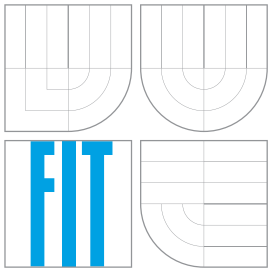
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

BEZPEČNOSTNÍ ANALÝZA WIFI SÍTÍ

SECURITY ANALYSIS OF WIFI NETWORKS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — MICHAL BUTELA
AUTHOR

VEDOUCÍ PRÁCE — DANIEL CVRČEK
SUPERVISOR

BRNO 2007

Zadání

Bezpečnostní analýza WiFi sítí

Security Analysis of WiFi Networks

Vedoucí:
Cvrček Daniel, doc. Ing., Ph.D., UITS FIT VUT

Oponent:
Malinka Kamil, Mgr., UITS FIT VUT

Přihlášen:
Butela Michal, Bc.

Zadání:

1. Vytvořte přehled a popis jednotlivých typů bezpečnostních mechanismů a přístupů k zajištění bezpečnosti bezdrátových sítí. Mechanismy budou pokrývat oblasti důvěrnosti a integrity dat, účtovatelnosti, autentizace, dostupnosti a auditu.
2. Proveďte analýzu a porovnání vybraných typů bezpečnostních mechanismů.
3. Proveďte testování systémů pro zajištění důvěrnosti a integrity dat a jejich vliv na rychlost a propustnost dané sítě. Mezi testovanými systémy budou WEP, WPA, WPA2, příp. IPSec a vhodné systémy na aplikační úrovni.
4. Proveďte analýzu a praktické odzkoušení dostupných nástrojů pro provádění útoků na systémy z bodu 3.
5. Vypracujte studii správného použití šifrovacích a autentizačních mechanismů z hlediska bezpečnosti, správy a uživatelské přívětivosti.

Část požadovaná pro obhajobu SP:
Body 1-3

Kategorie:
Bezpečnost

Literatura:

- Gavrilenko, Mikhailovksy, Mulbery: Wi-Foo: The Secrets of Wireless Hacking, Addison Wesley, 2004.

Licenční smlouva

Licenční smlouva je uložena v archivu Fakulty informačních technologii Vysokého učeni technického v Brne.

Abstrakt

Tento dokument popisuje prehľad bežne dostupných a používaných štandardov a mechanizmov pre zabezpečenie bezdrôtovej siete založenej na protokole Wi-Fi. Pokrýva všetky dôležité oblasti bezpečnosti zahrňujúc utajenie, integritu aj autentifikáciu. Prítomný je detailný rozbor a popis funkcie jednotlivých mechanizmov. Nasleduje popis možných útokov proti jednotlivým druhom zabezpečenia. V ďalších častiach dokumentu je zmeraný vplyv šifrovania na prenosovú rýchlosť. Ďalej sú to útoky na jednotlivé zabezpečovacie mechanizmy a napokon popis nasadenia centrálnej autentizácie.

Klíčová slova

Wi-Fi, 802.11, WEP, WPA, EAP, bezpečnost, analýza, BUSLab

Abstract

This document provides overview of commonly used standards and mechanisms for securing the wireless network based on Wi-Fi protocol. It is covering all important security areas including confidentiality, integrity and authentication. We can find here also detailed analysis and description of functionality of listed mechanisms. Description of possible attacks against listed security mechanisms. There is a measurement of influence of encryption to transfer speed in the another section. It's followed by attacks against particular security mechanisms. And finally, description of deployment of central authentication system.

Keywords

Wi-Fi, 802.11, WEP, WPA, EAP, security, analysis, BUSLab.

Citace

Michal Butela: Bezpečnostní analýza WiFi sítí, diplomová práce, Brno, FIT VUT v Brně, 2007

Bezpečnostní analýza WiFi sítí

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Daniela Cvrčka

. . . . . .
Michal Butela
22. května 2007

Obsah

Kapitola 1

Úvod

V dnešnej dobe je bezdrôtové pripojenie do počítačovej siete čoraz bežnejšie a rozšírenejšie. Je to veľmi pohodlný a efektívny spôsob ako pripojiť do siete notebook, alebo zasieťovať budovu, kde nie je možné nainštalovať klasickú drôtovú sieť. Keď vezmeme do úvahy výrazné zvyšovanie predaja notebookov, v ktorých je Wi-Fi karta prakticky povinnou výbavou, tak zhotovenie bezdrôtovej siete je neraz aj výhodnou alternatívou z hľadiska ekonomického. Takéto riešenie ale so sebou prináša aj riziká, ktoré sú neraz skryté alebo často podceňované. Bezdrôtové pripojenie pomocou štandardu Wi-Fi alebo protokolu 802.11 je principiálne realizované ako všesmerové rádiové vysielanie. Takéto rádiové vlny môže zachytiť s pomocou vhodného vybavenia prakticky ktokoľvek. Z tohoto dôvodu boli navrhnuté a nasadené viaceré zabezpečovacie mechanizmy. Niektoré sú viac, iné menej bezpečné. Mnohý správcovia sietí, respektívne prevádzkovatelia domácich bezdrôtových sietí vôbec svoje siete nezabezpečujú, alebo ich zabezpečujú nedostatočne. Je to zvyčajne spôsobené nedostatočnými informáciami z oblasti sieťovej bezpečnosti, zastaralým HW nepodporujúcim aktuálne rozšírenia alebo pohodlnosťou a podceňovaním situácie. V nasledujúcich kapitolách tejto práce je prehlad jednotlivých bezpečnostných mechanizmov, ich analýza a porovnanie. Nasleduje meranie ich vplyvu na efektivitu sieťového prenose a napokon štúdia vhodnosti ich nasadenia pre konkrétnu bezdrôtovú sieť.

Kapitola 2

IEEE 802.11

Štandard IEEE 802.11 je viac známy pod označením Wi-Fi. Je to protokol pre sieťovú komunikáciu, ktorý pracuje na prvej a druhej vrstve ISO/OSI modelu. Tento štandard bol prijatý roku 1997. Na jeho základe boli v nasledujúcich rokoch prijaté ďalšie štandardy z rodiny 802.11x, ktoré zdokonalovali, rozširovali a dopĺňali pôvodnú špecifikáciu. Prenos dát je uskutočňovaný elektromagnetickým vlnením na voľnom frekvenčnom pásme 2,4 GHz, prípadne v pasme 5 GHz. Protokol definuje najmä prenosové rýchlosti, frekvenčné pásma, formát dátových rámcov, fyzickú adresáciu sieťových prvkov a riešenie kolízii pri prenose. Prvotný návrh definoval prenosovú rýchlosť do 2 Mbs. Kedže je prenos bezdrôtový, sila signálu je závislá na množstve a type prekážok medzi vysielacom a prijímacom. Čím viac prekážok, tým väčšia strata signálu a následne aj zníženie rýchlosti. V praxi sú teda prenosové rýchlosti približne polovičné ako oficiálne rýchlosti, ktoré môžu byť dosiahnuté len za ideálnych podmienok, ako je priama viditeľnosť a žiadne kolízie na zdielanom médiu. V priebehu niekoľkých rokov boli vypracované a do praxe zavedené ďalšie štandardy, ktoré predovšetkým zvyšujú prenosovú rýchlosť. Medzi ne patria 802.11a, 802.11b a 802.11g. Porovnanie vlastností je v nasledujúcej tabuľke 2.1. Prevzaté z encyklopédie Wikipedia [4]

Protokol	**Rok uvedenia**	**Frekvencia**	**Modulacná rých.**	**Prenosová rých.**
802.11	1997	2.4 GHz	2 Mbps	1 Mbps
802.11a	1999	5.15-5.875 GHz	54 Mbps	25 Mbps
802.11b	1999	2.4 GHz	11 Mbps	6.5 Mbps
802.11g	2003	2.4 GHz	54 Mbps	25 Mbps
802.11n	2008	2.4 alebo 5 GHz	540 Mbps	200 Mbps

Tabulka 2.1: Prehlad štandardov.

2.1 802.11

Tento pôvodný protokol prvý krát definoval bezdrôtový prenos, v praxi nazývaný WiFi. Popisoval dve prenosové rýchlosti 1 Mbs a 2 Mbs. špecifikoval prenos s využitím infračerveného svetla ako aj s využitím elektromagnetických vĺn v pásme 2.4 Ghz. K praktickej implementácii s využitím IR svetla ale nikdy nedošlo. Štandard zahŕňa aj mechanizmus na riešenie kolízií. Kedže vzduch (el.-magnetické vlny) sú vo svojej podstate zdielaným médiom, je potrebné problém kolízií riešit. Použitou metódou je CSMA/CA - Carrier Sense Multiple Access / Collision Avoidance. Táto umožňuje na rozdiel od CSMA/CD, používanej na Eth-

ernete, kolíziám predchádzať a tak lepšie využívať prenosové pásmo. Táto prvotná verzia nebola masovo rozšírená aj keď bola implementovaná v zariadeniach od viacerých výrobcov.

2.2 802.11a

Štandard 802.11a bol prijatý v roku 1999 a v porovnaní s pôvodnou verziou má niekoľko zmien. Hlavnou z nich je navýšenie prenosovej rýchlosti na teoretické maximum 54 Mbs. V praxi je ale bežné približne 25 Mbs. Rýchlosť môže byť v prípade potreby znížená na hodnotu 48, 64, 24, 12, 9 alebo 6 Mbs. Dalšou podstatnou odlišnosťou je aj presun do pásma 5 Ghz. Z toho vyplýva že sieťové prvky pracujúce podľa tohto štandardu nie sú kompatibilné s verziami pre 2.4 Ghz. Výhodou presunu do tohto pracovného pásma je zamedzenie interferencií s inými vlnami v pôvodnom voľnom pásme 2.4 Ghz. Nevýhodou je menší dosah vysielaného signálu pri rovnakej sile. Z týchto dôvodov nie je táto verzia široko nasadzovaná a rozšírená.

2.3 802.11b

Táto verzia prispela k masovému rozšíreniu a nasadeniu bezdrôtového prenosu. Prispelo k tomu najmä možnosť použitia vo voľnom nelicencovanom frekvenčnom pásme 2.4 Ghz ako aj výrazné zvýšenie rýchlosti v porovnaní s prvotnou špecifikáciou. Maximálny prenos je koncipovaný na hranici 11 Mbs, v praxi sa však pohybuje okolo 7 Mbs pri použití UDP a 6 Mbs pri TCP protokole. Signál má väčší dosah v porovnaní s verziou 208.11a. Typicky sa pohybuje na úrovni 30m pri rýchlosti 11 Mbs. So zväčšujúcou sa vzdialenosťou klesá prenosová rýchlosť. Tá sa dokáže adaptovať na silu signálu a podla potreby sa prepnúť na jeden z pomalších režimov: 5.5, 2 a 1 Mbs. Táto verzia je v tomto období najrozšírenejšia.

2.4 802.11g

Tretia modifikácia bolo ratifikovaná v roku 1993. Jej rozšírenie nadviazalo na úspechy verzie 802.11b. V porovnaní s ňou priniesla výhody v podobe zvýšenia prenosovej rýchlosti až na 54 Mbs. Typicky však okolo 25 Mbs. Pracuje v rovnakom frekvenčnom pásme 2.4 Ghz. Zariadenia s podporou tohoto štandardu by mali by? spätne kompatibilné so zariadeniami verzie 802.11b. Pri móde kompatibility sa samozrejme zníži prenosová rýchlosť na pôvodnú hodnotu. Dosah vĺn pri verzii 802.11g je vyšší ako u jeho predchodcov. Maximálna rýchlosť sa však dramaticky znižuje s narastajúcou vzdialenosťou Inými slovami, maximálna prenosová rýchlosť je silno závislá na malých vzdialenostiach a priamej viditeľnosti. Prenosové rýchlosti ležia v rozsahu 6 - 54 Mbs. Pri spolupráci so sieťovým prvkom generácie 802.11b sa prepne na jednu s rýchlostí 11, 5.5, 2 alebo 1 Mbs.

2.5 802.11n

Návrh na tento štandard bol predložený v roku 1994. V roku 1996 vznikla tzv. Draft verzia, ktorá ale nebola organizáciou IEEE schválená a bola tak vrátená na ďalšie spracovanie a úpravy. Finálna verzia špecifikuje prenosovú rýchlosť až 540 Mbs. V reálnom nasadení sa tak počíta s pásmom približne 200 Mbs. To je približne 10 krát viac než verzia 802.11a alebo 802.11g. So schválením finálnej podoby štandardu sa počíta v priebehu rokov 2007 až 2008. Napriek tomu sa už v predaji vyskytujú implementácie založené na Draft špecifikácii.

2.6 Doplňujúce štandardy

Do rodiny štandardov 802.11x patrí aj množina ďalších, ktoré rozširujú či doplňujú funkčnosť vymenovaných protokolov. Zaoberajú sa napríklad bezpečnosťou, alebo zabezpečovaním kvality služieb. Medzi patrí napríklad:

- 802.11e – Quality of Service
- 802.11i – Enhanced security
- 802.11j – Japan extensions

Do tejto skupiny patrí aj množstvo ďalších štandardov, mnohé z nich sú v štádiu schvaľovania. V nasledujúcich kapitolách sa budem zaoberať práve bezpečnostnými mechanizmami a rozšíreniami, ktoré sú pre Wi-Fi nevyhnutné. Nebezpečenstvo odpočúvania prenosu spočíva na samotnej podstate zdielaného prenosového média - elektromagnetických vĺn.

Kapitola 3

Zabezpecenie IEEE 802.11

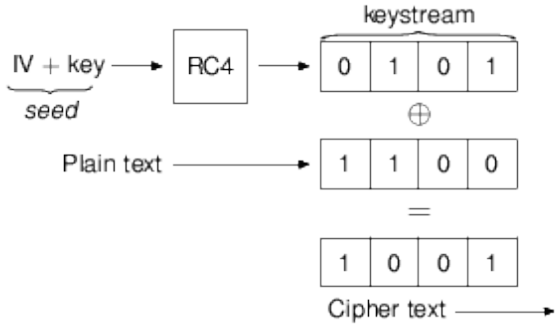
Zabezpečenie bezdrôtového prenosu je veľmi obsiahla a komplikovaná oblasť, tak ako bezpečnosť v oblasti IT sama osebe. Každý bezpečnostný mechanizmus, ci protokol by mal typicky zahŕňa tri oblasti:

- Confidentalitity – dôvernosť = ochrana proti neoprávnenému prezradeniu informácie
- Integrity – integrita = ochrana proti neoprávnenej modifikácii informácie
- Accesibility – dostupnosť = ochrana proti neoprávnenému odopretiu prístupu k dátam

Tieto tri oblasti sú pokryté každým zo zabezpečovacích schém. Medzi ne patria najmä mechanizmy zvané WEP (Wired Equivalent Privacy), ktorý je definovaný v samotnom štandarde 802.11. Pokročilými riešeniami sú WPA a WPA2 (Wi-Fi Protected Access). WPA2 je definované v samostatnom štandarde 801.11i a WPA je jeho podmnožinou, ktorá bola zavedená do praxe rok pred prijatím tohoto oficiálneho štandardu. Všetky tri normy zabezpečujú dôvernosť, integritu aj dostupnosť, ale líšia sa v pokročilosti mechanizmov, ktorými sú tieto vlastnosti zaručené. Volanie po vzniku samostatného pokročilého štandardu 802.11i bola zapríčinená nájdením závažných bezpečnostných dier v pôvodnom zabezpečovacom mechanizme. V nasledujúcich kapitolách bližšie popíšem princíp fungovania každého z nich.

3.1 WEP

Schéma WEP bola zahrnutá v pôvodnej špecifikácii 802.11 ako jediný a dostačujúci mechanizmus, ktorý poskytoval bezpečnosť. Skratka WEP znamená "Wired Equivalent Privacy", co môžeme voľne preložiť ako: "súkromie ekvivalentné ku komunikácii po drôte". Táto schéma používa prúdový kryptovací algoritmus RC4 na zašifrovanie dát a CRC na zabezpečenie integrity. Šifrovanie RC4 je symetrického typu, čo znamená že kódovanie aj dekódovanie prebehne využitím rovnakého algoritmu a použije sa ten istý kľúč. V tomto prípade je to 64 bitový šifrovací kľúč, ktorý vznikne zreťazením 40 bitového tajného kľúča a 24 bitovej hodnoty inicializačného vektoru. Vektor vznikne za použitia generátoru pseudonáhodných čísel. Algoritmus tento 64 bitový kľúč spracuje a vygeneruje šifrovací reťazec. Samotné zašifrovanie potom prebehne operáciou XOR medzi šifrovacím reťazcom a dátami. Znázornenie postupu je na nasledujúcom obrázku 3.1. Popis podľa Wikipedia [9].



Obrázek 3.1: šifrovanie

3.2 WPA

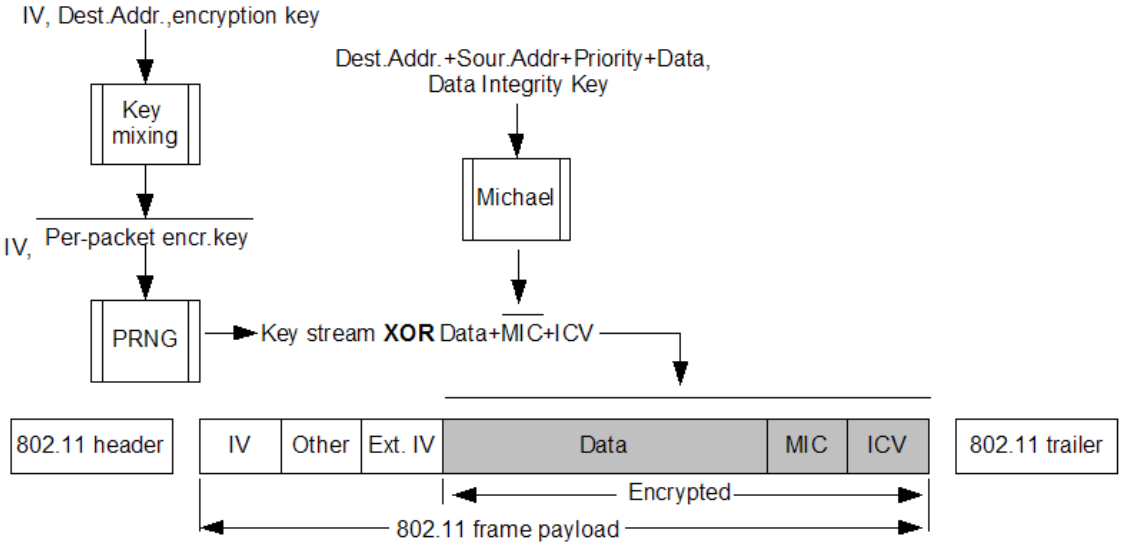
Systém WPA bol zavedený spoločnosťou Wi-Fi Alliance, ktorá sa stará o certifikáciu bezdrôtových zariadení. Jeho vznik a nasadenie bolo odozvou na nízku bezpečnosť, ktorú ponúkala schéma WEP. Skratka WPA znamená "Wi-Fi Protected Access". Je založená na vtedajšej draft verzii špecifikácie bezpečnostného rozšírenia 802.11i. Presnejšie na jej podmnožine. Pri návrhu WPA bola braná do úvahy najmä požiadavka aby hardware, ktorý už existoval a bol široko nasadený, bol schopný takéto zabezpečenie vykonávať. Bol zvýšený stupeň utajenia aj stupeň integrity. Zároveň bolo zavedené výrazné rozšírenie v podobe možnosti autentizácie užívateľov pomocou protokolu 802.1X. Popis podľa dok. MS [8].

3.2.1 Šifrovanie

Ako šifrovací algoritmus bol z dôvodu spätnej kompatibility použitý RC4. Na rozdiel od WEP je ale použitý šifrovací kľúč o dĺžke 128 bitov, ktorý je zložený s inicializačného vektoru o dĺžke 48 bitov a tajného kľúča o dĺžke 80 bitov. Tento tajný kľúč sa ale mení a je rôzny pre každý zaslaný paket. Schéma takéhoto šifrovania sa nazýva TKIP, čo znamená "Temporal Key Integrity Protocol". Použitie dlhšieho IV ako aj pravidelná zmena tajného kľúča zabezpečuje ochranu pred typom útoku, aký je možné podniknú? proti schéme WEP. Na začiatku ustálenia spojenia medzi klientom a AP si títo za pomoci autentizačného protokolu vymenia tzv. session keys. Tieto kľúče sú platné po dobu celého spojenia, avšak nepoužívajú sa priamo na šifrovanie ani integritu. Z týchto kľúčov sedenia sa pre každý paket generujú tzv. "pairwise temporal keys". Používajú sa dva druhy takýchto dočasných kľúčov: pre unicast komunikáciu a pre multicast a broadcast komunikáciu. "pairwise temporal key" pre každý druh komunikácie obsahuje okrem iného aj kľúč ktorým sa šifruje aktuálny rámec, plus kľúč ktorý sa používa na vypočítanie hash hodnoty. Detailný popis TKIP možno nájsť v literatúre [2].

3.2.2 Integrita

Na poskytnutie integrity bol použitý nový algoritmus zvaný MICHAEL. Ten ku každému rámcu prikladá tzv. MAC - "Message Authentication Code", v ktorom je zahrnuté aj čítač rámcov. Ten poskytuje na rozdiel od CRC skutočnú ochranu proti zmene obsahu rámcov a proti podvrhnutiu rámcov. CRC je totiž možné jednoducho dopočítať z dát, ktoré vytvoril útočník. MAC je niekedy označovaný aj ako MIC - "Message Integrity Code". Na výpočet



Obrázek 3.2: WPA šifrovanie

MIC používa MICHAEL integritný kľúč je obsiahnutý v "pairwise temporal key", ktorý je platný pre aktuálny rámec. Šifrovanie a dešifrovanie na obrázkoch 3.2 a 3.3.

