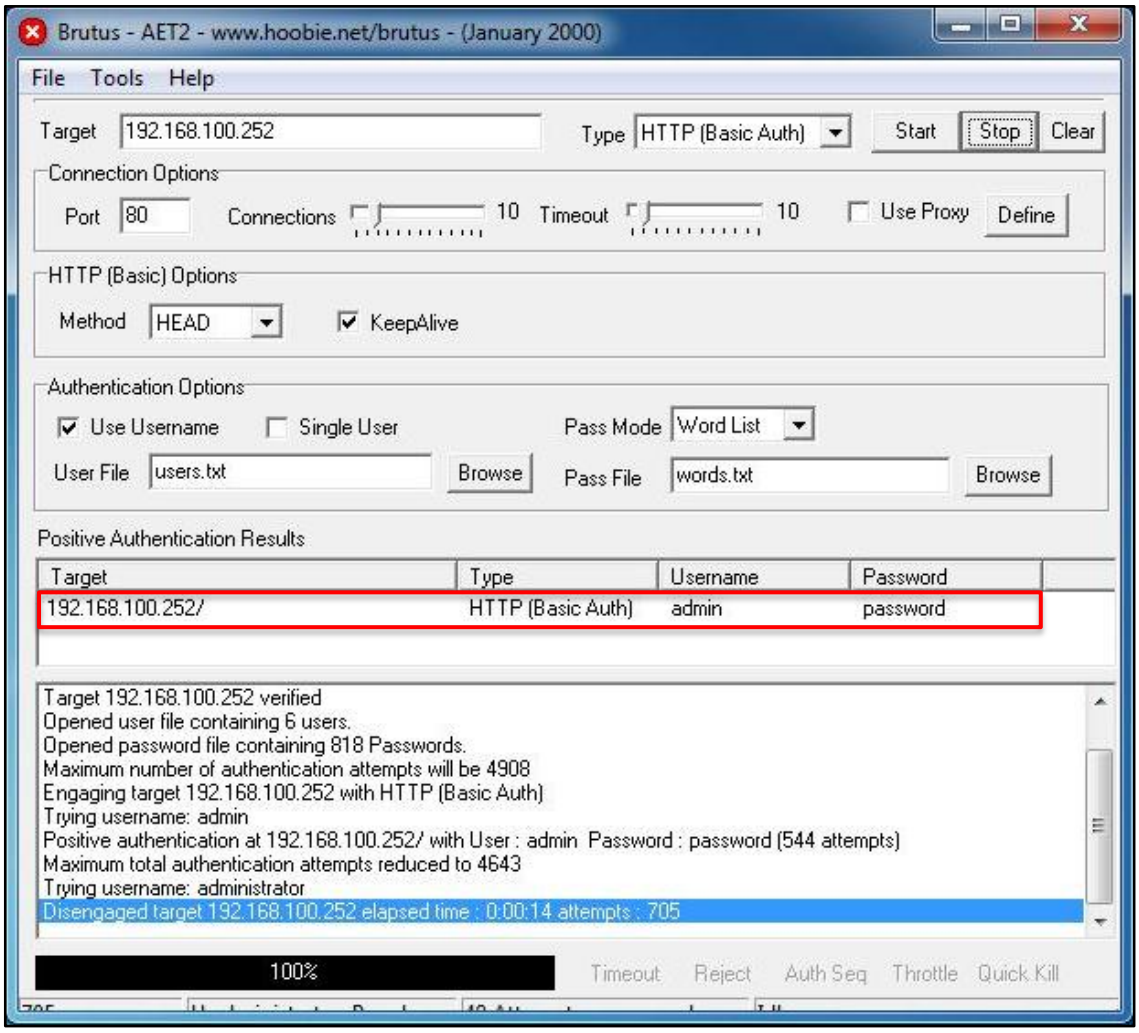
Cílová adresa AP byla tedy použita 192.168.100.252 a jako typ síťového protokolu byl zvolen HTTP s portem 80, neboť právě na něm běží webový server přístupového bodu. Aplikace Brutus umožňuje nastavit i počet spojení (Connections) a prodlevu mezi nimi (Timeout), aby přístupovému bodu bylo znemožněno pokusy klasifikovat jako DoS útok a zabránit tak dalšímu průběhu.

Denial of Service (Odmítnutí Služby) neboli DoS útok je technika sloužící k zahlcení serveru, služby, sítě nebo konkrétního počítače formou nekonečných požadavků. Útok může pocházet z jediného, na dálku řízeného (i lokálního) počítače, ale i z desítek, stovek nebo tisíců počítačů zapojených v síti. V tomto případě se jedná o DDoS útok (Distributed Denial of Service). Takovýmto útokem může být docíleno, že daná služba, server nebo síť nebude dostupná, nebude odpovídat, zhroutí se a bude nucena k restartu. [2]

Jako typ útoku na autentizaci AP byl opět zvolen slovníkový útok, sestávající se ze dvou wordlistů. Jeden pro uživatelské jméno (Username), druhý pak pro heslo (Pass). Aby mohla být demonstrována situace prolomení hesla do AP, byly použity základní slovníky

nejčastěji používaných přihlašovacích údajů. Slovník pro uživatelské jméno tak obsahoval pouhých šest výrazů a slovník pro heslo 818.

Po spuštění aplikace bylo heslo prolomeno za 14 sekund, kdy z celkového počtu 4908 kombinací, bylo vyzkoušeno 544.



Obrázek 27. Prolomení autentizačních údajů aplikací Brutus

Po získání přihlašovacích údajů přístupového bodu, byla kompletně převzata kontrola nad bezdrátovou sítí.

