Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Zabezpečení bezdrátových sítí typu Wi-Fi

HAVLÍČEK Tomáš

! ! !

Místo této strany vložíte zadání diplomové práce.

(Do jedné vazby originál a do druhé kopii)

! ! !

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Zabezpečení bezdrátových sítí typu Wi-Fi" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 25. března 2013 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Alexandru Vasilenkovi za odborný a vstřícný přístup při vytváření diplomové práce.

Zabezpečení bezdrátových sítí typu Wi-Fi

Wi-Fi based wireless network security

Souhrn

Práce se věnuje problematice zabezpečení bezdrátových sítí typu Wi-Fi. Představuje základní zařízení pro bezdrátové sítě a vysvětluje zabezpečení, kterými je lze chránit. V následujících kapitolách jsou popsány techniky přístupu do korporátních sítí a možné útoky útočníků. Posledním tématem teoretické části je monitorování bezdrátových sítí. Vysvětlení proč by se měly bezdrátové sítě monitorovat a co všechno tato složka bezpečnosti obsahuje. V praktické části je ukázáno prolomení zabezpečené sítě protokolem WPA2, poukázání na možná rizika a doporučení zabezpečení sítě. Druhá polovina praktické části se zabývá monitorováním bezdrátové sítě pomocí systému WIPS a vyhodnocením doporučení na zesílení zabezpečení bezdrátové sítě na základě zjištěných nedostatků. Součástí praktické části je i kapitola o prověření okolí bezdrátové sítě spektrální analýzou. Závěr práce je věnován praktické zkušenosti s hledáním a nalezením škodlivého zařízení v bezdrátové síti.

Klíčová slova: Wi-Fi, WEP, WPA2, Backtrack, WIPS, WIDS, SSID, Triangulace, Spektrální analýza, Autentizace

Summary

The work is dedicated to the security of wireless networks such as Wi-Fi. It provides the basic equipment for wireless networks and explains the security, which can be protected. The following chapters describe techniques for access to corporate networks and possible attacks of hackers. The last topic of theoretical part is monitoring of wireless networks, explanation why we should to monitor wireless network and what part of security contains. The practical part is showing cracking WPA2 secure network protocol, pointing out the potential risks and recommendations of network security. The second half deals with the practical part of the monitoring wireless network by WIPS and evaluate recommendations to strengthen wireless security on the basis of the identified shortcomings. The practical part also contains chapter about checking area by wireless spectrum analysis. The conclusion is devoted to the practical experience to the search and discover of malicious devices in wireless network.

Keywords: Wi-Fi, WEP, WPA2, Backtrack, WIPS, WIDS, SSID, Triangulation, Spectral analysis, Authentication

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

V dnešním světě hrají bezdrátové sítě Wi-Fi hlavní postavení. Nalézáme je opravdu všude kolem nás. Počet přenosných zařízení s podporou Wi-Fi v posledních letech rapidně stoupá a zvyšuje nároky na bezdrátové sítě. Můžeme zmínit volně přístupové body (tzv. hotspoty) v kavárnách až po zabezpečené firemní sítě. Přes tyto sítě jsou často sdíleny citlivé informace, a proto je ochrana velmi důležitá.

Zabezpečení bezdrátových sítí je jedním z hlavních prvků jak zamezit zneužití dat a informací. Někteří lidé nedávají důraz na jakékoliv zabezpečení a může se jim to hrubě nevyplatit. Pokud ovšem zvolí slabé zabezpečení, tak situace je téměř stejná a případný útočník může ovládnout celou bezdrátovou síť. Na základě těchto zjištění poukazuji v této práci na zlepšení zabezpečení bezdrátových sítí a představuji vhodné nástroje jak se starat o bezdrátovou síť. Bezdrátové sítě nelze jen vystavět a zprovoznit. Jeden z nejdůležitějších aspektů je se starat souvisle a vyvozovat z chování sítě, jak by se mohla vylepšit či více zabezpečit. V závěru praktické části diplomové práce se věnuji vyhledávání útočníků na bezdrátovou síť.

2 Cíl práce a metodika

2.1 Cíl práce

Jedním z hlavních cílů práce je upozornit na možná bezpečností rizika, která se objevují u bezdrátových sítí. Shrnout existující zabezpečení bezdrátové sítě pro domácí a podnikové použití. V praktické části se pokusit o prolomení pokročilejšího zabezpečení bezdrátové sítě.

V dalších částech budou shrnuta zařízení používaná v bezdrátových sítích a jejich použití. Z velké části bude práce zaměřena na monitorování bezdrátových sítí. Dále na analýzy a techniky, které lze použít a jejich praktické využití ve velkých organizacích. Praktická část se bude zabývat monitorováním bezdrátové sítě vhodným programem a budou vyvozena možná rizika jejího provozu. Dále bude pokus o zaměření škodlivého zařízení pomocí dostupných technik v bezdrátové síti.

2.2 Metodika

Diplomová práce se bude skládat ze dvou stěžejních částí. První část bude nazvaná „Teoretická východiska“ a druhá „Praktická část“. Teoretická část bude vycházet z dostupné literatury k tématu. Po jejím prostudování budou vysvětleny základní pojmy nutné pro porozumění problematiky. Budou popsány druhy zabezpečení, kterými se lze chránit před útočníky a také druhy zařízení, jaká se mohou objevit v bezdrátové síti. Pro korporátní sféru budou představeny způsoby ověřování uživatelů. Poslední část praktické části bude zaměřena na monitorování bezdrátových sítí, kde budou teoreticky popsány analýzy a techniky kontroly sítě.

V praktické části bude popsáno napadení bezdrátové sítě se zabezpečením WPA2. Bude tak dosahováno na vytvořené bezdrátové síti určené jen k těmto účelům. Počítač použitý k útoku bude použita speciální linuxová distribuce Backtrack 5. Budou zde využity poznatky popsané v teoretické části práce. Dalším předmětem praktické části bude monitorování bezdrátové sítě, ve které budou nalezeny problémy a bezpečnostní chyby, a

následně navržena možná řešení dané situace. Na závěr práce bude prakticky ukázáno, jak se může vyhledat škodlivé zařízení v bezdrátové síti.

3 Teoretická východiska

3.1 Bezdrátová technologie

3.1.1 Wi-Fi

Bezdrátové sítě pro přenos dat označujeme zkratkou Wi-Fi. Vychází ze standardu IEEE (Institute of Electrical and Electronics Engineers) 802.11 pro lokální bezdrátové sítě WLAN (wireless local area network). Název Wi-Fi původně neměl význam, ale časem slovní hříčkou si získal název podobný Hi-Fi (tzn. high fidelity – vysoká věrnost), z které by se dala chápat zkratka jako wireless fidelity čili bezdrátová věrnost. Tato technologie pracuje ve dvou frekvenčních pásmech a to 2,4 až 2,48 GHz a 5,1 až 5,8 GHz. Wi-Fi zařízení můžeme dnes najít v mnoha přenosných počítačích, mobilních telefonech a kapesních počítačích PDA (Zandl, 2003 stránky 1-3).

Technologie Wi-Fi sloužila původně k propojení bezdrátových zařízení za účelem výměny dat bez složitého připojení pomocí kabelů. Časem se začala využívat k připojení do sítě Internet, kde se stala velmi využívanou u firem, domácností nebo hotspotů. Je zde zajištěna velká mobilita bez složitého hledání přípojného bodu k síti LAN a bez nutnosti sebou nosit kabel pro připojení. Další výhodou je jistě připojení okolo 200 uživatelů na jedno vysílací zařízení bez nutnosti rozšiřování, jako je tomu u zařízení switch nebo hub (Zandl, 2003 stránky 1-3).

3.1.2 Wi-Fi Alliance (WFA)

Wi-Fi Alliance je obchodní skupina, která vlastní ochrannou známku Wi-Fi od roku 1999. Patří k neziskovému průmyslovému sdružení s více než 500 členskými společnostmi. Jejím cílem je podporovat růst bezdrátových lokálních sítí (WLAN) a zvýšování uživatelského komfortu pro domácí, mobilní a domácí zařízení. Aliance má testovací a certifikační program, který napomáhá ke kompatibilitě produktů založených na specifikaci IEEE 802.11. Tato organizace vlastní a řídí Wi-Fi

Wi-Fi Alliance

Zdroj:www.wi-fi.org

CERTIFIED loga, registrované ochranné známky, která jsou dovoleno umístit pouze na zařízení, která prošla testováním. Tyto testy zaručují velmi přísné testování, protože standardy nezahrnují jenom radiovou a datovou kompatibilitu, ale i bezpečnostní protokol a také nepovinné testy kvality služeb a správy napájení (Wi-Fi_Alliance, 2013).

3.2 Zařízení Wi-Fi

Při stavbě Wi-Fi sítí se můžeme setkat s velmi početným spektrem zařízení různých značek. Existují zařízení pouze pro stavbu sítě, ale v dnešní době se lze setkat s Wi-Fi technologií již ve spotřební elektronice jako třeba mobilní telefony nebo DVD přehrávače, a proto se budu zabývat jen zařízeními pro stavbu Wi-Fi sítě.

3.2.1 Přístupový bod (AP-Access point)

Obrázek 3-1 Jedno z nejmenších AP Asus WL-330G

zdroj: www.asus.cz

Přístupový bod je základním prvkem bezdrátových sítí. Stará se o komunikaci mezi bezdrátovou a kabelovou vrstvou. Směřuje provoz mezi bezdrátovými klienty a pevnou kabelovou sítí. Na přístupový bod se může připojit mnoho uživatelů a není třeba jej draze rozšiřovat. U levnějších přístupových bodů je možné připojit až 30 uživatelů najednou, u dražších je to až 254 uživatelů. Pokud bychom chtěli připojit více uživatelů, musíme pořídit další přístupový bod. S přibývajícími uživateli připojenými na jeden přístupový bod se snižuje také rychlost jejich připojení (Lupa.cz, 2012).

Obrázek 3-2 AP se dvěma anténami

zdroj: www.linksysbycisco.com

Přístupový bod má obvykle jednu anténu pro pokrytí bezdrátové sítě a 4 porty pro připojení 4 počítačů pomocí kabelů. Na trhu můžeme vidět i miniaturní přístupové body kapesní velikosti, jak je vidět na obrázku (Obrázek 3-1), napájení se zajišťuje přes USB počítače a připojení pomocí ethernet portu. V dnešní době můžeme vidět přístupové body s dvěma i třemi všesměrovými anténami (Lupa.cz, 2012).

Pokud má zařízení dvě antény, jak můžeme vidět na obrázku (Obrázek 3-2), jsou z důvodu potlačení vícecestné interference, což znamená, že pokud vysílací i přijímací zařízení používají všesměrovou anténu, a komunikují mezi sebou, dochází k odrazům signálu. Signál se šíří více cestami díky odrazům od překážek a ve výsledku dorazí k přijímacímu zařízení stejný signál s různým časovým posunem. Tento problém řeší dvě antény na přijímacím zařízení, kde se vybírá pro příjem anténa, která je v lepší pozici vůči vysílacímu zařízení (Zandl, 2003).

Přístupové body se třemi anténami se používají k rychlejšímu přenosu a tato technologie se nazývá MIMO. Technologie MIMO (multiple-input multiple-output) používá k vysílání a příjmu více antén a je označována jako standard 802.11n. Teoretická maximální rychlost tohoto přenosu je až 600 Mbit/s, v současné době reálná rychlost je zatím 200 Mbit/s (Stüber, 2004 stránky 271-273).

3.2.2 Uživatelská zařízení (klient)

K tomu, abychom se mohli připojit k přístupovému bodu, musí uživatel použít jedno ze zařízení pracujících v módu klient. Těchto zařízení najdeme na trhu více než přístupových bodů. Ale i některé přístupové body podporují klientskou funkci. Před připojením k požadované síti klientský adaptér prohledá sítě, které jsou v okolí. Poté již proběhne připojení k požadované síti, popřípadě vyžádání k zadání potřebných přihlašovacích údajů.

3.2.2.1 **Karta PCMCIA**

Na trh přišla karta PCMCIA mezi prvními Wi-Fi kartami (Obrázek 3-3). Je připojitelná pouze k notebookům se slotem PCMCIA. Slot vyvinula organizace PCMCIA (Personal Computer Memory Card International Association), která určila standardy pro karty rozšiřující notebooky. V dnešní době slot PCMCIA překonal slot ExpressCard s rychlejší přenosovou rychlostí. Tyto karty mají integrovanou všesměrovou anténu a lepší dokonce konektor pro připojení externí antény (Nathan J., 2003).

Obrázek 3-3 karta PCMCIA

zdroj: www.cisco.com

3.2.2.2 **Karta PCI**

Karta PCI patří k nejstarším kartám pro připojení k Wi-Fi (Obrázek 3-4). Používá se ve stolních počítačích a připojuje se do slotu PCI. Její instalace do počítače je poněkud složitější než v případě karet do slotů PCMCIA nebo ExpressCard. Karta má konektor RSMA pro připojení externí antény. Ke kartám jsou obvykle dodávány malé všesměrové antény, ale můžeme připojit i výkonnější anténu pro lepší signál (Nathan J., 2003).

Obrázek 3-4 PCI wi-fi karta
zdroj: widdayat.wordpress.com

3.2.2.3 **Externí USB karta**

Externí karta připojující se pomocí rozhraní USB (Obrázek 3-5). Ze všech karet má nejširší použití. Lze ji použít jak u stolních, tak u přenosných počítačů. Připojení je velmi rychlé a snadné. Externí Wi-Fi karty můžou i nemusí být vybavené interní anténou, obvykle však mají konektor pro anténu (Nathan J., 2003).

Obrázek 3-5 USB externí wi-fi karta
zdroj: thewifishop.net

3.2.2.4 **Adaptéry pro přenosné zařízení**

Adaptéry pro přenosná zařízení jako jsou kapesní počítače nebo chytré telefony, využívají operační systém Windows mobile. Pokud nemají integrovaný modul Wi-Fi, byly vyvinuty speciální Wi-Fi moduly do slotů pro Compact Flash a Secure Digital karty (Obrázek 3-6). Oba tyto adaptéry svou velikostí překonávají velikost paměťových karet (Nathan J., 2003).

Obrázek 3-6 SD wi-fi modul
zdroj: techrific.com.au

Wi-Fi modul do slotu Compact Flash bývá větších rozměrů a tak rozměry i váha chytrého telefonu narostou (Obrázek 3-7). Oproti tomu modul do slotu pro Secure Digital karty, který je velmi malý a i jeho hmotnost je srovnatelná s hmotností paměťové karty. Lze tak jednoduše doplnit starší zařízení o Wi-Fi technologii (Nathan J., 2003).

Obrázek 3-7 Compact Flash Wi-Fi modul

Zdroj: www.linksysbycisco.com

3.2.2.5 **MiniPCI karty**

Wi-Fi karty do MiniPCI slotu jsou dnes velmi využívané v přenosných počítačích a Routerboardech od firmy Mikrotik (Obrázek 3-8). Karta se připojuje pomocí 124 pinového konektoru do slotu MiniPCI a k připojení antén se používají konektory UFL (Nathan J., 2003).

Obrázek 3-8 MiniPCI Wi-Fi karta

zdroj:www.pc-houska.cz

3.2.2.6 **Tiskový server**

Pro snadné připojení tiskárny do sítě můžeme použít Wi-Fi tiskový server (print server). Můžeme jej použít bez náročného rozvodu kabeláže. Jde o zařízení se zabudovaným modulem Wi-Fi, elektronikou, konektorem pro připojení do sítě LAN a konektorem USB pro připojení tiskárny (Obrázek 3-9) (Nathan J., 2003).

Obrázek 3-9 Wi-Fi print server

zdroj:www.cybergb.com

Tiskový server se připojí k síti a nainstalují se ovladače požadované tiskárny. Díky takto připojené tiskárně je možné tisknout z každého počítače připojeného do této Wi-Fi sítě.

3.3 Zabezpečení bezdrátové sítě

Bezdrátové sítě Wi-Fi se mají velmi blížit drátovým sítím LAN. Jenže jsou zranitelnější více, než si myslíme. U drátových sítí by se mohl útočník fyzicky napojit kabelem do sítě LAN. V zabránění tohoto útoku můžeme použít pevné překážky, které by musel překonat. Jako například uložení prvků sítě, tj. serverů, switchů a dalších prvků do uzamčených prostorů (Coleman, a další, 2010 str. 10).

U bezdrátových sítí to bohužel tak jednoduché není, protože rádiový signál bezdrátových sítí se šíří všude. Jejich zabezpečení se časem zlepšuje, ale postupně zjišťujeme jak je někdy lehké toto zabezpečení prolomit. K nejlepším zabezpečení patří proto odstínění signálu možnými prostředky, aby se nešířil vně náš objekt a tak případný útočník nemá možnost proniknout do bezdrátové sítě a způsobit tak značné škody. Z tohoto důvodu se správci a stavitelé bezdrátových sítí musí neustále vzdělávat a implementovat nejnovější zabezpečení (Coleman, a další, 2010 str. 10).

Umožnění přístupu přes bezdrátovou síť do sítě LAN je přes bezdrátový portál, kde se ověří uživatel, jestli má přístup do sítě. Teprve poté se umožní identifikovat základními mechanismy sítě a umožnit tak plnohodnotné připojení (Coleman, a další, 2010).

Pro zabezpečení bezdrátové sítě se používá typicky pět hlavních komponent, kterými jsou:

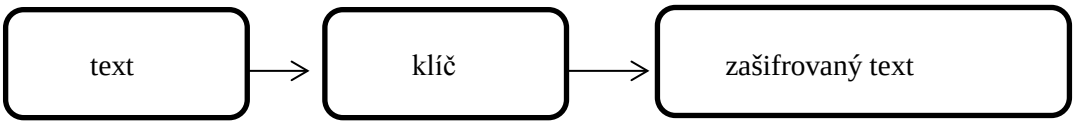
- Ochrana osobních údajů
- Autentizace, pověření a správa účtů
- Segmentace (členění)
- Sledování
- Strategie

3.3.1.1 **Ochrana osobních údajů**

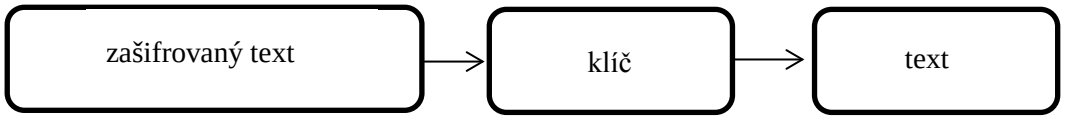
Ochrana osobních údajů je velmi stará, ať se váže k poštovnímu tajemství nebo komunikaci mezi osobami, které si sdílejí intimní informace. Pokud myšlenku nebo informaci sdílíte na delší vzdálenosti, vzniká problém s ochranou. I když informaci zakódujete, není jisté, že někdo další nedokáže tuto informaci rozluštit, přestože metody

kódování a dekódování byly vynalezeny a jsou stále zlepšovány. V tomto případě vzniká možnost, že informaci nedekóduje jen osoba, pro kterou byla informace, ale i další článek řetězce a to narušitel (Coleman, a další, 2010 str. 12).

K zašifrování se používá algoritmus s použitím klíče. Šifrování je odvozeno z řeckého slova a znamená skryté slovo. Cílem šifrování je vzít informaci čili text a pomocí procesu nebo algoritmu změnit text na zašifrovaný text (Obrázek 3-10). Obdobně funguje i dešifrování na straně příjemce (Obrázek 3-11). Celý proces šifrování můžeme vidět na následujících obrázcích. V počítačové technice se proces šifrování jmenuje kódování. Zjištění zašifrovaného textu bez znalosti klíče můžeme docílit kryptoanalýzou (čili dekódování klíče). Pokud je analýza úpěšná je odhalen klíč a tím je prolomeno šifrování (Coleman, a další, 2010).