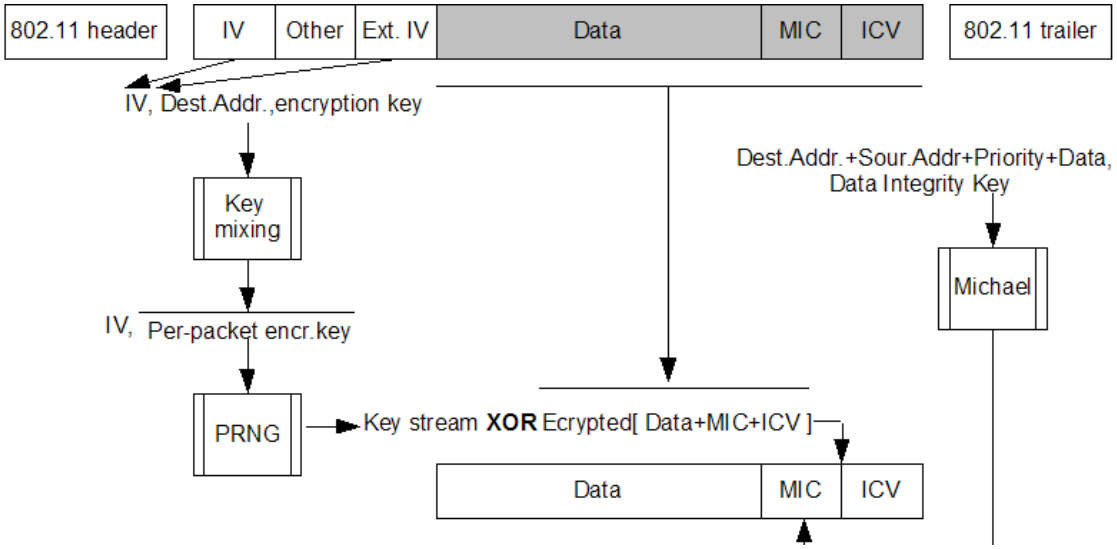
3.2.3 Autentizácia

Najvýznamnejšia časť, ktorá pribudla od éry WEP je možnosť autentizovať užívatelov. Na základe takejto autentizácie sú potom jednotlivým zariadeniam dynamicky generované a priraďované šifrovacie kľúče. To prináša okrem lepšej kontroly a prehľadu prihlásených užívateľov aj zbavenie sa povinnosti manuálne prideľovať všetkým rovnaký šifrovací kľúč. WPA poskytuje dve autentizačné schémy:

1. PSK mode
2. Enterprise mode

PSK mode: PSK znamená "PreShared Key". Tento mód sa odporúča jedine v prípade malých, napr. domácich sietí, v prípade kde nie je dostupný autentizačný server. V takomto prípade je nutné priradiť zdielané tajomstvo každej stanici aj prístupovému bodu. Toto heslo môže pozostávať z 8 až 63 ASCII znakov, alebo 64 hexadecimálnych číslic. Tento mód nás ale oberá a vyššie vymenované výhody autentizácie. Napriek tomu ale stále poskytuje vyššiu bezpečnosť z hľadiska utajenia a integrity. V tomto móde je ale potrebné dbať na to aby heslo bolo dostatočne komplexné, pretože na jeho základe sa šifruje komunikácia. Heslo by malo obsahovať minimálne 14 úplne náhodných znakov, pre zaručenie najvyššej bezpečnosti 22 úplne náhodných znakov.

Enterprise mode: Tento mód sa používa typicky vo firmách kde je požadovaná autentizácia užívateľov. Zároveň je nutné aby bol dostupný autentizačný server. Tento je väčšinou implementovaný ako RADIUS server a je umiestnený na samostatnom sieťovom serveri. Systém WPA definuje ale autentizačný proces prebiehajúci medzi klientskou stanicou a prístupovým bodom. Tento je popísaným autentizačným rámcom



Obrázek 3.3: WPA dešifrovanie

EAP. EAP znamená "Extensible Authentication Protocol". V prvom kole štandardizácie bola schválená jediná autentizačná metóda a to EAP-TLS. Neskôr boli zavedené aj ďalšie metódy:

1. EAP-TLS

   EAP-Transport Layer Security je prvý a zároveň najbezpečnejší typ autentizácie klienta. Tento typ autentizácie bol dlho jediným podporovaným pre WPA aj WPA2. Približne rok po vydaní štandardu WPA pribudlo do zoznamu podporovaných metód aj niekoľko ďalších. Pre EAP-TLS je typické, že pre overovanie vyžaduje jednak certifikát pre server, ale najmä klientské certifikáty pre každú bezdrôtovú klientskú stanicu. Takýto postup zabezpečuje maximálnu bezpečnosť, pretože odcudziť klientovi certifikát je pre útočníka národnejšie než zistiť jeho heslo. To je zároveň aj nevýhodou z hľadiska pracnej konfigurácie staníc.

2. EAP-TTLS

   EAP-Tunneled Transport Layer Security je zjednodušená forma autentizácie. V tomto prípade je požadovaný len certifikát pre server, klientské certifikáty nie sú potrebné. Táto verzia je široko podporovaná.

3. PEAPv0

   Protected EAP verzie 0 vznikol spoluprácou firiem Microsoft a Cisco. V tejto verzii je situácia podobná ako v predchádzajúcom prípade, čo znamená že potrebný je len certifikát pre server. Klient sa autentizuje pomocou mena a hesla, ktoré je zaslané protokolom MSCHAPv2. PEAP je v praxi dobre rozšírený a široko používaný. Hlavnou príčinou je zrejme vstavaná podpora v klientských systémoch Windows a zariadeniach Cisco. Poskytuje pokročilú bezpečnosť pri nízkych nárokoch na konfiguráciu.

4. PEAPv1

   Táto verzia nie je príliš rozšírená najmä z dôvodu slabej podpory v OS a sieťových zariadeniach. Cisco tento protokol čiastočne podporuje.

5. LEAP

   Ligh-weight EAP bol vytvorený firmou Cisco ako zjednodušená verzia EAP bez potreby akýchkoľvek certifikátov. Postupne bolo podpora zavedená aj medzi ostatnými výrobcami. Bezpečnosť tejto verzie je ale nízka a tak Cisco zaviedlo svoju novú verziu EAP-FAST.

Pre rozbor overovania bol použitý popis s encyklopédie Wikipedia [3].

3.3 WPA2

Štandard WPA2 je tiež známy pod menom protokolu 802.11i. Tento protokol bol prijatý v roku 2004. Obsahuje sadu bezpečnostných mechanizmov pre zabezpečenie protokolov 802.11x. Bol navrhnutý s prioritou poskytnutia čo najvyššieho stupňa zabezpečenia. Systém WPA je založený na podmnožine zabezpečovacích mechanizmov definovaných v 802.11i. WPA2 poskytuje nástroje pre utajenie a integritu sieťovej komunikácie a zároveň pre autentizáciu užívateľov. Nevýhodou WPA2 je spätná nekompatibilita so staršími klientskými kartami a prístupovými bodmi. Príčinou je nepostačujúci HW pre pokročilé šifrovanie.

3.3.1 Šifrovanie a integrita

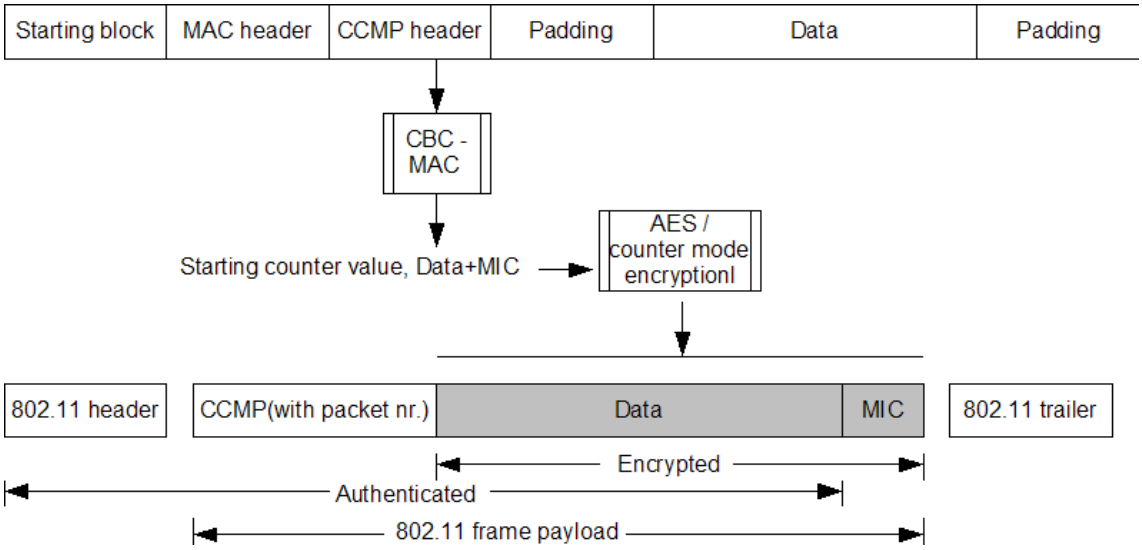
Šifrovanie ako aj integrita je založená na šifrovacom algoritme AES - Advanced Encryption Standard. Tento je v súčastnosti široko nasadzovaný a považovaný za dnešný vysoko bezpečný štandard. Je to symetrický algoritmus používaný na šifrovanie dát. Protokol WPA2 používa špeciálnu modifikáciu AES v podobe CCMP protokolu. Ten obsahuje podčasť zvanú CBC-MAC (Cipher Block Chaining-Message Authentication Code), ktorá vytvára MIC prenášaného rámcu. MIC má výslednú veľkosť 64 bitov a je vytvorený zreťazeným spracovaním 128 bitovych blokov dát. Počiatočný blok je tvorený z: príznakov, priority, zdrojovej adresy, čísla pakety a dlžky dát. Na rozdiel od WEP a WPA poskytuje tento postup zabezpečenie integrity celého Wi-Fi rámcu, vrátanie hlavičiek.

Kľúče potrebné na šifrovanie aj integritu sú dynamické menené pre každý prenášaný rámec, podobne ako pri WPA. Opäť sú použité 2 sady kľúčov: PTK (Pairwise Transient Key) pre unicast a GTK (Group Temporal Key), ktorý sa používa na šifrovanie multicast a broadcast komunikácie. V WPA2 sa nepoužívajú inicializačné vektory ale čísla paketov. Tieto majú rovnakú dĺžku ako IV vo WPA a to 48 bitov. Zobrazenie šifrovania a dešifrovania na obrázkoch 3.4 a 3.5. Popis podľa dokumentu MS [7]. Detailný popis CCMP v literatúre [2].

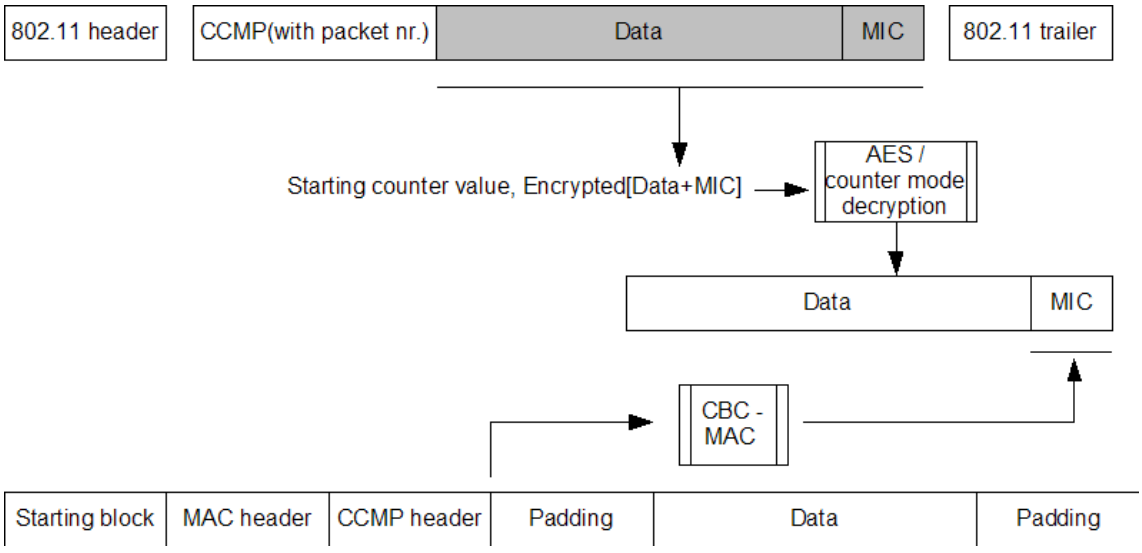
3.3.2 Autentizácia

Autentizácia užívateľov je rovnaká ako v prípade WPA. Prvým prijatým overovacím mechanizmom bol EAP-TLS. Nasledovne bolo prijatých niekoľko dalších:

1. EAP-TLS
2. EAP-TTLS
3. PEAPv0
4. PEAPv1
5. LEAP



Obrázek 3.4: WPA2 šifrovanie



Obrázek 3.5: WPA2 dešifrovanie

Kapitola 4

Porovnanie bezpečnostných mechanizmov a ich slabé miesta

V predchádzajúcej kapitole boli popísané základné bezpečnostné mechanizmy určené pre zabezpečenie Wi-Fi sietí. Poskytujú ale rôzny stupeň zabezpečenia z hľadísk utajenia, integrity a autentizácie. Zároveň sa odlišujú aj z hľadiska podpory v rôznych typoch HW zariadení ako aj v náročnosti konfigurácie sieťového prostredia. Táto kapitola zahrnuje analýzu popísaných systémov, prehlad ich slabých miest a možné útoky. Pre úplnosť sú zahrnuté aj bezpečnostné protokoly, ktoré fungujú na vyšších vrstvách a v niektorých prípadoch môžu byt použité ako alternatívne riešenie.

4.1 WEP

Mechanizmus WEP je prvý, základný a najmenej bezpečný spôsob pre zaistenie bezdrôtových sietí. Poskytuje základné šifrovanie Wi-Fi rámcov. Pre zabezpečenie integrity je použitý kontrolný súčet CRC, ktorého hodnota je zahrnutá v rámci zašifrovaných dát. Možnosť autentizácie nie je v základnej špecifikácii zahrnutá. Útoky na autentizáciu teda nie sú možné. Rovnako útok na samotnú integritu nie je možný pretože je zabezpečená kontrolným súčtom CRC. Na vytvorenie jeho hodnoty sa nepoužíva žiadny tajný kľúč a daný algoritmus je verejne známy. Hodnota CRC je zašifrovaná, teda po prelomení šifrovania je automatický prelomená aj ochrana integrity. Proti šifrovaniu je možné podniknúť niekoľko typov útokov.

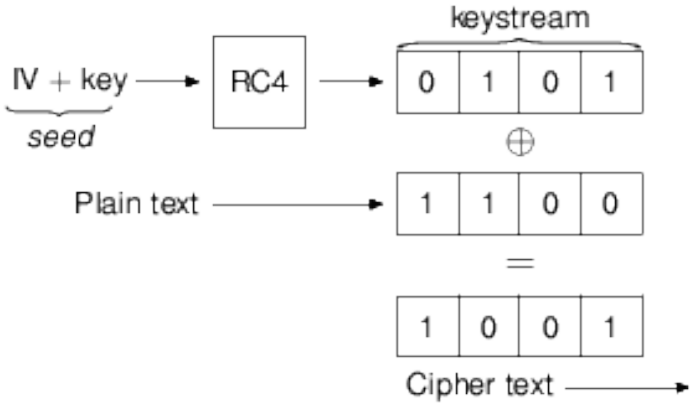
Najjednoduchším ale nie veľmi účinným je tzv. "Brute Force Attack", čiže útok hrubou silou. Ten postupne skúša zakryptované dáta rozšifrovať a skúša všetky možné kombinácie hodnôt šifrovacieho kľúča. Získané údaje nasledovne porovnáva z tzv. čistým textom. Keďže prenášané dáta sa vždy začínajú hlavičkami protokolov, používajú sa ako čistý text na porovnávanie so získanými hodnotami. Ak nastane zhoda, tak sme práve našli šifrovací kľúč. Použiteľnosť tejto metódy silne závisí na množstve možných kombinácií hodnôt kľúča. Pri základnom šifrovaní 64 bitovým kľúčom je tento tvorený zreťazení 24 bit hodnoty IV, ktorá je volne čitateľná v rámci a samotného 40 bit tajného kľúča. To znamená, že môžeme vytvoriť 2 na 40, čo je viac než 1099 miliárd kombinácií. Tieto všetky je ale možné otestovať na výkonnom CPU používanom v bežných PC v priebehu 30 - 45 dní. S požitím distribuovanej siete sa môžeme dostať na veľmi použiteľné časové doby. V prípade šifrovania 128 bitovým kľúčom, je dlžka tajného kľúča 104 bitov a útok hrubou silou nie je použiteľný.

Pokročilejší, efektívnejší a rozšírenejší typ útoku je tzv. "FMS Attack". Ten je pomenovaný podla iniciálok jeho tvorcov: Fluhrer, Mantin, Shamir. Tento typ útoku využíva tri

slabé miesta použitého šifrovacieho algoritmu RC4:

1. Slabé inicializačné vektory
2. Generovanie IV s rovnakou hodnotou
3. Predpokladané hodnoty prvých bytov nešifrovaných dát

Pod pojmom slabé inicializačné vektory rozumieme také hodnoty IV, na základe ktorých je možné ľahko zistiť hodnotu tajného kľúča. Zároveň počet možných hodnôt IV je len 16,7 milióna, čo zaručuje ich pomerne časté opakovanie sa. V praxi je ale pravdepodobnosť výskytu rovnakých IV omnoho vyššia. Väčší počet takýchto paketov znamená mat viac vzoriek pri ktorých poznáme prvú časť šifrovacieho kľúča, zašifrované dáta a predpokladané hodnoty nešifrovaných dát. Po získaní dostatočného množstva takýchto údajov je možné zistiť tajný kľúč vo veľmi krátkom časovom intervale. Rádovo sa jedná o minúty. Na vykonanie takéhoto útoku je v súčastnosti voľne dostupných niekoľko nástrojov. Tento typ útoku je efektívny pre dlžku kľúča 64 aj 128 bitov.



Obrázek 4.1: RC4 algoritmus

Dalším spôsobom útoku, ktorý vyžíva skutočnosť že všetci bezdrôtový účastníci zdieľajú to isté heslo, je odcudzenie notebooku jedného z klientov . Následovne má klient plný prístup k bezdrôtovej sieti.

Z hľadiska podpory v HW zariadeniach je dnes použitie WEP prakticky bezproblémové. Podpora je zahrnutá v takmer každej klientskej karte ako aj v prístupových bodoch. Až na výnimky prvej generácie bezdrôtových adaptérov je WEP podporovaný prakticky všade automaticky.

Z pohľadu zložitosti konfigurácie klientských staníc a prístupových bodov je požadované minimálne úsilie zo strany správcu siete ako aj zo strany užívateľov. Z dôvodu jednoduchého prelomenia tohoto zabezpečenia sa odporúča tento kľúč často meniť. To môže priniesť zvýšené nároku na správu siete ako aj problém s distribúciou klúča ku všetkým klientom, najmä ak tento kľúč musí zostať utajený.

Informácie čerpané prevažne z knihy WI-FOO [10].

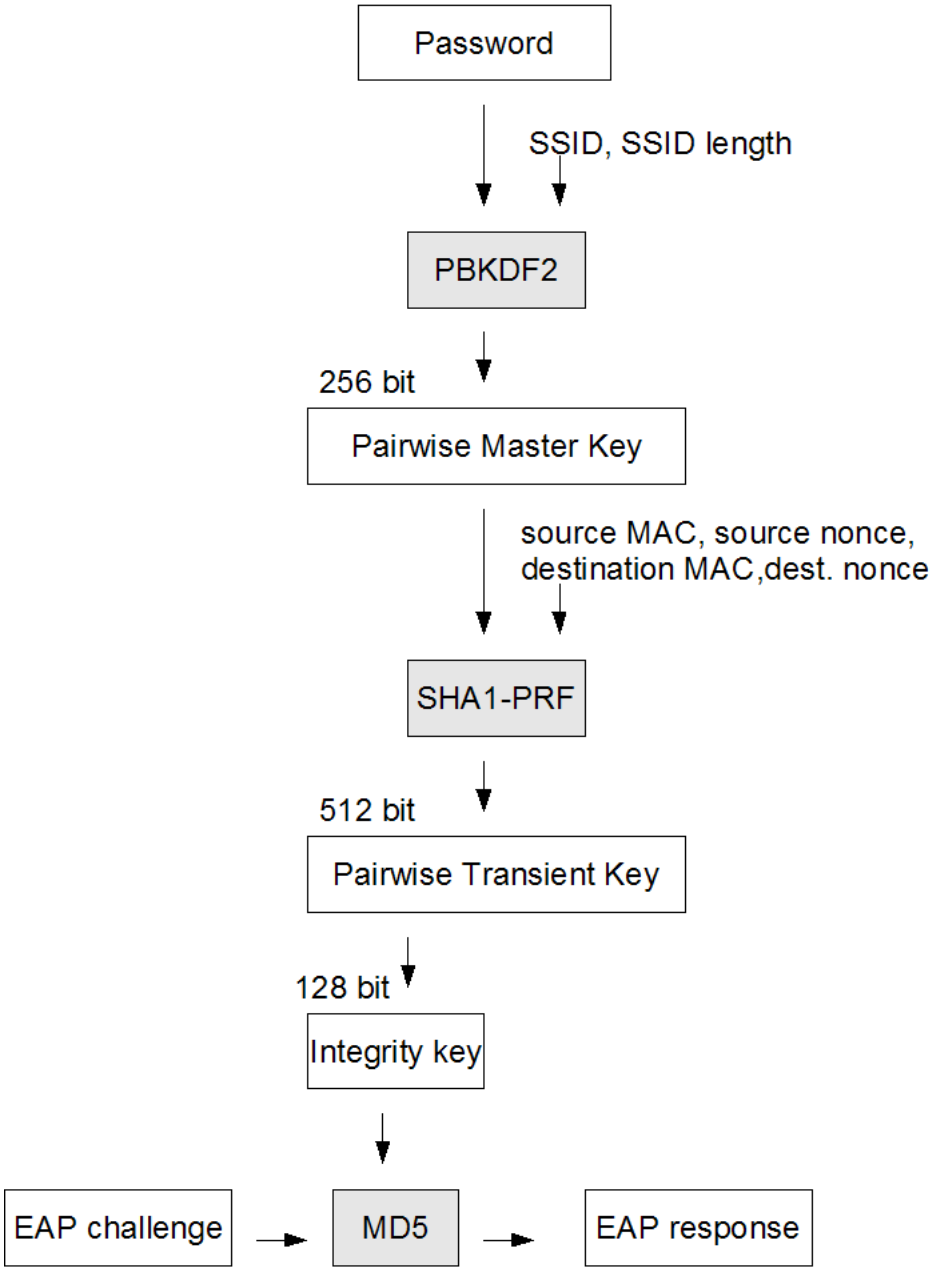
4.2 WPA

Mechanizmus WPA je pokročilý protokol, ktorý poskytuje zabezpečenie utajenia, solídne zabezpečenie integrity a autentizáciu voliteľného stupňa. Šifrovanie a integrita sú zabezpečované nezávislo dvoma rôznymi algoritmami a každý z nich používa rôzny šifrovací kľúč. Autentizácia je uskutočnená pomocou autentizačného rámca 802.1X za použitia zdielaného hesla alebo pomocou Radius servera, kde sú autentizačné informácie zasielané v paketoch EAP. Proti tomuto je niekoľko typov útokov.