5.2.5 Zhodnocení útoku

Penetrační test scénáře B využil slabiny, kterou nabízí autentizační proces stanice přihlašující se k přístupovému bodu. Zachycení potřebného handshaku, stejně jako zjištění SSID identifikátoru, bylo v tomto případě vynuceno pomocí deautentizace. Doba trvání celkového útoku byla při takto simulovaných nastaveních pouze 20 minut, nicméně hesla pro zabezpečení jak Wi-Fi sítě, tak i přístupového bodu, byla zvolena s ohledem, aby byl

slovníkový útok úspěšný. V praxi se tedy doba může mnohonásobně lišit v závislosti na použité složitosti hesla a vhodně zvoleném slovníku.

5.3 Scénář C

Poslední testovaný scénář, který měl být podroben penetračním testům, byl zvolen tak, aby odpovídal maximálnímu možnému zabezpečení, které nabízí většina současných přístupových bodů bez použití jakýchkoli dodatečných hardwarových bezpečnostních prvků. Bezdrátová síť byla tedy zabezpečena pomocí WPA2 (ačkoli ze statistiky vyplynulo jako nejméně nasazované). Stejně jako v předchozím případě bylo vysílání SSID broadcastu znemožněno a celá bezpečnost byla ještě podpořena filtrováním MAC adres povolených klientů. Přístup k administraci AP byl rovněž chráněn přihlašovacími údaji. Zadání scénáře je tedy následující:

- SSID broadcast skryt
- zabezpečení WPA2
- filtrování MAC adres
- autentizace k přístupovému bodu

Tento scénář byl testován na přístupovém bodu Cisco Linksys WRT320N

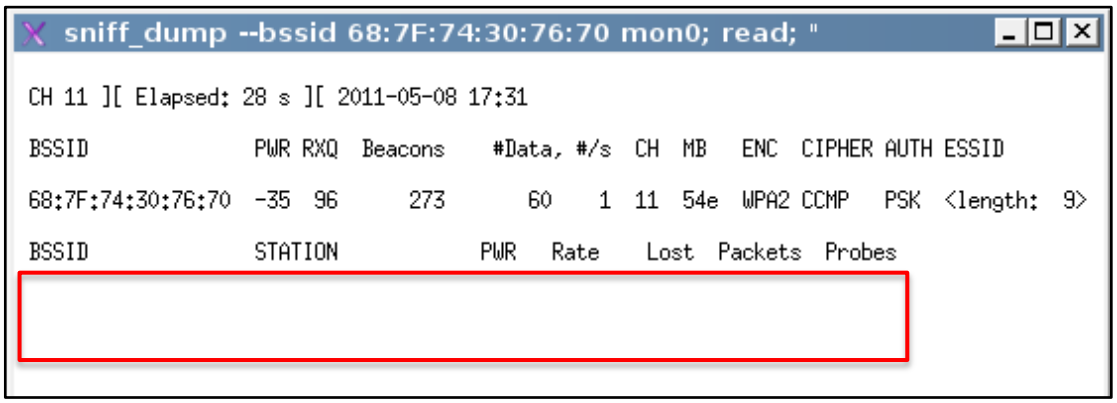
5.3.1 Zranitelnosti WPA2

Jak již bylo zmíněno v teoretické části, standard IEEE 802.11i, Wi-Fi aliancí certifikovaný jako WPA2, byl původně navrhovaný bezpečnostní mechanizmus, ze kterého dříve vzešlo WPA. Tudíž i jeho zranitelnosti jsou oproti WEP značně omezeny a jedinou možností, jak by tento mechanizmus mohl být napaden, je pokusit se získat PSK klíč z autentizačního procesu stejně jako je tomu u WPA. Je tedy opět potřeba zachytit 4 – Way Handshake již jednou asociované stanice. Ačkoli WPA2 podporuje pro zpětnou kompatibilitu starší TKIP, přístupový bod byl v tomto případě nastaven na modernější protokol CCMP.

5.3.2 Penetrační test scénáře C

Po přepnutí bezdrátového adaptéru do monitor módu v aplikaci Gerix Wifi Cracker, byla provedena detekce WLAN sítí v jeho dosahu. Z ní bylo zjištěno, že testovaná síť se nachází v blízkosti bezdrátového adaptéru (útlum -35dB PWR), MAC adresa přístupového bodu je 68:7F:74:30:76:70 (BSSID), vysílá na kanálu 11 (CH) a její maximální přenosová rychlost je 54Mb. Dále, že síť je zabezpečena pomocí WPA2 (ENC), konkrétně pak

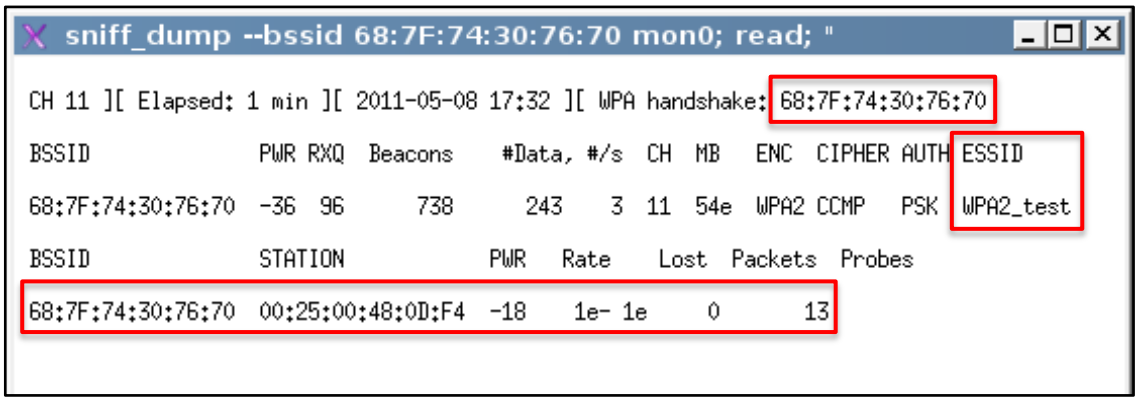
protokolem CCMP (CIPHER) a autentizace je prováděna skrze PSK, čili před sdílený klíč. Vysílání SSID broadcastu je vypnuto, ale jeho délka je 9 znaků (length: 9).Na Wi-Fi síti se v době sniffování nenalézal žádný klient