Obrázek 3-10 - zašifrování textu (Coleman, a další, 2010)



Obrázek 3-11 - dešifrování textu (Coleman, a další, 2010)

Věda, která se snaží o ukrytí zasílané zprávy je steganografie. Zde hlavním úkolem je nesrozumitelnost nebo schování zprávy v textu. Tato technika, se například používá u vodotisků, které používají umělci a fotografové k ochránění obrazů a fotografií. Bohužel tato technika se v bezdrátových sítích zatím nevyužívá. Využívá se v případech, kde není obvyklé a tedy nečekané (Coleman, a další, 2010 str. 13).

3.3.1.2 **Autentizace, pověření a správa účtů (AAA)**

Autentizace (Authentication) je způsob, kterým se zjišťuje identita uživatele. Uživatel se identifikuje na základě ověření jako je uživatelské jméno a heslo nebo digitální certifikáty (Coleman, a další, 2010 str. 15).

Pověření (Authorization) zahrnuje udělování přístupů do síťových zdrojů a služeb. Pokud však před pověřením neproběhne v pořádku autentizace uživatele tak uživatel nedostane přístup do sítě (Coleman, a další, 2010 str. 15).

Správa účtů (Accounting) je sledování využívání síťových zdrojů uživateli. U každého uživatele se zaznamenává historie zdrojů, ke kterým měl přístup a v jaký čas. Na základě těchto údajů můžeme snadno nalézt viníka průniku do sítě přes bezdrátovou síť do sítě LAN (Coleman, a další, 2010 str. 15).

3.3.1.3 **Segmentace**

Pro zabezpečení sítě je důležité mít silné šifrování a také AAA řešení (ověření, pověření a správu účtů). Další neméně důležitou součástí je segmentace. Zařazení uživatelů do skupin podle toho co je na jednotlivých sítích vytvářeno. S citlivými daty by měli uživatelé pracovat jen na sítích LAN a pro práci s ne příliš důležitými daty na sítích Wi-Fi. Pro tyto skupiny můžeme určovat pravidla přístupů a služeb jako firewall, směrování (routování), VPN a VLAN (Coleman, a další, 2010 str. 15).

3.3.1.4 **Sledování**

Sledování (Monitoring) sítě je prvek po úspěšném nastavení a stavbě bezdrátové sítě. Sleduje se, jestli síť pracuje podle očekávání a je důležité neustále kontrolovat případné útoky a průniky. Sledování provozu se může přirovnat k lidem chodícím do a z firmy. Můžeme přesně určit kdo, a kdy vstoupil do podniku (Coleman, a další, 2010 str. 16).

Pro administrátora bezdrátové sítě je velmi důležité sledovat tento provoz. Pro sledování sítě se používá systém WIDS (Wireless Instruction Detection System), který identifikuje a zaznamenává útoky z bezdrátového rozhraní. Dalším systémem je WIPS (Wireless Instruction Prevention System) jež dokáže, tak jako WIDS, zhodnotit zařízení v síti na oprávněná a neoprávněná. WIPS k těmto vlastnostem navíc přidává možnost znemožnění komunikace s naší sítí zařízením, ze kterých je veden útok (Coleman, a další, 2010 str. 16).

3.3.1.5 **Strategie**

Zabezpečení bezdrátových sítí a sledování útoků je naprostou nezbytností. Jenže i zabezpečení může být bezcenné, pokud uživatelé sdílí svoje heslo s dalšími. Proto strategie bezdrátových sítí musí být jasně daná. Prosazovat zpevnění účinnosti všech Wi-Fi zabezpečujících komponent (Coleman, a další, 2010 str. 30).

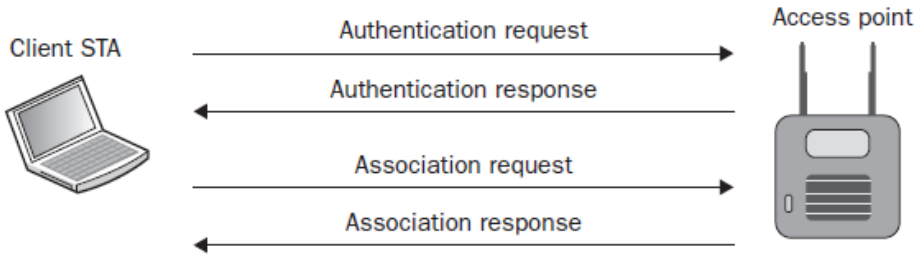
3.3.2 Ověření (Authentication)

Ověření je jeden ze dvou kroků potřebných k připojení k bezdrátové síti. Ověření můžeme přirovnat k zapojení síťového kabelu LAN do počítače. A tak funguje i ověření u bezdrátových sítí, kde komunikuje klientské zařízení s přístupovým bodem. Rozeznávají se dva typy ověřovacích metod a to otevřený systém autentizace (Open System authentication) a autentizace se sdíleným klíčem (Shared Key authentication) (Coleman, a další, 2010 str. 32).

3.3.2.1 **Otevřený systém autentizace (Open System authentication)**

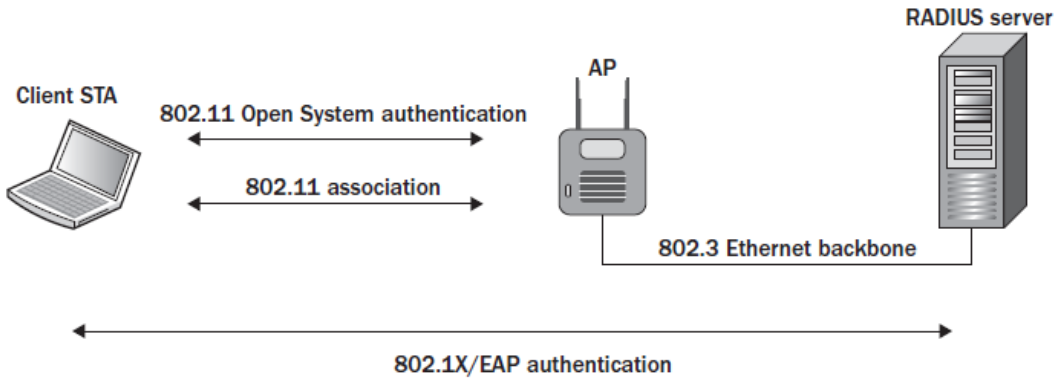
Otevřený systém autentizace je jednodušší z dvojice metod pro ověření identity. Poskytuje autentizaci bez provádění jakéhokoliv typu ověření klienta. Mezi klientským zařízením a přístupovým bodem se vymění uvítací rámce, kterým se říká nulová autentizace, protože u této autentizace není žádná výměna ověření nebo identifikace mezi zařízeními (Coleman, a další, 2010 str. 33).

Při otevřené autentizaci se vyměňují rámce mezi klientskou stanicí a přístupovým bodem, které pocházejí ze základního nastavení služeb (basic service set – BBS). Při sekvenci se zasílají dvě zprávy autentizace. První zpráva uplatňuje identitu a žádá o autentizaci. V druhé zprávě vrací výsledek autentizace, jestliže je výsledek autentizace kladný, je prohlášení vzájemné autentizováno. Tím končí autentizace a zařízení jsou připravena k další komunikaci v síti. Celý proces autentizace můžeme vidět na následujícím obrázku (Obrázek 3-12) (Coleman, a další, 2010 str. 33).



Obrázek 3-13 - Procesu autentizace

V současnosti se otevřená autentizace používá výhradně se spojením asociace se serverem Radius, dříve byla tato autentizace ve spojení s WEP (Wired Equivalent Privacy) zabezpečením, které je již v dnešní době nedostatečné. Otevřená autentizace probíhá přes protokol 802.1X/EAP, kde klientská stanice komunikuje přes přístupový bod s RADIUS serverem (Obrázek 3-11) (Coleman, a další, 2010 str. 34).



Obrázek 3-12- Otevřená autentizace a 802.1X/EAP autentizace

3.3.2.2 **Shared Key authentication**

Autentizace sdíleným klíčem (Shared Key authentication) se používá u zabezpečení WEP (dále v kapitole 3.3.3) k autentizaci klientských stanicí. Kde klíč je statický a je nastaven jak na klientské stanici, tak na přístupovém bodu. Pokud se tento klíč neshoduje tak nedojde k autentizaci zařízení. Autentizace vychází z otevřené autentizace a přibírá další zprávy komunikace mezi zařízeními, přesněji řečeno čtyři zprávy (Coleman, a další, 2010 str. 35).

Klientská stanice vyšle autentizační žádost k přístupovému bodu, který odešle text v autentizační odpovědi. Klientská stanice tento text zakóduje příslušným klíčem a zasílá zpět přístupovému bodu v další autentizační zprávě. Přístupový bod poté dekóduje zprávu svým klíčem a porovná ji s odeslaným textem. Pokud se tyto texty shodují, odesílá potvrzující autentizační rámec klientské stanici a tím vzniká status *vzájemně autentizováno*. Statický klíč se po autentizace používá také k šifrování dat při komunikaci zařízení. Jestliže se neshodují texty, odesílá se zamítavá odpověď (Coleman, a další, 2010 str. 35).

Autentizace se sdíleným klíčem je více zabezpečená, než otevřená autentizace. Jenže právě sdílený klíč vytváří bezpečnostní riziko. Kdokoliv zachytí komunikaci úspěšné autentizace mezi klientským zařízením a přístupovým bodem snadno rozluští klíč pro přístup do zabezpečené sítě. Protože se tento klíč používá jak k autentizaci, tak k šifrování dat, má útočník plný přístup do sítě (Coleman, a další, 2010 str. 35).

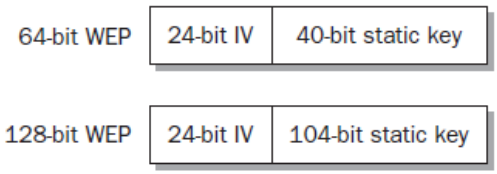
3.3.3 Zabezpečení WEP

Zabezpečení WEP (Wired Equivalent Privacy) se mělo přiblížit pevným sítím LAN. Je potřeba dopředu říci, že toto zabezpečení je již dlouhá léta překonáno. Originální standard definuje 64-bitové a 128-bitové šifrování. Hlavními třemi předpoklady zabezpečení WEP jsou: důvěrnost, kontrola přístupu a integrita dat (Coleman, a další, 2010 str. 38).

Úkolem důvěrnosti bylo zachovat soukromí dat šifrováním před samotným přenosem. Kontrola přístupu zajišťuje přístup do sítě, pokud se neshodují klíče klientského zařízení a přístupového bodu. Na závěr datová integrita kontrolování hodnot ICV (Integrity Check Value), která je připočítávána k datům před šifrováním a je použita k následné kontrole, že data nebyla změněna (Coleman, a další, 2010 str. 38).

U slabšího 64-bitového šifrování se klíč skládá z 24-bitového inicializačního vektoru (Initialization Vector IV) a 40-bitového statického klíče. Inicializační vektor je použit v zasílaném textu při autentizaci a pro každý rámec je vytvořen nový. Maximum kombinací inicializačních vektorů je přibližně 16 miliónů, takže se hodnoty dále používají

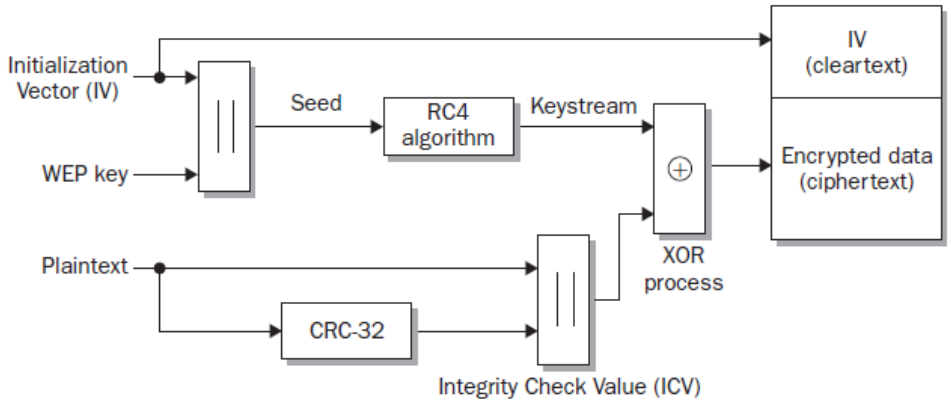
opakovaně. Při použití 128-bitového WEP klíče se používá stejný inicializační vektor jako u předchozího 64-bitového šifrování a pouze statický klíč využívá 104 bitů. Obě tyto varianty WEP šifrování jsou na následujícím schématu (Obrázek 3-13) (Coleman, a další, 2010 str. 39).



Obrázek 3-14- skladba WEP klíče u zabezpečení WEP

Zařízení podporují až 4 WEP klíče ze kterých uživatel vybere implicitní klíč pro přenos dat. Jedná se o statický klíč, který se používá k šifrování dat přenášených přes bezdrátovou síť. Klient nebo přístupový bod mohou používat jeden klíč pro šifrování odcházející komunikace a jiný klíč k dešifrování přijaté komunikace. Každý z těchto klíčů se však musí na obou stranách (vysílací/přijímací) shodovat (Coleman, a další, 2010 str. 40).

Na následujícím schématu (Obrázek 3-14) můžeme vidět celý proces zašifrování textu pomocí WEP klíče. Obdobným procesem se na přijímané straně provádí dešifrování. WEP šifrování má několik slabých míst, o kterých se následně zmíníme. Na základě těchto slabých míst mohou útočníci získat WEP klíč a tak se dostat do bezdrátové sítě (Coleman, a další, 2010 str. 41).



Obrázek 3-15 - zabezpečení WEP postup šifrování (Coleman, a další, 2010 str. 41)

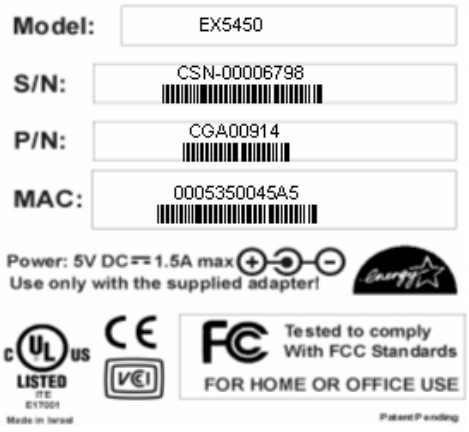
K útoku na kolizi inicializačního vektoru dochází při velkém provozu na síti. Máme jen asi 16 miliónů inicializačních vektorů a tak se po čase začínají opakovat. Pokud útočník tento provoz zachytí tak dokáže z kolize, tedy rámců se stejným inicializačním vektorem, zjistit WEP klíč za předpokladu dostatečného počtu opakování stejných rámců (Coleman, a další, 2010 str. 41).

Útok na slabý klíč se odvíjí od ARC4 algoritmu, kde je plán klíčů a tak generuje slabé inicializační klíče. Útočník poté velmi jednoduše může získat tajný klíč z obnovených inicializačních klíčů (Coleman, a další, 2010 str. 41).

Útok založený na zpětném zasílání rámců umožňuje narušiteli rychlejší sběr slabých inicializačních vektorů v bezdrátové síti, kde je jen velmi malý provoz (Coleman, a další, 2010 str. 41).

3.3.4 Filtrování MAC adres

MAC (Media Access Control) adresa slouží k jednoznačnému určení zařízení. Každé zařízení má svoji jedinečnou adresu skládající se ze 48 bitů, kterou žádné jiné zařízení nemůže mít. Adresa je zapsaná hexadecimálně a zapisuje se jako šestice dvojciferných čísel oddělených pomlčkami nebo dvojtečkami. Někdy je na zařízeních uvedena adresa bez pomlček či mezer. Na obrázku (Obrázek 3-15) je uveden náhled na štítek zařízení, kde je uvedena MAC adresa (Pužmanová, 2005 str. 59).

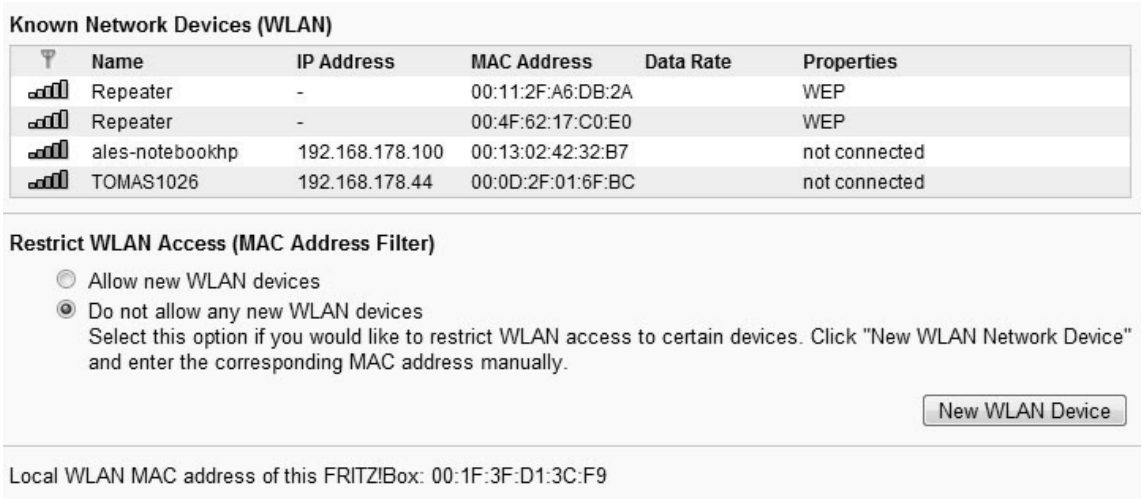


Obrázek 3-16 štítek z wi-fi zařízení

zdroj:www.chippc.com

Ochrana filtrováním adres umožňuje omezení jen na povolené klientské stanice k přístupu do sítě na základě jedinečné MAC adresy zařízení. Zařízení, která nejsou ve výčtu MAC adres (Obrázek 3-16), nemohou přistupovat do sítě. MAC adresu zařízení je

ale možné zfalšovat a každý amatérský útočník tak může obejít filtrování adres. Protože převážná většina nabízených bezdrátových adaptérů nabízí možnost její změny. Pokud to adaptér neumožňuje je řada programů na zfalšování MAC adresy. Pro zjištění MAC adresy, která je povolená MAC filtrováním, stačí odposlechnout malé množství paketů při komunikaci mezi klientským zařízením a přístupovým bodem. Z těchto důvodů plyne, že filtrování MAC adres je jen jako doplňkový nástroj ochrany, který musí být vždy doplněn dalším zabezpečením (Coleman, a další, 2010 str. 49).



Obrázek 3-17 Seznam MAC adres u zařízení Fritz!Box (zdroj: autor práce)

3.3.5 SSID Segmentace

Další způsob, jak zvýšit ochranu bezdrátové sítě, je vytvoření nezávislých přístupových bodů s různými SSID (Service Set Identifier) a virtuální sítě VLAN (Virtual LAN). SSID je identifikátor bezdrátové sítě, který vysílá přístupový bod. Na jeho základě se uživatel připojuje k dané bezdrátové síti (Coleman, a další, 2010 str. 49).