Útok na šifrovanie je v tomto prípade nárocnejší ako v pri útoku na WEP a je úspech závisí na viacerých okolnostiach. Kedže šifrovacie kľúče sú pri WPA pravidelne obmieňané, tak útok popísaný v predchádzajúcej kapitole nemá zmysel a nie je vykonateľný. Vzhľadom na to, že šifrovací kľúč je pre každý paket iný, tak nie je šanca odchytiť dostatočné množstvo IV, na zistenie tohoto kľúča. Dynamická rotácia kľúčov prebieha tak pri používaní 802.1X autentizácie ako aj pri móde so zdielaným tajomstvom. Práve pri tomto druhom móde sú šifrovacie kľúče odvodzované zo zdielaného tajomstva. V prípade že je tento zdielaný reťazec príliš krátky, je možné zneužiť to na útok. Zo zdielaného reťazca, ktorý musí byt rovnaký na každej stanici, sa vygeneruje tzv. PSK (PreShared Key). Na je ho generovanie sa použije verejne známa kryptografická funkcia PBKDF2. Ako vstup poslúži: zdielané heslo, ESSID a jeho dlžka. Výsledkom je 256 bitový kľúč PMK (Pairwise Master Key). V prípade že zdielané heslo je príliš krátke, je možné ho spätne zistiť. V priebehu sieťovej komunikácie sa pre každý packet vygenerujú tzv. PTK (Pairwise Transient Key). Pre úspešný útok je potrebné odchytiť 4 pakety obsahujúce dáta protokolu EAP, ktoré sú zasielané pri počiatočnej autentizácii stanice. Tieto 4 pakety obsahujú tzv. Four Way Handshake. V jednom z nich je obsiahnutý čistý text a další z nich obsahuje MIC vypočítaný z tohoto textu. Typ samotného útoku je tzv. Brute Force Dictionary Attack, ciže slovníkový útok hrubou silou. Postupne sa snažíme vytvoriť PMK známou funkciou PBKDF2 za pomoci hodnoty SSID. Z neho potom vytvoríme PTK za pomoci zdrojovej a cieľovej MAC adresy ako aj zaslaného náhodného čísla - všetky obsiahnuté v odchytených štyroch paketoch. Z PTK vyberieme časť používanú ako integritný kľúč a vytvoríme MIC hodnotu z odchyteného čistého textu. Produkt potom porovnáme z odchytenou hodnotou MIC. Ak hodnoty sedia, tak sme našli kľúč. Tento útok je pomerne náročný a jeho úspech je silne závislý na použití krátkeho slovníkového hesla v PSK móde.

Sada mechanizmov WPA bola navrhovaná na základe predbežnej špecifikácie štandardu 802.11i, ale bol pri tom braný veľký ohľad na spätnú kompatibilitu s HW. To znamená že boli zvolené najsilnejšie možné algoritmy tak, aby mohli bežať na štandardne používaných sieťových zariadeniach. To platí najmä pre klientské karty. Väčšina klientských kariet, ktoré podporujú WEP, sú schopné podporovať aj WPA po nahratí novej verzie firmware. U prístupových bodov je väčšinou nutné vymeniť HW.

Z pohľadu zložitosti konfigurácie je tento princíp komplikovanejší. Užívateľ musí zvoliť požadovanú metódu šifrovania aj autentizácie. Zároveň musí mat vytvorené užívateľské meno a heslo. Správca siete zas musí spravovať autentizačný server s databázou užívateľov. V prípade že sa rozhodne používat autentizáciu EAP-TLS, je nutné vystaviť všetkým užívateľom ich klientské certifikáty a nainštalovať ich na stanice. To predstavuje vo väčšine prípadov príliš veľkú zátaž pre správcu ako aj pre užívateľov. Mód so zdielaným kľúčom je jednoduchý na konfiguráciu, ale má obmedzenie napríklad v auditovaní. Vhodným kompromisom je použiť autentizáciu bez klientských certifikátov. Mali by sme ale zotrvať pri metóde, kde je potrebný certifikát pre server. Existujú aj zjednodušené metódy bez serverového certifikátu, napríklad LEAP. Tento mechanizmus má ale zneužitelnú slabinu,



Obrázek 4.2: WPA pre-shared mode

na ktorú možno zaútočiť tak pri použití s WPA ako aj WPA2. Popis je zahrnutý v nasledujúcej kapitole. Popis podľa knihy WI-FOO [10].

Popis operácií znázornených na obrázku 4.2 :

1. Užívateľom zadané heslo, identifikátor AP a jeho dĺžka sa použijú ako vstup do funkcie PBKDF2. Výstupom je tzv. "Pairwise Master Key". Tento je používaný po celú dobu komunikácie

2. PMK spolu s zdrojovou a cieľovou fyzickou adresou a náhodnými číslami sa použijú ako vstup do fukcie SHA1-PRF. Výstupom je tzv. " Pairwise Transient Key". Ten sa mení s každým rámcom.

3. Vyberieme časť PTK, ktorý slúží na zabezpečenie integrity a použijeme ho ako kľúč pre funkciu MD5. Pomocou tejto vypočítame hash z "EAP Challenge" paketu a porovnáme s "EAP Response".

4.3 WPA2

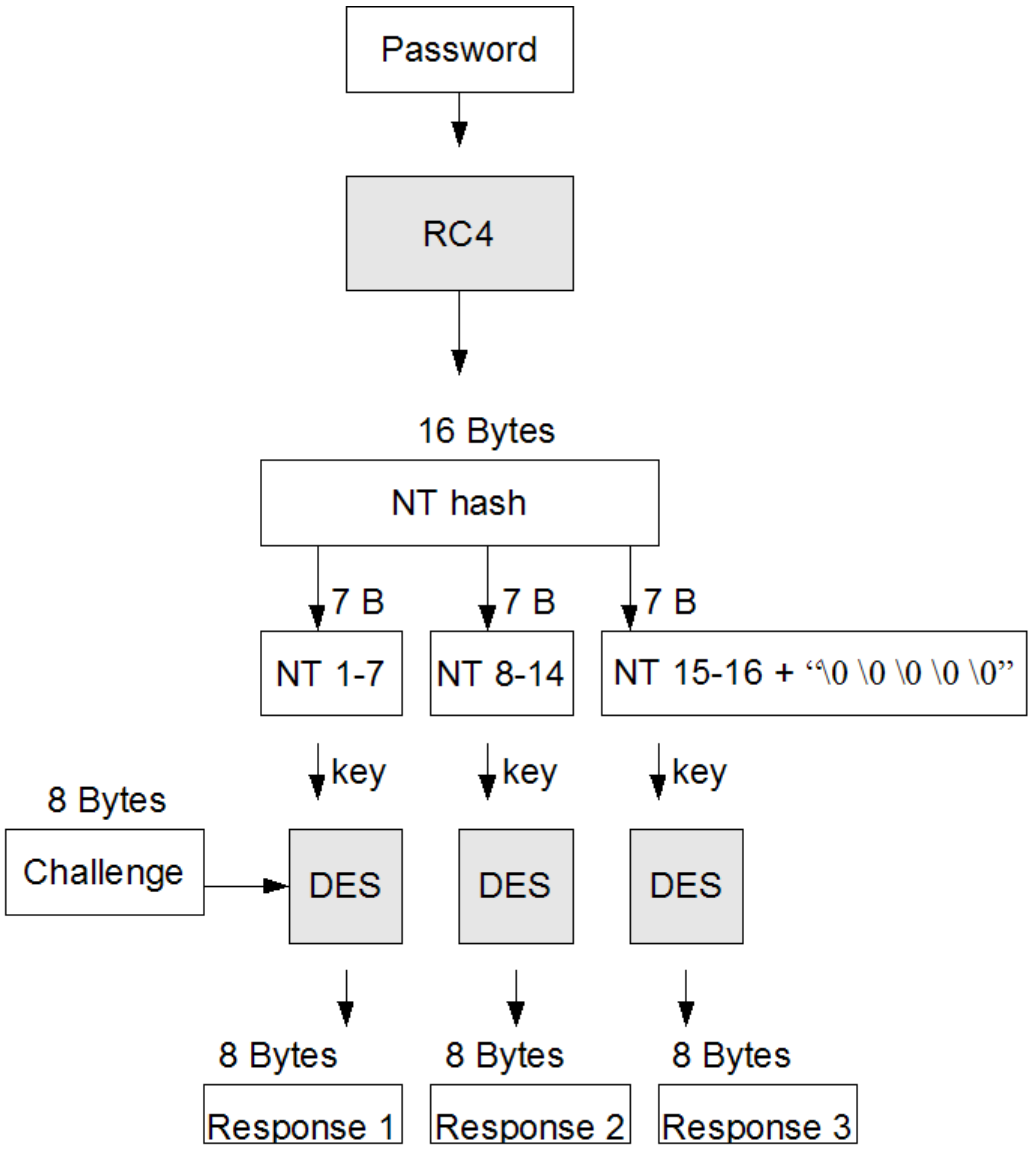
Mechanizmus WPA2 je plnohodnotná sada zabezpečovacích protokolov, ktoré zabezpečujú vysoký stupeň utajenia a integrity ako aj autentizáciu voliteľného stupňa. Šifrovanie a integrita sú založené na princípe silného symetrického algoritmu AES. Pre oba prípady sú použité rozličné kľúče. Autentizácia je uskutočnená pomocou autentizačného rámcu 802.1X za použitia zdielaného hesla alebo pomocou Radius servera, kde sú autentizačné informácie zasielané v paketoch EAP.

V súčastnosti nie sú známe žiadne efektívne a prakticky vykonateľné útoky, ktoré by zneužívali chyby v samotnom algoritme AES, alebo v jeho implementácii použitej konkrétne pre WPA2. Proti tomuto zabezpečeniu nie je možné uspieť s ani jedným z vyššie popísaných typov útokov. Do úvahy ale pripadá útok na autentizačný mechanizmus EAP.

Útok na autentizáciu je možné vykonať len v prípade že použijeme autentizačnú schému, ktorá obsahuje nejaké slabé miesto. V prípade že je nasadený tzv. Enterprise mode, tak sa na autentizáciu využíva zvyčajne rámec 802.1X, ktorý poskytuje priestor pre nasadenie niekoľkých protokolov. Jedným z nich je aj protokol LEAP - Lightweight Extensible Authentication Protocol. Ten je proprietárnym produktom spoločnosti CISCO, ale je široko podporovaný a nasadzovaný v praxi. Verejne je dostupný popis pre implementáciu klientskej časti a ďalší popis je možné získať analýzou paketov. Autentizácia prebieha na princípe výzva - odpoveď (chalenge - response). Vo chvíli keď sa klient pripája, tak mu AP pošle náhodne vygenerovanú výzvu v dĺžke 8 bytov. Klient má u seba uložený NT hash z hesla o dĺžke 16 bytov. Z neho sa vytvoria 3 DES kľúče o celkovej dĺžke 3 x 56 bitov, čo je 21 bytov. Za chýbajúcich 5 bytov sa doplnia nuly. V tomto implementačnom zjednodušení je skrytá zneužitelná medzera. Klient totiž prijme výzvu, ktorá je zaslaná ako čistý text a odpovie tri krát, zakaždým zašifruje DES-om zašifrovanú výzvu, za postupného použitia všetkých troch kľúčov. Kedže môžeme odchytiť nezašifrovanú výzvu a môžeme rovnako odchytiť odpoveď zašifrovanú tretím kľúčom, v ktorom je 5 zo 7 bytov tvorených nulami, je možné bez problémov zistiť zostávajúce 2 byty DES kľúča, ktoré sú de-facto posledné 2 byty NT hash-u užívatelského hesla. Znalosť posledných 2 bytov NT hash-u hesla značne redukuje počet možných hesiel, z ktorých je možné vytvoriť takto končiaci sa hash. To je dobrým predpokladom pre uskutočnenie slovníkového útoku. Z databáze bežne používaných hesiel vytvoríme ich NT hash-e (pomocou algoritmu MD4). z tých potom vyberieme len tie ktoré

končia na získané 2 byty. Ak nastane táto zhoda, tak použijeme prvých 7 a druhých 7 bytov hash-u ako DES kľúč a zašifrujeme výzvu, ak nastane zhoda s odpoveďou, ktorú zasielal klient pre AP, tak sme našli heslo. Užívateľské meno je prenášane v paketoch v nešifrovanej podobe. Takto získame prístup do siete. Úspech tohoto útoku ale spočíva v splnení predpokladu, že užívateľ použije slovníkové heslo. Postupnosť je znázornená na obrázku 4.3

Popis podľa knihy WI-FOO [10].



Obrázek 4.3: LEAP autentizácia

4.4 WEP vs. WPA

Pri porovnaní protokolov WEP a WPA zistíme, ?e je medzi nimi veľký rozdiel, aj keď z ich stručného popisu by sme to nemuseli očakávať. Sada WEP bola navrhnutá aby pre WiFi poskytla súkromie ekvivalentné ku klasickej sieti (Wired Equivalent Privacy). Praktická aplikácia je ale dosť vzdialená od tejto myšlienky. Špecifikácia WEP definuje funkcionalitu pre autentizáciu, utajenie aj integritu. Rovnakú funkcionalitu poskytuje aj WPA. Z hľadiska praktického nasadenia je ale možné vybadať veľké rozdiely medzi WEP a WPA.

WEP môžeme použiť bez autentizácie alebo s autentizáciou zdielanou. To znamená, že ako identifikačné údaje užívateľa sa použije jedine zdielaný tajný kľúc, ktorý je potrebný na šifrovanie. Takýto princíp ale nie je v zhode z definíciou plnohodnotnej autentizácie a výrazne obmedzuje možnosti auditu a autorizácie prístupu k rôznym zdrojom. WPA môžeme použiť v tzv. zdielanom móde, ktorý je veľmi podobný WEP a má teda aj rovnaké obmedzenia. V móde s autentizáciou pomocou Radius serveru ale poskytuje plnú autentizáciu ako ja možností s ňou spojených. Na Radius serveri je definovaná databáza užívateľov, takže vždy môžeme identifikovať aktuálne pripojeného klienta a vykonávať audit a autorizovať mu prístup. WEP nám teda de-facto autentizáciu neposkytuje, WPA ju voliteľne poskytuje.

Z hľadiska utajenia sú principiálne WEP aj WPA na rovnakej úrovni, avšak z pohľadu praktického sú tieto dve úrovne odlišné. V oboch prípade je nám poskytnutá ochrana proti nechcenému odpočúvaniu dát na zdielanom médiu. Šifrovací algoritmus WEP má ale implementačnú chybu, ktorú je možné zneužiť a ľahko zistiť šifrovací kľúč, bez ohľadu na to či má dĺžku 64 alebo 128 bitov. V prípade WPA je použitý šifrovací algoritmus, ktorý odstraňuje slabiny zistené vo WEP a nie je ho možné jednoducho prelomiť. Jednou z možností je zistenie zdielaného hesla v zdielanom móde. To je ale možné len v prípade, že je použité krátke slovníkové heslo. V prípade použitia tzv. Enterprise módu je možné zistiť užívatelské heslo, ak je použitý slabý autentizačný protokol (LEAP) a slovníkové heslo. WEP nám neposkytuje uspokojujúci stupeň utajenia, WPA ho poskytuje pri dodržaní odporúčaných postupov.

Z pohľadu integrity je riešenie ponúkané pri WEP zjavne nedostatočné, pretože ako algoritmus je použitý cyklický súčet CRC32. Ten sa typicky nasadzuje pre kontrolu chýb pri prenose a kedže jeho hodnota nie je samostatne zašifrovaná, tak jeho funkčnosť je len obmedzená. Hodnota CRC je šifrovaná spolu s prenášanými dátami, takže pri prelomení šifrovania, sme zároveň automaticky prelomili aj ochranu integrity. Pri WPA je integrita zaručená algoritmom MICHAEL za použitia samostatného integritného kľúča. Je ale treba podotknúť že pri slovníkovom útoku či už v zdielanom móde alebo proti LEAP autentizácii získame hlavné heslo úživateľa , z ktorého ľahko odvodíme integritný kľúč.

Podpora WEP je zaručená prakticky vo všetkých sieťových zariadeniach. WPA je podporované v takmer všetkých klientských adaptéroch po nahraní novej verzie firmware. WPA je ale podporovaná len v novších prístupových bodoch.

Konfigurácia WEP je minimálna a prakticky bezproblémová. Nastavenie siete s WPA, si žiada menšiu konfiguráciu staníc a rozsiahlu konfiguráciu AP aj autentizačného serveru. V niektorých prípadoch je dokonca nutné inštalovat klientom ich certifikáty.

4.5 WPA vs. WPA2

Mechanizmus WPA bol navrhnutý na predbežnej špecifikácii protokolu 802.11i, čo je len iné označenie pre WPA2. Teda WPA je podmnožinou skupiny mechanizmov definovaných vo

WPA2. Oba prístupy nám poskytujú rovnaké možnosti autentizácie. Pre utajenie a integritu máme pri WPA je len jednú možnosť, no pri WPA2 si môžeme zvoliť z dvoch alternatív.

Autentizácia je pre WPA2 zhodná ako pre WPA. Popísaná bola v predchádzajúcej kapitole.

WPA zabezpečuje utajenie použitím algoritmu TKIP a integritu pomocou alg. MICHAEL. Tieto algoritmy sú jednoduché a rýchle. WPA2 ponúka rozšírenie v podobe možnosti šifrovania aj podpisovania pomocou modifikácie algoritmu AES (Advanced Encryption Standart). Ten je v súčastnosti považovaný za jeden z najspoľahlivejších a v praxi nasadzovaných riešení. Má ale zvýšené nároky na HW prostriedky. Momentálne nie je známa žiadna bezpečnostná chyba v samotnom algoritme ani v jeho implementácii pre WPA2.

Mierne problematické môže byt nasadenie WPA2 v reálnej situácii. Väčšinou si totiž vy?aduje výmenu sieťových prvkov klientov ako aj AP. V prípade WPA2 postačuje len výmena AP. Zavedenie WPA2 tak môže znamenať nevyhnutné investície do siete.

Zo strany zložitosti konfigurácie sieťového prostredia, je situácia rovnaká pre oba prípady. Náročnosť je závislá na type použitej autentizácie.

4.6 Celkové porovnanie

Protokol	**WEP**	**WPA**	**WPA2**	**IPsec**
Utajenie	nízke	vysoké	veľmi vysoké	veľmi vysoké
Integrita	žiadna	vysoká	veľmi vysoká	veľmi vysoká
Autentizácia	nie	áno	áno	.áno
Konfigurácia	jednoduchá	stredne zložitá	stredne zložitá	zložitá
OSI vrstva	2	2	2	3
podpora v HW	veľmi široká	ľiroká	užšia	HW nezávislé

Tabulka 4.1: Porovnanie

Kapitola 5

Vplyv zabezpečenia na efektivitu prenosu dát

Jednotlivé druhy zabezpečenia predstavujú zvýšenú réžiu pre prístupový bod aj pre klienta. Týka sa to najmä šifrovania a zabezpečovania integrity. Istú námahu treba vynaložiť aj na cyklické generovanie a distribúciu kľúčov pri WPA. Zvýšená réžia môže spôsobiť pokles reálnej prenosovej rýchlosti. Jednak z dôvodu nutnosti pridávania rozširujúcich hlavičiek, ale aj z dôvodu nutnosti neustáleho šifrovania a dešifrovania prúdu dát.

Reálne testovanie priepustnosti som vykonával pomocou prístupových bodov od firmy MikroTik, ktoré sú momentálne najrozšírenejšie medzi používanými prístupovými bodmi. Zároveň poskytujú podporu všetkých bežne požadovaných protokolov, rozsiahle možnosti konfigurácie a spoľahlivú prevádzku za rozumnú cenu.

Používaný model obsahuje 2,4 Ghz aj 5 Ghz kartu. Poskytuje podporu WEP, WPA aj WPA2 spolu so všetkými možnosťami autentizácie. Zariadenie je osadené procesorom Infineon, ktorý je taktovaný na frekvenciu 175 Mhz. To je pravdepodobne limitujúcim faktorom pri použití pokročilého zabezpečenia. V praxi je ale možné nasadiť modely s procesormi Infineon 270 Mhz, alebo dokonca s Intel P4.

Táto kapitola obsahuje popis meraní, ktoré boli vykonané s rôznymi nastaveniami prístupového bodu. Na prenos bol použitý protokol 802.11g s maximálnou podporovanou rýchlosťou 54 Mbs. Táto rýchlosť je ale rýchlosť modulačná a reálne prenosové rýchlosti sa nachádzajú v trochu inej sfére.

Vypracoval som niekoľko typov meraní priepustnosti. Začal som meraním prenosu umelo generovaných dát s použitím nástroja Bandwidth test, ktorý je súčasťou AP Mikrotik. Na porovnanie ponúkam meranie so štandardným nastavením AP ako aj s využitím špeciálnych rozšírení. Nasledujú testy prenosu reálnych dát medzi dvoma PC, ktoré sú prepojené pomocou dvoch AP. Na doplnenie uvádzam aj testy prenosu reálnych dát medzi PC a AP ako aj medzi PC a výkonnej?ou verziou AP.

Všetky testy boli vykonané v laboratórnych podmienkach. Výsledky v skutočnej prevádzke sa môžu mierne odlišovať. Rýchlosť prenosu môže byť ovplyvnená jednak atmosférickými podmienkami ako aj rôznych rušením spôsobeným inými rádiovými vlnami vo voľných rádiových pásmach 2,4 Ghz a 5 Ghz.