Obrázek 28. Detekce testované sítě scénáře C – žádný aktivní klient

5.3.3 Odhalení SSID a zachycení 4 – Way Handshake

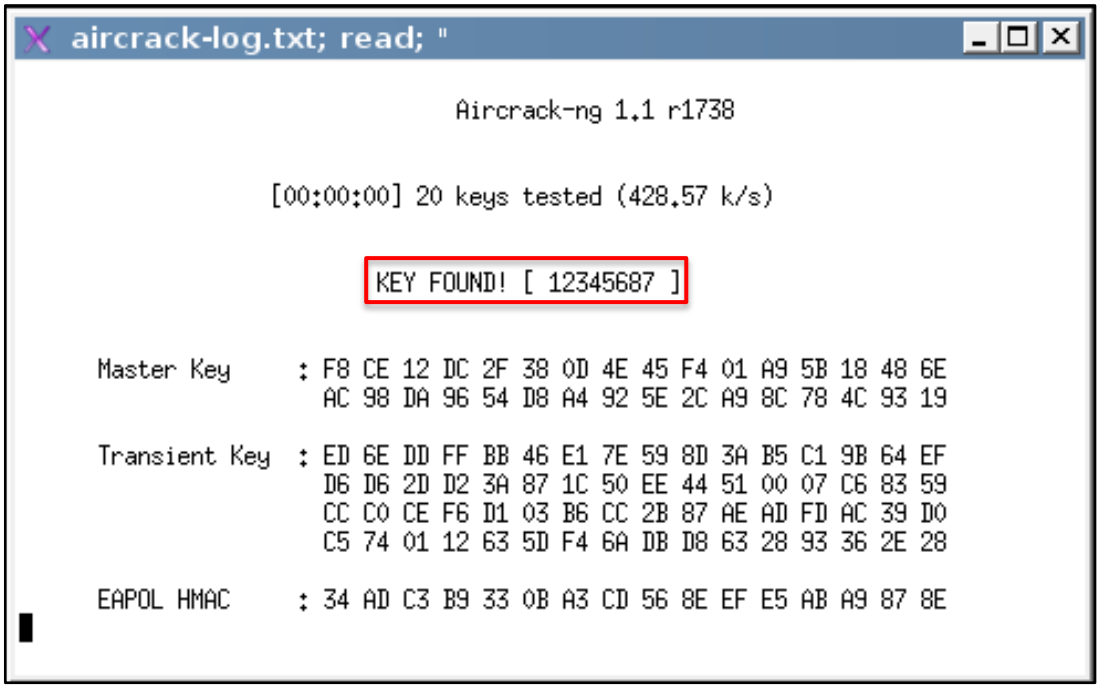
Zachycení handshaku nebylo tentokrát vynuceno pomocí deautentizace klienta, nýbrž statických sniffováním sítě, kdy bylo vyčkáváno, než se stanice, která zná PSK klíč, znovu připojí. Tato stanice byla simulována druhým PC, jehož MAC adresa byla také zapsána v seznamu povolených MAC adres nakonfigurovaných na přístupovém bodu.



Obrázek 29. Zachycený handshake a odhalené SSID po autentizaci stanice

5.3.4 Prolomení zabezpečení

Zachycený handshake byl poté opět podroben slovníkovému útoku, kdy heslo bylo kvůli laboratorním podmínkám vybráno s ohledem na použitý wordlist. Zabezpečení WPA2 bylo po spuštění crackování okamžitě prolomeno (00:00:00), kdy bylo průměrnou rychlostí 430 klíčů za sekundu vyzkoušeno pouhých 20 možností.

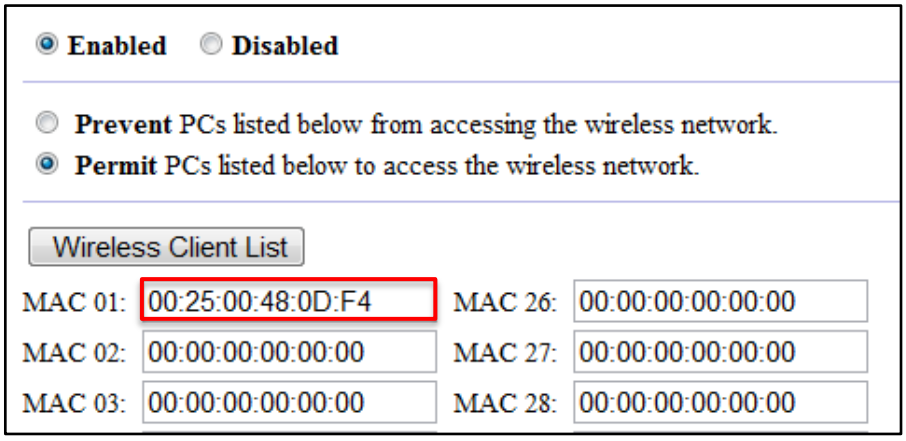


Obrázek 30. Prolomení WPA2 slovníkovým útokem

Ani WPA2 používající protokol CCMP se symetrickou blokovou šifrou AES tak neprokázal odolnost vůči tomuto útoku.

5.3.5 Filtrování MAC adres

Aby byla v tomto scénáři ještě zvýšena úroveň bezpečnosti, bylo na přístupovém bodu aktivováno filtrování MAC adres, kde pouze stanice s MAC adresu uvedenou v tomto seznamu, měly povolen přístup do sítě.