Řešení SSID segmentace se zpravidla využívá ve firemní sféře bezdrátových sítí, kde je možno oddělit různé skupiny uživatelů. Jsou nastavena různá SSID pro různé skupiny uživatelů. Pro každý přístupový bod tak je nastavena VLAN a tedy i omezený přístup do některých částí sítě. Obvykle je vytvořeno nastavení VLAN pro hosty, hlasové služby a nakonec data. V VLAN pro hosty nemusí mít bezdrátová síť žádné zabezpečení a slouží jen pro přístup na internet. Pro hlasové služby se obvykle volí WPA2-personal a

telefony jsou připojeny k VoIP serveru. Pro datový přenos se volí silnější zabezpečení WPA2 – enterprise a uživatelům je zajištěn plný přístup do sítě, po předchozí autentizaci. Problém v SSID segmentaci je nastavení všech přístupových bodů individuálně a dále nastavení VLAN pravidel pro připojení skupin uživatelů. V současnosti je tato segmentace vysoce doporučována k zajištění zvýšené bezpečnosti (Coleman, a další, 2010 stránky 49-51).

3.3.6 Maskování SSID

Další možností, jak zvýšit bezpečí bezdrátové sítě, je skrytí vysílané administrativní signalizace, která obsahuje základní údaje o síti, jako je SSID, tedy název bezdrátové sítě. Při tomto nastavení běžní uživatelé tuto síť nenaleznou. Pokud tedy uživatelé nebudou znát jméno bezdrátové sítě, nemohou se k síti připojit. Pokud uživatelé budou skenovat okolní sítě, přístupový bod vrací odpověď, kde pole SSID je naplněno nulovou hodnotou (Coleman, a další, 2010 str. 51).

V současnosti mohou zručnější uživatelé tyto skryté bezdrátové sítě objevit. A to například s programem NetStumbler, který dokáže vyhledat i skryté bezdrátové sítě. Tento program pracuje jako chytrá skenovací pomůcka. Chová jako klientské zařízení, které má přístup do dané skryté sítě. Přístupový bod na toto zařízení odpovídá zprávou, kde je již správné SSID obsaženo a tak i tyto sítě nejsou zcela skryty (Coleman, a další, 2010 str. 51).

Dalším způsobem jak odhalit skryté bezdrátové sítě je využití zachycování paketů. I v tomto případě dokáže zkušený uživatel zjistit SSID skryté bezdrátové sítě. Z uvedených fakt vyplývá, že tato varianta zabezpečení je pouze doplňkovým nástrojem, který prodlužuje čas napadnutí sítě útočníkem. Před běžnými uživateli zůstane bezdrátová síť skryta (Coleman, a další, 2010 stránky 51-52).

3.3.7 802.1X řízený přístup

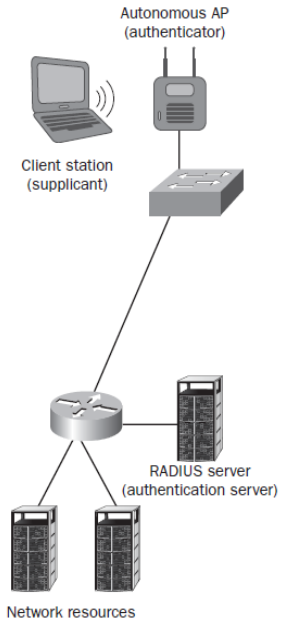
802.1X standard je řízení přístupu na základě přidělování portů. Tato metoda využívá autorizační rámec, který povolí přístup do sítě pomocí portů. Standard 802.1X je implementován jak do bezdrátové tak drátové sítě. Skládá se ze tří komponent, které jsou vysvětleny v následujících podkapitolách (Coleman, a další, 2010 str. 52).

3.3.7.1 **Žadatel (Supplicant)**

V případě bezdrátových sítí je žadatelem klientské zařízení žádající o přístup do sítě. Každý žadatel má unikátní autentizační údaje, kterými se ověří u autentizačního serveru. K tomuto ověření se používá autentizační protokol EAP (Extensible Authentication Protocol), přes který probíhá komunikace s autentizačním serverem (Coleman, a další, 2010 str. 110).

3.3.7.2 **Ověřovatel (Authenticator)**

Funkcí ověřovatele (tedy přístupového bodu) je předávání zpráv mezi žadatelem a autentizačním serverem (Obrázek 3-17). Komunikace je vedena jen ve 2. vrstvě modelu OSI, která umožňuje jen omezené služby. Vytváří se 2 porty: kontrolovaný a nekontrolovaný. Nekontrolovaný port umožňuje jen EAP autentizační provoz a kontrolovaný port blokuje veškerou komunikaci do té doby, dokud není zařízení autentizováno (Coleman, a další, 2010 str. 110).



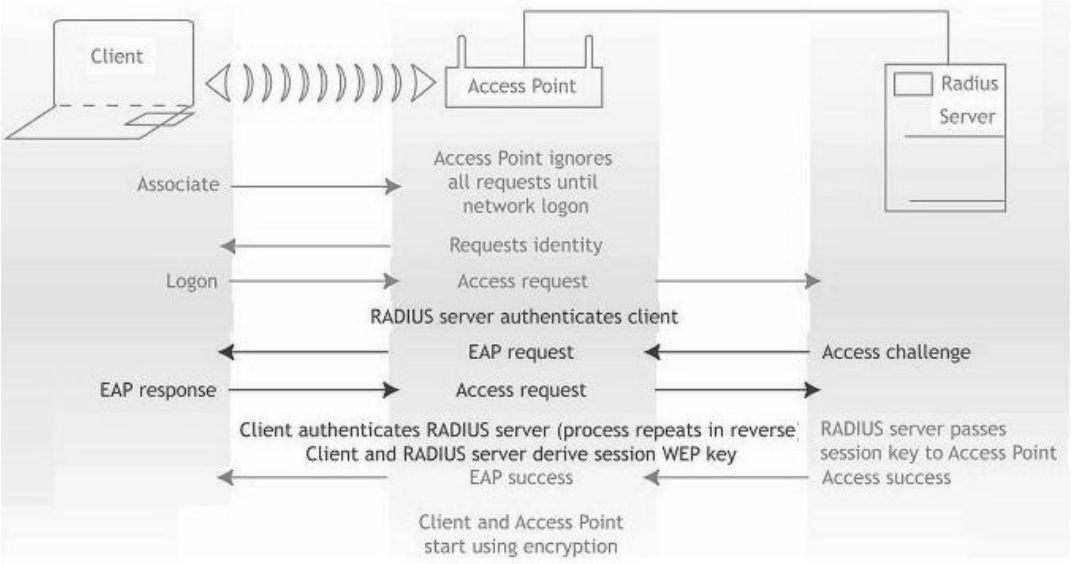
Obrázek 3-18 - Komunikace mezi žadatelem a autentizačním serverem (Coleman, a další, 2010)

3.3.7.3 **Autentizační server (Authentication server)**

Autentizační server (často označován RADIUS) spravuje pověření žadatelů a spravuje databázi uživatelů s jejich právy. Komunikuje i s dalšími uživatelskými

databázemi. Pokud žadatel se chce připojit k síti je vyhledán v databázi a jsou mu přiřazena práva komunikace v síti. V zabezpečení bezdrátových sítích je autentizační server jednou z nejvíce využívaných metod. Jeho komunikaci se zařízením můžeme vidět na schématu (Obrázek 3-18) (Coleman, a další, 2010 stránky 119-120).

K ověření uživatelů přes autentizační server k přístupu do sítě se využívají různé techniky. Uživatelské jméno/heslo je nejjednodušší formou identifikace žadatele. Pro zadávání se udává ještě doména uživatele, ve které se nachází. Další ověření může probíhat na základě digitálního certifikátu, který zajišťuje šifrování následné komunikace a používá se například u internetového bankovnictví. Můžeme mít dva typy certifikátů a to ze strany serveru nebo klienta. Certifikáty mají vlastní časovou životnost, po které musí být znovu obnoveny (Coleman, a další, 2010 stránky 123-125).



Obrázek 3-19- Způsob autentizace a komunikace mezi klientem a Radius serverem (zdroj: AirMagnet - live capture)

Často využívaným způsobem pro autentizaci jsou hesla pro jedno přihlášení, která se neopakují. K tomuto účelu se používá generátor hesel (Obrázek 3-19). Jedná se o přívěšek na klíče, kde na displeji se mění hesla v intervalu 30 nebo 60 sekund. Hesla, která jsou v generátoru v přesné okamžiky, jsou stejná v autentizačním serveru a vyhodnocuje se shoda hesel (Coleman, a další, 2010 str. 126).

Každý uživatel má přiřazen svůj osobní generátor hesel. Uživatel používá k autentizaci uživatelské jméno, osobní heslo a heslo z generátoru. Pokud heslo z generátoru zadávané při autentizaci nebude správné, pak autentizace neproběhne úspěšně. Životnost generátorů hesel jsou 2 roky, po kterých se vyčerpá rozsah hodnoty hesel (Coleman, a další, 2010 stránky 126-127).

Pro ověření při autentizaci se dále dají používat chytré karty (Smart Cards). Zde se na čipu karty uchovávají zabezpečené informace o uživateli. U této karty se informace obvykle nedají zkopírovat ani změnit. Informace o uživateli se obvykle blíží klientskému certifikátu. V nynější době většina laptopů, které využívají větší korporace, mají čtečku těchto chytrých karet již zabudovanou. Pokud ji nemají, tak existují externí čtečky přes port USB (Coleman, a další, 2010 str. 128).

Obrázek 3-20 - Generátor hesel (zdroj: www.tokenguards.com)

Asi nejvíce bezpečným způsobem ověření by se dala označit biometrika. Zahrnuje ověření osoby pomocí prvků lidského těla, které jsou naskenovány a uchovávány na autentizačním serveru. Pokud použijeme tyto údaje spolu s heslem k ověření uživatele, získáme jeden z nejbezpečnějších způsobů zabezpečení spolu s nízkou cenou. Řada dnešních počítačů má již integrovány čtečky otisků prstů. Další způsob ověření může být například na základě skenování obličeje, kde se pomocí kamery počítače zjistí vzdálenosti mezi očima, ústy a nosu. Bohužel toto ověření vyžaduje webovou kameru, která je často ve firmách zakázána z důvodu možnosti úniku informací z pracoviště (Coleman, a další, 2010 str. 131).

3.3.8 WPA / WPA2 - personal

Zabezpečení WPA/WPA2 – personal se využívá ve sféře SOHO (small office, home office), čili v malých firmách a domácnostech.

Nejdříve bylo představeno zabezpečení WPA (Wi-Fi Protected Access) jen jako dočasné zabezpečení do doby, než bude ratifikována standard 802.11i. V té době podporovalo jen TKIP/RC4 dynamický generátor šifrovacích klíčů. Tato metoda je určena pro potřebu malých organizací a při autentizaci používá přístupovou frázi (heslo). Výhodou oproti zabezpečení WEP jsou již dynamické klíče a nezadávání hesla pomocí hexadecimálních znaků nebo decimálních číslic. Přístupová fráze musí být v rozsahu 8-63 znaků z tabulky ASCII (Coleman, a další, 2010 stránky 222-223).

V roce 2004 bylo představeno zabezpečení WPA2, které přidává k zabezpečení WPA šifrování CCMP/AES. Byly tak zachovány všechny prvky a to i PSK (Preshared Keys) autentizace, kterou si vysvětlíme následně (Coleman, a další, 2010 str. 223).

3.3.8.1 **Preshared Keys, Passphrases**

PSK (Preshared Keys) čili předsdílené klíče s délkou 256 bitů (64bit hexadecimálně) se používají k silnému zabezpečení sítí. Klíč je konfigurovaný na všech zařízeních, jak na přístupových bodech, tak na klientských zařízeních. Protože je však problém si zapamatovat 64 znakový klíč a poté ho ještě zadávat do všech zařízení v síti, zadávají se kratší hesla, např. přístupovou frázi. Abychom získali z přístupové fráze PSK klíč, je potřeba ho nejprve převést pomocí následujícího vzorce (Coleman, a další, 2010 str. 224).

$$PSK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256)$$

Přístupová fráze je zkombinována s SSID a 4096 krát zamíchána k vytvoření 256 bitového PSK klíče. Tímto způsobem je umožněno jednodušší použití pro koncové uživatele. Dále se PSK klíč používá jako hlavní párovací klíč (PMK – pairwise master key). PMK klíč je vstupem pro 4-Way Handshake, který generuje dynamické klíče. Role PMK je natolik klíčová, že pokud útočník získá PMK klíč odvozený z přístupové fráze, tak

mu již zbývá jen odposlechnout komunikaci 4-Way Handshake mezi přístupovým bodem a klientským zařízením. Tak získá PTK klíč, kterým lze dešifrovat následnou komunikaci (Coleman, a další, 2010 str. 227).

Dalším důvodem proč se samotné WPA nepoužívá ve větších organizacích je znalost hesla do bezdrátové sítě u osob, která již vystoupila z organizace. Heslo by bylo nutné změnit při každém vystoupení osoby z organizace. Dále pokud uživatel sítě sdělí heslo 3 osobě, ta ihned získá přístup do celé sítě. Proto je vhodnější zabezpečení WPA do menších organizací a domácností. V následující tabulce (Obrázek 3-21) je přehled zabezpečení a jejich autentizačních metod a použitých šifrovacích klíčů (Coleman, a další, 2010 str. 232).

802.11 Standard	Wi-Fi Alliance Certification	Authentication Method	Encryption Method	Cipher	Key Generation
802.11 legacy		Open System or Shared Key	WEP	RC4	Static
	WPA-Personal	WPA Passphrase (also known as WPA PSK and WPA Pre-Shared Key)	TKIP	RC4	Dynamic
	WPA-Enterprise	802.1X/EAP	TKIP	RC4	Dynamic
802.11- 2007	WPA2-Personal	WPA2 Pass-phrase (also known as WPA2 PSK and WPA2 Pre-Shared Key)	CCMP (mandatory)	AES (manda-tory)	Dynamic
			TKIP (optional)	RC4 (optional)	
802.11-2007	WPA2-Enterprise	802.1X/EAP	CCMP (mandatory)	AES (manda-tory)	Dynamic
			TKIP (optional)	RC4 (optional)	

Obrázek 3-21 - Přehled zabezpečení bezdrátových sítí (Coleman, a další, 2010)

3.4 Monitoring zabezpečení bezdrátové sítě

Jestliže je bezdrátová síť zabezpečená měli bychom se věnovat jejímu monitoringu. V dnešní době existují programy a zařízení, kterými je možno skenovat bezdrátovou síť a zjišťovat informace o případných útocích. Jednoduššími zařízeními dokážeme skenovat nejbližší síť a to můžeme provádět za pomoci laptopu či chytrého telefonu. Jenže toto řešení není komplexní a je proto potřeba mít řešení, které bude monitorovat a tím i ochraňovat bezdrátovou síť 24 hodin denně 7 dní v týdnu (Coleman, a další, 2010 str. 372).

3.4.1 Prevenční systémy pro bezdrátové sítě

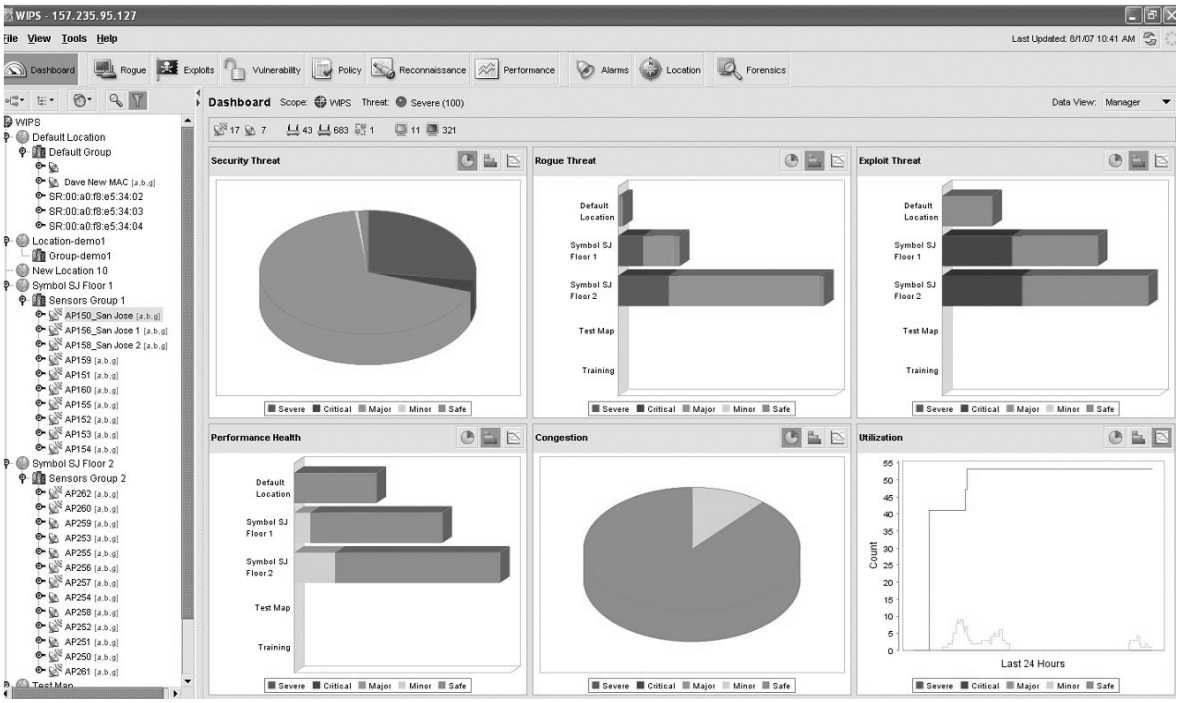
Pro zjištění narušení bezdrátové sítě se používají detekční systémy narušení tzv. WIDS (wireless intrusion detection system). Často jsou označovány také jako WIPS prevence před narušeními (wireless intrusion prevention system), protože tyto systémy dokáží zmírnit útok. Oba tyto systémy sdílejí mnoho informací a pomůcek, které pomáhají administrátorům a správcům zabezpečení sítě, při údržbě a zabezpečení provozu bezdrátové sítě (Coleman, a další, 2010 str. 373).

WIPS a WIDS systémy využívají kombinaci senzorů a zařízení ke sběru a analýze provozu v bezdrátové síti. Takto vytvořený systém dokáže sbírat informace z více míst (senzorů) a zpracovávat je 24 hodin denně. Případně reagovat na určité kritické situace. WIPS systém dokáže například zabránit autorizovanému zařízení, aby se nedopatřením připojilo na útočníkův nepoctivý přístupový bod a tak byly prozrazeny citlivé údaje (Coleman, a další, 2010 str. 373).

WIDS systém, jak napovídá název, detekuje a upozorňuje na útoky v okolí bezdrátové sítě. Funkce WIPS ochraňuje bezdrátovou síť na základě metod detekce a upozornění. Oba tyto systémy používají tři základní prvky a to WIDS/WIPS server, senzory a prostředí pro správu (Obrázek 3-21) (Coleman, a další, 2010).