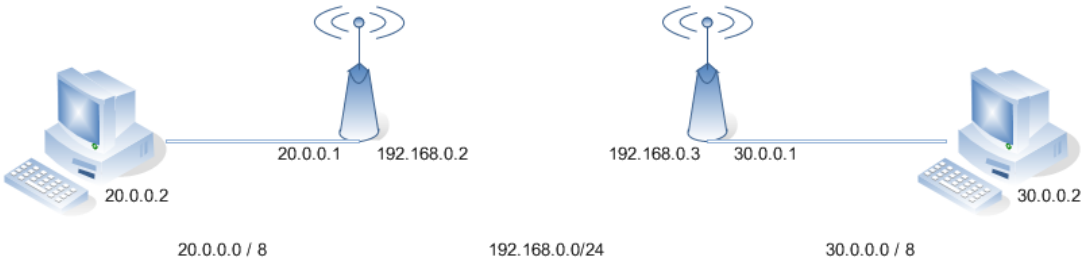
Meranania neboli vyhotovené s primárnym zameraním sa na úplnú presnosť odmeraných hodnôt. Sú prípustné odchýlky, ktoré sa ale pohybujú rádovo v percentách. Pre naše účely je takáto presnosť úplne postačujúca, pretože výsledky nám slúžia primárne na vzájomné porovnanie efektivity prenosu pri použití jednotlivých typov zabezpečenia.

5.1 Postup meraní

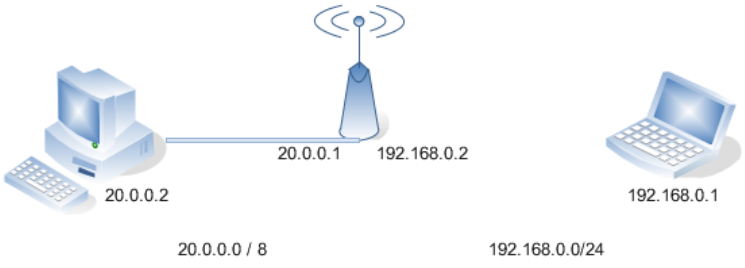
Pri včetkých meraniach som použil nasledovné komponenty:

- AP s doskou RouterBoard 112 resp. 230
- Laptop s OS Windows XP SP2
- Desktop s OS Linux Fedora

Presný popis dosiek RouterBoard použitých v AP sa nachádza v prílohe B. Pri každom druhu merania som postupoval tak, že som daný typ pokusu zopakoval 2 krát a zapísal som priemernú hodnotu. Týmto som predišiel chybe merania spôsobenej chvíľkovou zmenou okolitých podmienok. Namerané hodnoty nie sú úplne presné, ale vznikli ako odhad primerných hodnôt pri danom type meraní. Postup by mal byť postačujúci pre tieto potreby.



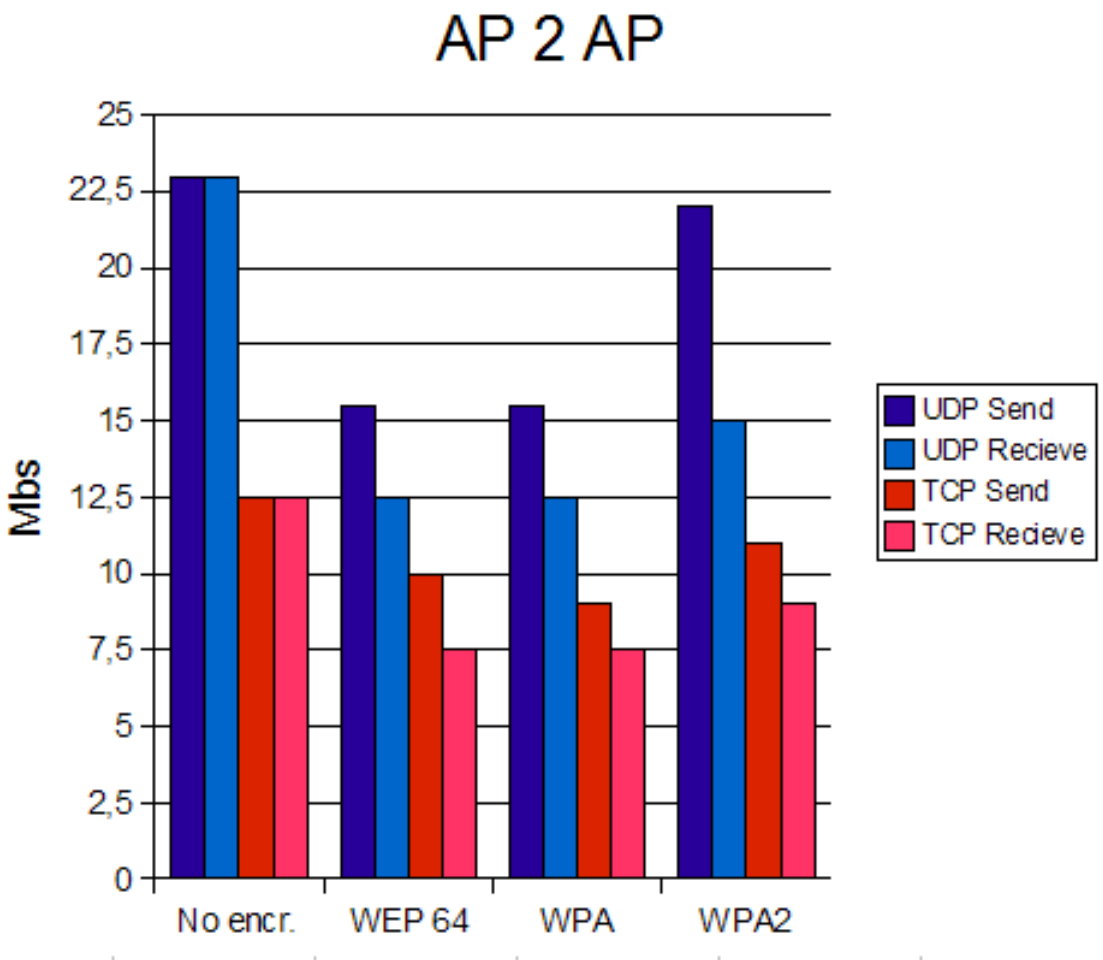
Obrázek 5.1: Merania medzi PC



Obrázek 5.2: Merania medzi PC a AP

5.2 Štandardné merania medzi AP

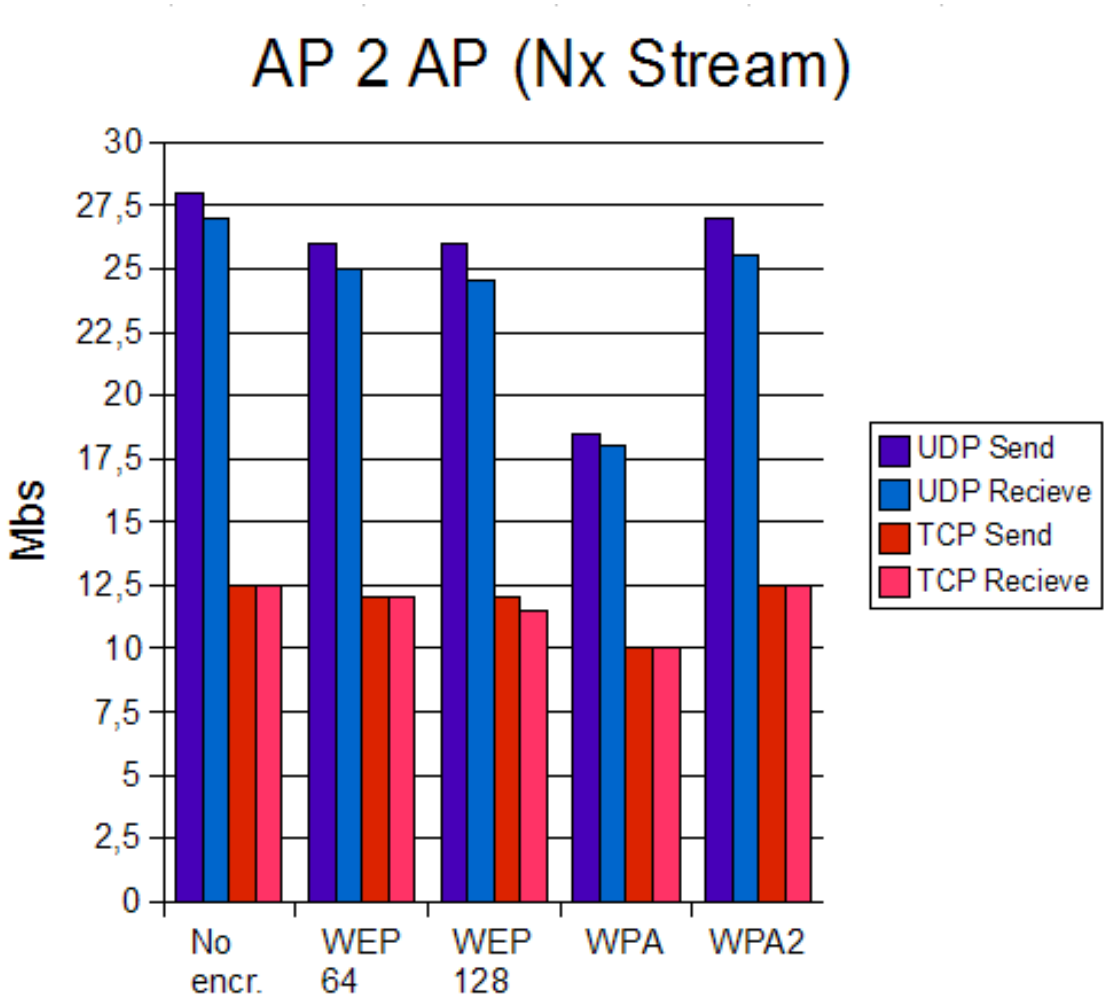
Táto prvá sada meraní bola zhotovená meraním priepustnosti medzi dvoma AP. Dáta boli generované s použitím Bandwidt serveru zabudovaným v AP Mikrotik. Z priloženého grafu môžeme vyčítať niekoľko dôležitých skutočností. V prvom rade je badateľný markantný rozdiel medzi prenosom pomocou UDP a TCP protokolu. Kedže UDP je nespojovaný protokol bez záruky doručenia dát, tak jeho nízka réžia nám zaručuje omnoho rýchlejší prenos dát než je to pri použití protokolu TCP. V tomto prípade môžeme povedať že protokol UDP prenesie za rovnakú časovú jednotku približne o 40 percent viac dát než TCP. Zároveň vidíme, že prenosová rýchlosť výrazne klesá pri použití aj najjednoduchšieho typu zabezpečenia. Pri zapnutí WEP klesne reálny prenos o približne 30 percent. Rozdiel medzi WEP a WPA1 je minimálny, tak?e voľba medzi týmito dvoma spôsobmi zabezpečenia prakticky nijako neovplyvní efektivitu prenosu dát. Prekvapivé výsledky nám ponúka meranie WPA2 s použitím šifrovania založenom na AES v CCM móde. V tomto prípade badať prijateľný pokles prenosovej rýchlosti, ktorý predstavuje v priemere približne 20 percent. Výsledky zobrazené na obrázku 5.3.



Obrázek 5.3: Priepustnosť

5.3 Rozšírené merania medzi AP

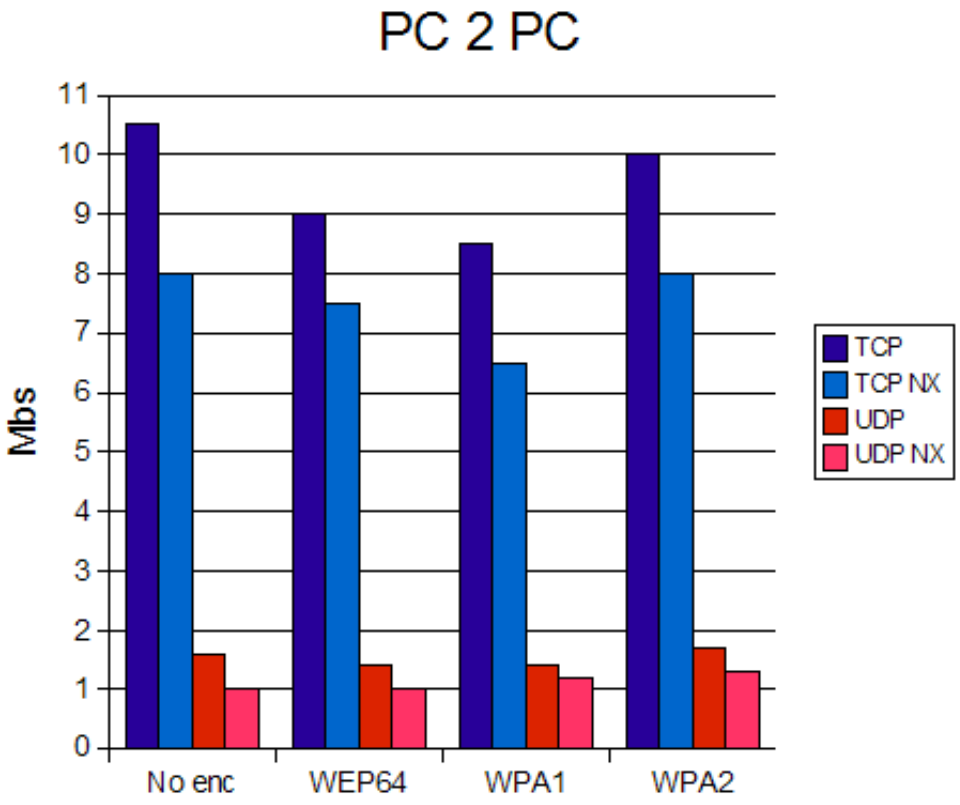
V tejto sade meraní som povolil na prístupových bodoch využitie proprietárneho rozšírenia nazvaného NX Stream. Toto nastavenie umožňuje spojiť dokopy niekoľko Wi-Fi rámcov a zaslať ich naraz. je ale nutné aby túto vlastnosť podporovali obe strany, ktoré sa zúčastňujú na prenose. Túto vlastnosť teda typicky nenájdeme podporovanú na strane klientov. Je ale vhodné ju použit na tzv. "backbone connections" medzi dvoma AP. Zapnutie tohoto rozšírenia nám prináša zaujímavý nárast reálnej prenosovej rýchlosti. V prípade UDP je to nárast o približne 20 percent. Na protokol TCP to prakticky vplyv nemá. Ak sa pozrieme na efektivitu prenosu pri použití jednotlivých typov zabezpečenia, tak z priloženého grafu môžeme opäť vypozorovať niekoľko skutočností. Pri zapnutí WEP je pokles prenosu minimálny a predstavuje menej ako 10 percentnú stratu. To platí pre použitie 64 aj 128 bitového kľúča. Situácia sa výrazne mení pri použití zabezpečenia WPA. Tu nastáva výrazná strata efektívnej prenosovej rýchlosti. V porovnaní s nešifrovaným prenosom je to 25 percentná strata pri TCP a dokonca 35 percentná strata pri UDP. Pri použití WPA2, ale nebadať takmer žiadnu stratu v porovnaní s bežným prenosom. Výsledky zobrazené na obrázku 5.4.



Obrázek 5.4: Priepustnosť s NX Stream

5.4 Merania medzi PC

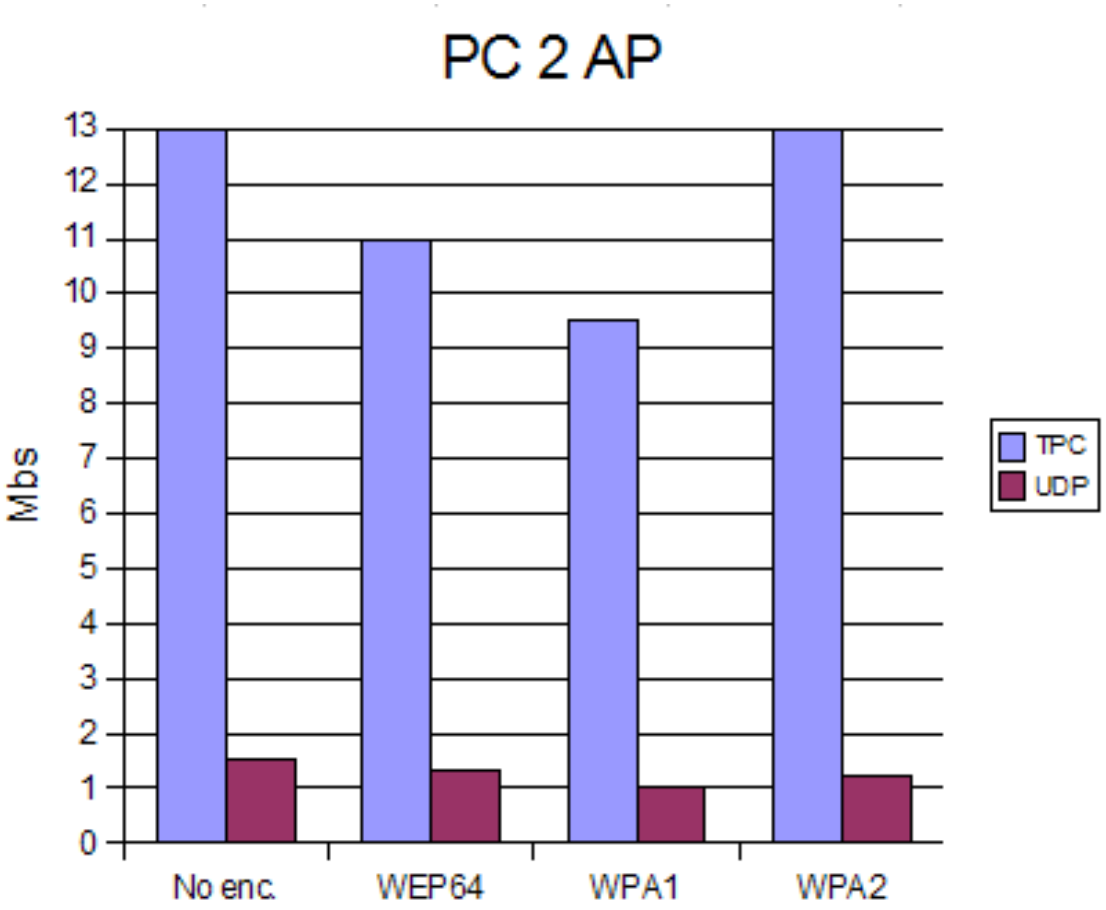
Tieto merania boli vyhotovené pomocou vytvorenia jednoduchej siete pozostávajúcej z dvoch PC a z dvoch AP. Každé PC bolo pripojené pomocou 100 Mbs Ethernet protokolu na svoj AP. Prístupové body navzájom boli spojené bezdrôtovým 54 Mbs protokolom WiFi 802.11g. Vznikli tak tri rôzne podsiete a prístupové body slúžili zároveň ako smerovače pre preposielanie paketov medzi jednotlivými sieťami. Proces smerovania bol riadený na základe statických záznamov, takže zaťaženie AP bolo minimálne. Sektory siete pripojenej pomocou UTP Ethernet káblov zároveň poskytovali prenosové pásmo s takmer dvojnásobnou šírkou v porovnaní s použitým WiFi protokolom na bezdrôtovom segmente testovacej siete. Výkon oboch PC bol pre dané testy dostatočný, až výrazne naddimenzovaný, takže nespôsobovali žiadne spomaľovanie prenosu, čo bolo priebežne monitorované. Celková rýchlosť tak závisela len na možnostiach AP. Prenášané dáta boli skutočné údaje prenášané pomocou FTP (TCP) a TFTP (UDP) protokolov z jedného PC na druhé. Prenosová rýchlosť s využitím UDP ale bola z mne neznámych dôvodov značne nízka, takže ju nebudem brať do úvahy. Z porovnania TCP prenosu ale môžeme povedať že použitie WEP znamená v porovnaní s nešifrovaným prenosom spomalenie približne 10 a? 15Pri použití protokolu WPA môžeme vypozorovať až 20šifrovanie pomocou AES algoritmu použitom pri WPA2 nevykazuje takmer žiadne strany na rýchlosti prenosu. Na meranie rýchlosti prenosu dát bola použitá linuxová utilita Iptraf. Výsledky zobrazené na obrázku 5.5.