Obrázek 31. Filtrování MAC adres na AP se zadanou adresou klienta

Níže je uveden výpis terminálových příkazů, pomocí nichž byla změněna původní MAC adresa bezdrátového adaptéru, na MAC adresu stanice, která je povolena na AP.

```
1. root@bt:~# airmon-ng stop mon0

   Interface       Chipset         Driver

   wlan0           RTL8187         rtl8187 - [phy1]
   mon0            RTL8187         rtl8187 - [phy1] (removed)

2. root@bt:~# ifconfig wlan0
   wlan0     Link encap:Ethernet  HWaddr 00:c0:ca:46:8b:a4
             UP BROADCAST MULTICAST  MTU:1500  Metric:1
             RX packets:0 errors:0 dropped:0 overruns:0 frame:0
             TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

3. root@bt:~# ifconfig wlan0 down
4. root@bt:~# macchanger --mac 00:25:00:48:0D:F4 wlan0
   Current MAC: 00:c0:ca:46:8b:a4 (Alfa, Inc.)
   Faked MAC:   00:25:00:48:0d:f4 (unknown)
5. root@bt:~# ifconfig wlan0 up
6. root@bt:~# ifconfig wlan0
   wlan0     Link encap:Ethernet  HWaddr 00:25:00:48:0d:f4
             UP BROADCAST MULTICAST  MTU:1500  Metric:1
             RX packets:0 errors:0 dropped:0 overruns:0 frame:0
             TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

   root@bt:~#
```

Obrázek 32. Změna MAC adresy v terminálovém okně

1. Vypnutí monitor módu na bezdrátovém adaptéru (mon0 – removed)
2. Zobrazení původní hardwarové adresy – 00:c0:ca:46:8b:a4
3. Vypnutí bezdrátového interfacu
4. Konfigurace jiné hardwarové adresy bezdrátového interfacu
5. Zapnutí bezdrátového interfacu
6. Zobrazení nové hardwarové adresy – 00:25:00:48:0d:f4

Poté co byla emulována MAC adresa legitimní stanice, prolomeno heslo a odhalen SSID identifikátor, bylo možno se do Wi-Fi sítě připojit, ačkoliv již dříve byla jedna stanice se stejnou MAC adresou s přístupovým bodem asociována.

Tento postup tedy odhalil, že filtrování hardwarových adres může tvořit určitý stupeň bezpečnosti, avšak pro sofistikovaného útočníka není problém tuto překážku překonat a přístup do sítě získat.

Postup jak zjistit adresu přístupového bodu, prolomit jeho zabezpečení a získat kompletní kontrolu nad bezdrátovou sítí, byl shodný jako u předchozího scénáře.

5.3.6 Zhodnocení útoku

Útok na síť zabezpečenou pomocí WPA2 se nelišil mnoho od útoku na předchozí WPA. Tato skutečnost plyne z toho, že u obou případů je využito stejné zranitelnosti, tedy autentizačního procesu. Odhalení řetězce SSID i zachycení handshaku bylo provedeno pouhým pasivním odposloucháváním sítě a filtrování MAC adres celý útok prodloužilo pouze o emulování požadované hardwarové adresy. Celková doba útoku tak trvala opět méně než 20 minut.

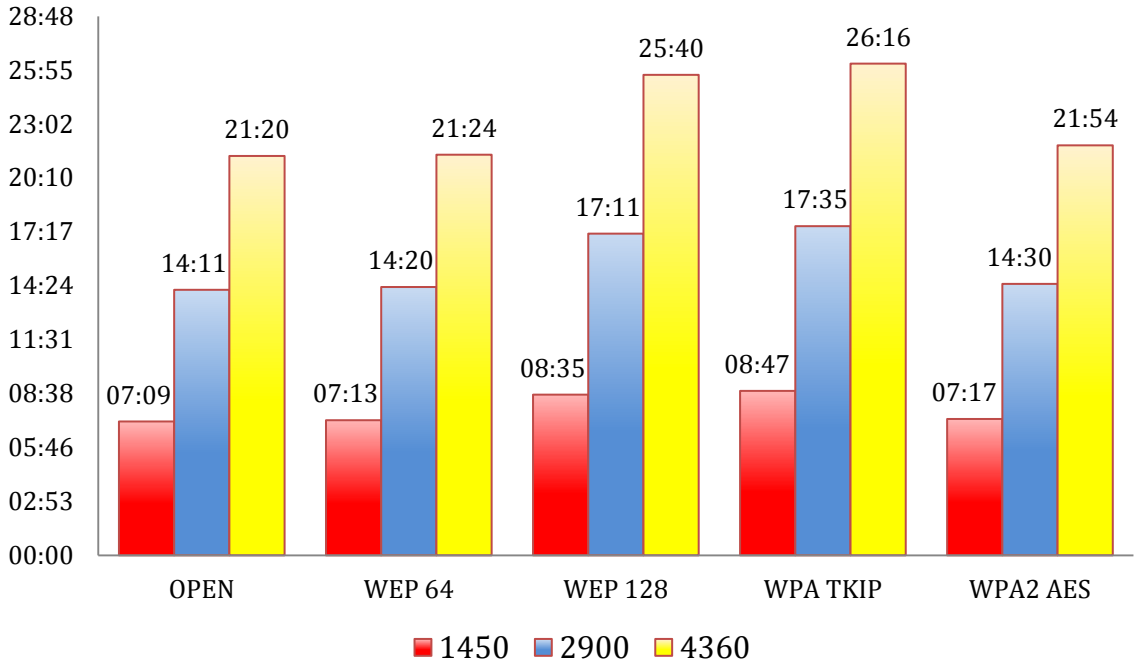
5.4 Vliv šifrování komunikace na propustnost sítě

Každé bezpečnostní řešení sebou přináší režii spojenou s šifrováním komunikace. Působení tohoto procesu bylo otestováno, aby bylo možno vyhodnotit, který bezpečnostní mechanizmus nejvíce ovlivňuje propustnost sítě.