Hlavní události zjišťované WIDS/WIPS systémy:

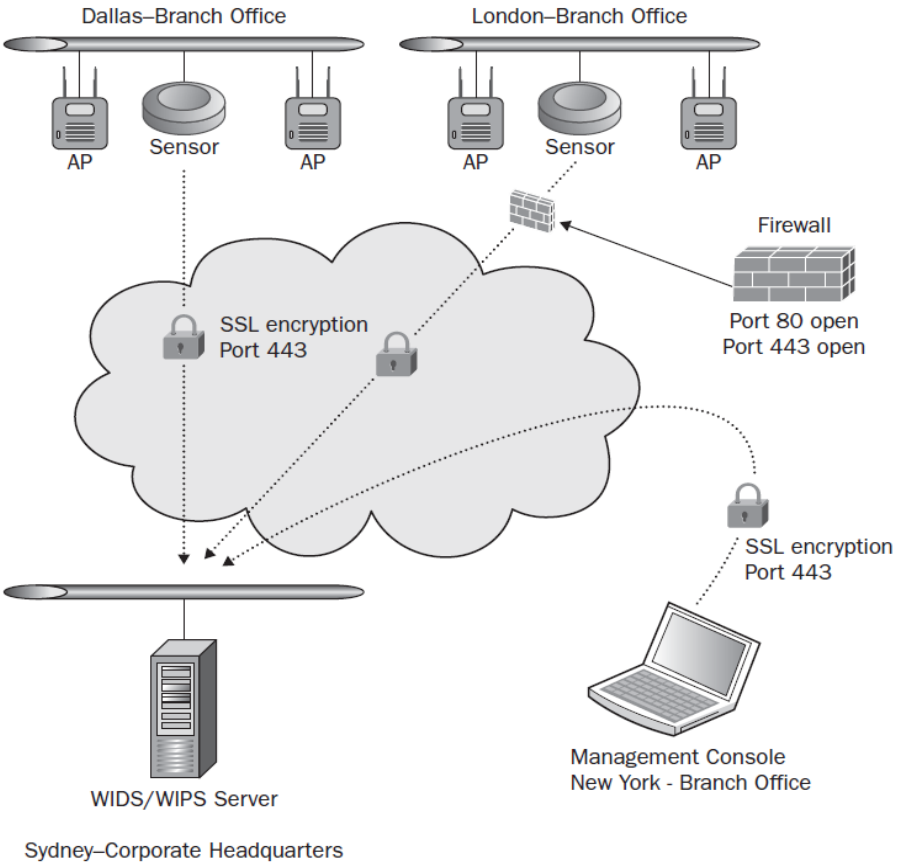
- Wardriving
- Injekce rámců
- Služby odepření přístupu
- Falešné MAC adresy
- Útoky na autentizační mechanismus (například EAP)
- Špatně nakonfigurované přístupové body
- Útoky na zabezpečenou komunikaci (například WEP)
- Nepoctivé přístupové body
- Nepoctivé přístupové body připojené do vnitřní sítě
- Podvrhující přístupové body
- Dvojitá příloha



Obrázek 3-22- prostředí pro správu monitorování bezdrátové sítě (zdroj: www.kodys.cz)

Server WIPS/WIDS vystupuje jako nástroj pro sledování bezpečnosti a shromažďování naměřených údajů. Server využívá analýzu chování, analýzu protokolů a RF spektrální analýzu k detekci potenciálních útoků. Analýza chování se zabývá

zjišťováním anomálií u bezdrátové sítě a analýza protokolů sleduje datové rámce, které nejsou zašifrovány. Spektrální RF analýza monitoruje sílu signálu a odstup signál-šum. Z této analýzy můžeme vyhodnotit pokrytí bezdrátovou sítí a její kapacitu (Coleman, a další, 2010 str. 373) (Chaouchi, a další, 2009 str. 140).



Obrázek 3-23 - schéma zapojení senzorů, WIDS serveru a ovládacího zařízeni

3.4.1.1 **Senzory pro monitorování bezdrátových sítí**

Z hlediska umístění senzorů jde o jejich strategické umístění, kde je nutné odposlouchávat veškerou komunikaci bezdrátové sítě. Senzory jsou vlastně ušima a očima celého systému monitorování. Senzory využívají podobnou techniku jako přístupové body a skenují celé pásmo 14 kanálů v pásmu 2,4 GHz a také 23 kanálů v pásmu 5 GHz. Komunikace mezi senzory a serverem je zašifrovaná pomocí tunelu SSL (secure sockets layer). Dále je posílána zpráva IDS serveru, která indikuje funkčnost a je nazývána také jako bití srdce. Nastavení může probíhat přes telnet, SSH nebo webové rozhraní.

V současnosti existují zařízení, která jsou kombinací přístupového bodu a senzoru. Zde jsou 2 vysílací prvky na pásmu 2,4GHz a 5GHz a jeden, který monitoruje obě zmíněná pásma. Na schéma (Obrázek 3-22) můžeme vidět zapojení senzorů a ovládacího softwaru. Pomocí jednoho WIDS serveru, můžeme obsluhovat více poboček a analyzovat tak provoz vzdáleně odkudkoliv na světě (Coleman, a další, 2010 str. 382).

Obrázek 3-24 - senzor (zdroj: www.fluekenetworks.com)

Některé programy je možno nainstalovat do počítače a proměnit ho tak ve WIDS/WIPS řešení. Dále se budeme věnovat tomuto tématu. Řešení využívá kartu pro bezdrátové připojení k monitorování okolního provozu bezdrátových sítí. Hardware v počítači je důležitý, protože ne všechny karty jsou podporovány. Karta musí splňovat kritérium pro přepnutí do monitorovacího módu (Coleman, a další, 2010 str. 374).

3.4.1.2 **Rozmístění monitorovacích senzorů**

Jakmile zavádíme WIDS/WIPS monitorovací systém tak nastává otázka: Kolik musíme (nebo potřebujeme) umístit senzorů? Na tuto otázku se špatně odpovídá a obvykle závisí na rozpočtu a jaké síťové zdroje budou chráněny zabezpečením monitorováním bezdrátové sítě. Samozřejmě je nejlepší mít neomezený počet monitorovacích zařízení, ale to je nereálné (Coleman, a další, 2010 str. 383).

Každá specializovaná firma má svá doporučení a návody, kolik senzorů je potřeba k monitorování. Jako standard se uvádí jeden monitorovací senzor na 3 až 5 přístupových bodů. Umístěny jsou strategicky tak, že se pokrytí senzory překrývá. Další možností umístění senzorů je stanoviště na okrajích budovy, kde bude pokryt i prostor mimo budovu. Je tak možno vypátrat útoky z vnějšku budovy. Některé z lepších softwarů pro modelování bezdrátové sítě dokáží navrhovat vhodná místa pro umístění senzorů. Pro vojenské využití se používá poměr jednoho senzoru na dva přístupové body nebo dokonce i v poměru 1:1, jeden senzor na přístupový bod (Coleman, a další, 2010 str. 384).

3.4.1.3 **Klasifikace zařízení**

Veškerá komunikace bezdrátové sítě je zachycena WIDS/WIPS řešením a to včetně informací předávaných na 2 vrstvě OSI modelu. Takže každé zařízení vysílající v rozsahu bezdrátových sítí bude zachyceno senzory, pokud je v jejich dosahu. WIDS/WIPS systémy komunikují s přístupovou vrstvou a určují, která zařízení jsou připojena přes kabely LAN. Pomocí těchto údajů se identifikují zařízení v síti, jestliže se jedná o přístupový bod, klientskou stanici nebo ad-hoc klientskou stanici. Na základě získaných informací se sestaví klasifikační tabulka, ve které jsou zařízení rozdělena do několika skupin (povolená, nepovolená, sousedící a nepoctivá) (Coleman, a další, 2010 str. 384).

Jako povolená zařízení jsou klasifikována ta, která se nacházejí v bezdrátové síti a jsou ověřená. Ověřená zařízení se obvykle zadávají do systému WIDS/WIPS k jejich správnému klasifikování. Síťový administrátor tak může například manuálně označit každé zařízení, které monitorovací systém odhalil, nebo se importuje seznam MAC adres povolených zařízení do systému. Do tohoto seznamu jsou přidána automaticky klientská zařízení, která byla řádně autentizována (Coleman, a další, 2010 str. 384).

Jako nepovolené přístroje jsou vyhodnoceny ty, které se automaticky připojily do bezdrátové sítě, ale nejsou klasifikovány jako škodící. Neznámá zařízení jsou shledána jako nepovolená zařízení. Jsou nadále zkoumána a určuje se, zda jsou budoucí potenciální hrozbou. Dalším postupem je analyzování těchto zařízení a případně jejich zařazení do kategorie sousedních zařízení (Coleman, a další, 2010 str. 385).

Jako sousední zařízení se klasifikuje jakákoliv klientská stanice (nebo přístupový bod), která je detekována systémem WIPS/WIDS a je známa její identita. Tento typ zařízení jsou obvykle neověřená zařízení, která se nachází v blízkosti bezdrátové sítě a nepovažují se za hrozbu. Patří například sousedícímu podniku nebo jiné instituci (Coleman, a další, 2010 str. 385).

Škodící zařízení jsou klientská zařízení nebo přístupový bod, která ruší bezdrátovou síť nebo představují potenciální hrozbu útoku. Ze známých případů je nejčastější případ připojeného přístupového bodu do drátové sítě LAN a toto zařízení nepatří správci sítě.

WIDS/WIPS systém dokáže takovéto škodlivé zařízení omezit jeho fungování v síti (Coleman, a další, 2010 str. 385).

Monitorovací systémy mají možnost automatické klasifikace zařízení a rozdělení tedy do skupin. Používají se k tomu různé proměnné zahrnující například autentizační metody, šifrovaní, SSID a další. U automatické klasifikace se musí postupovat obezřetně a musí být jistota, že jen autorizovaná zařízení budou klasifikována (Coleman, a další, 2010 str. 385).

3.4.1.4 **Detekce škůdců**

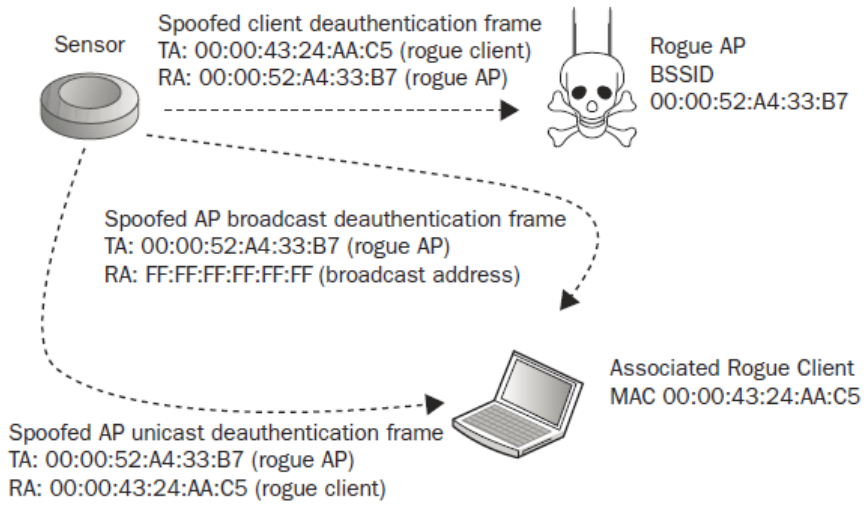
Jak jsme se zmínili již dříve, škodná zařízení jsou přístupové body, které nevlastní správce sítě a jsou připojená do drátové sítě LAN. Monitorovací systémy se snaží tato zařízení vypátrat a omezit jejich funkčnost. Vyhledává se místo, kde je tento přístupový bod zapojen do drátové infrastruktury sítě. Zjištění, zda se jedná o škodné zařízení, je poněkud složitá, protože tato zařízení se mohou autorizovat (Coleman, a další, 2010 str. 386).

Jeden z efektivních způsobů detekce pro klasifikování škodného přístupového bodu je vznášení dotazů na přepínač přístupové vrstvy pomocí Simple Network Management Protocol (SNMP), kde spojíme MAC adresy s fyzickými porty přepínače. Z těchto údajů se sestaví tabulka spojení MAC adresy a fyzických portů. Následně se tato tabulka porovnává se zařízeními, která jsou autorizovaná. Jakmile nebude shoda MAC adresy zařízení v tabulce autorizovaných zařízení, jedná se o neautorizované. Takto je detekován škodný přístupový bod v síti (Coleman, a další, 2010 str. 386).

3.4.1.5 **Zmírnění škůdců**

Jakmile jsou klasifikováni škůdci v síti, tak systém WIPS zasáhne a zmírní možný útok. Nejúčinnějším nástrojem je zasílání deautentizačních rámců, které jsou zasílány tak, jako by byly zasílány přímo škůdcem (změněná MAC adresa na MAC adresu škůdce – Spoof MAC adress). Po tomto útoku na škůdce, všechna zařízení k němu připojená se odpojí. Jinak všechna zařízení snažící se připojit do sítě přes škůdce jsou nadále

deautentizována. Tím je nemožné se připojit přes škodný přístupový bod (Rogue AP) a je tedy vyřazen z provozu (Obrázek 3-24). Popsaná obrana proti škůdcům by se měla používat opatrně, aby se nestalo, že by byl takto vyřazen z provozu legitimní přístupový bod. Proto je lepší volit manuální obranu systémem WIPS. Správce sítě vyhodnotí pomocí popsaného postupu, jestli zařízení je či není škůdce a pak případně provede manuální zásah. Různí výrobci uvádějí vlastní názvy pro zmíněnou funkci jako například: vzdušný terminátor, vypínač škůdců nebo „blokovač“ škůdců (Coleman, a další, 2010 str. 384).



Obrázek 3-25- Deautentizace škodícího přístupového bodu (Coleman, a další, 2010)

3.4.2 Vyhledávání zařízení

Po klasifikování zařízení můžeme využít možnosti WIPS/WIDS systému k nalezení umístění škodného přístupového bodu. Pokud máme zanesen do systému plán budovy, dokáže graficky určit okruh senzorů, kde se přibližně nachází škodný přístupový bod. Tato funkce se samozřejmě může použít i pro zaměření zařízení, která jsou autorizovaná v síti. K určení polohy se používají hodnoty síly signálu RSSI (received signal strenght indicator), které jsou získány ze senzorů a autorizovaných přístupových bodů (Coleman, a další, 2010 str. 392) (Chaouchi, a další, 2009 str. 144).

Další využívanou technikou je historie pohybu zařízení. Na plánu je možné vidět graficky budovy, kde se zařízení vyskytovalo v minulosti. Pokud se přemístil přístupový bod do jiného místa, je velmi pravděpodobné, že se jedná o škodící přístupový bod (Coleman, a další, 2010 str. 392).

3.4.2.1 **Triangulace**

K zaměření polohy zařízení se používá metoda triangulace (RF triangulation). Zde se vychází ze známého umístění senzorů k hledání zařízení s neznámou polohou. Každý ze senzorů poskytuje informace o síle signálu RSSI hledaného zařízení, pokud je v dosahu. Jakmile je silnější signál hledaného zařízení, tj. hodnota RSSI je vyšší, je pravděpodobné, že senzor je v blízkosti hledaného zařízení. Senzory s nižší úrovní signálu jsou vyřazeny z hledání zařízení pro větší vzdálenost. Ze tří nebo i více senzorů s nejvyššími hodnotami RSSI určíme umístění hledaného zařízení obvykle s přesností okolo 10 metrů, což nám plně dostačuje k nalezení zařízení (Coleman, a další, 2010 str. 393).

3.4.2.2 **Metoda otisků prstů**

Přesnější metodou než triangulace je metoda otisků prstů (RF fingerprint). Používá se stejná technika jako u triangulace jen s tím rozdílem, že se získávají data nejenom ze senzorů a přístupových bodů, ale také z klientských zařízení. Sbírají se hodnoty RSSI a vychází se z předpokladu, že zařízení s podobnými hodnotami RSSI musí být v blízkosti hledaného zařízení. Následujícím způsobem lze určit polohu hledaného zařízení s přesností 1 až 2 metry (Coleman, a další, 2010 str. 395).

3.4.2.3 **RF kalibrace**

Další metodou k zaměření hledaného zařízení je RF kalibrace (calibration). Za pomoci bezdrátového zařízení, obvykle přenosného počítače, se pohybujeme prostorem a zjišťujeme hodnoty signálu RSSI hledaného zařízení. Následně metodou triangulace nebo otisků prstů (RF fingerprint) naměřené hodnoty vyhodnotíme a určíme tak polohu zařízení (Coleman, a další, 2010 str. 395).

3.4.2.4 **Časové rozdíly příjmů**

Poslední způsob vyhledávání bezdrátových zařízení je založen na časově rozdílných příjmech TDoA (Time difference of arrival). Zjišťujeme časy přijmutí signálu na třech a více senzorech, který byl vyslán ve stejný okamžik. Na každém senzoru dorazí signál v jiný časový okamžik, vzhledem ke vzdálenosti vysílače. Rychlost cesty rádiového signálu je známý faktor. Jestliže je hledané zařízení na polovině vzdálenosti mezi dvěma senzory, tak rozdíl časů přijmutí signálu bude nulový. Ze získaných časů z jednotlivých senzorů lze určit vzdálenost hledaného zařízení (Coleman, a další, 2010 str. 394).

Z výše popsaných technik je časová metoda TDoA nejlepší. Nepotřebuje procházet daný prostor nebo určovat polohu známých zařízení. Popsanou metodu můžeme provádět i s přenosným zařízením k dohledání přesné polohy zařízení. Obvykle se používá graf vykreslující čas přijmutí nebo zvukové znamení s navyšujícím zvukem (Coleman, a další, 2010 str. 395).

3.4.3 WIDS/WIPS analýzy

Systémy pro monitorování bezdrátových sítí sbírají mnoho dat ze senzorů. Pro vyhodnocení informací je dále potřeba analyzovat všechna data, což může být náročné. Každý systém WIDS/WIPS používá různé softwary a moduly, které zjednodušují analyzování obrovského počtu sebraných dat.

3.4.3.1 **Analýza příznaků**

Systém WIPS/WIDS používá analýzu příznaků pro zjištění vniknutí nebo napadnutí bezdrátové sítě. Známé příznaky jsou definovány v databázi systému WIPS/WIDS, která jich čítá stovky. Analýza příznaků probíhá na první a druhé vrstvě modelu OSI. Podoba hledání příznaků, vedoucí k napadnutí bezdrátové sítě, se blíží antivirovým programům a databáze s příznaky se neustále aktualizuje. Správci sítě si mohou vytvořit i vlastní příznaky útoků, které jsou specifické pro jejich bezdrátovou síť (Coleman, a další, 2010 str. 399).

3.4.3.2 **Analýzy chování**

Analýza chování bezdrátové sítě slouží k rozpoznávání změn chování od normálního chování bezdrátové sítě. Porovnává chování, jak se chovala síť při minulých měřeních. Může být velmi důležité takto sledovat síť, protože některé anomálie nedokážou být detekčním systémem odhaleny. Analýza příznaků hledala známé příznaky útoků. Analýza chování hledá nové neznámé formy útoků nebo hrozby bez příznaků (Coleman, a další, 2010 str. 398).

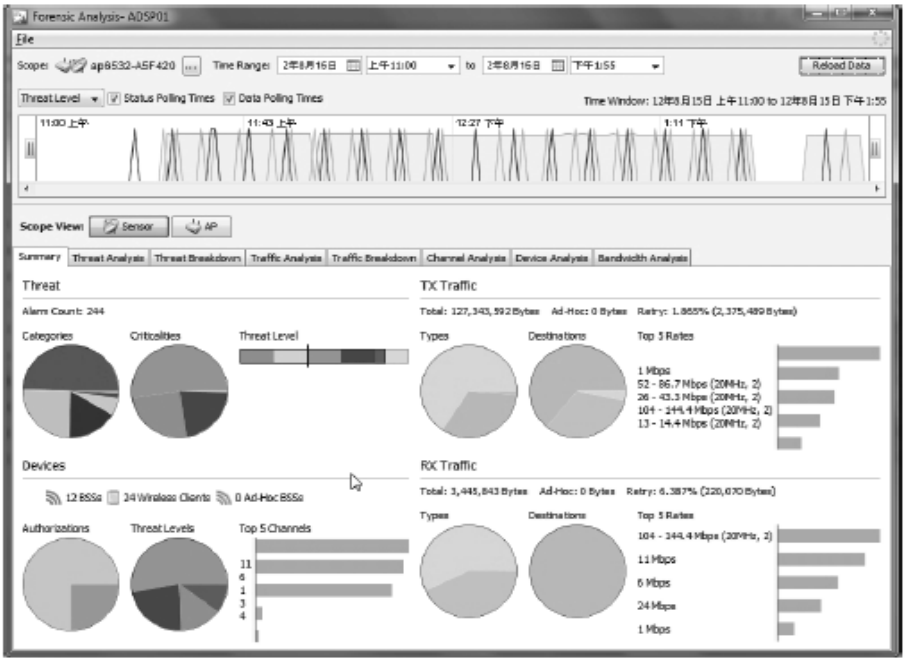
Nejúspěšnějším útokem na bezdrátovou síť se stává ten, který není ještě známý, nazývaný jako nultý den útoku (zero day attack). Obvykle se změní chování bezdrátové sítě a tato změna je detekována. Abnormality systém WIPS/WIDS dokáže hlásit správci sítě, jen se musí správně nastavit, při jaké úrovni systém bude hlásit změnu. Pokud bude nastaven citlivě, bude alarm stále upozorňovat na změny, které však nejsou nebezpečím. Jakmile by správce nastavil kontrolu změn na necitlivou úroveň, stává se síť zranitelnou (Coleman, a další, 2010 str. 399).