Obrázek 5.5: Priepustnosť medzi dvoma PC

5.5 Merania medzi AP a PC

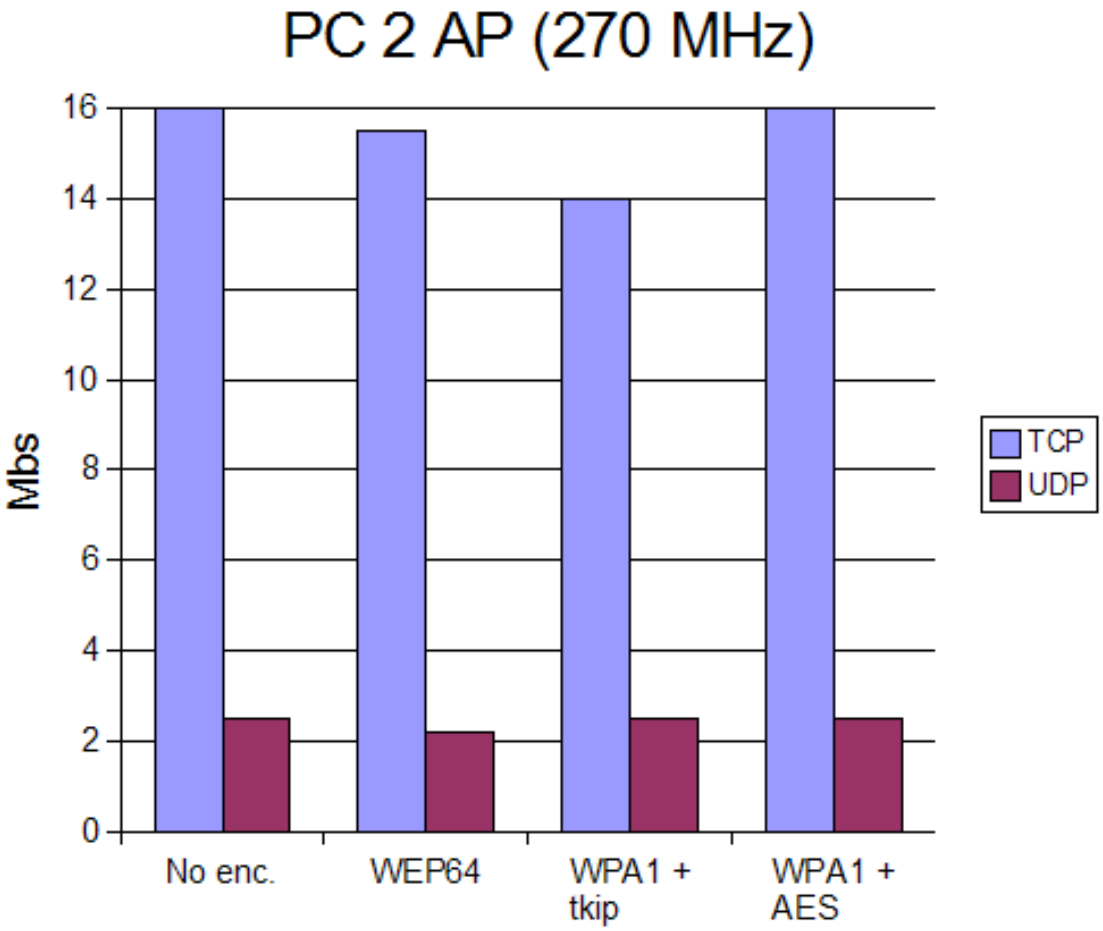
Pri tejto verzii zapojenia komponentov som jedno PC pripojil priamo na AP za použitia bezdrôtovej karty a protokolu WiFi a druhé PC bolo pripojené k AP pomocou UTP Ethernet káblu. Vznikli teda 2 siete, pričom prístupový bod ich vzájomne prepájal za použia dvoch rôznych prístupových médií a protokolov. Aj v tomto prípade slúžil prístupový bod ako jednoduchý smerovač medzi dvoma sieťami. Meranie bolo opäť realizované rovnakým spôsobom ako v predchádzajúcej sad meraní. Opäť sa opakoval príliš pomalý prenos pomocou protokolu UDP, takže ani tento krát nebude použitý pre výsledné porovnávanie. V porovnaní s ňou ale môžeme ľahko vypozorovať celkové zvýšenie prenosových rýchlostí. To je závislé na procesore, ktorý sa stará o šifrovanie a dešifrovanie dát. Relatívne spomalenie v závislosti na type zabezpečenia v porovnaní s nešifrovaným prenosom ale zodpovedá predchádzajúcemu príkladu. Zhodne s minulým meraním bol prenos realizovaný pomocou kopírovania dát z jedného PC na druhé s použitím protokolov FTP (TCP) a TFTP (UDP). Rýchlosť prenosu bola zaznamenaná za použitia nástroju IPtraf. Ani v tomto prípade nedošlo ku značnému čerpaniu systémových zdrojov ani jedného z PC. Výsledky sú zobrazené v nasledujúcom grafe. Výsledky zobrazené na obrázku 5.6.



Obrázek 5.6: Priepustnosť medzi PC a AP

5.6 Doplnkové merania

Ako doplnok uvádzam poslednú sériu meraní, ktorá je prakticky zhodná s predchádzajúcim spôsobom zapojenia. Architektúra siete aj spôsob prenosu dát sa nezmenili. Jediný rozdiel, ktorý tu nastáva je zmena modelu použitého prístupového bodu. Ide o takmer zhodný model, ktorý sa ale od predchádzajúceho modelu odli?uje typom procesoru. Tento model má procesor taktovaný na frekvencii 270 Mhz, čo prakticky dvojnásobok v porovnaní s doteraz testovaným modelom. Reálne sa to prejaví ďalším nárastom prenosových rýchlostí. čo sa týka relatívneho spomalenia pri použití jednotlivých zabezpečovacích mechanizmov, tak je výsledok, prakticky podobný s predchádzajúcimi dvoma meraniami. Použitím mechanizmu WEP sa prenos spomalí o približne 5 %, po nasadení mechanizmu WPA môžeme badať spomalenie o zhruba 15%. Štandard WEP2 nebol vo verzii OS tohto prístupového bodu podporovaný, tak som ako alternatívu zvolil WPA1 s AES. Znovu je zjavné, že AES nespôsobuje žiadnu stratu na efektivite prenosu dát. Výsledky zobrazené na obrázku 5.7.



Obrázek 5.7: Priepustnosť medzi PC a veľkým AP

5.7 Záver meraní

Zo všetkých nameraných hodnôt pri rôznorodých konfiguráciách môžeme odvodiť niekoľko výsledných pozorovaní. V prvom rade sú to hodnoty relatívnych poklesov prenosových rýchlostí v závislosti na zabezpečovacom mechanizme. Pri nasadení štandardu WEP je badateľný pokles rýchlosti v rozmedzí približne 10 - 20 percent v porovnaní s nezabezpečenou verziou. Po použití štandardu WPA som zistil približne 20 - 30 percentné spomalenie prenosu údajov v porovnaní s východzou konfiguráciou. Ochrana poskytnutá štandardom WPA2 so šifrovaním AES neprináša prakticky žiadne negatívne dopady na efektivitu transferu dát. Z hľadiska reálneho nasadenia na skutočnej bezdrôtovej sieti je po konzultácii so správcom prijateľná hodnota cca. 15 percentnej straty prenosového pásma na úkor bezpečnosti. To z hry vyhradzuje WPA1. Použiteľnými variantami teda sú WEP a WPA2. Je všeobecne známe že norma WEP predstavuje pomerne ľahko prelomiteľnú bariéru. Niekoľko útokov si ukážeme v nasledujúcej kapitole. Optimálnym riešením z hľadiska pomeru bezpečnosť / výkon je teda WPA2. Jeho nasadenie je ale nutné zvážiť, pretože nie je plne podporované na starších typoch WiFi zariadení. Ďalšia skutočnosť, ktorá je zrejmá je to, že rýchlosť prenosu je pri šifrovaní limitovaná rýchlosťou procesora AP ako aj klientov. Keďže výkon pracovných staníc je dnes viac než dostatočný, tak úzkym hrdlom sa stávajú prístupové body, kde sa výrobcovia snažia udržať nízku cenu na úkor hrubého výkonu. Nárast efektivity prenosu je priamo úmerný rýchlosti CPU, ktoré je zabudované v AP. To môžeme badať z porovnania posledných dvoch meraní. Treťou podstatnou informáciou, ktorú môžeme vyčítať z nameraných hodnôt je HW akcelerácia šifrovania AES. To je realizované kryptografickým modulom priamo na WiFi karte a nezaťažuje tak hlavný CPU nutnosťou šifrovania dát. Sumarizáciou zistení sa dostávame k finálnemu odporúčaniu, ktoré hovorí: "Pre maximálne utajenie a integritu dát prenášaných po WiFi sieť a najmenej negatívny dopad na efektivitu prenosu je najvhodnejším riešením WPA2, ale jedine s HW podporou na strane klientov aj prístupových bodov."

Na úplný záver ešte musím dodať, že tieto merania sa vzťahujú na prístupové body firmy Mikrotik. Použité CPU pracovali na frekvencii 175, resp. 270 Mhz. Mierny pokles prenosovej rýchlosti pri použití WEP, resp. výraznejší pokles pri použití WPA1 je spôsobený nedostatočným výkonom CPU v AP. Šifrovanie AES je akcelerované priamo na bezdrôtovom adaptéri. Je možné, že implementácia na iných AP je efektívnejšia, prípadne je tam použitý špeciálny typ šifrovacieho koprocesora. Toto meranie teda demonštruje, že v niektorých prípadoch môže zabezpečenie siete znížiť jej priepustnosť, ktorá by v praxi nemala byť výrazne ovpilvnená.

Kapitola 6

Útoky na slabé miesta zabezpečovacích mechanizmov

V kapitole c.4 je pri porovnaní jednotlivých druhov zabezpečenia aj popis slabín jednotlivých schém a možností ich zneužitia. Niekoľko z nich som vykonal a podnikol pár útokov proti jednotlivým druhom zabezpečenia. V nasledujúcej časti ponúkam kompletný popis ich vykonania, vrátane použitých nástrojov, HW aj SW vybavenia. Táto kapitola je dôkazom možnosti prelomenia jednotlivých druhov ochrany. Zároveň zahŕňam aj popis situácie a prostredia, v ktorom útok prebehol. Väčšina z nich bola uskutočnená v laboratórnych podmienkach, ale prikladám aj jednu názornú ukážku z reálneho života. Tento posledný útok bol vykonaný s uvedomením a dovolením od prevádzkovateľa tejto bezdrôtovej siete. Z hľadiska bezpečnosti a rešpektovania práva na súkromie, nebudem uvádzať presné identifikačné ani lokalizačné údaje danej siete. Zároveň chcem čitateľa informovať, že pri žiadnom útoku nedošlo k narušeniu súkromia, odcudzeniu privátnych informácií ani k inému právnemu, či morálnemu priestupku. Pri popise úrovni náročnosti útokov vychádzam zo skrípt predmetu Bezpečnost informačních systému. Pri popise znalostí a zručností útočníka sa zasadzujem do kategórie: "Hacker zo záujmu". Z hľadiska náročnosti útoku môžem útočníka zaradiť do kategórie "skúsený" a použité vybavenie do kategórie "bežné vybavenie". Tieto kategórie sú definované v norme ITSEM. Celkovo boli vykonané tri typy útokov. Prvým z nich je prelomenie šifrovania WEP a to vo verzii s použitím 64 bit ako aj 128 bit kľúča. Druhým je prelomenie šifrovania WPA1 pri použití zdielaného kľúča. Tretím útokom je odhalenie skrytej identifikácie prístupového bodu. Môj posledný útok je principiálne zhodný s prvým. Rozdiel je len v tom, že prebehol v reálnych podmienkach.

6.1 Použité nástroje

Na úspešné vykonanie jednotlivých útokov je potrebné použiť nasledujúce vybavenie. Je nutné vybaviť sa ako po stránke HW tak aj po stránke SW. Rovnako je nutné použit tie správne verzie OS, ovládačov a nástrojov. Nezanedbateľné sú samozrejme aj potrebné znalosti. Z hľadiska dostupnosti nástrojov nejde o žiadne výnimočné kusy HW ani SW. Všetka HW výbava sa dá bežne zakúpiť v každom obchode s výpočtovou technikou za prijateľnú cenu. Zo strany SW výbavy som použil OS a nástroje ktoré sú zdarma dostupné na Internete, resp. sú prístupné študentom FIT - VUT cez program MSDN Academic Alliance. Všetky útoky boli uskutočnené na notebooku kategórie Centrino s využitím zabudovanej WiFi karty Intel, resp. častejšie pomocou prídavnej karty s čipsetom Atheros, ktorá

podporuje monitorovací mód a injekciu paketov. Operačný systém bol striedavo Windows XP, resp. rôzne Linux Live CD distribúcie. Pod OS Windows som nainštaloval ovládače WildPackets. Pod OS Linux som použil pribalené ovládače Madwifi, resp. IPW2200. Ako hlavný nástroj na všetky útoky som použil sadu AirCrack-ng. Tá pozostáva z niekoľkých nástrojov na odchytávanie(airodump) a injekciu(aireplay) paketov plus lámanie WEP a WPA(aircrack). Táto sada utilít je dostupná ako pre Linux, tak aj pre Windows. OS Windows je možné použit len na pasívne útoky a to len s využitím externej WiFi karty s čipsetom Atheros. OS Linux je vďaka pokročilým ovládačom možné použit na pasívne útoky s využitím karty Atheros ako aj zabudovanej karty Intel. S prídavnou kartou je možné vykonať aj aktívny útok.

6.2 Zoznam použitého HW a SW vybavenia:

HW:

- Laptop Siemens Amilo PRO - CPU Pentium M 1.73 GHz
- MiniPCI WiFi card - Intel PRO/Wireless 2200BG
- PCMCIA WiFi card - Wistron PCMCIA Cardbus 802.11a/b/g

OS:

- Windows XP Pro SP2
- Ubuntu Live CD v 6.06
- Hakin9 Live CD v 2.9

Drivers:

- Madwifi (Atheros), IPW 2200 (Intel) - for Linux
- WildPackets Atheros Wireless Driver - for Windows

Utilities (AirCrack-ng v 0.6.2 / 0.7):

- airodump-ng
- aireplay-ng
- aircrack-ng

Jednotlivé použité linuxové distribúcie, ovládače, nástroje a slovníky je možné stiahnuť zdarma na nasledujúcich adresách:

Ubuntu 6.06 http://ubuntu-releases.sh.cvut.cz/dapper/ubuntu-6.06.1-desktop-i386.iso

Hakin9 2.9 ftp://hakin9.wavenet.pl/pub/h9l

WildPackets for Win begin werbatim http://products.wildpackets.com/?v=4a4be5hds3np0048&s=1 endverbatim

AirCrack-ng for Win http://download.aircrack-ng.org/aircrack-ng-0.6.2-win.zip

AirCrack-ng for Lin http://download.aircrack-ng.org/aircrack-ng-0.7.tar.gz

dictionaries http://www.openwall.com/wordlists/

6.3 WEP

Útok proti zabezpečeniu pomocou WEP, presnejšie odhalenie WEP kľúča, patrí medzi najviac diskutované útoky. Najjednoduchší variant je tzv. pasívny útok, kde zapneme odchytávanie zašifrovaných paketov po detekcii prítomnosti WiFi siete zabezpečenej pomocou WEP. Tento variant je na jednej strane zvyčajne časovo náročná, na strane druhej ale vyhovuje paranoickým útočníkom, pretože takmer nie je šanca na ich odhalenie. Útokom typu "brute-force" sa nebudem zaoberať pretože pre 128bit kľúč je neprijateľný. Vyskúšal som tak FSM útok. Ten spočíva v odchytení dostatočného množstva paketov a následného odhalenia kľúča. V prípade, že na sieti neprebieha žiadny prenos dát, tak nemáme šancu kľúč odhaliť. V prípade, že ale prenos prebieha, ale prenesené množstvá sú príliš malé, tak si môžeme dodatočný prenos dogenerovať sami. Použijeme tzv. injekciu paketov. Na to je ale potrebná WiFi karta, ktorá to podporuje a OS Linux, pretože verzie ovládačov pre Windows toto nepodporujú. Pre jednoduchosť som teda zvolil základný pasívny útok.

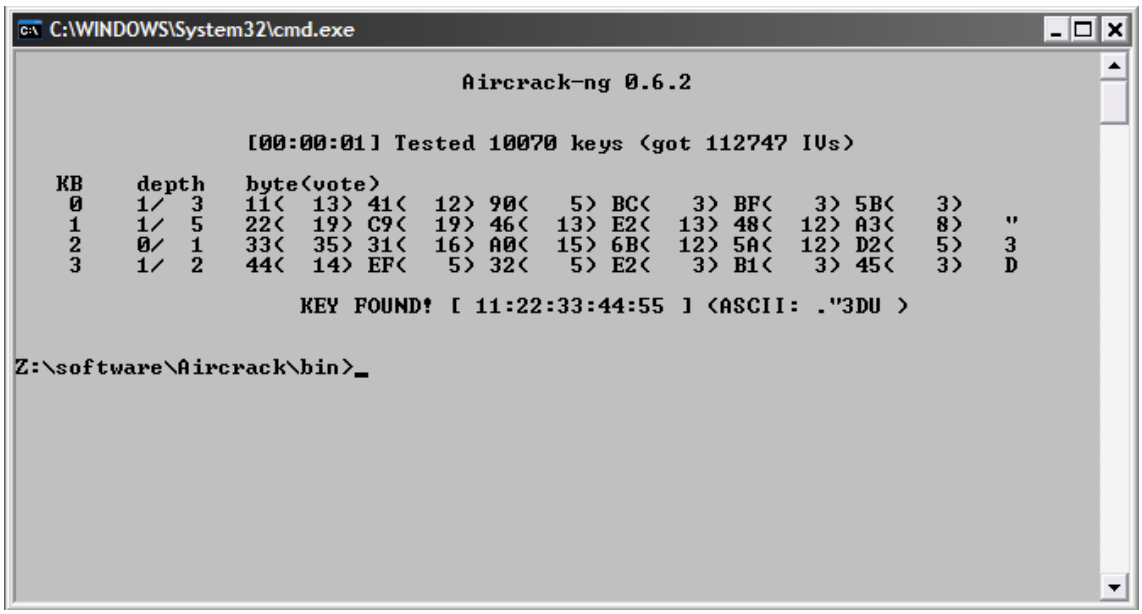
Použité nástroje:

OS Windows XP

WiFi card PCMCIA Atheros

drivers WildPackets

utilities airodump, aircrack



Obrázek 6.1: Odhalenie 64 bit kľúča WEP

6.3.1 Postup vykonania útoku

1. Vložit PCMCIA kartu Atheros do laptopu
2. Nainštalovať ovládače WildPackets pre Atheros

3. Nainštalovať sadu nástrojov AirCrack

4. Z inštalačného adresára spustiť aplikáciu *"airodump-ng.exe"*. Následovne je nutné vybrať bezdrôtový adaptér z ponúknutého zoznamu (PCMCIA), ďalej špecifikovať typ použitého čipsetu (Atheros), vybrať číslo kanála podla frekvenčného pásma, na ktorom prebieha komunikácia, zadať prefix mena súboru, do ktorého sa uložia zachytené dáta a vybrať si, či sa budú ukladať celé rámce, alebo len hodnoty IV (stačí uchovať len IV).

5. Po ukončení odchytávania dát spustíme aplikáciu *"Aircrack-ng GUI.exe"*. Zadáme cestu k súboru odchytených IV a po zaškrtnutí voľby *"Use advanced WPA or WEP options"* môžeme špecifikovať dĺžku kľúča, ktorý chceme odhaliť, prípadne SSID prístupového bodu, ktorý nás zaujíma. Tieto údaje sú nepovinné, ale v prípade, že vieme ich hodnoty, tak urýchlia prelomenie kľúča. Samotný proces lámania spustíme tlačidlom *"Launch"*. Výsledky sú zobrazené na obrázkoch 6.1 a 6.2.

Úspech tohoto útoku silne závisí na množstve odchytených dát. Presnejšie na množstve odchytených hodnôt IV. Na stránkach tvorcu nástroja AirCrack sú udávané hodnoty cca. 300 000 hodnôt IV pre prelomenie 64bit klúca a až 1 000 000 hodnôt IV pre prelomenie 128bit kľúča. Pri mojich viacnásobných pokusoch v laboratórnych podmienkach som meraniami došiel k nasledujúcim záverom. Bezpečné hodnoty, pri ktorých sa väčšinou podarí kľúč prelomiť sú:
64bit kľúč: 150 000 IV = 100 MB prenesených dát
128bit kľúč: 400 000 IV = 400 MB prenesených dát

Minimálne hodnoty, ku ktorým sa mi podarilo dostať sú: 110 000 IV pre 64bit a 300 000 IV pre 128bit. Na nasledujúcich obrázkoch sú ukážky prelomenia 64bit aj 128bit kľúčov spolu s ich hodnotami a časom samotného prelomenia. Potrebný čas bol 1 resp. 4 sekundy.

Pre lepšie priblíženie situácie, v ktorej bol experiment zrealizovaný prikladám jeho popis. Sieť bola vytvorená z dvoch AP, ktoré boli navzájom bezdrôtovo spojené, jeden z nich fungoval v režime prístupového bodu, druhý ako klient. Na Ethernet port každého AP bolo pripojené PC. Pevné sieťové segmenty boli nakonfigurované s IP adresami z odlišných podsietí. Prístupové body tak zastávali súčasne funkciu smerovačov. Toto zapojenie je prakticky zhodné so zapojením použitým pre meranie priepustnosti v kapitole 5.3. Jediný rozdiel je použite WiFi karty zapojenej do jedného z PC na odchytávanie prenose na šifrovanom bezdrôtovom segmente. Prenos bol generovaný prenosom dát pomocou FTP protokolu z jedného PC na druhé. Viacnásobným odchytávaním dát pri prenose medzi dvoma PC, pričom kvantitu údajov som postupne znižoval až na minimálne hodnoty, pri ktorých bolo prelomenie kľúča úspešné. Takýto postup nám dáva prehlad o reálnom množstve dát, ktoré musia byt prenesené bezdrôtovou sieťou. Tieto merania som zopakoval pre 64 i 128bit kľúč.

Rovnaký útok je možné zrealizovať aj s alternatívnym vybavením - OS Linux Hakin9 a WiFi Intel.