Měření probíhala na bezdrátové síti standardu IEEE 802.11g, kde roli přístupového bodu zastával Cisco Linksys WRT320N a přenos dat probíhal mezi dvěma stanicemi (MS Windows 7 x Mac OS 10.6 Snow Leopard). Pro přenos dat posloužily 3 soubory o velikosti 1450, 2900 a 4360MB. Přístupový bod byl odpojen od Internetové sítě, aby šířka pásma nebyla ovlivněna dalšími přenosy jako např. softwarové aktualizace stahované na pozadí. U každého přenášeného souboru byla zaznamenána přenosová rychlost a čas, za kterou byl celý soubor přenesen. Naměřené údaje jsou uvedeny v tabulce níže.

Velikost [MB]	Open	WEP 64	WEP 128	WPA TKIP	WPA2 AES
1 450	7:09	7:13	8:35	8:47	7:17
2 900	14:11	14:20	17:11	17:35	14:30
4 360	21:20	21:24	25:40	26:16	21:54
Rychlost [MB/s]	3,50	3,42	2,90	2,83	3,40

Tabulka 4. Naměřené hodnoty šifrované komunikace



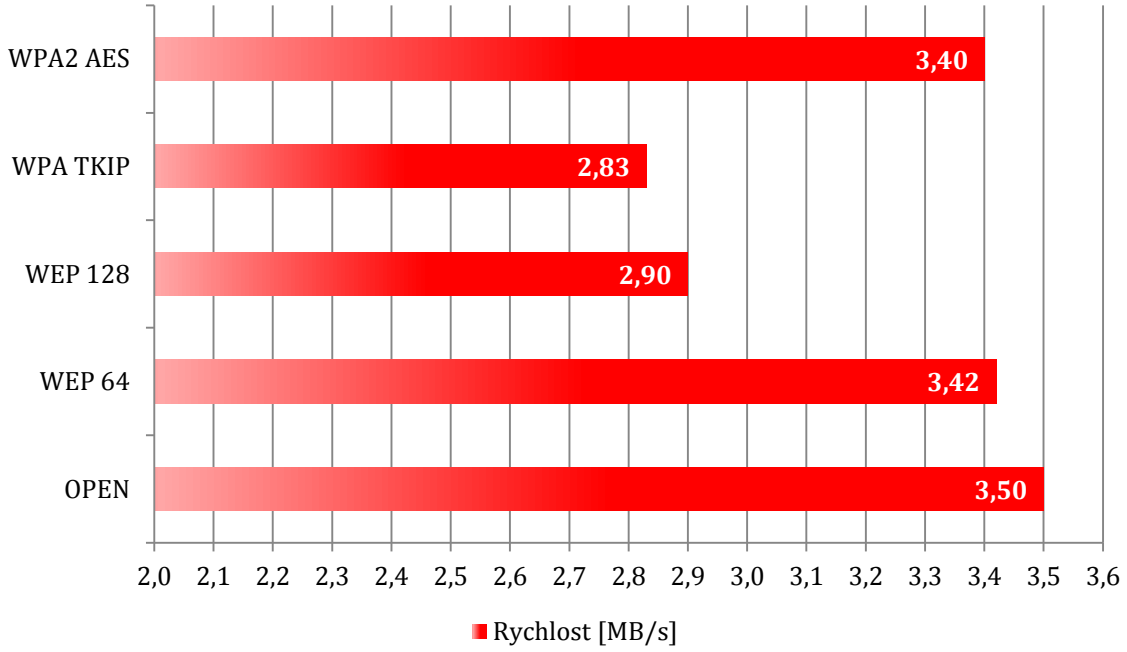
Graf 3. Časy přenosů jednotlivých souborů

Rychlosti u každého přenosu se lišily řádově v setinách MB/s a ve výsledku byly pro celé zabezpečení zprůměrovány. Měření potvrdilo předpoklad, že nejvyšší rychlosti dosáhla síť Open, čili bez jakéhokoli zabezpečení. Ta tedy stanovila základ pro porovnání s ostatními zabezpečenými sítěmi. Síť šifrována protokolem WEP s délkou klíče 64 bitů již uvedla pozorovatelné zpoždění v přenosové rychlosti, které bylo ještě více znatelné u 128 bitové verze, kde se jednalo o celých 17%. Délka klíče tedy měla nezanedbatelný vliv na rychlost přenosu. U zabezpečení WPA šifrovaného pomocí protokolu TKIP byla tato ztráta ještě větší a to konkrétně 19% oproti nešifrované komunikaci. Naopak zabezpečení WPA2, využívající šifru AES, bylo v celkové přenosové rychlosti zastoupeno pouhými třemi procenty.

Open	WEP 64	WEP 128	WPA TKIP	WPA2 AES
100%	98%	83%	81%	97%

Tabulka 5. Procentuální vyjádření propustnosti jednotlivých šifrovaných sítí

Naměřené hodnoty však nemusí být směrodatné a mohou se lišit v závislosti na výrobci AP a jeho implementaci daného zabezpečení a standardu. Měření však potvrdila, že šifrování bezdrátové komunikace není zcela transparentní a uvádí do celkové propustnosti sítě latenci, která se u přenosu objemnějších souborů může projevit i v řádově jednotkách minut.



Graf 4. Přenosová rychlost jednotlivých šifrovaných spojení

5.5 Vyhodnocení penetračních testů

Možností jak dnes zabezpečit bezdrátovou WLAN síť je několik. V penetračních testech demonstrovaných scénářů byla většina z těchto praktik teoreticky popsána, realizována a následně podrobena útokům, které využívají dosud známých slabin a zranitelností.

Vypnutí SSID broadcastu nebylo již při svém navržení koncipováno jako jedna z metod zabezpečení bezdrátové sítě a zobrazení tohoto identifikátoru, vysílaného v čitelné podobě (plaintext), bylo možno odhalit jak prostým pasivním odposlechem, tak vynucenou deautentizací asociovaných klientů. Skrytí tohoto vysílání může být užitečné pouze tehdy, nechceme-li avizovat danou síť ve svém okolí. Proti útočníkům však neposkytuje žádný stupeň ochrany.