3.4.3.3 **Spektrální analýza**

Spektrální analýza se zabývá měřením signálu a možnými rušeními bezdrátové sítě. Měření se provádí spektrálními analyzátory. Monitorují zařízení, která nejsou uvedena ve standardu pro bezdrátové sítě a mohou to být: videokamery, bezdrátové telefony nebo mikrovlnné trouby. Všechna uvedená zařízení mohou způsobovat interference a rušit chod bezdrátové sítě. Široko-spektrální analyzátory jsou velmi drahé přístroje a tak pro menší a střední firmy jsou nedostupné. Řešením jsou analyzátory navrhnuté jen pro bezdrátové sítě, které neanalyzují celé frekvenční pásmo a jejichž cena je tak dostupná i pro menší podniky. V současnosti je nejlepší implementace analyzátorů do senzorů, které máme rozmístěné v síti. Následně můžeme analyzovat zdroje rušení 24 hodin denně (Coleman, a další, 2010 str. 400).

3.4.3.4 **Forenzní analýzy**

Forenzní analýzy se používají k rychlému vysledování akcí bezdrátového zařízení v síti a to během několika minut. Administrátor sítě tak může sledovat a přehrát záznam připojení a komunikace zařízení minutu po minutě. Analýza tak vytvoří přehled a grafy o zařízení, které může představovat určitou hrozbu. Jak můžeme vidět na následujícím obrázku (Obrázek 3-25) výsledek forenzní analýzy. Nejdříve si vybereme zařízení, o kterém chceme zjistit výsledky analýzy a nastavíme časový interval, který se má zpracovat. Ve výsledcích můžeme zjistit aktivitu zařízení, sílu signálu, odeslaná a přijímaná data. Dále jsou zaznamenány útoky a hrozby, které v historii zařízení podniklo (Coleman, a další, 2010 str. 401).



Obrázek 3-26- Výsledek forenzní analýzy (zdroj:http://www.cyberonair.com)

3.4.3.5 **Analýzy výkonnosti**

Užitečnou doplňkovou funkcí jsou analýzy výkonosti sítě. Na základě sběru velkého množství dat kvůli bezpečnosti sítě, můžeme tato data použít i ke zlepšení výkonu sítě. Odhalit dokáže nadměrný roaming mezi zařízeními, nadměrný provoz mezi bezdrátovou a drátovou sítí LAN a další údaje o provozu, které snižují výkonost bezdrátové sítě. Zjišťují se stavy bezdrátové sítě ve špičce, mimo špičku a v době kdy není

nikdo k síti připojen. Na základě těchto stavů si může administrátor utvořit lepší obraz, jak se chová bezdrátová síť (Coleman, a další, 2010 str. 403).

Analýza výkonosti probíhá po celou dobu provozu a sleduje jednotlivá zařízení. Jakmile dochází k poklesu výkonu sítě, upozorňuje administrátora alarmem dříve, než uživatel by poznal snížení výkonu sítě. Pokud budou přístupové body přetíženy opakovaně, upozorňuje to na fakt, že by se měla bezdrátová síť rozšířit o další přístupové body (Coleman, a další, 2010 str. 403).

3.4.4 Monitorování

Základem nepřetržitého monitorování je upozornění správce sítě na útoky nebo náhlé události. Upozornění nebo také alarmy je možno přednastavit, na jaké události má systém WIPS/WIDS upozorňovat. Po vyhodnocení upozornění správcem sítě provede dané úkony k jeho vyřešení. (Coleman, a další, 2010 str. 404)

3.4.4.1 **Prosazování zásad**

Prosazování zásad a pravidel v bezdrátové síti je jednou z podmínek fungující sítě. Určuje pravidla v oblasti výkonu, užití, bezpečnosti nebo použitých zařízení. Organizace si musí být jistá, že všechna zařízení dodržují stanovená pravidla a používají bezpečností protokoly. Zásady a pravidla musí být definována jak pro přístupové body tak klientská zařízení. Protože špatně nastavená zařízení v síti, jsou jedním z nejčastějších provinění proti bezpečnosti bezdrátové sítě. Pokud někdo v síti použije jiný protokol pro ověření, tak systém WIPS/WIDS spustí alarm a upozorní tak správce sítě (Coleman, a další, 2010 stránky 404 - 408).

U klientského zařízení je zásadou nastavení minimální hodnoty signálu při autentizaci z důvodu zabránění potencionálních útoků zvenčí budovy. Systém WIPS/WIDS může použít deautentizační rámce k odpojení klientského zařízení, které je špatně nakonfigurováno. Bezpečnost bezdrátové sítě je silná jen do takové míry, do které jsou dodržována pravidla a zásady (Coleman, a další, 2010 stránky 404 - 408).

3.4.4.2 **Alarmy a upozornění**

Systém WIDS/WIPS dokáže pomocí svých senzorů zachytit jakékoliv zařízení vysílající v pásmu 802.11. Jakmile detekuje jakýkoliv přenos, tak pokud je nutné upozorní na tuto skutečnost příznačným alarmem. Alarmy a upozornění se vážou k dané situaci, která vzejde od analýzy příznaků, analýzy chování, forenzní analýzy a dalších. Vyvstávají tak dále otázky, co dělat při takovém upozornění:

- Co toto upozornění znamená?
- Musím být informován o každém detekovaném zařízení?
- Kdo je zodpovědný za upozornění?
- Je systém pod útokem?
- Je dané chování normální nebo přijatelné?
- Jsou všechna následující zařízení patřící organizaci?
- Jsou zařízení organizace v bezpečí?

Na relevantní otázky je dobré si odpovědět a vyvodit řešení. V systémech WIPS/WIDS po upozornění na určitou událost následuje i doporučení, jak vyřešit problém. Navrhuje tak odpovědi na dříve vyřčené otázky ohledně bezpečnosti. Pokud se uživatel nebo návštěvník připojí do bezdrátové sítě osobním zařízením, které není zaregistrováno v organizaci, spustí tak alarm upozorňující na tuto skutečnost. Chování alarmů se liší podle výrobce systému WIDS/WIPS a také nastavením správců sítě. Alarmy můžeme rozdělit do následujících kategorií:

- Chování
- Využití
- Výkon
- Dodržování zásad
- Průzkum
- Škodící aktivity
- Chyby zabezpečení

V jednotlivých kategoriích můžeme nastavovat citlivost, kde nastavujeme v rozsahu „všechno je v pořádku“ až po maximální citlivost „jsme pod útokem“. Upozornění ze systému je možné posílat pomocí emailu, sms nebo aplikace ve smartphonu. K zasílání upozornění si vybereme jen závažnější narušení bezpečnosti bezdrátové sítě (Coleman, a další, 2010 stránky 406 - 409).

3.4.4.3 **Zprávy a hlášení**

Ve vyšších verzích systémů WIPS/WIDS můžeme generovat hlášení. Buď je můžeme generovat manuálně, nebo se vytváří automaticky podle naplánovaného kalendáře. Ukládání a zkoumání hlášení je zásada jak udržet zabezpečenou a zdravou bezdrátovou síť. Dokumentace je důležitá pro případné změny v síti, jako navýšení počtu přístupových bodů, a její předložení nadřízeným v organizaci. Hlášení pokrývá všechny části od zabezpečení, přes pokrytí až po výkon sítě (Coleman, a další, 2010 str. 410).

4 Praktická část

4.1 Napadení bezdrátové sítě se zabezpečením WPA2

V této kapitole je popsáno prolomení bezdrátové sítě se zabezpečením WPA2 s šifrováním TKIP. Testování proběhlo na přístupovém bodě vlastněném autorem práce a nebyla tak narušena jiná bezdrátová síť. K prolomení bezdrátové sítě byl použit přenosný počítač, ve kterém byl nainstalován operační systém Linux verze Backtrack 5 R3. V počítači je vhodný bezdrátový adaptér, který je možno přepnout do monitorovacího módu.

4.1.1 Backtrack 5 R3

Nástroj Backtrack 5 R3 je linuxová distribuce, jež umožňuje testování bezpečnosti nejen bezdrátových, ale i kabelových sítí. Z bezdrátových sítí můžeme jmenovat například: Wi-Fi, bluetooth a WiMAX. Celý nástroj je zajímavý tím, že jej používají jak hackeři tak, správci sítí a je bezplatně ke stažení na internetu.

V distribuci systém můžeme spouštět z Live DVD nebo jej nainstalovat na počítač. Live DVD znamená, že po vložení disku do mechaniky je zaveden operační systém a na daný počítač se nic neinstaluje, což je výhodou pro mnoho uživatelů. Systém Backtrack obsahuje nástroje seřazené v následujících kategoriích:

- Enumerace
- Využití slabin
- Scannery
- Zjištění hesel
- Hledání slabin kódu
- Maskování
- Tunelovací protokol
- Odchytávání paketů
- Nástroje pro bezdrátové sítě
- Forensní nástroje

- Reversní inženýrství
- Databázové nástroje
- Bluetooth nástroje
- Cisco nástroje

V dalších kapitolách bude popsán útok pomocí této linuxové distribuce Backtrack.

4.1.2 Nastavení přístupového bodu

Jako přístupovým bod byl použit ASUS WL500g premium. V nastavení byl zapnut DHCP server pro automatické přidělování IP adres z rozsahu 192.168.178.20 – 192.168.178.60. Jméno bezdrátové sítě bylo nastaveno na DPWLAN (DP – diplomová práce) vysílaném na třetím kanálu s automatickým přepínáním rychlostí přenosu na základě signálu.

Šifrovací metoda byla zvolena WPA-PSK, kde u následujícího modelu zařízení se jedná o WPA2-Personal. Dále si můžeme toto označení zabezpečení WPA2 ověřit na obrázku skenování sítí (Obrázek 4-3). Jako WPA klíč bylo zvoleno heslo **5up3123x417**. Protokol byl zvolen TKIP, které je slabší než AES a tedy snáze prolomitelné. Celé nastavení přístupového bodu je možno vidět na následujícím obrázku (Obrázek 4-1).

Obrázek 4-1- Nastavení přístupového bodu (zdroj: autor práce)

4.1.3 Nastavení bezdrátového adaptéru

Jestliže máme v počítači vhodný adaptér pro přepnutí do monitorovacího režimu, tak použijeme následující příkazy. Nejdříve adaptér aktivujeme, což se provede příkazem:

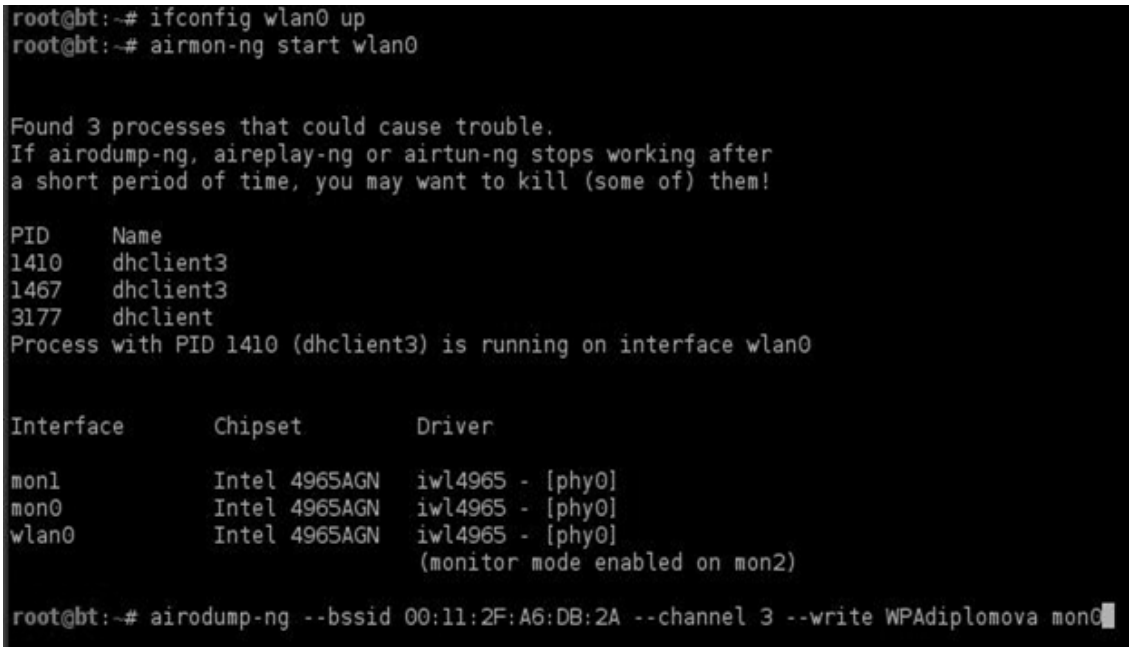
ifconfig wlan0 up

Ifconig slouží pro nastavení síťových adaptérů v počítači. Wlan0 je označení základního adaptéru v přenosných počítačích pro bezdrátový adaptér. Funkce **up** daný adaptér povolí.

Když bezdrátový adaptér je zprovozněn, musíme jej uvést do monitorovacího režimu. To provedeme příkazem:

airmon-ng start wlan0

Příkaz airmon-ng start je spuštění aplikace pro nahrání driverů pro monitorování. Wlan0 je jen výběr adaptéru, na který chceme použít příkaz. Sled příkazů je na následujícím obrázku (Obrázek 4-2).



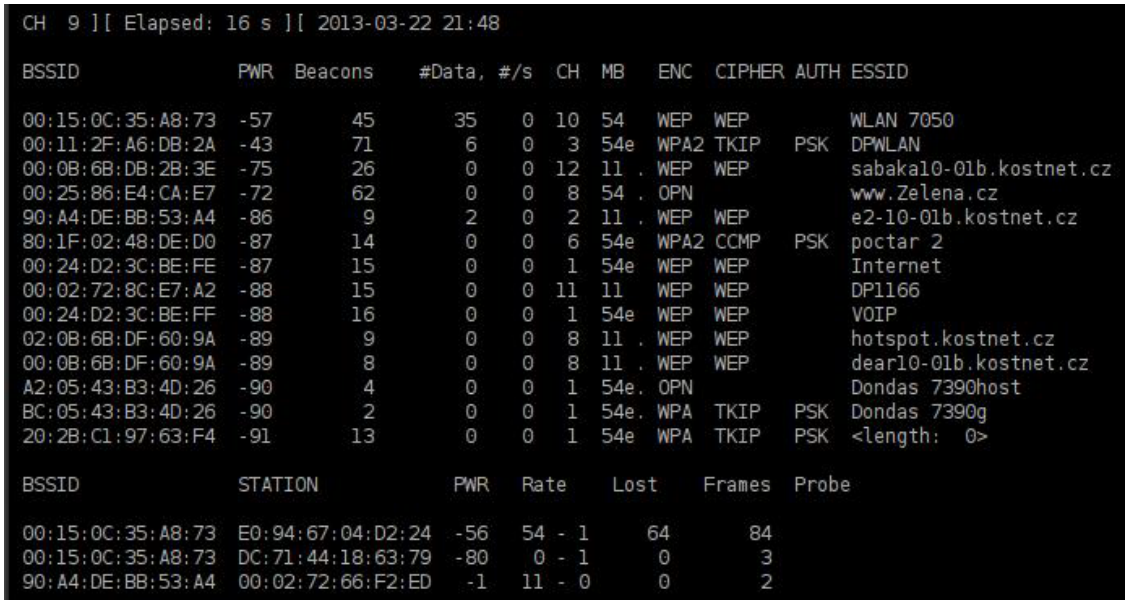
Obrázek 4-2 - Příprava bezdrátového adaptéru do monitorovacího módu (zdroj: autor práce)

4.1.4 Zachycení paketů autentizace

Nejprve prohledáme kanály v okolí, abychom nalezli cíl našeho útoku. Zjistíme základní údaje o vysílaném přístupovém bodu. Prohledávání kanálů začneme příkazem:

airdump-ng mon0

Kde airdump-ng je utilita pro skenování a zachytávání komunikace. Mon0 opět vybere adaptér pro monitorování a dále se s ním budeme setkávat v příkazech. Na obrázku (Obrázek 4-3) pak můžeme vidět informace o našem přístupovém bodu. BSSID je MAC adresa přístupového bodu 00:11:2F:A6:DB:2A, které vysílá na kanálu 3. Šifrováním WPA2 a protokolem TKIP. Ve sloupci ESSID jsou uvedeny názvy sítí. Dále jsou uvedeny informace o síle signálu, vyslaných rámcích a režimu rychlosti zařízení.



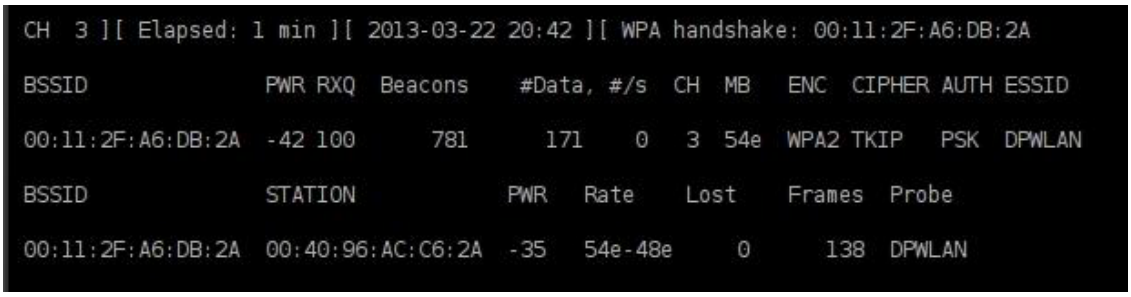
Obrázek 4-3- Skenování okolních sítí, naším cílem je DPWLAN (zdroj: autor práce)

Po nastavení prohledání kanálů v okolí, nastavíme odposlech komunikace mezi zařízeními. Pro útok použijeme zachycení počáteční komunikace, nazývané v angličtině handshake. Při této komunikaci dochází mezi zařízeními k jejich vzájemnému ověření.

Pro zachytávání a ukládání komunikace mezi zařízeními použijeme příkaz za použití nástroje airodump-ng a to:

airodump-ng --bssid 00:11:2F:A6:DB:2A --channel 3 --write WPAdiplomova mon0

Když identifikujeme příkaz, tak bssid je MAC adresa přístupového bodu, od kterého budeme zachytávat komunikaci na kanále 3 a budeme zapisovat (--write) do souboru WPAdiplomova. Soubor vygenerovaný bude mít příponu .cap (od slova capture) a budeme s ním dále pracovat. Samotné zachycení komunikace můžeme vidět na obrázku dole (Obrázek 4-4). Jakmile zachytíme komunikaci připojení nového uživatele, bude to zobrazeno v pravém horním rohu, kde je potvrzeno WPA hadnshake. Budeme odchytávat pakety, dokud se některé zařízení nebude přihlašovat k přístupovému bodu.