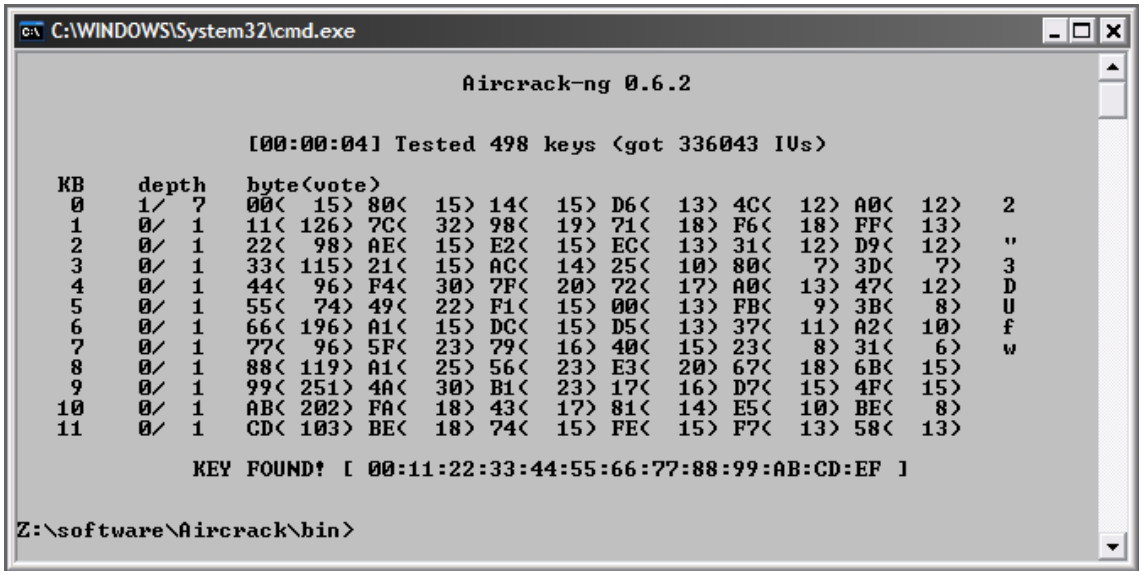
Alternatívne použitelné nástroje:

OS Linux Hakin9

WiFi card PCI Intel

drivers IPW2200

utilities airodump, aircrack



Obrázek 6.2: Odhalenie 128 bit klúca WEP

6.4 WPA

Chyby v implementácii mechanizmov na utajenie a integritu dát pre štandardy WPA a WPA2 nie sú známe, resp. nie je známy spôsob ich zneužitia. Jediná chyba, ktorá je dobre známa a za istých podmienok úspešne zneužiteľná je autentizácia. Princíp overovania identity je spoločný ako pre WPA, tak aj pre WPA2. Jej prelomenie je teda možné v oboch štandardoch. Pri autentizácii ale musíme rozlišovat, či ide o tzv. zdielaný mód, ale je použitý centrálny autentizačný server. Úspešné vykonanie útoku je možné len pre zdielaný mód, prípadne aj pri centrálnom overovaní, avšak len za podmienky, že je použitý slabý autentizačný protokol. Takým je napríklad LEAP od firmy Cisco, ktorý sa ale odporúča nahradiť novou bezpečnou verziou EAP FAST. V mojom prípade som sa zameral na zneužitie overovania v móde so zdielaným kľúčom. Jeho kompromitáciou získame prístup do siete a zároveň nie je možné odhaliť našu identitu. Je to dôsledok spoločného kľúča pre všetkých užívateľov a situácia je teda veľmi podobná ako v prípade použitia WEP. Útok je opäť popísaný v predchádzajúcich kapitolách. Nejde pri ňom o zneužitie rovnakej chyby ako pri WEP ale o odchytenie autentizačného procesu. Presnejšie o rámce reprezentujúce spôsob "výzva a odpoveď". Kľúčom k úspechu je teda odchytenie autentizačných rámcov,ktoré obsahujú reťazec, ktorý zasiela AP klientovi a ten následne odpovedá jeho zašifrovanou verziou pomocou kľúča odvodeného od zdielaného kľúča. To znamená, že potrebujeme zachytiť len malé množstvo paketov, ale tých "správnych" paketov. Následne spustíme tzv. "offline" útok, kde skúšame zašifrovať reťazec výzvy pomocou jedného zo slovníkových hesiel a porovnávame ho s odpoveďou. K tomu je potrebný rozsiahly slovník. Akcia bola realizovaná na OS Windows s použitím AirCrack. Jedná sa o typ pasívneho útoku.

Použité nástroje:

OS Windows XP

WiFi card PCMCIA Atheros

drivers WildPackets

utilities airodump, aircrack

dictionary EN openwall

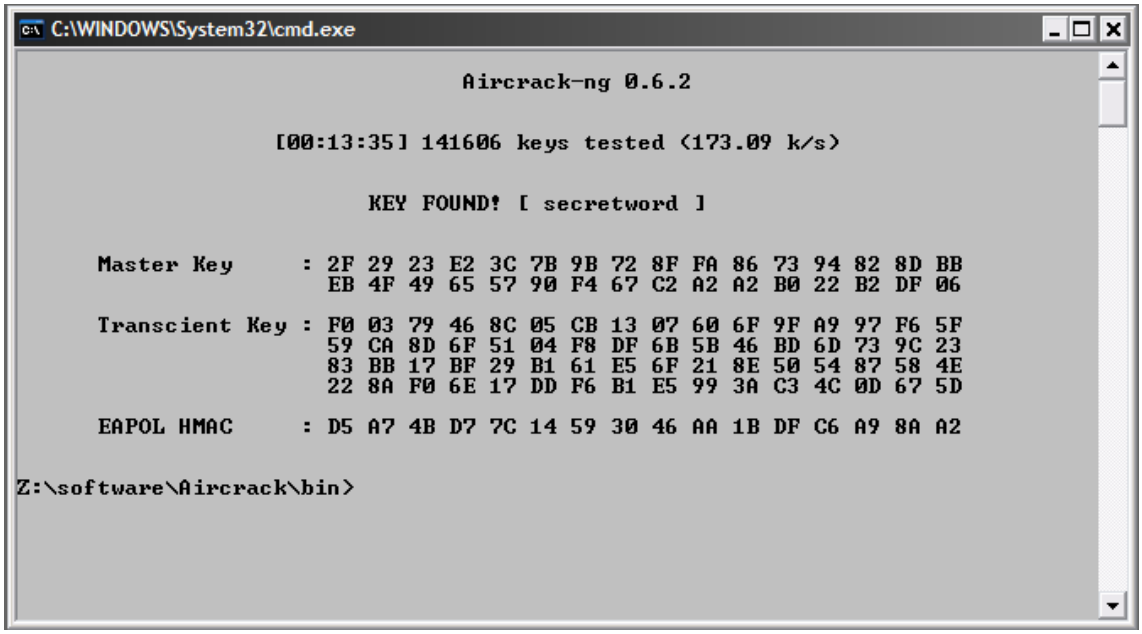
6.4.1 Postup vykonania útoku

1. Vložiť PCMCIA kartu Atheros do laptopu
2. Nainštalovat ovládace WildPackets pre Atheros
3. Nainštalovat sadu nástrojov AirCrack
4. Z inštalačného adresára spustiť aplikáciu *"airodump-ng.exe"*. Následovne je nutné vybrat bezdrôtový adaptér z ponúknutého zoznamu (PCMCIA), ďalej špecifikovať typ použitého čipsetu (Atheros), vybrať číslo kanála podla frekvenčného pásma, na ktorom prebieha komunikácia, zadať prefix mena súboru, do ktorého sa uložia zachytené dáta a vybrať si, či sa budú ukladať celé rámce, alebo len hodnoty IV (v tomto prípade je nutné ukladať celé rámce).
5. Po tom ako sme si istý, že sme zachytili proces autentizácie spustíme aplikáciu *"Aircrack-ng GUI.exe"*. Prepneme sa na záložku *"WPA"* a zadáme cestu ku slovníku. Samotný lámanie kľúča spustíme tlačidlom *"Launch"*.

Úspech tohoto útoku je silne závislý na niekoľkých skutočnostiach. Prvým predpokladom je že je použitý zdielaný autentizačný mód. Ďalším z nich je skutočnosť, že medzi zachytenými rámcami je zachytený aj proces overovania aspoň jedného klienta. Najpodstatnejšou limitáciou je ale nutnosť použitia triviálneho slovníkového hesla, ktoré je obsiahnuté v nami použitom slovníku. Pre demonštráciu tohto druhu útoku som použil anglický slovník, ktorý som získal z vyššie uvedenej adresy. Zoznam obsahuje takmer 450 000 anglických slov a postupností znakov, ktoré môžu byt použité ako heslo. Tento slovník ale neobsahuje zďaleka všetky slová anglického jazyka. Nenašiel som tam niekoľko slov, ktoré by som použil ja sám ako slovníkové heslo. Navyše použitý zoznam neobsahuje kombinácie bežných slov vytvorené s použitím rôznych predpôn, či prípon. Nástroj AirCrack tiež neskúša vytvárať viacslovné kombinácie zo slov obsiahnutých v poskytnutom slovníku. Rýchlosť vyskúšania všetkých slovných hesiel závisí jednak od rýchlosti CPU a tiež od rozsiahlosti slovníka. Na procesore Pentium M 1,73 GHz trvalo vyskúšanie 450 000 slov cca. 15 minút.

Popis experimentálneho prostredia a siete je nasledovný. Použil som dva AP, ktoré som vzájomne prepojil. Jeden z nich bol nakonfigurovaný ako prístupový bod, druhý ako klient. Ako zabezpečovací mechanizmus som nastavil WPA v móde so zdielaným kľúčom. Kedže oba AP sú od rovnakého výrobcu, tak sa automaticky po spustení spoja. Prebehne tak autentizácia pomocou tzv. "challenge-response handshake". Pre vykonanie útoku je potrebné odchytiť len túto inicializačnú komunikáciu a nie je nutný žiadny další dátový prenos. Postačilo teda zapnúť odchytávanie paketov pomocou prídavnej WiFi karty v monitorovacom móde a reštartovat AP, ktorý bol v klientskom móde. Ten po nabehnutí požiadal o overenie identity. Zobrazenie výsledku je na nasledujúcom obrázku. Potrebný čas bol vyše 13 minút. Výsledok je na obrázku 6.3.

Rovnaký útok je možné zrealizovať aj s alternatívnym vybavením - OS Linux Hakin9 a WiFi Intel.



Obrázek 6.3: Odhalenie zdielaného kľúča WPA

6.5 Skryté SSID

Tento útok je špeciálneho typu pretože nie je namierený proti zneužívaniu žiadnej z chýb v dostupných bezpečnostných mechanizmov. Nejde teda o prelomenie ochrany utajenia, integrity dát ani autentizácie. Je to demonštrácia nedokonalosti spôsobu ochrany bezdrôtových sietí, ktoré sú skryté. Pod týmto pojmom sa rozumie nastavenie AP tak, aby nevysielal identifikátor siete SSID. Následkom toho sa táto bezdrôtová sieť nezobrazí v zozname dostupných sietí, aj keď sa klient nachádza v pokrytí jej signálom. Klientské PC, ktoré sa chce na takúto sieť pripojiť musí mat explicitne špecifikované SSID na svojej strane. Len v takomto prípade je potom umožnené klientovi pripojiť sa. Samozrejme môže nasledovať aplikácia ďalších bezpečnostných mechanizmov ako WEP, či WPA. Skryté SSID teda môže byt použité ako jediný ochranný mechanizmus alebo môže byt použitý ako prvá línia obrany. Na detekciu signálu AP, ktorý nevysiela svoj SSID je nutné použiť špeciálny nástroj. Medzi ne patrí napríklad volne dostupná utilita pre OS Windows NetStumbler, alebo môžeme použiť odchytávanie paketov v monitorovacom móde pomocou airodump-ng, ktorý zároveň vypisuje zoznam dostupných AP spolu s ich MAC adresou, bez ohľadu na to, či vysielajú ich SSID. Vykonanie samotného útoku je zvyčajne veľmi rýchle, ale musí mu predchádzať dôkladné vybavenie sa vhodnými HW aj SW prostriedkami. V prvom rade je nutné použiť WiFi kartu s ovládačmi ktoré umožňujú tzv. injekciu paketov. Pod týmto pojmom rozumieme vysielanie WiFi rámcom na určitej frekvencii bez nutnosti predchádzajúcej asociácie s vybraným AP. Toto v bežnej situácii nie je možné. Takúto možnosť nám ponúkajú len ovládače pre OS Linux pre vybrané WiFi adaptéry. Preto som pre tento útok použil OS Linux spolu s PCMCIA kartou Atheros a ovládačmi MadWifi. Zároveň je nutné použiť druhý WiFi adaptér, ktorý pasívne zachytáva dáta v monitorovacom móde. Podstata tohoto útoku spočíva v tom, že SSID je utajené počas celej komunikácie klienta s AP. Výnimkou je re-asociácia klienta voči AP. Tá môže nastať z rôznych príčin, ale je možné ju vyvolať aj umelo. To znamená vyslať na používanej frekvencii pakety s podvrhnutou zdrojovou MAC

adresou klienta, ktorý je aktuálne asociovaný s AP. Ako cieľová adresa bude použitá MAC adresa AP. Tieto adresy je možné jednoducho zistiť pomocou nástroja airodump-ng. Táto falošná de-asociácia vyvolá automatickú re-asociáciu, ktorá už ale obsahuje SSID identifikátor. Tieto pakety potom musíme odchytiť na druhom WiFi adaptéri, ktorý priebežne odchytáva pakety. Na tieto účely postačí WiFi Intel s ovládačmi IPW2200. Tieto odchytené dáta uložíme a pomocou nástroja na analýzu sieťovej komunikácie, napríklad WireShark, nájdeme SSID identifikátor. Tento typ útoku patrí medzi aktívne útoky. Pri jeho vykonávaní v praxi, tak útočníkovi hrozí isté riziko, že bude odhalený.

Použité nástroje:

OS Linux Ubuntu

WiFi card PCMCIA Atheros, PCI Intel

drivers MadWifi, IPW2200

utilities aireplay, airodump

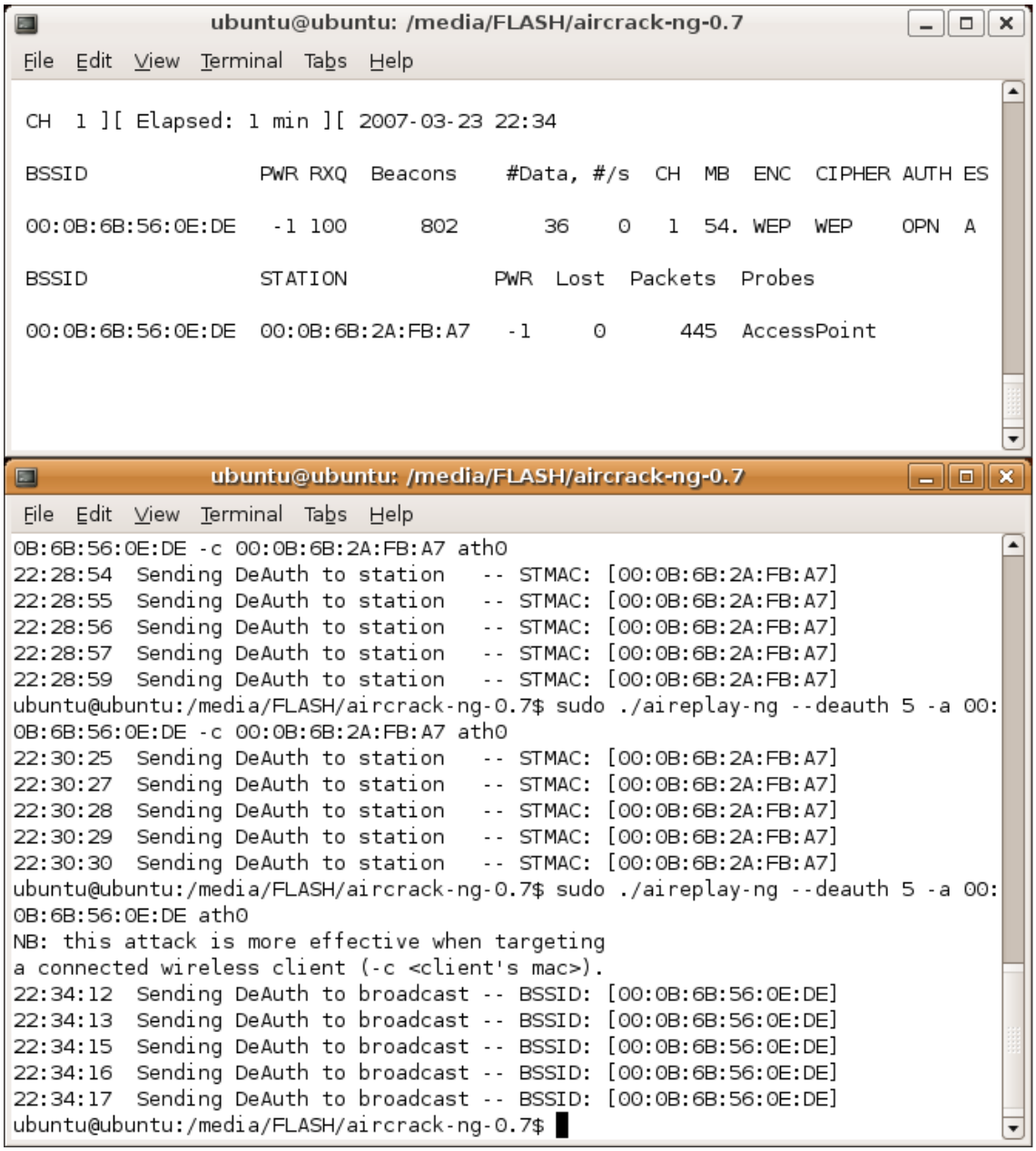
6.5.1 Postup vykonania útoku

1. Do laptopu vložit PCMCIA kartu Atheros
2. Nabootovat Linux Ubuntu 6.06 z live CD
3. Pripojit diskovú partíciu alebo USB disk, kde sa nachádzajú binárne súbory nástroja AirCrack-ng. Ten odporúčam vopred preložiť pod inou Linux distribúciou založenou na Debian-e (napr. Knoppix)
4. Oba bezdrôtové karty by mali byt správne detekované a ich ovládače automaticky nainštalované. Overíme to výpisom pomocou príkazu *"iwconfig"*.
5. Spustíme odchytávanie paketov pomocou adaptéru Intel v monitorovacom móde. Použijeme nástroj *"airodump-ng"*. V parametroch špecifikujeme sieťový adaptér, kanál na ktorom prebieha komunikácia a vyžiadame zápis získaných dát do súboru, ktorého meno zadáme. Ako výsledok sa nám zobrazí výpis dostupných AP spolu s ich MAC adresami ako aj výpis MAC adries klientov, ktorí sú na nich pripojení. Meno SSID nebude ale viditeľné.
6. Následne spustíme falošnú de-autentizáciu. Máme na to dve možnosti. Buď si vyberieme jedného z klientov, ktorí sú pripojený na cieľový AP a nasimulujeme odpojenie pomocou jeho MAC, alebo skúsime tzv. Broadcast de-autentizáciu. Prvý spôsob je spolahlivejší. Proces spustíme príkazom zobrazeným na obrázku 6.4.

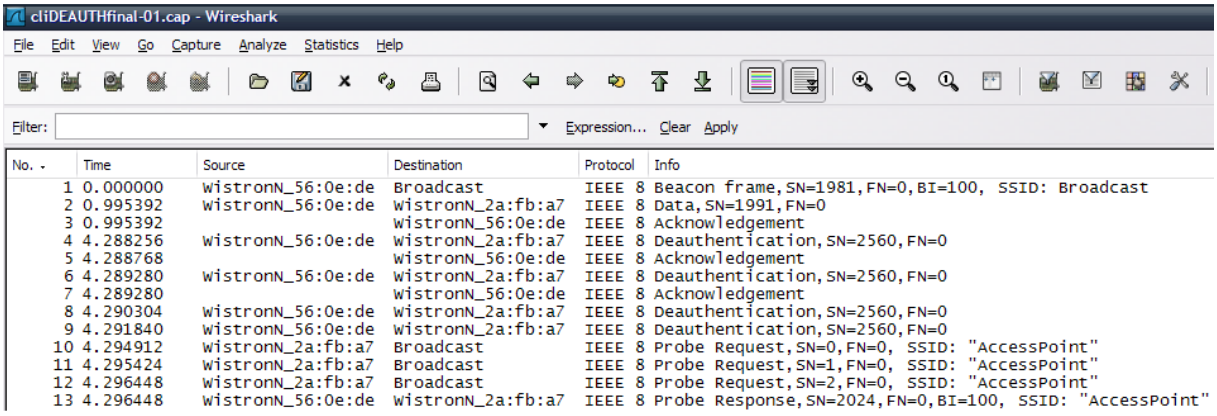
   Kde číslo 5 znamená počet vyslaných de-autentizácii.
7. Ukončíme odchytávanie paketov a súbor s príponou *".cap"* otvoríme bežným sieťovým analyzátorom. Použiť môžeme napr. WireShark. V mojom prípade som ho nainštaloval na OS Windows. Názov SSID nájdeme jednoducho.

Úspech tohto útoku opäť závisí od viacerých skutočností. V prvom rade je nutné použiť WiFi adaptér, ktorý podporuje injekciu paketov. Rovnako je nevyhnutné použit OS Linux s tou správnou verziou ovládačov. Pre kartu Atheros sa mi podarilo nájsť jedinú z bežne používaných Live CD distribúcií a to Ubuntu 6.0.6. Zároveň potrebujeme druhý bezdrôtový

adaptér. Pre ten ale postačí podpora pasívneho odchytávania v monitorovacom móde. Na tie účely výborne poslúži karta Intel, ktorá je v rôznych verziách obsiahnutá vo väčšine obľúbených laptopov označených "Centrino". Zároveň je pre úspešné odhalenie AP so skrytým SSID nutné ho najprv lokalizovať. Podstatným faktom je aj to, že v dobe útoku musí byt k AP pripojený aspoň jeden bezdrôtový klient. Výsledok je na obrázku 6.5.



Obrázek 6.4: Podvrhnutá de-autentizácia



Obrázek 6.5: Odhalenie skrytého SSID

6.6 Útok na reálnu sieť

Posledný z vykonaných útokov, je principiálne zhodný s prvým z poskytnutého zoznamu. Ide teda o prelomenie šifrovania WEP. Rozdiel je ale v tom, že tento pokus prebehol v reálnom prostredí. Ide o súkromnú sieť, ktorá je využívaná tromi klientmi. AP je nastavené tak, že vysiela identifikátor SSID. Na zabezpečenie je použitý mechanizmus WEP s kľúčom dĺžky 128 bitov. Nie je tam žiadne obmedzenie podla MAC adresy klienta. Ďalšie informácie o umiestnení a popise siete nebudem z dôvodu ochrany súkromných informácií a možnosti zneužitia uvádzať. Útok bol ale vykonaný s vedomím prevádzkovateľa. Ten rovnako súhlasil so zverejnením odhalenej hodnoty WEP kľúča. Pre bližší popis situácie uvádzam nasledovný popis. Na AP bol pripojený jeden klient. Ten v priebehu celej doby sledoval video stream z internetovej televízie. HW a SW výbava, ako aj postup je zhodný s kapitolou 6.3. Samotné odchytávanie dát trvalo približne 5h 30min. Počas tejto doby som odchytil asi 300 000 hodnôt IV. To je zároveň minimálny počet IV, pri ktorom sa mi podarilo prelomiť zabezpečenie pomocou 128 bit kľúča. Samotné rozlúsknutie už potom bolo otázkou niekoľkých sekúnd. To znamená, že v praxi je časovo najnáročnejšia časť získanie dostatočného množstva dát. Na prelomenie 64 bit kľúča zvyčajne postačí niekoľko hodín, pri veľmi vysokom využívaní siete dokonca niekoľko minút. Na 128 bit kľúč sa tieto časy pohybujú vyššie. Môžu zabrať aj celý deň. Pod pojmom nízke, resp. bežné využívanie siete rozumieme komunikáciu typu: prezeranie web stránok, písanie e-mailov a podobne. Pojem vysoké využívanie siete popisuje proces sledovania audio/video streamu, sťahovanie dát väčšieho objemu a podobne. Veľmi podstatným faktorom je aj počet aktuálne pripojených klientov. Ten sa dá zistiť jednoducho pomocou nástroja *"airodump-ng"*. V momente keď detekujeme AP aj klienta, ale tí nie sú navzájom asociovaný, sa nám útok nepodarí. Odchytíme síce malý počet WiFi rámcov, sú to len synchronizačné rámce a nie sú zašifrované.