Nastavení filtrování MAC adres na přístupovém bodu, ať už formou blacklistu nebo whitelistu, také nezvyšuje bezpečnost WLAN sítě. Změna MAC adresy útočníkova NIC adaptéru je možná snadno dostupnými nástroji nebo terminálovými příkazy pro všechny platformy dnes nejpoužívanějších operačních systémů. Útočník tak může získat přístup do chráněné sítě se znalostí pouze jediné MAC adresy asociované stanice. (V průběhu testu bylo zjištěno, že zapnutý DHCP server na AP přidělil již jednou použitou IP adresu i druhému bezdrátovému adaptéru s emulovanou MAC adresou). Tento krok tedy také

neposkytuje formu ochrany, ale pouze doplnění zabezpečení jako jsou WEP, WPA nebo WPA2.

Penetrační testy potvrdily, že ani bezpečnostní mechanizmus WEP neposkytuje potřebou úroveň zabezpečení. Od doby jeho vzniku již bylo nalezeno několik zranitelností, kde mezi hlavní slabiny patří použití stejného klíče u všech zařízení v síti. Dále pak distribuce a změna klíčů, která se musí provádět manuálně (automatická změna není podporována), umožnění komunikace dvou stanic se stejnou MAC adresou a v neposlední řadě statický a krátký klíč s opakujícím se IV a slabým šifrovacím algoritmem RC4. Prakticky tyto nedostatky potvrdil penetrační test scénáře A, kde jak 64, tak i 128 bitový šifrovací klíč byl prolomen pouze s rozdílem nasbíraných inicializačních vektorů.

Jedním z řešení jak toto zabezpečení vylepšit, je použití WEP s dynamicky generovanými klíči, kde se po předem definované době klíče automaticky změní. Nicméně v základu tato technologie zůstává stejná (stále RC4 šifra) a při velkém množství přenesených dat, lze dočasně vygenerovaný klíč prolomit. Navíc je tato technologie proprietární a záleží tak na každém výrobci, zdali a jak tuto funkci implementuje.

Prolomit zabezpečení WEP se však nemusí vždy podařit. V průběhu praktických testů bylo na přístupovém bodu Linksys WRT320N zjištěno, že zahazoval packety kratší než 40 bytů a útok tedy nemohl být realizován. Implementace tohoto typu zabezpečení se tak může lišit v závislosti na výrobci přístupového bodu. WEP se tedy hodí především pro starší zařízení, která nedisponují novějšími technologiemi v podobě WPA nebo WPA2. Tvoří tedy alespoň základní ochranu před uživateli, kteří využívají nezabezpečené WLANy k připojení do sítě Internet. Pro útočníka však nejsou velkou překážkou.

U zabezpečení WPA a WPA2 byla většina zranitelností WEPu eliminována, a tak se útok zaměřuje na výměnu klíčů při autentizačním procesu. Je ho však možné provést pouze u verze WPA/WPA2 Personal s před sdíleným PSK klíčem a dostupnými klienty na síti. Tento útok byl prakticky znázorněn ve scénáři B a C, kdy byl zachycen handshake jak pasivním sniffováním dané sítě, tak aktivní deautentizací přihlášené stanice. Takto získaný handshake může být následně podroben slovníkovému útoku nebo útoku hrubou silou. Skládá-li se však heslo z 20+ znaků, které je navíc složeno kombinacemi malých a velkých písmen, číslic a dalších speciálních znaků např. z ASCII tabulky, lze toto heslo považovat za dostatečné silné, neboť slovníkový útok i útok hrubou silou by i na vysoce výkonném PC/serveru trval nepřiměřeně dlouho. Bezpečnost tohoto mechanizmu může být podpořena

zkrácením tzv. Rekying intervalu na co nejkratší dobu, kdy bude automaticky změněn GTK klíč.

Penetrační testy také potvrdily, že ačkoli je WPA2 v kombinaci s protokolem CCMP robustnější zabezpečení než WPA, lze jej prolomit slovníkovým útokem

Další možností jak zvýšit bezpečnost WLAN sítě je zapnout izolaci klientů. Tato volba, kterou nabízejí téměř všechny přístupové body (defaultně vypnuta), sice nezabrání prolomení hesla nebo pasivnímu odposlechu, ale znemožní přihlášení cizí stanice do sítě.

Jiné řešení jak zabezpečit bezdrátovou síť se nabízí skrze standard IEEE 802.1X a autentizaci vůči AAA serveru jako např. RADIUS. Toto řešení je však finančně nákladné a dostupné především v korporátní sféře. Další alternativa, jak posílit zabezpečení WLAN sítě, je doplnit stávající síťovou infrastrukturu o hardwarové bezpečnostní prvky jako jsou IDS nebo IPS systémy. Tato řešení jsou však už velice finančně nákladná.

Omezení vysílacího výkonu přístupového bodu a správné zvolení a nastavení antén je také možnost, kterou lze omezit riziko útoku na Wi-Fi síť. Jsou-li signálem pokryty pouze požadované prostory, které jsou navíc vhodně doplněny dalšími bezpečnostními nástroji (CCTV, fyzická ostraha), je tak útočníkovi znemožněna samotná fyzická podstata útoku.

Softwarové nástroje sloužící pro monitorování sítě sice žádnou bezpečnost neposkytují, mohou však sloužit ke zjištění nežádoucích stanic (narušitelů) a zvýšeného provozu na síti.

5.6 Doporučené zabezpečení

Z penetračních testů vyplynulo, že nejvhodnější volbou jak zabezpečit bezdrátovou WLAN síť je WPA2 s protokolem CCMP. Toto zabezpečení, spolu se silným klíčem, poskytuje v současnosti dostatečnou ochranu, není finančně nákladné, podporuje jej již drtivá většina zařízení a také režie spojená s přenosem, uvedená tímto mechanizmem, je zanedbatelná.