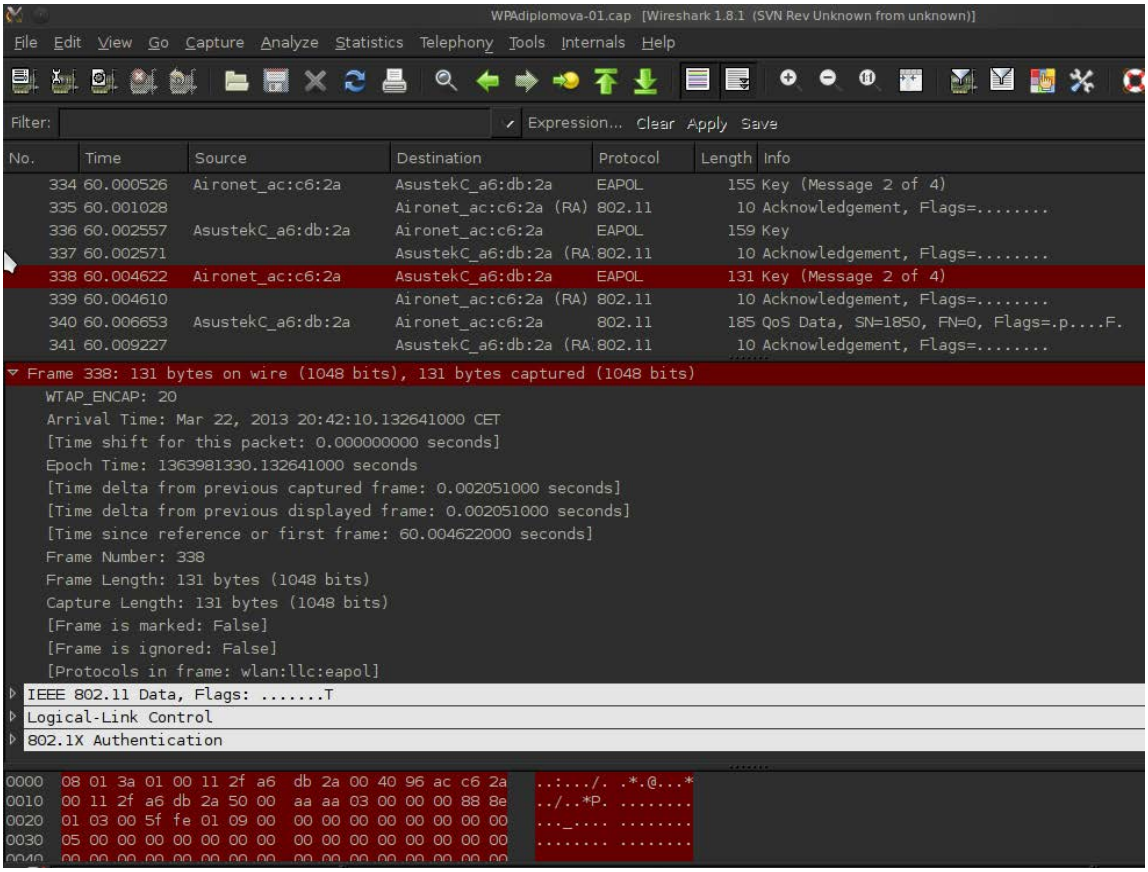
Obrázek 4-4- Zachycení komunikace oveřování (zdroj: autor práce)

Doba, než se připojí nový uživatel, by mohla být velmi dlouhá a tak můžeme toto zrychlit pomocí příkazu deautentizace. Ovlivníme tak všechna zařízení přihlášená k přístupovému bodu a odpojíme je. To bude mít za následek, že se zařízení znovu přihlásí a zachytíme ověřovací komunikaci. K tomuto postupu nám pomůže příkaz:

aireplay-ng --deauth 0 -a 00:11:2F:A6:DB:2A -e DPWLAN mon0

4.1.5 Analýza paketů

Po úspěšném zachycení komunikace mezi zařízeními zkontrolujeme soubor WPAdiplomova-01.cap. V souboru najdeme protokol s názvem EAPOL, kterým probíhala komunikace handshake při ověřování (Obrázek 4-5). K prohlížení souboru jsem použil program Wireshark, který slouží pro zachytávání a analýzu paketů, ale umožňuje i filtrovat zobrazené pakety podle typu a také provádět analýzy.



Obrázek 4-5 - Program Wireshark, který analyzuje odchytlé pakety (zdroj: autor práce)

4.1.6 Získání hesla

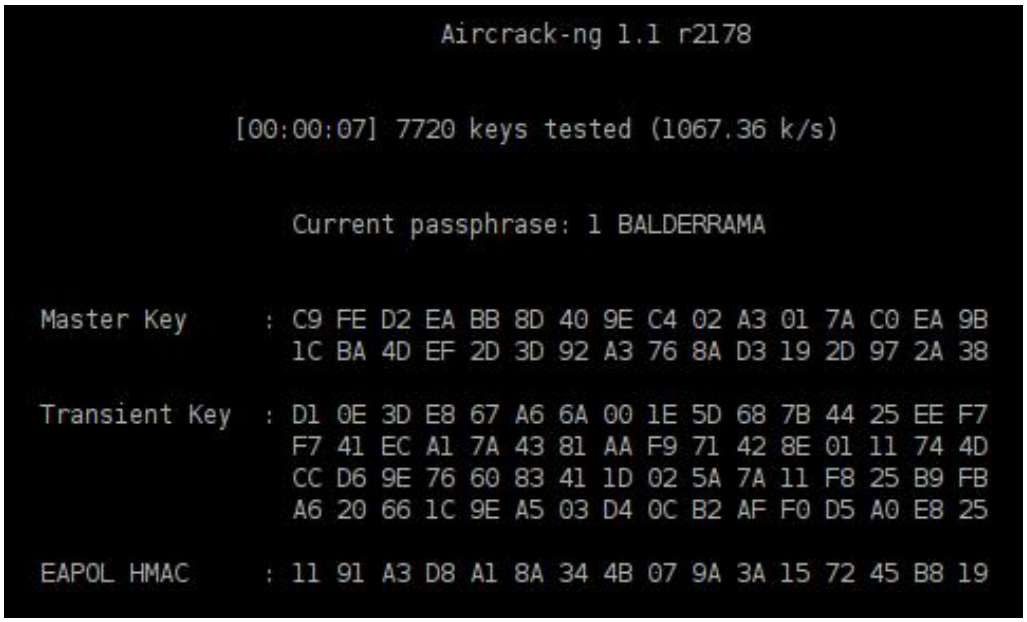
Získání hesla bude probíhat na základě ověřování a hledání příslušného hesla ve slovnících hesel. Je to jediný snadný způsob, jak prolomit heslo. Další způsoby jsou technicky velmi náročné na hardware. Úspěšnost útoku na WPA2 v tomto případě závisí na tom, jak dobrý máme slovník hesel. Uvedená distribuce linuxu Backtrack již slovník

hesel obsahuje, ale speciální slovník pro konkrétní zemi by zvýšil pravděpodobnost nalezení správného hesla. Zároveň i obsáhlejší slovník míru úspěšnosti zvyšuje.

Pro zjištění hesla použijeme aircrack-ng a slovník hesel darkc0de, ve kterém se budeme pokoušet nalézt heslo. K analýze nám poslouží zachycená komunikace handshake mezi zařízeními. Použijeme následující příkaz:

aircrack-ng WPAdiplomova-01.cap -w /pentest/passwords/wordlists/darkc0de.lst

Následuje hledání hesla, kde se postupně testují hesla. Na obrázku (Obrázek 4-6) je vidět čas testování a kolik hesel již bylo testováno (7720). Dále je zobrazeno testované heslo (1 BALDERRAMA) a počet klíčů testovaných za sekundu (1067 k/s). V dolní části je hlavní klíč, transitní klíč a protokol EAPOL.



Obrázek 4-6 - Hledání přístupového fráze do bezdrátové sítě (zdroj: autor práce)

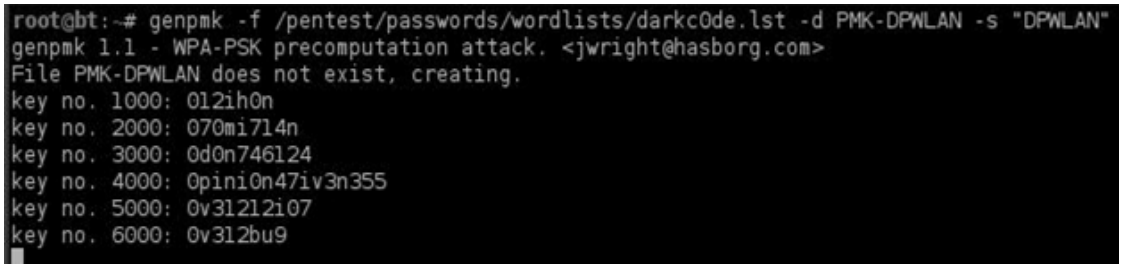
Přibližně po otestování asi 100 tisíc klíčů se podařilo získat heslo do sítě DPWLAN. Můžeme tak vidět na obrázku (Obrázek 4-7), kde je zobrazen i hlavní klíč. Podařilo se nám tak získat heslo, které jsme zadali do přístupového bodu.

Obrázek 4-7 – Přístupová fráze byla nalezena (zdroj: autor práce)

Hledání hesel je hardwarově náročné. Výkonný počítač zvýší rychlost vyhledávání hesla neboť databáze hesel jsou velmi obsáhlé. Existuje další způsob jak zrychlit prohledávání klíčů a to vytvořením nového listu hlavních klíčů (nazývaný PMK – Pairwise Master Key) přímo pro aircrack-ng, který bude vytvořen na základě SSID jména přístupového bodu, který chceme napadnout.

List hlavních klíčů vygenerujeme spojením hesla a názvem přístupového bodu. Použijeme příkaz:

genpmk -f /pentest/passwords/wordlists/darkc0de.lst –d PMK-DPWLAN –s „DPWLAN“



Obrázek 4-8 - Vytváření databáze hesel pro DPWLAN (zdroj: autor práce)

Dále si již použije nově vytvořený list s hlavními klíči k hledání hesla. Čas vyhledání hesla se tak zkracuje na 20 % oproti předchozímu pokusu. Příkaz je zobrazen na obrázku (Obrázek 4-9).

Obrázek 4-9 - Příkaz pro zjištění hesla pomocí vytvořené databáze hesel (zdroj: autor práce)

4.2 Monitorování bezdrátové sítě

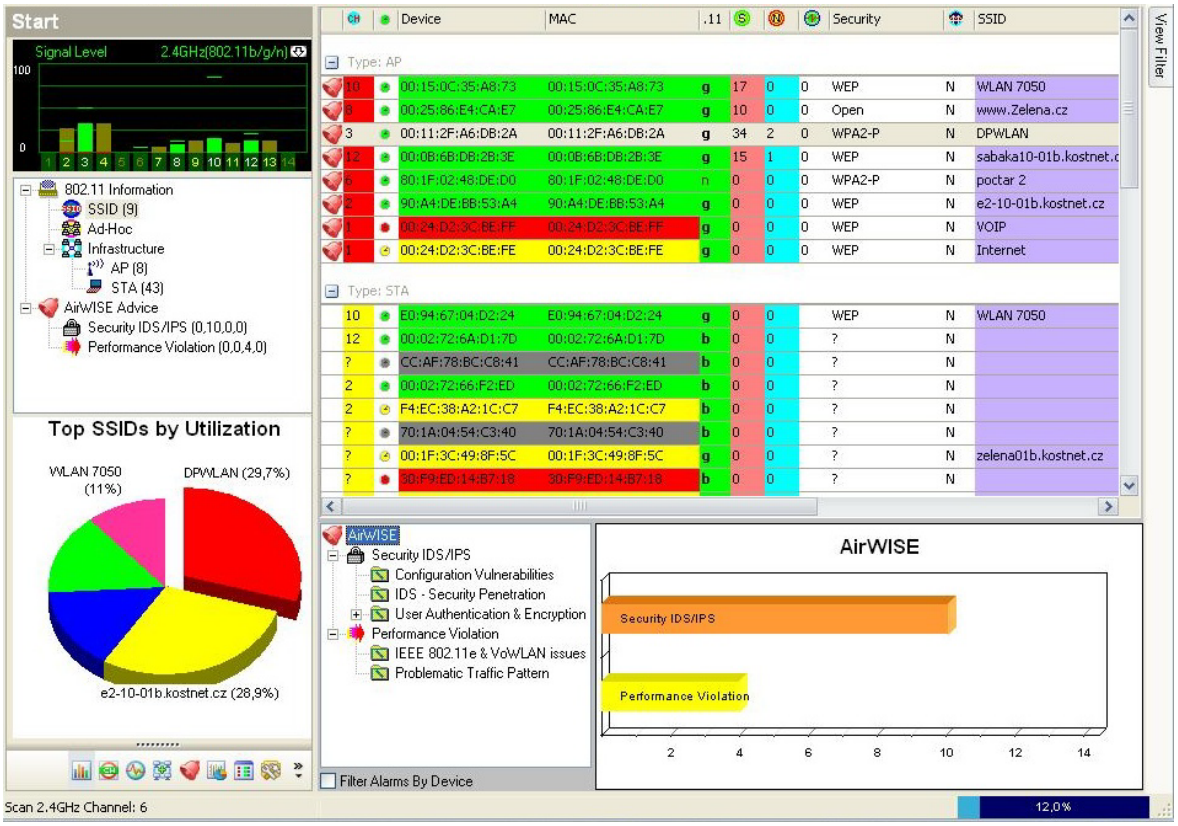
Jak bylo již zmíněno, v předešlých kapitolách, monitorování sítě je neméně důležité jako zabezpečení sítě samotné. V následujících kapitolách se zaměřím na sledování bezdrátové sítě DPWLAN (kanál 3) a pokusím se vyhodnotit možné problémy u bezdrátové sítě.

K monitorování bezdrátové sítě budeme používat program AirMagnet od stejnojmenné společnosti ve verzi 7.5. Program slouží k analýze bezdrátové sítě a jde o mobilní verzi systému detekce narušeních WIPS/WIDS.

4.2.1 Analýza bezdrátové sítě

Po spuštění programu vidíme přehledně přístupové body a stanice k nim připojené. O každém přístupovém bodu jsou informace jako MAC adresa, síla signálu, použité zabezpečení a jméno vysílané sítě SSID (Obrázek 4-10). U přístupových bodů, kde hrozí určité nebezpečí, je ikona červeného zvonku. Ta upozorňuje na možné nebezpečí v zabezpečení nebo problém bezdrátové sítě. Tato upozornění spravuje srdce celého analyzátoru a to AirWISE. V pravém dolním rohu je zobrazen sloupcový graf, kde je patrno počet identifikovaných problémů se zabezpečením (Security IDS/IPS) a počet porušení v oblasti hardwaru.

Dále je možno vidět využití jednotlivých přístupových bodů na kruhovém grafu. Vidíme zde, že naše bezdrátová síť DPWLAN je využita z 29,7%. V levém horním rohu monitoru je spektrum kanálů s úrovní signálů.

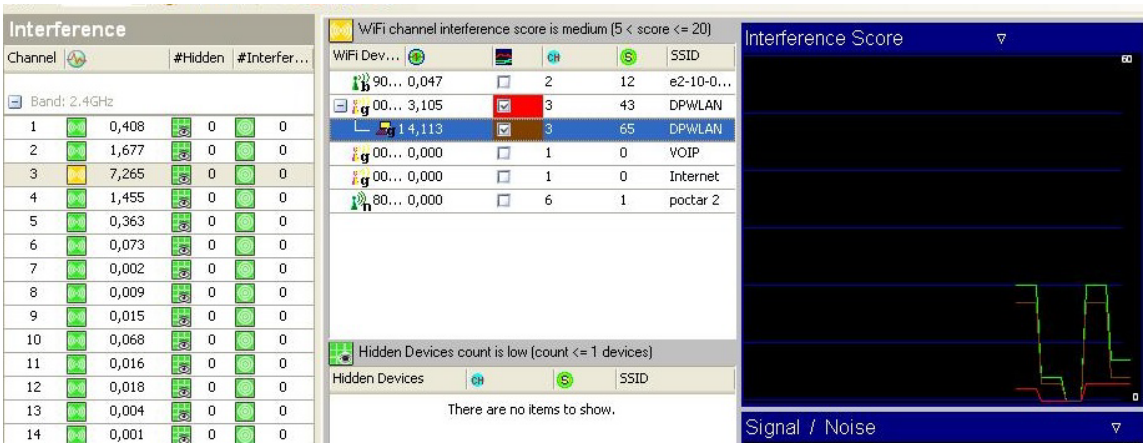


Obrázek 4-10 - AirMagnet - Live Capture - souhrn přístupových bodů a zařízení (zdroj: autor práce)

4.2.2 Spektrální analýza

Spektrální analýza se zabývá interferencemi mezi kanály. Způsobovat interferenci může celá řada zařízení jako mikrovlnné trouby, bezdrátové telefony a videokamery. Mimo uvedené přístroje může být interference způsobena i dalšími jevy. Například při poslání deautentizačního rámce na přístupový bod se začne objevovat interference na použitém kanálu (kanál 3) a dokonce i na sousedních kanálech 2 a 4. Tento jev můžeme vidět na následujícím obrázku (Obrázek 4-11), kde jsou vidět jednotlivé kanály.

Pokud interferenční skóre je do čísla 5, tak se jedná o slabou interferenci, skóre 5 až 20 je střední a 20 a více je vysoká interference. Jenom kanál 3, na kterém je náš přístupový bod, má střední interferenci označenou žlutou ikonou, jinak ostatní kanály jsou jen se slabou interferencí. Výsledkem spektrální analýzy je tedy stanovisko, že nedochází k závaznějším interferencím.

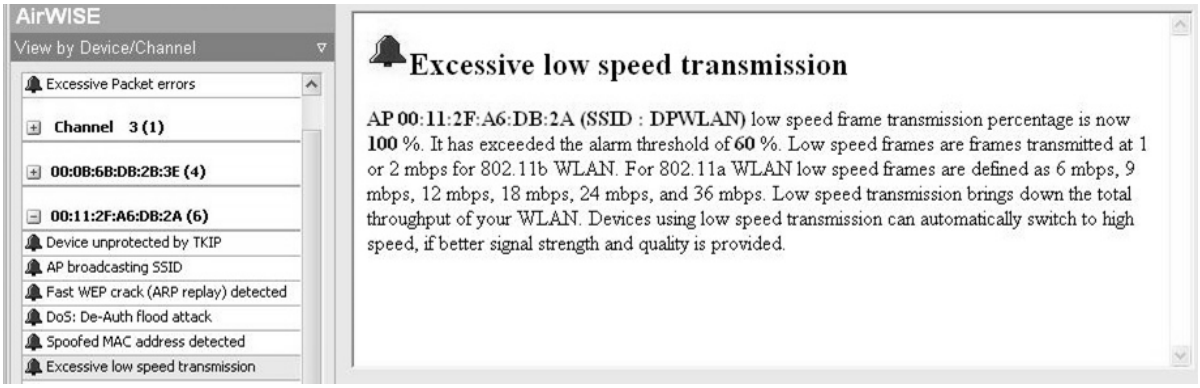


Obrázek 4-11 - Spektrální analýza bezdrátové sítě (zdroj: autor práce)

4.2.3 Upozornění na útoky a výstrahy

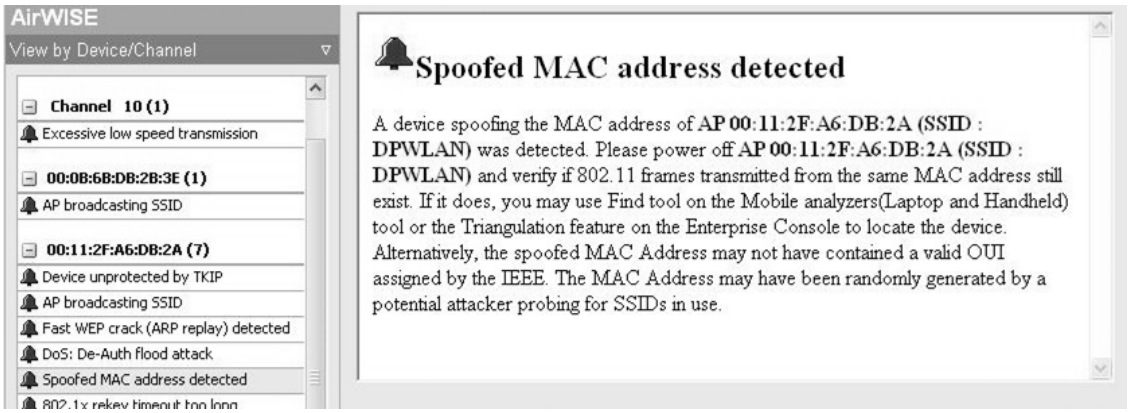
Prostředí AirWISE upozorňuje na možná nebezpečí zabezpečení nebo nastavení bezdrátové sítě a navrhuje možná řešení problémů. U bezdrátové sítě DPWLAN nalezlo jisté nedostatky a vydalo několik upozornění.