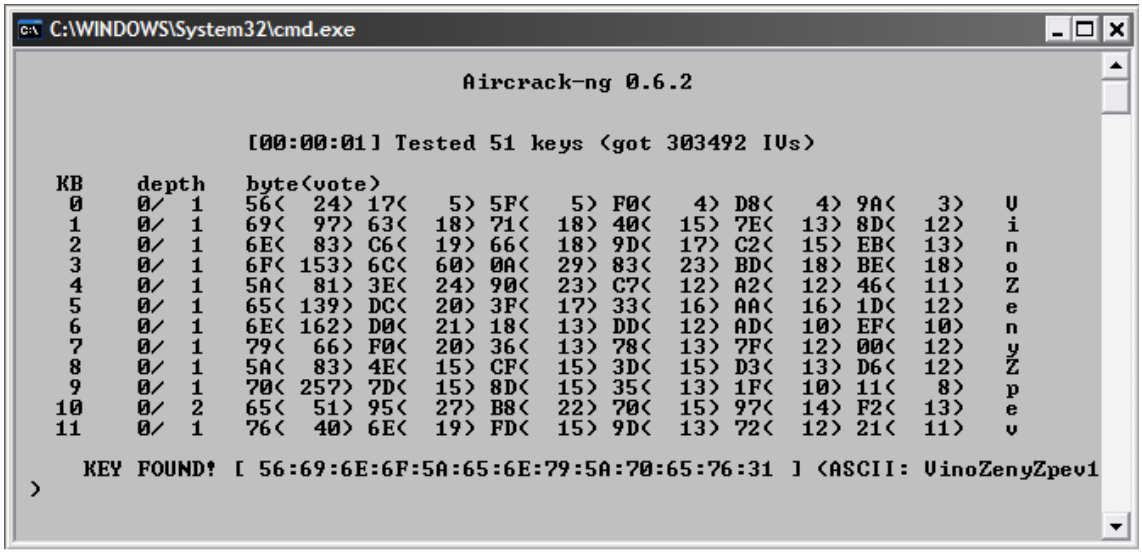
Použité nástroje:

OS Windows XP

WiFi card PCMCIA Atheros

drivers WildPackets

utilities airodump, aircrack



Obrázek 6.6: Prelomenie ochrany reálnej WiFi siete

Popis vykonania útoku je zhodný z popisom uvedeným v kapitole 6.3.

6.7 Možné problémy

Prvou skutočnosťou, ktorá zrejme prekvapí začínajúceho útočníka, resp. správcu siete, je fakt, že nie všetky bezdrôtové adaptéry, resp. ich ovládače možno použiť na rôzne druhy útokov. Vo všeobecnosti môžeme povedať, že najmenšia podpora pre útoky je pre adaptéry Intel a OS Windows. Karty Intel umožňujú jedine pasívne útoky, aj to za podmienky použitia OS Linux a vhodného ovládača. Aktívne útoky nie sú podporované. Lepšie sú na tom špeciálne rozširujúce WiFi s čipsetmi Atheros, Prism alebo Hermes. Tie sa ale bežne nepoužívajú ako vstavané riešenia v štandardných laptopoch. Tieto karty podporujú zväčša pasívne útoky s OS Windows a aktívne útoky s OS Linux. V skratke môžeme povedať, že kombinácia WiFi Atheros + OS Linux je najlepším riešením, pričom kombinácia WiFi Intel + OS Windows je pre útočníka nepoužiteľná. Tento fakt, je ale kladne prispieva k akémusi implicitnému stavu zabezpečenia bezdrôtových sietí.

Ďalším nepríjemným prekvapením môže byť poznanie, že nie všetky verzie ovládačov sú tie pravé pre úspešné vykonanie útoku. V tomto prípade mám na mysli ovládače pre WiFi

kartu Atheros. Tie sú často zahrnuté v bežných Linuxových distribúciach, avšak často vo verzii, s ktorou buď adaptér nefunguje vôbec, alebo nejde prepnúť do monitorovacieho módu.

Pre útoky na Wifi rozširujeme 3 stupne použiteľnosti WiFi adaptéru. Prvým z nich podpora tzv. Promiskuitného módu. Ten umožňuje zachytávať rámce, ktoré nenesú našu fyzickú adresu. V tomto prípade ale musíme byť pripojený k AP. Použiť ho môžeme len na tzv. "sniffing". Druhým stupňom je podpora monitorovacieho módu. Ten umožňuje to isté čo promiskuitný mód, ale v tentokrát nemusíme byť pripojený k AP. Prináša to možnosť pasívnych útokov. Poslednou métou je podpora tzv. "packet injection". To znamená, že môžeme dáta nie len prijímať, ale ich aj vysielať a to bez nutnosti byť asociovaný s daným AP.

V neposlednej rade musím pripomenúť, že pre úspešnú realizáciu pasívneho útoku voči WEP alebo WPA-PSK nepostačí len prítomnosť samotného AP ani AP a klientskej stanice. Je nutné aby bol klient pripojený na AP a zároveň prebiehal prenos dát. Ak klient nie je s AP asociovaný, tak zachytíme jedine synchronizačné rámce a tie nie sú šifrované. Musí isť o prenos užitočných dát. Minimálne fakt, že klient je asociovaný s daným AP zväčša postačí, pretože na sieti zvykne prebiehať komunikácia typu broadcast, ktorú majú na svedomí protokoly NBT, CDP, RIP...

6.8 Záver útokov

Účelom tejto kapitoly bolo poskytnúť prehľad známych a zneužiteľných chýb v jednotlivých zabezpečovacích mechanizmoch pre WiFi. Zároveň som demonštroval na praktických príkladoch ako na jednotlivé slabiny zaútočiť. Tie znázorňujú stupeň náročnosti úspešneho vykonania útoku z pohľadu potrebných znalostí útočníka, technického vybavenia a potrebného času. Medzi všeobecne známe slabiny, ktoré je možné zneužiť patrí obídenie filtrovania podľa MAC adresy, odhalenie skrytého SSID, prelomenie WEP šifrovania, prelomenie EAP-PSK autentizácie a LEAP autentizácie pre WPA1 a WPA2. Existuje niekoľko málo ďalších útokov, ktorými som sa nezaoberal. Napríklad tzv. "KoreK chopchop attack", ktorý spočíva v zneužití CRC32 ako algoritmu na zaručenie integrity. Pri tomto útoku sa odchytí šifrovaný paket a ten sa opakovane pozmení a zasiela späť na AP. Napokon tak odhalíme celý nešifrovaný obsah, avšak praktické použitie takéhoto útoku je dosť mizivé. Ďalším príkladom útoku môže byť "Man In the Middle", kde medzi klienta a AP postavíme podvrhnuté vlastné AP. Takýto útok je ale pomerne náročný a komplikovaný. Ak by sme mali zhrnúť celkovo známe slabiny protokolov a možnosti útoku na nich, tak dôjdeme k nasledujúcemu zoznamu:

1. WEP - útok na šifrovanie a integritu (nástroj: aircrack-ng, weplab,...)
2. WPA PSK - slovníkový útok na autentizáciu (nástroj: aircrack-ng)
3. WPA Enterprise - bezpečné (okrem LEAP - nástroj: asleap)
4. WPA2 PSK- slovníkový útok na autentizáciu (nástroj: aircrack-ng)
5. WPA2 Enterprise - veľmi bezpečné (okrem LEAP - nástroj: asleap)

Kapitola 7

Autentizácia

Autentizácia užívateľov pri pripájaní sa do bezdrôtovej siete je rovnako dôležitá ako zaistenie utajenia a integrity prenášaných dát. Protokol WEP poskytuje len zdieľanú autentizáciu, to znamená, že všetci užívatelia sa prihlasujú rovnakým zdieľaným heslom. Takáto autentizácia je veľmi obmedzená. Na jednej strane obmedzuje prístup do siete len užívateľom, ktorý toto heslo poznajú. Na strane druhej ale neposkytuje žiadnu možnosť ako jednotlivých užívateľov od seba odlíšiť. To prakticky znemožňuje akýkoľvek efektívny audit. Rovnako v prípade zkompromitovania tohoto hesla je nevyhnutné zmeniť zdieľané heslo, distribuovať ho bezpečným kanálom všetkým užívateľom a prekonfigurovať všetky klientské stanice. Podobnú funkcionalitu ponúka aj WPA-PSK resp. WPA2-PSK. Proti týmto autentizačným mechanizmom je ale jednoduché zaútočiť a prelomiť ich ochranu.

Omnoho komplexnejší a bezpečnejší prístup ponúka tzv. "WPA Enterprise" mód. Toto pokročilé riešenie je možné použiť v kombinácii s WPA alebo WPA2 zabezpečením. Overovanie užívateľov prebieha voči autentizačnému serveru RADIUS. Ten následne využíva vlastnú zjednodušenú databázu užívateľských účtov, alebo môže využívať externú adresárovú službu v podobe OpenLDAP, MS Active Directory alebo podobnú, prípadne SQL databázu. WPA Enterprise mód sa nazýva aj WPA-EAP, čo je výstižnejšie pomenovanie, pretože na overenie sa používa práve EAP protokol. EAP znamená "Extensible Authentication Protokol". Je to teda rozšíriteľný overovací protokol a umožňuje overovať identitu klienta rôznymi spôsobmi. Medzi ne patrí aj použite klientského certifikátu, SmartCard, alebo niektorého zo zjednodušených mechanizmov. Tie môžu umožňovať jednosmerné alebo vzájomné overenie. Medzi ne patria EAP-TTLS, PEAP, LEAP a ďalšie. Popísané sú v kapitole 3.2.3.

Prvá z možných variant pre autentizáciu, ktorá bola zavedená spolu so štandardom WPA1 je EAP-TLS. Táto metóda je najbezpečnejšia zo všetkých a široko podporovaná v OS aj v HW, vrátane relatívne starých typov klientských adaptérov. Jej veľkou nevýhodou je ale náročnosť na konfiguráciu, kde je potrebné vystaviť a nainštalovať certifikát pre každú klientskú stanicu. Toto je v mnohých prípadoch nepredstaviteľná záťaž pre správcov siete ako aj samotných klientov.

Následne bolo zavedených niekoľko ďalších mechanizmov. Tie nepožadujú klientské certifikáty, ale väčšinou je potrebné vystaviť a nainštalovať certifikát pre autentizačný server. Vo všeobecnosti môžeme povedať, že HW, ktorý podporuje zabezpečenie WPA podporuje len EAP-TLS autentizáciu, zatiaľ čo HW certifikovaný pre WPA2 podporuje aj väčšinu ďalších overovacích mechanizmov. Z hľadiska podpory v OS sa zameriam na najpoužívanejšie klientské operačné systémy. Podľa štatistík serveru navrcholu.cz [5] mal na Českom trhu systém MS Windows XP zastúpenie v podobe 79 % a MS Windows 2000 v podobe 10%. Ostatné systémy sú štatisticky zanedbateľné. V OS Windows XP a 2000 je vs-

tavaná podpora pre EAP-TLS a PEAPv0 autentizáciu. Keďže je prvá verzia s klientskými certifikátmi prakticky nepoužiteľná, tak nám zostáva metóda PEAP. V nasledujúcej tabuľke uvádzam prehľad najrozšírenejších overovacích metód. Po porovnaní všetkých tabuľkových aspektov vychádza ako najlepšia voľba EAP-TTLS alebo PEAPv0. Výťazom je PEAP, kvôli podpore v OS Windows. Údaje čerpané z knihy Real 802.11 Security [2].

Protokol	**EAP-TLS**	**EAP-TTLS**	**PEAPv0**	**PEAPv1**	**LEAP**
Bezpečnosť	veľmi vysoká	vysoká	vysoká	vysoká	nízka
Konfigurácia	zložitá	stredne zložitá	stredne zložitá	stredne zložitá	jednoduchá
Cert.serveru	áno	áno	áno	áno	nie
Cert.klienta	áno	nie	nie	nie	nie
Podpora v OS	veľmi široká	široká	široká	úzka	stredná

Tabulka 7.1: Prehlad štandardov.

7.1 Praktická konfigurácia WPA-EAP auntentizácie

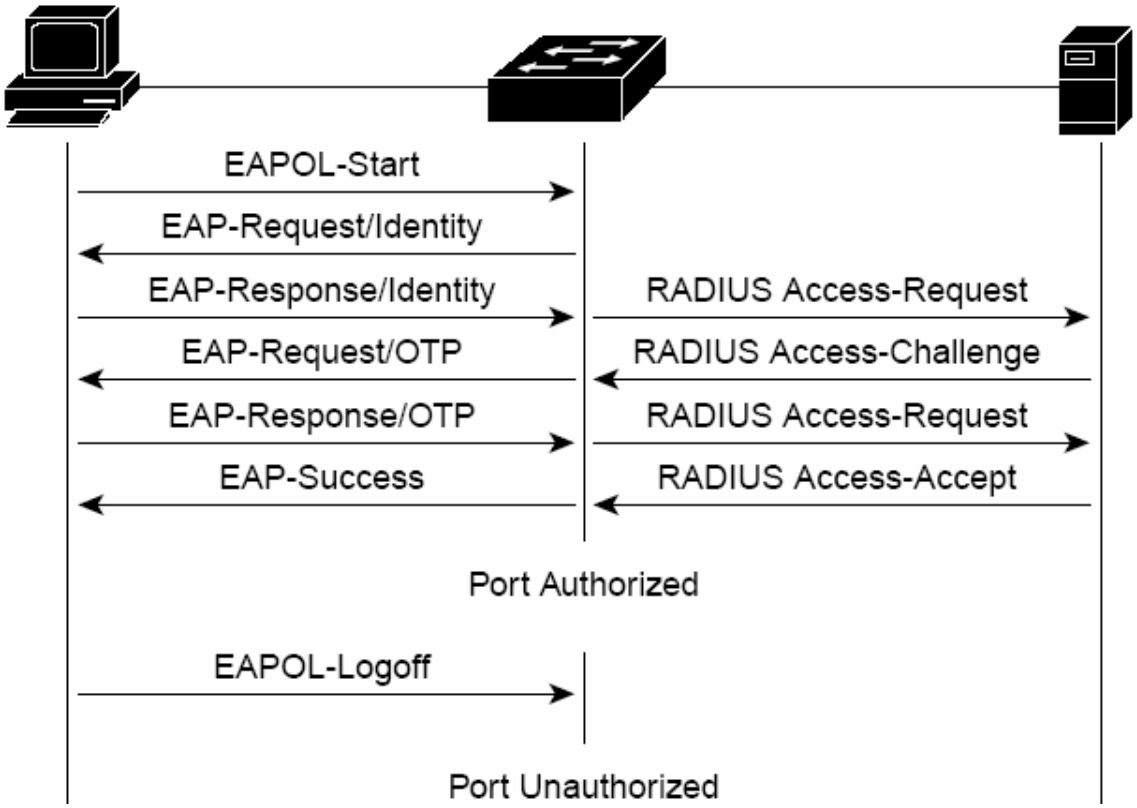
V tejto časti uvádzam praktickú ukážku konfigurácie centralizovanej autentizácie pre overovanie užívateľov pri bezdrôtovom prístupe do siete. Jej prínosom by mal byť reálny odhad o tom, čo všetko musí urobiť správca siete aby úspešne nasadil bezpečný autentizačný mechanizmus do svojej siete. Pri tomto riešení sú vždy vstupujú do hty 3 základné komponenty:

1. Klient
2. Prístupový bod (RADIUS klient)
3. Autentizačný server (RADIUS)

Pri výbere konkrétnych zástupcov všetkých komponent som postupoval tak, aby som pokryl čo najširšie spektrum potenciálnych klientov a zákazníkov. Inými slovami som zvolil tie najrozšírenejšie riešenia. Zároveň som ale dbal na to, aby to nebolo na úkor bezpečnosti, či jednoduchosti konfigurácie. Ako klient bol použitý laptop s WiFi kartou zahrnutou v konfigurácii "Centrino". V tomto prípade Intel BG2200. Rovnaká, alebo širšia podpora štandardov je ale zahrnutá vo všetkých ostatných kartách typu v laptopoch typu "Centrino". Ako operačný systém som zvolil Windows XP SP2. Ako prístupový bol som použil AP firmy Mikrotik. Tento typ je veľmi rozšírený a ponúka veľmi rozsiahle možnosti konfigurácie a podporu štandardov pri zachovaní prijateľnej ceny. Na post autentizačného serveru som vybral open source riešenie FreeRadius. Tento RADIUS server je celosvetovo najpoužívanejším riešením. Konkurenčnými riešeniami je IAS server od Microsoft-u a ACS - obdobné riešenie od firmy CISCO. FreeRadius je určený pre OS typu UNIX a v tomto prípade bol nasadený na Linuxovej distribúcii.

7.1.1 Zapojenie siete

Sieť na ktorej prebiehala simulácia realizácie centrálneho autentizačného riešenia pozostávala z troch aktívnych prvkov. RADIUS server, AP a klientské PC. V tomto prípade mali server a Ethernet rozhranie AP verejné IP adresy. Segment na ktorom je bezdrôtové rozhranie mal adresy z privátneho rozsahu. Na zabezpečenie konektivity s externou sieťou bola poučitá technológia NAT. Táto ale použite EAP autentizácie nijako nekomplikuje. V reálnom



Obrázek 7.1: Autentizačná schéma EAP

nasadení je samozrejme možné používať na preposielanie dát medzi dvoma rozhraniami AP aj bežné smerovanie IP paketov. EAP komunikácia medzi klientom a AP je zapúzdrená do EAPOL paketov, komunikácia medzi AP a RADISU serverom zas do RADIUS paketov. V tomto modeli vystupuje prístupový bod len ako sprostredkovateľ. Celý overovací mechanizmus je znázornený na nasledujúcom obrázku a sa dá veľmi zjednodušene popísať v nasledujúcich šiestich krokoch (tie sú zároveň zobrazené na obr. 7.1):

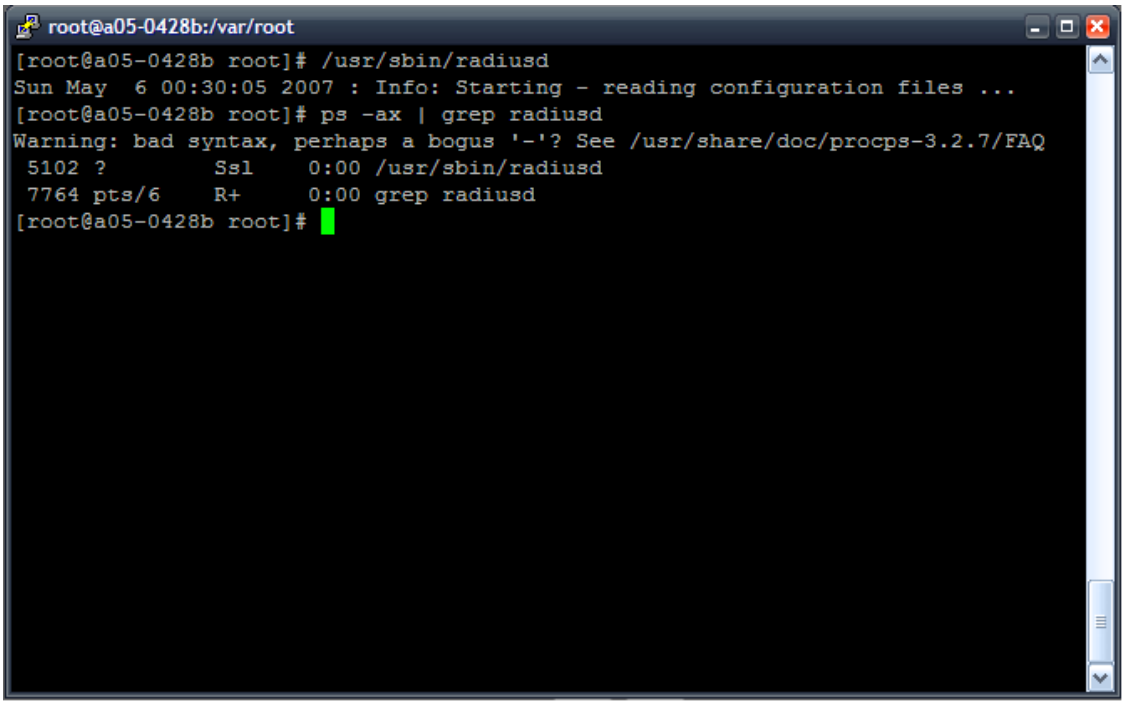
1. Klient inicializuje komunikáciu s AP
2. AP vyžiada klienta aby sa identifikoval
3. Klient pošle AP svoje prihlasovacie meno, AP prepošle autentizačnú žiadosť RADIUS serveru
4. RADISU server vygeneruje výzvu pre nového klienta a zašle ju AP, AP ju prepošle klientovi
5. Klient pošle AP odpoveď na obdržanú výzvu, AP ju prepošle RADIUS serveru
6. RADIUS server autentizuje klienta a pošle AP kladnú alebo zápornú odpoveď, AP ju prepošle klientovi.

7.1.2 Konfigurácia serveru

V roli centrálneho autentizačného serveru som použil FreeRadius. Je to open-source projekt, ktorý je určený pre nasadenie na rôznych UNIX-ových typoch OS. V tomto prípade som zvolil spojenie s OS Linux. Táto kombinácia je celosvetovo najpoužívanejším riešením a zároveň predstavuje bezplatné riešenie z hľadiska ceny samotného SW. K tomu musíme samozrejme prirátať cenu potrebnú na nasadenie a konfiguráciu, prípadne ďalšie výdaje spojené napríklad s obstaraním serverového certifikátu vydaného známou certifikačnou autoritou. V tejto kapitole sa zároveň pokúsim priblížiť náročnosť konfigurácie FreeRadius serveru. Konfigurácia AP a klientov je zahrnutá v nasledujúcich kapitolách.