U starších zařízení nekompatibilních s WPA2 je doporučeno použít zabezpečení WPA opět s dostatečně silným šifrovacím klíčem. WEP již lze použít jen v krajních případech, kdy ani jedno z dříve jmenovaných řešení není k dispozici.

U domácích Wi-Fi sítí je pro SSID doporučeno použít nějaký abstraktní název (např. WLAN, Internet, Wi-Fi). U korporátních pak, toto vysílání zcela skrýt, popřípadě přidat filtrování MAC adres a využít autentizaci pomocí IEEE 802.1X. Využití těchto možností však záleží na konkrétním nasazení sítě a je tedy individuální.

ZÁVĚR

Cílem této diplomové práce bylo popsat význam penetračních testů a jejich nasazení u Wi-Fi sítí. V teoretické části byly uvedeny výhody a nevýhody bezdrátových sítí a jejich základní rozdělení. Dále pak dnes nejčastěji používané standardy, topologie a frekvenční pásma. V několika kapitolách byly popsány možnosti zabezpečení bezdrátových sítí a jejich základní principy.

Praktickou část tvořily tři pracovní scénáře, které simulovaly zabezpečení Wi-Fi sítí v reálných situacích. Cílem každého penetračního testu bylo prolomit zabezpečení a převzít úplnou kontrolu nad bezdrátovou sítí. Každá Wi-Fi síť byla chráněna jiným zabezpečením a doplněna dalšími bezpečnostními prvky. U každé metody zabezpečení byla popsána zranitelnost, na kterou byl proveden praktický útok.

Penetrační testy odhalily, že bezpečnostní mechanizmus WEP poskytuje slabé zabezpečení a takto zabezpečená bezdrátová síť je prolomitelná. WPA poskytuje vyšší bezpečnost, ale protože je založen na protokolu TKIP, který používá stejnou RC4 šifru, je možné i toto zabezpečení prolomit. Při těchto testech bylo využito slovníkového útoku jak na prolomení zabezpečení, tak i administraci přístupového bodu. Zabezpečení WPA2 s protokolem CCMP poskytuje sice robustnější zabezpečení, ale i ono podlehlo slovníkovému útoku.

Ani další dostupné možnosti zabezpečení jako skrytí SSID nebo filtrování MAC adres nepředstavovaly v útoku velký problém a sloužily pouze jako doplnění zabezpečení.

V praktické části byly také provedeny testy, které měly porovnat propustnost Wi-Fi sítě v závislosti na použitém šifrování. Z těchto informací bylo zjištěno, že v poměru přenosová rychlost/bezpečnost je nejlepší bezpečnostní mechanizmus WPA2, který ovlivňoval celkovou propustnost sítě pouze minimálně.

Na závěr byly všechny penetrační testy vyhodnoceny a uvedena doporučení, jaké dostupné možnosti zabezpečení použít, aby byla bezdrátová Wi-Fi síť co nejvíce bezpečná.

ZÁVĚR V ANGLIČTINĚ

The aim of this thesis was to describe the importance of penetration tests and their deployment for the Wi-Fi networks. In the theoretical part were introduced the advantages and disadvantages of wireless networks and their basic classification. Furthermore, most commonly used standards today, topologies and frequency bands. In several chapters were described security options for wireless networks and their basic principles.

The practical part consisted of three working scenarios that simulate the security of Wi-Fi networks in real situations. The aim of each penetration test was to break the security and take complete control over wireless network. Each Wi-Fi network was protected by different security and other added security features. For each method was described a vulnerability, for which was made a practical attack.

Penetration tests have revealed that the security mechanism WEP provides weak security and wireless network secured this way is breakable. WPA provides higher security, but because it is based on the TKIP, which uses the same RC4 cipher, it is possible to break even this security. In these tests, was used a dictionary attack to break both the security and administration of the access point. WPA2 with CCMP protocol provides robust security, but it succumbed to dictionary attack too.

Nor other available security options such as hiding the SSID or the MAC address filtering don’t pose a big problem in the attack and served only as a complement to security.

In the practical part were also carried out tests, which were to compare the throughput of Wi-Fi network depending on the encryption. From these informations, it was found that the ratio of the bitrate/safety is the best security mechanism WPA2, which influencing the overall throughput of only the minimally.

At the conclusion were all penetration tests evaluated and were introduced recommendations, which security options are available in order to wireless Wi-Fi network as safe as possible.

SEZNAM POUŽITÉ LITERATURY

[1] WEBER, Filip; KNAPOVSKÝ, Miroslav. *Svět sítí* [online]. 28.10.2007 [cit. 2011-03-14]. Penetrační testy v bezpečnostní analýze informačního systému. Dostupné z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=309>.

[2] JASNÝ, Libor. *Malware a sociální inženýrství*. [s.l.], 2009. 50 s. Bakalářská práce. UTB Zlín.

[3] *DC IT* [online]. 2010 [cit. 2011-03-14]. Penetrační testy. Dostupné z WWW: <http://www.dcit.cz/cs/bezpecnost/penetracni-testy>.

[4] ZAJÍČEK, Martin. *DCIT* [online]. 20.11.2008 [cit. 2011-03-14]. DC IT Publikace. Dostupné z WWW: <http://www.dcit.cz/cs/system/files/Bezpecnostny%20audit%20a%20penetracne%20testy.pdf>.

[5] MIKO, Karel. *DCIT* [online]. 20.5.2009 [cit. 2011-03-14]. Interpretace výsledků penetračních testů. Dostupné z WWW: <http://www.dcit.cz/cs/system/files/CIMIB_Penetracni-testy.pdf>.