Prvním nedostatkem je nízká přenosová rychlost, která je způsobena slabým signálem. Z toho vyplývá nízká celková propustnost bezdrátové sítě. Na následujícím obrázku (Obrázek 4-12) je upozornění na tento problém s vysvětlením, proč nastalo. Pokud je slabý signál, je snížena rychlost přepnutím zařízení do pomalejšího režimu. Obvykle to bývají rychlosti 1 až 2 mb/s. Navrhovaným řešením je zesílení signálu a kvality příjmu. Toho docílíme výměnou antény na přístupovém bodě nebo zařazením dalšího přístupového bodu pro zvýšení signálu.



Obrázek 4-12 - AirWISE upozornění na nízkou propustnost sítě (zdroj: autor práce)

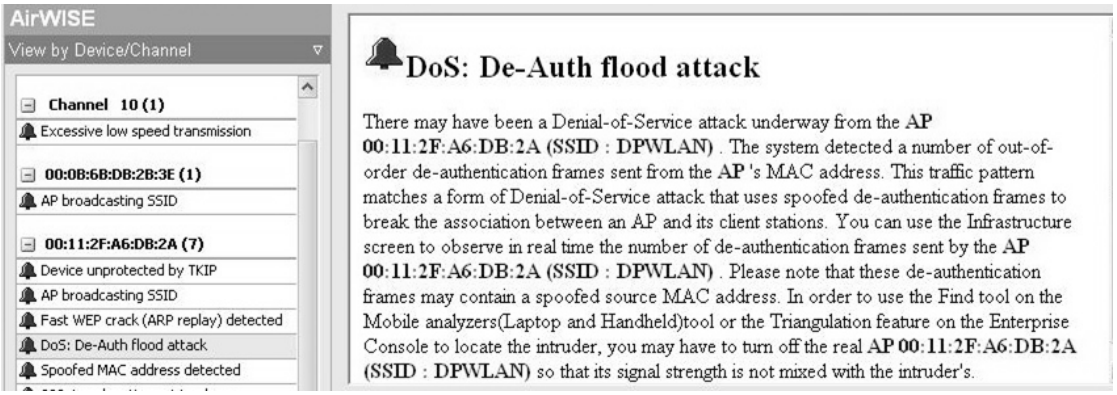
Dalším upozorněním je detekce zařízení, které má stejnou MAC adresu jako přístupový bod naší bezdrátové sítě (Obrázek 4-13). Toto zjištění naznačuje útok na přístupový bod a jde o pokus vytvořit škodný přístupový bod, na který by se připojila klientská zařízení z bezdrátové sítě DPWLAN. Doporučení, jak se bránit popsanému útoku, je vypnout přístupový bod a snažit se nalézt zařízení triangulací nebo další popsanou metodou vyhledávání zařízení. Vyhledávání může probíhat přímo programem AirMagnet. Praktickému vyhledávání zařízení se budu věnovat v další kapitole.



Obrázek 4-13 - AirWISE detekováno zařízení s falešnou MAC adresou (zdroj: autor práce)

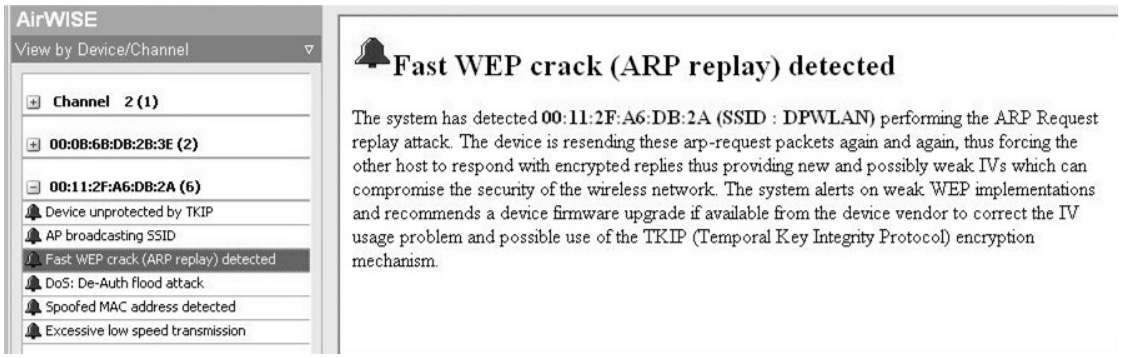
Následujícím upozorněním je výstraha před deautentizačním útokem (Obrázek 4-14). Bylo zjištěno zasílání deautentizačních rámců. Následkem je odpojení všech zařízení od přístupového bodu a musí proběhnout opětovné připojení. Způsob zasílání těchto rámců se používá k zachycení úvodní komunikace mezi zařízeními. Deautentizační rámce byly vyvolány útokem z přenosného počítače s linuxovou distribucí Backtrack.

Navrhovaným řešením pro tuto situaci, je nalezení útočníka triangulací jako v předchozím případě.



Obrázek 4-14 - AirWISE zjištěn útok pomocí deautentizačního rámce (zdroj: autor práce)

Posledním zjištěným útokem na bezdrátovou síť je navození umělého provozu (Obrázek 4-15). Útočník se snaží zachytit co největší množství paketů pro následné vyhodnocení a zjištění přístupového hesla do bezdrátové sítě. Navrhovaným řešením je implementace silnějšího zabezpečení bezdrátové sítě. Případné řešení může být i v aktualizaci zařízení a použití jiného šifrování.



Obrázek 4-15 - AirWISE zjištění útoku na zabezpečení bezdrátové sítě

4.3 Vyhledání škodlivého zařízení v bezdrátové síti

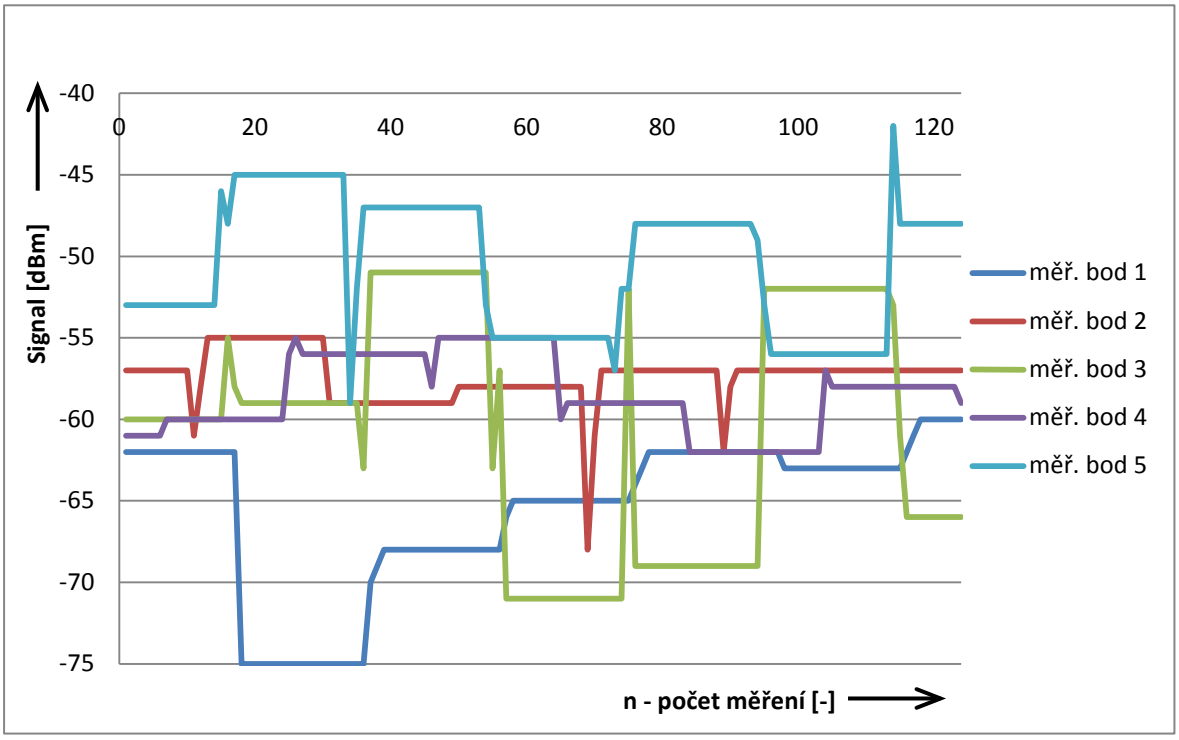
Nalezení škodlivého zařízení (přístupového bodu) bude probíhat na základě dříve popsané metody triangulace. Signál zařízení se bude měřit na 5 měřících bodech, které je možné vidět na schématu (Obrázek 4-16) a bude měřeno v dBm (udává sílu signálu v dB na 1 mW). Měřit se bude dvěma způsoby. Pomocí přenosného počítače programem AirMagnet a chytrým telefonem s operačním systémem Android a programem Wifi Analyzer. Z výsledků měření se bude následně určovat poloha a zaměření škodlivého zařízení.

Obrázek 4-16 - Schéma budovy s označenými měřícími body (zdroj: autor práce)

4.3.1 Hledání zařízení pomocí AirMagnet

Hledání zařízení pomocí přenosného počítače a softwaru AirMagnet bude probíhat měřením signálu v jednotlivých měřících bodech. Signál v každém měřícím bodu se bude měřit po dobu 30 sekund, aby došlo k případnému vyloučení chyby měření. Hodnoty budou zaznamenány a vyhodnoceny graficky. Výsledkem bude průměrná hodnota signálu v každém bodu a následné grafické vyobrazení na plánu budovy.

Na následujícím grafu (Obrázek 4-17) je možno vidět výsledky měření v jednotlivých měřících bodech. V grafu jsou patrné rušivé vlivy okolí, kde se signál skokově zlepšil, nebo se objevily tzv. špičky. Po dobu měření 30 sekund program zaznamenal 124 hodnot signálu. Všechny tyto hodnoty jsou v tabulce v přílohách.

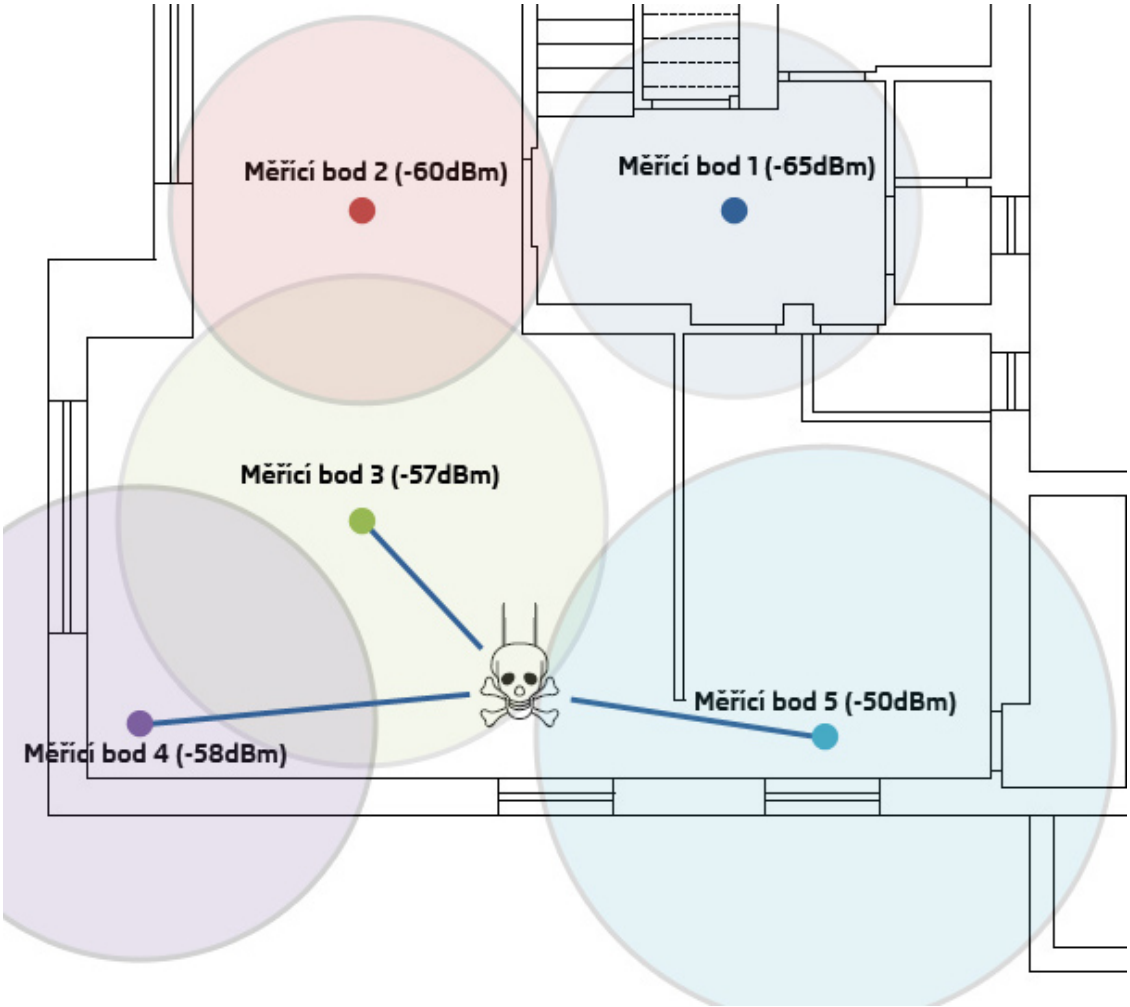


Obrázek 4-17 - Měření signálu škodlivého přístupového bodu Airmagnet (laptop) (zdroj: autor práce)

V následující tabulce (Tabulka 1) jsou uvedeny průměrné hodnoty z jednotlivých měřících bodů. Nejvyšší hodnota byla naměřena u měřícího bodu číslo 5 a to -50,47dBm. Z toho vyplývá, že škodlivý přístupový bod se bude nacházet v blízkosti tohoto bodu. Ze známých měřících pozic byla určena přibližná lokace hledaného zařízení.

	měř. bod 1	měř. bod 2	měř. bod 3	měř. bod 4	měř. bod 5
průměrná hodnota (dBm)	**-65,50**	**-60,59**	**-57,38**	**-58,46**	**-50,47**

Tabulka 1 - Průměrné naměřené hodnoty signálu na jednotlivých měřících bodech (zdroj: autor práce)



Obrázek 4-18 - Grafické schéma budovy s vyhodnocením a zjištěním přibližné polohy škodlivého zařízení (zdroj: autor práce)

Vyhodnocení je graficky vyobrazeno na schématu budovy (Obrázek 4-18). Dále jsou zaneseny naměřené hodnoty u jednotlivých měřících bodů a graficky vynesen signál v podobě kružnic okolo měřících bodů. Metodou triangulace byly vybrány 3 měřící body s nejvyšším signálem. Mezi těmito měřícími body je hledané zařízení. Vzdálenost hledaného zařízení je blíže měřícím bodům, které mají vyšší signál.

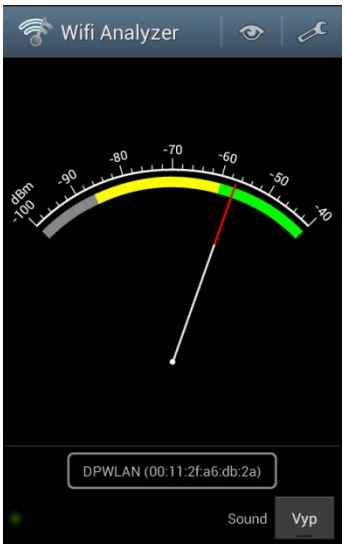
4.3.2 Hledání zařízení pomocí Wifi Analyzer

Dalším způsobem jak vyhledat škodlivé zařízení je pomocí chytrého telefonu s použitím programu Wifi Analyzer. Signál se bude snímat postupným průchodem 5 měřících bodů. V každém měřícím bodě bude zařízení ustáleno v přesné pozici a poté sejmuta hodnota pomocí funkce screenshot (uložení obrázku obrazovky (Obrázek 4-19)). Následujícím způsobem projdeme měřící body pětkrát po sobě.

n - měření	měř. bod 1	měř. bod 2	měř. bod 3	měř. bod 4	měř. bod 5
1	-73	-53	-54	-60	-48
2	-73	-62	-60	-63	-59
3	-71	-65	-55	-65	-54
4	-72	-60	-59	-70	-56
5	-70	-66	-53	-53	-57
průměrná hodnota (dBm)	**-71,8**	**-61,2**	**-56,2**	**-62,2**	**-54,8**

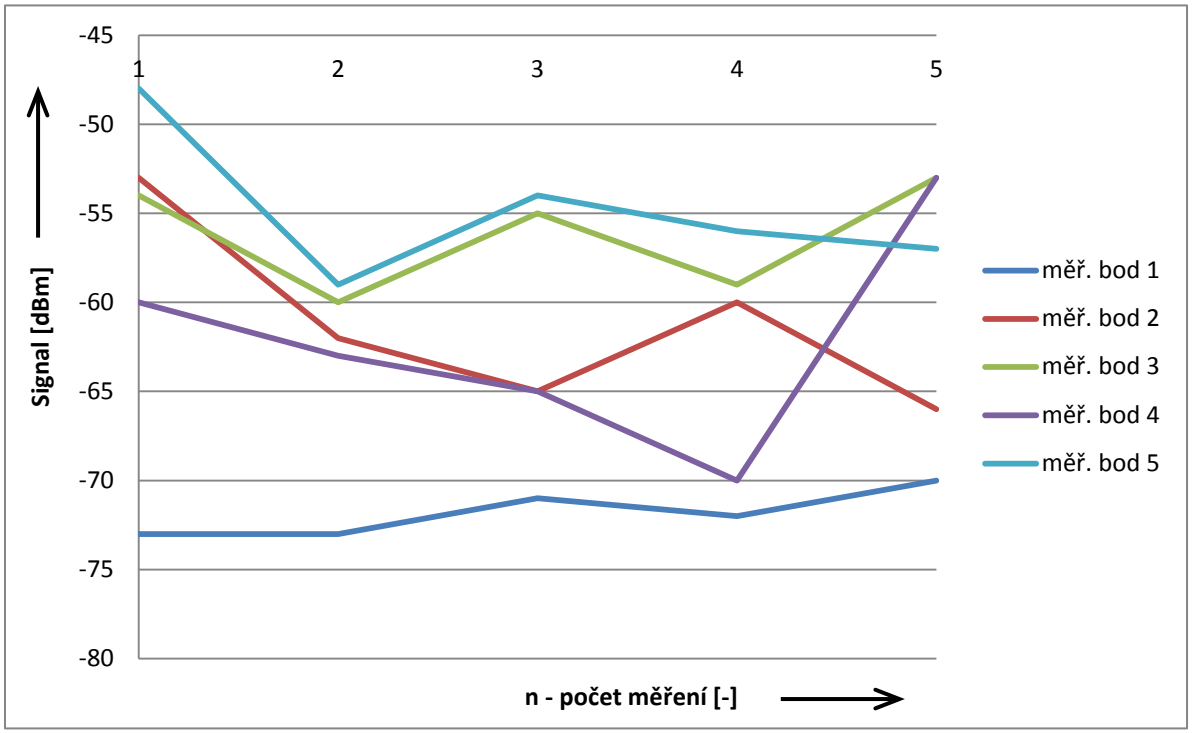
Tabulka 2 - Naměřené hodnoty úrovní signálu v měřících bodech pomocí Wifi Analyzer (zdroj: autor práce)

V tabulce (Tabulka 2) jsou vidět naměřené hodnoty signálu a spočtená průměrná hodnota. S nejvyšším signálem byl vyhodnocen měřící bod 5 s -54,8dBm. Můžeme tedy předpokládat, že škodlivý bod, bude v jeho blízkosti.