[6] *Cisco* [online]. 2011 [cit. 2011-03-14]. Cisco Networking Academy. Dostupné z WWW: <http://www.cisco.com/web/learning/netacad/index.html>.

[7] *Cisco* [online]. 2011 [cit. 2011-03-14]. Co je potřeba vědět o bezdrátových sítích. Dostupné z WWW: <http://www.cisco.com/web/CZ/solutions/smb/products/wireless/wireless_primer.html#1>.

[8] ZANDL, Patrick. *WiFi Praktický průvodce*. Brno : Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

[9] PETERKA, Jiří. *EArchiv : Báječný svět počítačových sítí* [online]. 2007 [cit. 2011-03-14]. Část XXIV: Wi-Fi. Dostupné z WWW: <http://www.earchiv.cz/b07/b0400001.php3>.

[10] VO-R/12/08.2005-34. *Všeobecné oprávnění*. [s.l.] : Český telekomunikační úřad, 2005. 5 s.

[11] MRÁZEK, Štěpán. *Svět Hardware* [online]. 25.2.2005 [cit. 2011-03-14]. Test Access Pointů: úvod do problematiky. Dostupné z WWW: <http://www.svethardware.cz/art_doc-9D16ACAB1AAA0450C1256F9B0043C8FA.html>.

[12] FRAZEE, Kirsten. *Ati* [online]. 23.2.2011 [cit. 2011-03-14]. ATI Relationship with Wi-Fi Alliance® Reinforces Value of Technology Incubators for Startup Organizations. Dostupné z WWW: <http://www.ati.utexas.edu/blog/wp-content/uploads/wifi-alliance-logo.jpg>.

[13] PUŽMANOVÁ, Rita. *Lupa* [online]. 9.4.2002 [cit. 2011-03-14]. Bezdrátové lokální sítě WLAN podle IEEE. Dostupné z WWW: <http://www.lupa.cz/clanky/bezdratove-lokalni-site-wlan-podle-ieee/>.

[14] PUŽMANOVÁ, Rita. *Lupa* [online]. 16.4.2002 [cit. 2011-03-14]. Bezdrátové lokální sítě WLAN podle IEEE II. Dostupné z WWW: <http://www.lupa.cz/clanky/bezdratove-lokalni-site-wlan-podle-ieee-ii/>.

[15] PUŽMANOVÁ, Rita. *Lupa* [online]. 1.11.2007 [cit. 2011-03-14]. Bezpečnost WiFi záleží jen na vás. Dostupné z WWW: <http://www.lupa.cz/clanky/bezpecnost-wifi-zalezi-jen-na-vas/>.

[16] PUŽMANOVÁ, Rita. *Lupa* [online]. 8.7.2004 [cit. 2011-03-14]. WLAN konečně bezpečné. Dostupné z WWW: <http://www.lupa.cz/clanky/wlan-konecne-bezpecne/>.

[17] PETERKA, Jiří. *EArchiv : WLAN a Wi-Fi* [online]. 2002 [cit. 2011-03-14]. Vyznáte se ve standardech?. Dostupné z WWW: <http://www.earchiv.cz/b02/b0900014.php3>.

[18] LEHEMBRE, Guillaume. *HSC* [online]. 2006 [cit. 2011-03-14]. Bezpečnost Wi-Fi – WEP, WPA a WPA2. Dostupné z WWW: <http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf>.

[19] KUCHAŘ, Martin. *Pc tuning* [online]. 2.2.2005 [cit. 2011-03-15]. Firewall - obrňte své počítače... Dostupné z WWW: <http://pctuning.tyden.cz/software/ochrana-pocitace/4296-firewall-obrnte_sve_pocitace>.

[20] PECHO, Peter. *Lupa* [online]. 12.2.2010 [cit. 2011-03-15]. Proč firewall?. Dostupné z WWW: <http://www.lupa.cz/clanky/proc-firewall/>.

[21] *Www.cisco.com* [online]. 2011 [cit. 2011-04-17]. WLAN Radio Frequency Design Considerations. Dostupné z WWW: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/RFDesign.html#wp1001145>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAA	Authentication, Authorization and Accounting
ACS	Access Control System
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BSA	Basic Service Area
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CCK	Complementary Code Keying
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CCTV	Closed Circuit Television
CGI	Common Gateway Interface
CRC32	Cyclic Redundancy Check 32
ČTÚ	Český Telekomunikační Úřad
DDoS	Distributed Denial of Service
DDoS	Distributed Denial of Service
DFIR	Diffused Infrared
DNS	Domain Name Systém
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EIRP	Equivalent Isotopically Radiated Power
EIRP	Equivalent Isotropically Radiated Power

ESA	Extended Service Area
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
ETSI	European Telecommunications Standards Institute
EZS	Elektronický Zabezpečovací Systém
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
FTP	File Transfer Protocol
GTK	Group Transient Key
HTTP	Hypertext Transfer Protocol
HW	Hardware
IBSS	Independent Service Set
IDS	Intrusion Detection Systém
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPS	Intrusion Prevention System
ISM	Industrial, Scientific and Medical
IV	Initialization Vector
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MIC	Message Integrity Check
MIMO	Multiple Input Multiple Output
MZS	Mechanický Zábranný Systém

NFS	Network File System
NIC	Network Interface Card
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
OUI	Organizational Unique Identifier
P2P	Peer to Peer
PBKDF2	Password-Based Key Derivation Function 2
PEAP	Protected Extensible Authentication Protocol
PMK	Pairwise Master Key
PSK	PreShared Key
PTK	Pairwise Transient Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RC4	Ron's Code 4
RFMON	Radio Frequency Monitor
RPC	Remote Procedure Call
RSN	Robust Security Network
SMB	Sereve Message Block
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
SW	Software
TELEC	Japan Telecom
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
UNII	Unlicensed National Information Infrastructure

USA	United States of America
VoIP	Voice over Internet Protocol
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WHOIS	Z angličtiny Who is?
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