Obrázek 4-19 - Wifi Analyzer (zdroj: autor práce)

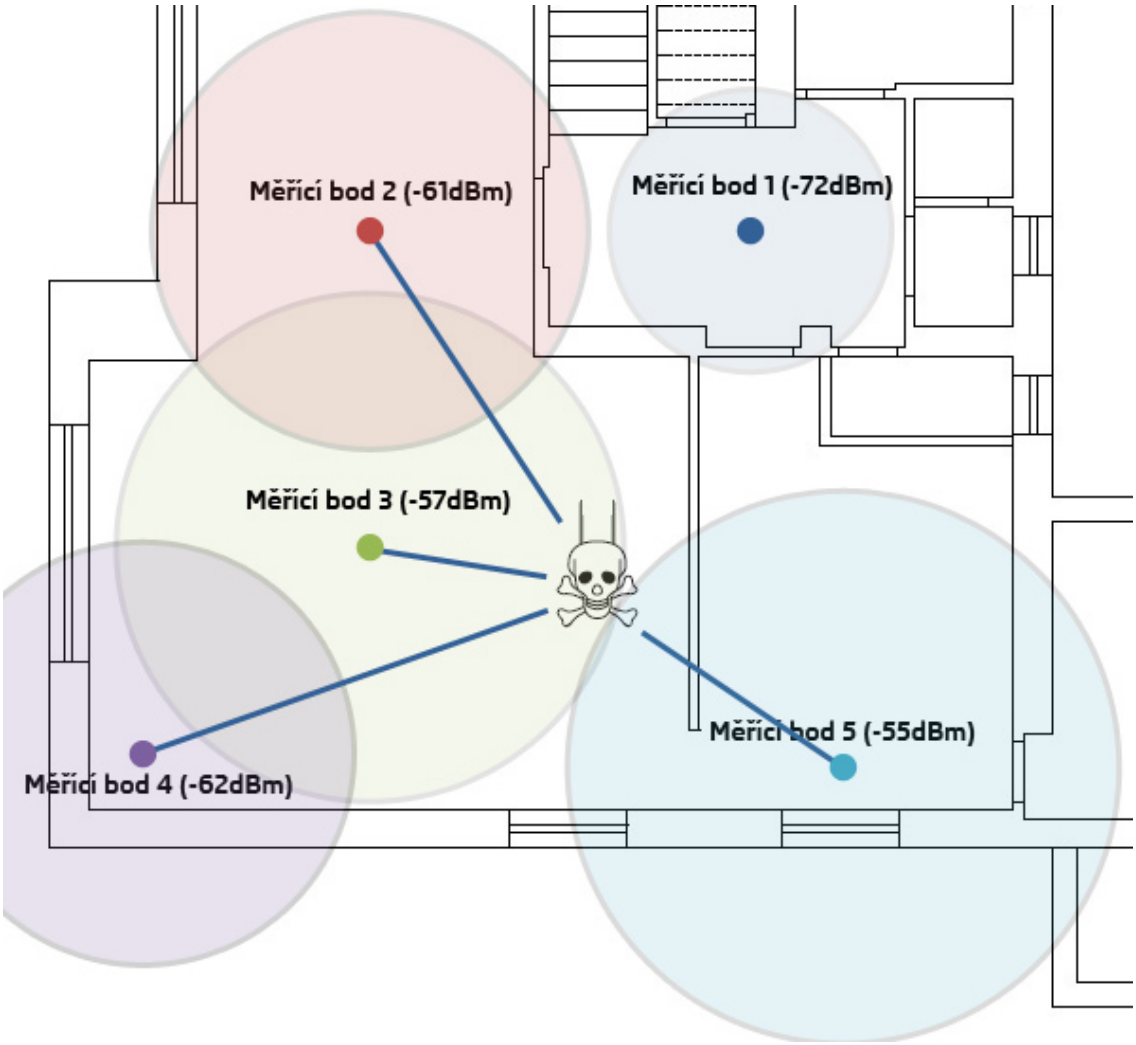
Grafické vyobrazení signálu v jednotlivých měřících bodech je vidět na následujícím grafu (Obrázek 3-16). V měřících bodech 2 a 4 došlo při měřeních 4 a 5



Obrázek 4-20 - Měření signálu škodného přístupového bodu pomocí Wifi Analyzer (zdroj: autor práce)

k výrazným odchylkám oproti předcházejícím hodnotám. Tato výrazná odchylka mohla být způsobena rušením nebo chybou měření. I přes výrazné nedostatky měření, kdy se snímala jen jedna hodnota signálu v měřícím bodě, tak na následujícím schématu budovy (Obrázek 4-21) se zakreslenými hodnotami signálu v měřících bodech, je výsledkem přibližné zaměření škodlivého přístupového bodu. S ohledem na přesnost triangulace, kde odhadovaná přesnost je zaměření zařízení do 10 metrů.

V měřícím bodu 4 a 2 jsou signály téměř totožné a proto jsou zařazeny oba měřící body do hledání pozice škodlivého zařízení. Zařízení se bude s velkou pravděpodobností nacházet blízko spojnice mezi měřícími body 3 a 5. Signál zachycený v těchto bodech je téměř stejný (měřící bod 3 = -57dBm a měřící bod 5 = -55dBm). Z teorie vychází, pokud by byl signál rovný v obou měřících bodech, leželo by zařízení přesně v rovině proložené osou spojnice mezi těmito body.



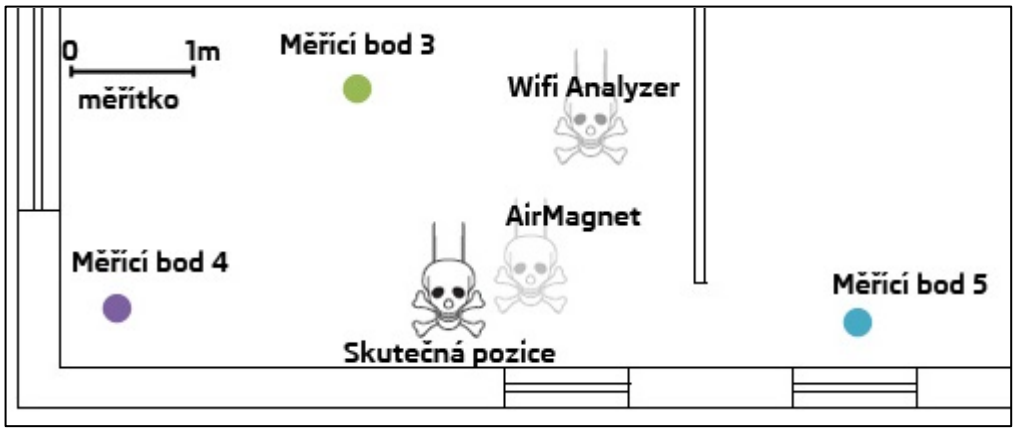
Obrázek 4-21 - Schéma budovy se zaměřeným škodlivého zařízení pomocí Wifi Analyzer (zdroj: autor práce)

5 Výsledky a diskuse

Praktická část, zabývající se napadením bezdrátové sítě se zabezpečením WPA2 dokazuje, že nevhodně nastavené zabezpečení WPA2 lze prolomit. Jednou ze slabin zabezpečení je heslo do bezdrátové sítě, které je třeba volit dostatečně silné a mělo by se skládat z velkých a malých písmen, číslic a případně dalších tisknutelných znaků. Útok na zabezpečenou bezdrátovou síť v rámci praktické části trval přibližně 5 minut a z toho samotné prolomení klíče 2 minuty. Tyto časy, ale i úspěšnost útoku, závisí na heslu do bezdrátové sítě.

Monitorováním bezdrátové sítě DPWLAN bylo zjištěno, že je třeba zvyšovat propustnost sítě. Ta závisí na signálu přístupového bodu a řešením je instalace silnější antény nebo změna umístění zařízení. Systém WIPS detekoval zařízení se změněnou MAC adresou, kde se mohlo jednat o zařízení útočníka. Ověření funkce monitorovacího systému bylo provedeno útokem na bezdrátovou síť. Útok byl detekován a byla navrhnuta nová bezpečnostní opatření. Výsledkem spektrální analýzy bylo zjištěno, že na kanálu 3 vysílaném sítí DPWLAN je nízká interference (rušení). Zajímavým výsledkem bylo, že interference se může vyvolat zasíláním deautentizačních rámců na přístupový bod.

Závěrečná část praktické části se věnovala vyhledávání škodlivého zařízení v bezdrátové síti. Využívaly se 2 typy zařízení pro vyhledávání, které změřily signál škodlivého zařízení v 5 měřících bodech. Prvním zařízením byl přenosný počítač s programem, který zjišťoval aktuální sílu signálu a zaznamenával ji do souboru po dobu 30 sekund. Měřením bylo získáno 124 hodnot síly signálu a vysoký počet hodnot zajišťuje



Obrázek 5-1 - Srovnání výsledků zaměření škodlivého zařízení (zdroj: autor práce)

vyšší přesnost naměřených výsledků. Z výsledků měření byla určena poloha škodlivého zařízení s přibližnou přesností do 2 metrů od skutečné polohy zařízení, jak je vidět na schématu (Obrázek 5-1).

Druhým vyhledávacím zařízením byl chytrý telefon se softwarem Wifi Analyzer. Zde je výsledek měření zatížen větší chybou z důvodů sběru pouze 5 hodnot v každém měřícím bodě a nižší citlivostí zařízení. Škodlivé zařízení v tomto případě bylo zaměřeno s přesností do 3 metrů od skutečné polohy zařízení. Srovnání vyhledávacích technik je vidět na obrázku (Obrázek 5-1).

6 Závěr

Bezdrátové sítě jsou a budou velmi užívané jak v domácí sféře, tak v korporátní. Tato diplomová práce upozornila na možná bezpečnostní rizika a prakticky ukázala prolomení bezpečnosti bezdrátové sítě. Byla prolomena bezdrátová síť se zabezpečením WPA2. Uživateli nebo správci sítě může tato práce pomoci s výběrem prostředků a postupů ve zvolení vhodného zabezpečení tak splnila cíl a shrnula možná zabezpečení bezdrátové sítě.

Monitorováním bezdrátové sítě bylo dokázáno, že samo monitorování je významným nástrojem pro ochranu a zlepšování výkonu sítě. Jednotlivé analýzy bezdrátové sítě v praktické části poukázaly na nedostatky, které je potřeba vyřešit. Monitorování bezdrátové sítě se ukázalo jako prvek, který by měly korporátní instituce používat ke zvýšení bezpečnosti. Lze tak čelit hrozbě útoků a zlepšovat provoz sítě.

Jeden z posledních cílů práce bylo nalezení škodlivého zařízení v bezdrátové síti. Škodlivé zařízení bylo nalezeno 2 odlišnými nástroji a bylo zjištěno, že se zařízení podařilo vyhledat s menší odchylkou, než se uvádí v teoretické části. Přínosem je nalezení škodlivého zařízení, které po zneškodění již dále nenarušuje bezpečnost bezdrátové sítě.

Diplomová práce tak splnila stanovené cíle a shrnula možná zabezpečení bezdrátové sítě.

7 Seznam použitých zdrojů

Coleman, David, a další. 2010. *CWSP Certified Wireless Security Professional.* Indianapolis : Wiley Publishing, 2010. ISBN 978-0-470-43891-6.

Chaouchi, Hakima a Laurent-Maknavicius, Maryline. 2009. *Wireless and Mobile Network Security.* Hoboken : John Wiley & Sons, Inc., 2009. ISBN 978-1-84821-117-9.

Lupa.cz. 2012. Co je to přístupový bod. *Lupa.cz.* [Online] 15. Listopad 2012. [Citace: 15. Listopad 2012.] http://tutorialy.lupa.cz/jak-na-wifi/access-point-co-to-je-a-cim-se-lisi/.

Nathan J., Muller. 2003. *Wi-Fi for the enterprise.* New York : McGraw-Hill Professional, 2003. ISBN 978-0-07-141252-0.

Pužmanová, Rita. 2005. *Bezpečnost bezdrátové komunikace - Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G.* Brno : CP Books, 2005. ISBN 80-251-0791-4.

Stüber, Gordon. 2004. *Broadband MIMO-OFDM Wireless.* [Dokument PDF] 2004.

Wi-Fi_Alliance. 2013. Wi-Fi Alliance. *Wi-Fi Alliance.* [Online] 15. Leden 2013. [Citace: 15. Leden 2013.] http://www.wi-fi.org/about/organization.

Zandl, Patrick. 2003. *Bezdrátové sítě WiFi.* Praha : Computer Press, 2003. stránky 1-3. ISBN 80-7226-632-2.

8 Přílohy

Příloha č. 1 – Naměřené hodnoty úrovně signálu AirMagnet

Příloha č. 2 – Srovnání výsledků zaměření škodlivého zařízení

Příloha č. 1 – Naměřené hodnoty úrovně signálu AirMagnet (zdroj: autor práce)

n	měř. bod 1	měř. bod 2	měř. bod 3	měř. bod 4	měř. bod 5
1	-62	-60	-57	-61	-53
2	-62	-60	-57	-61	-53
3	-62	-60	-57	-61	-53
4	-62	-60	-57	-61	-53
5	-62	-60	-57	-61	-53
6	-62	-60	-57	-61	-53
7	-62	-60	-57	-60	-53
8	-62	-60	-57	-60	-53
9	-62	-60	-57	-60	-53
10	-62	-60	-57	-60	-53
11	-62	-60	-61	-60	-53
12	-62	-60	-58	-60	-53
13	-62	-60	-55	-60	-53
14	-62	-60	-55	-60	-53
15	-62	-60	-55	-60	-46
16	-62	-55	-55	-60	-48
17	-62	-58	-55	-60	-45
18	-75	-59	-55	-60	-45
19	-75	-59	-55	-60	-45
20	-75	-59	-55	-60	-45
21	-75	-59	-55	-60	-45
22	-75	-59	-55	-60	-45
23	-75	-59	-55	-60	-45
24	-75	-59	-55	-60	-45
25	-75	-59	-55	-56	-45
26	-75	-59	-55	-55	-45
27	-75	-59	-55	-56	-45
28	-75	-59	-55	-56	-45
29	-75	-59	-55	-56	-45
30	-75	-59	-55	-56	-45
31	-75	-59	-59	-56	-45
32	-75	-59	-59	-56	-45
33	-75	-59	-59	-56	-45
34	-75	-59	-59	-56	-59
35	-75	-59	-59	-56	-52
36	-75	-63	-59	-56	-47
37	-70	-51	-59	-56	-47

n	měř. bod 1	měř. bod 2	měř. bod 3	měř. bod 4	měř. bod 5
38	-69	-51	-59	-56	-47
39	-68	-51	-59	-56	-47
40	-68	-51	-59	-56	-47
41	-68	-51	-59	-56	-47
42	-68	-51	-59	-56	-47
43	-68	-51	-59	-56	-47
44	-68	-51	-59	-56	-47
45	-68	-51	-59	-56	-47
46	-68	-51	-59	-58	-47
47	-68	-51	-59	-55	-47
48	-68	-51	-59	-55	-47
49	-68	-51	-59	-55	-47
50	-68	-51	-58	-55	-47
51	-68	-51	-58	-55	-47
52	-68	-51	-58	-55	-47
53	-68	-51	-58	-55	-47
54	-68	-51	-58	-55	-53
55	-68	-63	-58	-55	-55
56	-68	-57	-58	-55	-55
57	-66	-71	-58	-55	-55
58	-65	-71	-58	-55	-55
59	-65	-71	-58	-55	-55
60	-65	-71	-58	-55	-55
61	-65	-71	-58	-55	-55
62	-65	-71	-58	-55	-55
63	-65	-71	-58	-55	-55
64	-65	-71	-58	-55	-55
65	-65	-71	-58	-60	-55
66	-65	-71	-58	-59	-55
67	-65	-71	-58	-59	-55
68	-65	-71	-58	-59	-55
69	-65	-71	-68	-59	-55
70	-65	-71	-61	-59	-55
71	-65	-71	-57	-59	-55
72	-65	-71	-57	-59	-55
73	-65	-71	-57	-59	-57
74	-65	-71	-57	-59	-52
75	-65	-52	-57	-59	-52
76	-64	-69	-57	-59	-48

n	měř. bod 1	měř. bod 2	měř. bod 3	měř. bod 4	měř. bod 5
77	-63	-69	-57	-59	-48
78	-62	-69	-57	-59	-48
79	-62	-69	-57	-59	-48
80	-62	-69	-57	-59	-48
81	-62	-69	-57	-59	-48
82	-62	-69	-57	-59	-48
83	-62	-69	-57	-59	-48
84	-62	-69	-57	-62	-48
85	-62	-69	-57	-62	-48
86	-62	-69	-57	-62	-48
87	-62	-69	-57	-62	-48
88	-62	-69	-57	-62	-48
89	-62	-69	-62	-62	-48
90	-62	-69	-58	-62	-48
91	-62	-69	-57	-62	-48
92	-62	-69	-57	-62	-48
93	-62	-69	-57	-62	-48
94	-62	-69	-57	-62	-49
95	-62	-52	-57	-62	-53
96	-62	-52	-57	-62	-56
97	-62	-52	-57	-62	-56
98	-63	-52	-57	-62	-56
99	-63	-52	-57	-62	-56
100	-63	-52	-57	-62	-56
101	-63	-52	-57	-62	-56
102	-63	-52	-57	-62	-56
103	-63	-52	-57	-62	-56
104	-63	-52	-57	-57	-56
105	-63	-52	-57	-58	-56
106	-63	-52	-57	-58	-56
107	-63	-52	-57	-58	-56
108	-63	-52	-57	-58	-56
109	-63	-52	-57	-58	-56
110	-63	-52	-57	-58	-56
111	-63	-52	-57	-58	-56
112	-63	-52	-57	-58	-56
113	-63	-52	-57	-58	-56
114	-63	-53	-57	-58	-42
115	-63	-61	-57	-58	-48

n	měř. bod 1	měř. bod 2	měř. bod 3	měř. bod 4	měř. bod 5
116	-62	-66	-57	-58	-48
117	-61	-66	-57	-58	-48
118	-60	-66	-57	-58	-48
119	-60	-66	-57	-58	-48
120	-60	-66	-57	-58	-48
121	-60	-66	-57	-58	-48
122	-60	-66	-57	-58	-48
123	-60	-66	-57	-58	-48
124	-60	-66	-57	-59	-48
průměr	**-65,5**	**60,58870968**	**-57,37903226**	**-58,45967742**	**-50,46774194**

Příloha č. 2 – Srovnání výsledků zaměření škodlivého zařízení (zdroj: autor práce)