Inštalácia

V prvom rade je nutné nainštalovať OS Linux na vopred pripravený HW server. Pre jednoduchosť som použil Live distribúciu ADIOS Linux. Táto distribúcia je zameraná na sieťové služby a správu sietí a FreeRadius je v nej už pred-inštalovaný. Bežným postupom bude asi inštalácia jednej z bežne používaných distribúcií a následné doinštalovanie FreeRadius-u. Jeho najnovšiu verziu je možné získať z adresy www.freeradius.org. Následná inštalácia sa vykoná príkazmi: *"./configure", "make", "make install"*, ktoré spustíme v adresári so zdrojovými súbormi. Spustiteľné súbory sa nainštalujú do adresára *"usr/sbin/"*, konfiguračné súbory nájdeme v adresári *"etc/raddb/"* a logovacie súbory v adresári *"var/log/"* Samotný RADIUS server spustíme príkazom *"/usr/sbin/radiusd"*. V prípade, že nebude zobrazená žiadna chybová hláška, tak všetko prebehlo v poriadku. Overenie, že daný démon skutočne beží vykonáme príkazom *"ps -ax — grep radiusd"*. Akcia je znázornená na obr. 7.2.



Obrázek 7.2: Spustenie a overenie behu FreeRadius

Konfigurácia

Fáza konfigurácie FreeRadius serveru pre použitie s PEAP overovaním pozostáva z editácie niekoľkých konfiguračných súborov. Konkrétne sú to nasledujúce štyri: "client.conf", "users, "radiusd.conf", "eap.conf" . Prvý z nich obsahuje zoznam RADIUS klientov, teda prístupových bodov, druhý obsahuje zoznam uzívateľov a ich prístupové heslá. Tretí súbor slúži na globálnu konfiguráciu RADIUS serveru a posledný z nich na špecifickú konfiguráciu EAP protokolu. Začneme súborom "client.conf" . na jeho začiatok pridáme našeho RADIUS klienta, čiže IP adresu prístupového bodu. Pridávame v?dy adresu rozhrania, ktorým je AP pripojené k RADIUS serveru. Rovnako špecifikujeme zdieľane heslo. Rovnaký reťazec musíme špecifikovať aj na AP. RADISU server totiž bude komunikovať len s tými RADIUS klientmi u ktorých bude súhlasiť ich zdieľané heslo. Pre každé AP môžeme špecifikovať inú frázu. Posledným parametrom, ktorý zadáme je krátke meno. Záznam vyzerá nasledovne:

```
    client 147.229.220.150 {
secret = BUSlab
shortname = AP
}
```

Potom upravíme súbor "users" . V ňom špecifikujeme mená a heslá koncových užívateľov, ktorí sa pripájajú do našej bezdrôtovej siete. V tomto prípade pridáme na začiatok konfiguračného súboru následujúci riadok:

```
"testuser" User-Password == "testpass"
```

Nasleduje editácia súboru *"radiusd.conf"* . V ňom nastavíme parametre ovplyvňujúce celú službu RADIUS. Najprv vyžiadame logovanie autentizácie, pre lepší prehľad a prípadné odlaďovanie chýb. Následne vynútime použitie protokolu MMPE (MS PointToPoint Encryption), ktorý je používaný v spojení s PEAP a tiež uprednostníme silný typ šifrovania. Napokon vyžiadame zápis detailného logu pre autentizáciu a zasielanie odpovedí klientom. Do súboru pridáme tieto údaje (v zátvorke je uvedené číslo riadku):

```
log_auth = yes (296)
use_mppe = yes (667)
require_encryption = yes
require_strong = yes
detail auth_log (1128)
detail reply_log (1145)
auth_log (1789)
reply_log (2038)
```

Posledný súbor, pomocou ktorého nastavíme náš RADIUS server je *"eap.conf"*. V ňom sa nachádza špecifikácia akým spôsobom sa použije EAP protokol. V ňom nastavíme, že na výmenu hesla použijeme MSCHAPv2 protokol a HASH hesla, ktorý sa zasiela sa vytvorí pomocou algoritmu MD5. Následne nastavíme použitie certifikátu pre server. FreeRadius má v jeho predvolenej inštalácii pred-pripravený certifikát pre server. Ten je ale vydaný a podpísaný lokálnou certifikačnou autoritou, takže je pre klienta nedôveryhodný. Na túto ukážku ale postačuje. V reálnom nasadení sa predpokladá použitie certifikátu, ktorý získame od jednej z dobre známych certifikačných autorít. Napríklad certifikát pre RADISU server vydaný firmou Verisign je možné získať z ich stránok za poplatok približne 7000 KČ ročne.

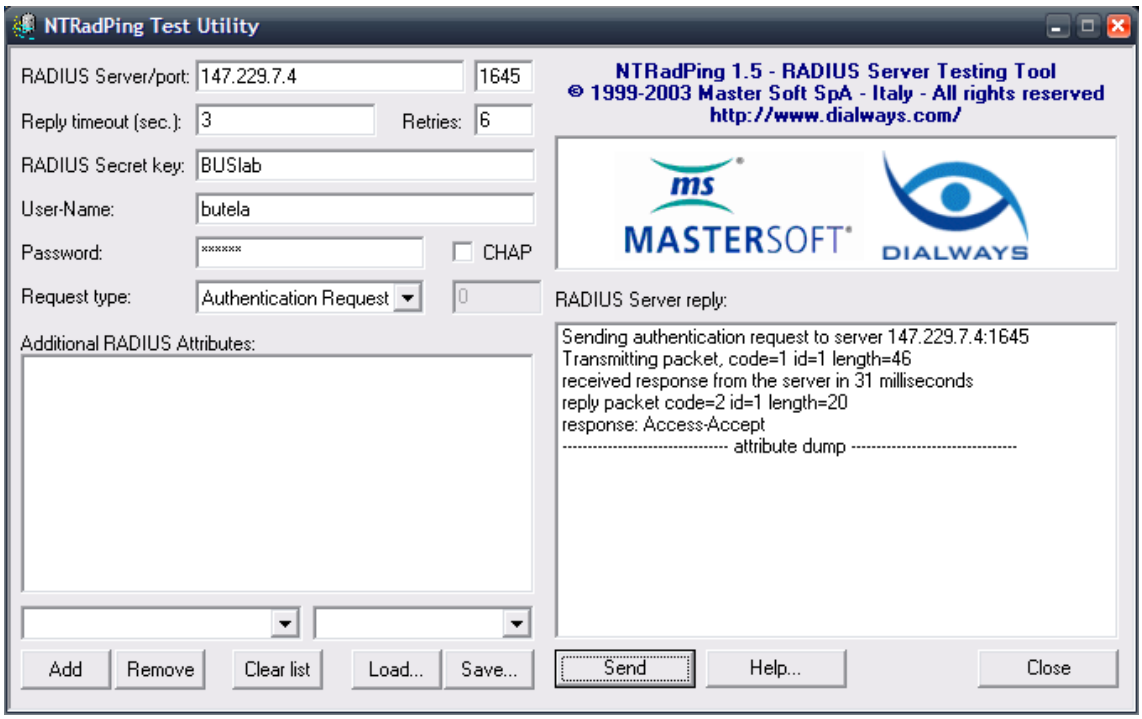
Pre pred-pripravený certifikát stačí odkomentovať riadky so špecifikovaným hodnotami. Vo výslednom súbore by sa teda mali nachádzať odkomentované, prípadne pozmenené tieto riadky:

```
default_eap_type = md5
default_eap_type = mschapv2 tls
{
private_key_password = whatever
private_key_file = /certs/cert-srv.pem
certificate_file = /certs/cert-srv.pem
CA_file = /certs/demoCA/cacert.pem
dh_file = /certs/dh
random_file = /certs/random
}
peap {
default_eap_type = mschapv2
}
```

Následne je nevyhnutný reštart služby. Najprv ukončíme bežiaci proces príkazom *"kill"* a spustíme službu, tak ako predtým. Pri spustení za načítajú nastavenia konfiguračných súborov. Popis čerpaný prevažne z knihy Radius [1].

Overenie

V prípade, že máme konfiguráciu ukončenú, môžeme previesť základný test dostupnosti, funkčnosti a správnej konfigurácii RADIUS serveru. Použijeme na to nástroj *"NTRadPing"*.

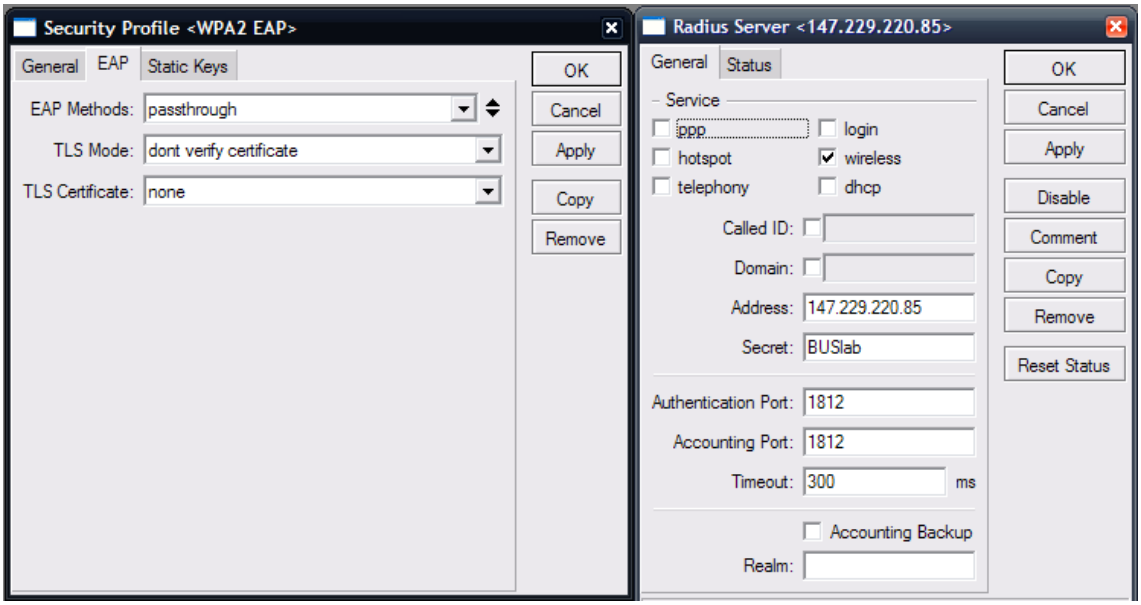


Obrázek 7.3: RadiusPing

Je to nástroj firmy MasterSoft, ktorý je možné zdarma stiahnuť zo stránok "www.dailwais.com". Jeho použitie je bezplatné a je určený pre OS Windows NT. Ideálny postup riešenia je pripojiť bezdrôtového klienta k AP bez zabezpečenia a najprv otestovať funkčnosť RADIUS serveru nástrojom NTRadPing. V prípade, že test prebehne úspešne, môžeme pokračovať v konfigurácii AP a napokon nastaviť klienta. V prípade, že tento test neprebehne úspešne, môžeme skontrolovať logovací súbor serveru, nájsť a opraviť prípadný problém, či chybu. Po spustenínástroja NTRadPing zadáme IP adresu RADIUS serveru a port na ktorom služba beží. Podľa špecifikácie protokolu RADIUS je to port číslo 1812. V praxi sa ale veľmi často používa aj port 1645. Port na ktorom bude služba bežať je možné špecifikovať v globálnom konfiguračnom súbore služby FreeRadius. Následne špecifikujeme zdieľané heslo, ktoré sme nastavili v konfigurácii pre daného RADIUS klienta. Pokračujeme zadaním mena a hesla pre koncového užívateľa a vyberieme typ dotazu *"Authentication Request"* . Tlačidlom *"SEND"* odošleme požiadavok na server a následne by sa nám v pravej časti programu mala zobraziť kladná odozva, tak ako je to zobrazené na obrázku 7.3.

7.1.3 Konfigurácia AP

Druhým prvkom, ktorý musíme nastaviť je prístupový bod. Tu sa môže konfigurácia mierne rôzniť, v závislosti od výrobcu daného zariadenia. Táto konfigurácia je ale vcelku jednoduchá, takže by nemal byť žiadny problém adaptovať ju na akýkoľvek prístupový bod. Základ spočíva v nastavení používania EAP autentizácie v móde, kde AP preposiela žiadosti na RADIUS server. Ďalej musíme špecifikovať adresu RADIUS serveru, port na ktorom služba beží a zdieľané tajomstvo. Na konfiguráciu AP Mikrotik použijeme grafický konfiguračný nástroj *"Winbox"* . Ten je zdarma stiahnuteľný a použiteľný zo stránok *"www.mikrotik.com"*. Je určený pre OS Windows. K AP sa môžeme pripojiť buď pomocou sériového portu, Ethernet káblu alebo bezdrôtovo. Najjednoduchším spôsobom pre úvodnú konfiguráciu je Ethenet kábel. MAC adresa AP je detekovaná automaticky a po ustálení spojenia môžeme začať s konfiguráciou. V prvom rade vytvoríme bezpečnostný profil. AP obsahuje 2 bezdrôtové karty, vyberieme si jednu z nich. Voľbou *"Wireless"* v hlavnom menu a záložkou *"Security Profiles"* sa dostaneme ku konfigurácii zabezpečenia. Tlačidlom *"+"* pridáme nový bezpečnostný profil. Na záložke *"General"* vyberieme buď *"WPA EAP"* alebo *"WPA2 EAP"*, podľa toho aký typ šifrovania použijeme. K dispozícii je *"TKIP"* alebo *"AES"*. Môžeme zvoliť aj viac volieb súčasne, ale vždy sa použije tá najbeznešia dostupná alternatíva. Dôležité je ale zrušiť voľbu *"PSK"*. Zadáme ešte meno profilu a prejdeme na záložku *"EAP"*. Tam vyberieme nasledovné voľby- *"EAP Methods: passthrough", "TLS Mode: dont verify", "TLS Certifikate: none"*. Prípadné overovanie platnosti serverového certifikátu prenecháme na klientov. V ďalšom kroku musíme nami vytvorený profil aplikovať. Najprv voľbou *"Interfaces"* v hlavnom menu vyberieme nami používané bezdrôtové rozhranie. Predpokladám, že jeho základná konfigurácia už bola vopred vykonaná. Zvolíme teda bezdrôtové rozhranie a novom okne vyberieme záložku *"wireless"*. Vo voľbe *"Security Profile"* vyberieme zo zoznamu existujúcich profilov, ten ktorý sme pred chvíľou vytvorili. Potvrdíme všetky nastavenia. Poslednou potrebnou akciou je predloženie parametrov autentizačného serveru. Tie nájdeme pod voľbou *"Radius"* v hlavnom menu. V novom okne vyberieme služby, pre ktoré má byť RADIUS server použitý, postaší vybrať službu *"wireless"*. Nasleduje špecifikácia adresy, portu a hesla. Voľby nastavíme nasledovne - *"Address: 147.229.220.85", "Secret: BUSlab", "Authentication Port: 1812", "Accounting Port: 1812"*. Potvrdíme. Konfigurácia:

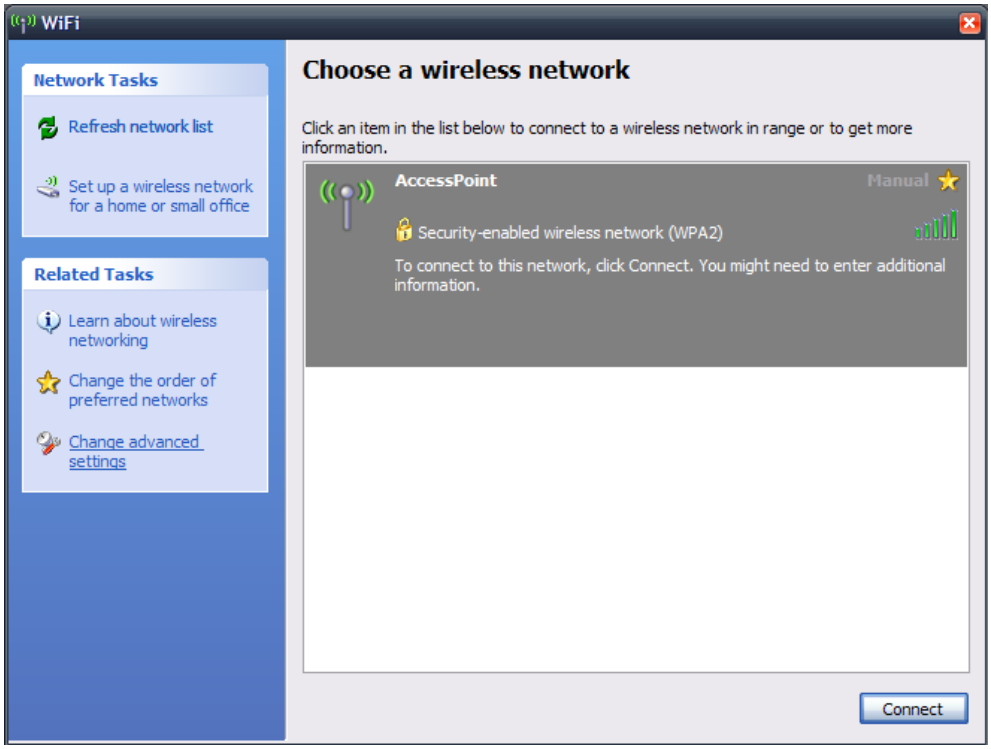


Obrázek 7.4: Konfigurácia prístupového bodu

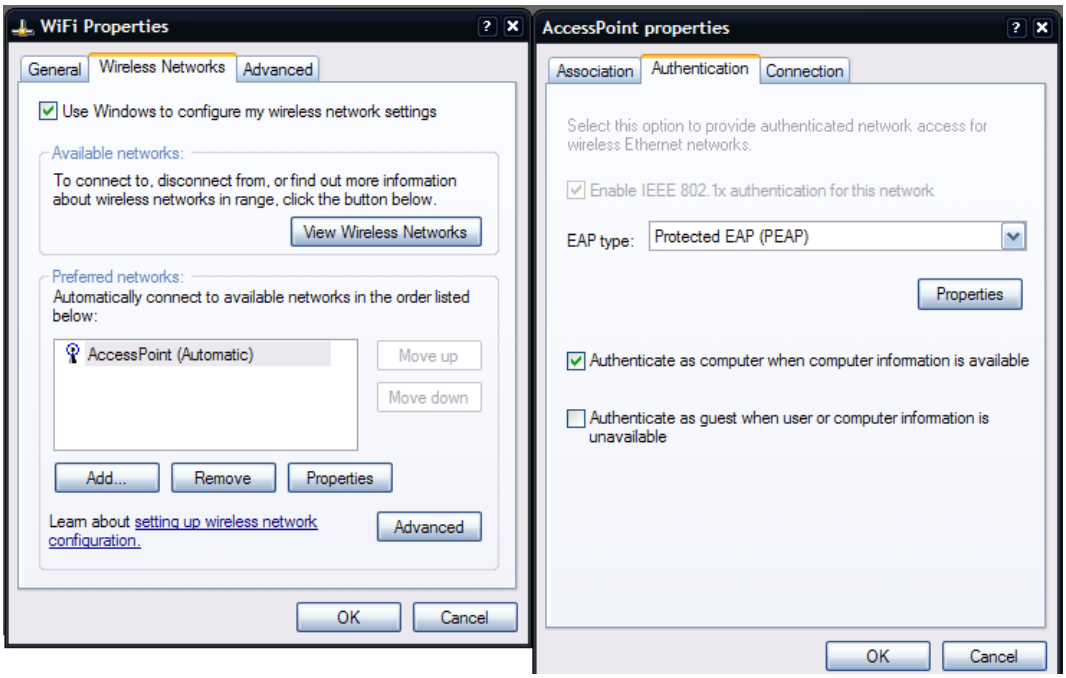
7.1.4 Konfigurácia klienta

Ako ukážkového klienta som použil notebook s WiFi kartou Intel BG2200 a OS Windows XP SP2 EN. Táto konfigurácia je najviac generalizujúca a pokrýva tak najširšie spektrum prípadných užívateľov. Postup pripojenie je nasledovný. Povolíme bezdrôtový adaptér a zobrazíme zoznam dostupných sietí. To dostaneme voľbou *"View Available Wireless Networks"* na ikone bezdrôtového pripojenia. Vyberieme našu sieť (v tomto prípade pomenovanú ako *"AccessPoint"*) a pripojíme sa k nej voľbou *"Connect"*. Typ šifrovania sa detekuje správne, avšak pripojenie sa nepodarí. Dôvodom je použitie predvoleného autentizačného mechanizmu. Ním je vyžiadanie klientského certifikátu alebo SmartCard. Overovací mechanizmus teda musíme nastaviť manuálne. Na zozname dostupných bezdrôtových sietí vyberieme voľbu *"Change Advanced Settings"*.

V novom okne vyberieme záložku "Wireless Networks". Vyberieme našu sieť zvolíme voľbu *"Properties"*. V novom okne vyberieme záložku *"Authentication"*. Typ EAP zmeníme na - *"EAP type: Protected EAP (PEAP)"*. Pokračujeme voľbou *"Properties"*. V novom okne zrušíme voľbu *"Validate server certificate"*. V reálnej situácii by sme ale mali túto voľbu nechať zaškrtnutú a na strane serveru použiť certifikát podpísaný dôveryhodnou CA. Od použitia takéhoto certifikátu závisí celková bezpečnosť našej siete. Klienti by sa mali autentizovať jedine voči podpísanému serveru. V inom prípade môže dôjsť k útoku založenému na podvrhnutí identity AP a RADIUS serveru. Skontrolujeme, či je ako overovací model použitý EAP MSCHAPv2. Ak nie, tak zvolíme *"Select Authentication Method: Secured Password (EAP MS-CHAP v2)"*. Posledné nastavenie, ktoré je nutné zmeniť nájdeme skryté pod voľbou *"Configure..."* Tam zrušíme voľbu *"Automatically use..."*. Všetky zmeny potvrdíme. Vrátime sa do zoznamu dostupných sietí a pokúsime sa pripojiť znova. Tentokrát sme požiadaný o zadanie užívateľského mena a hesla. Vpíšeme naše identifikačné údaje a políčko pre doménu necháme prázdne. Autentizácia by mala prebehnúť úspešne a sme pripojený do siete. Konfiguračné dialógy sú zobrazené na obrázkoch 7.5 až 7.8.



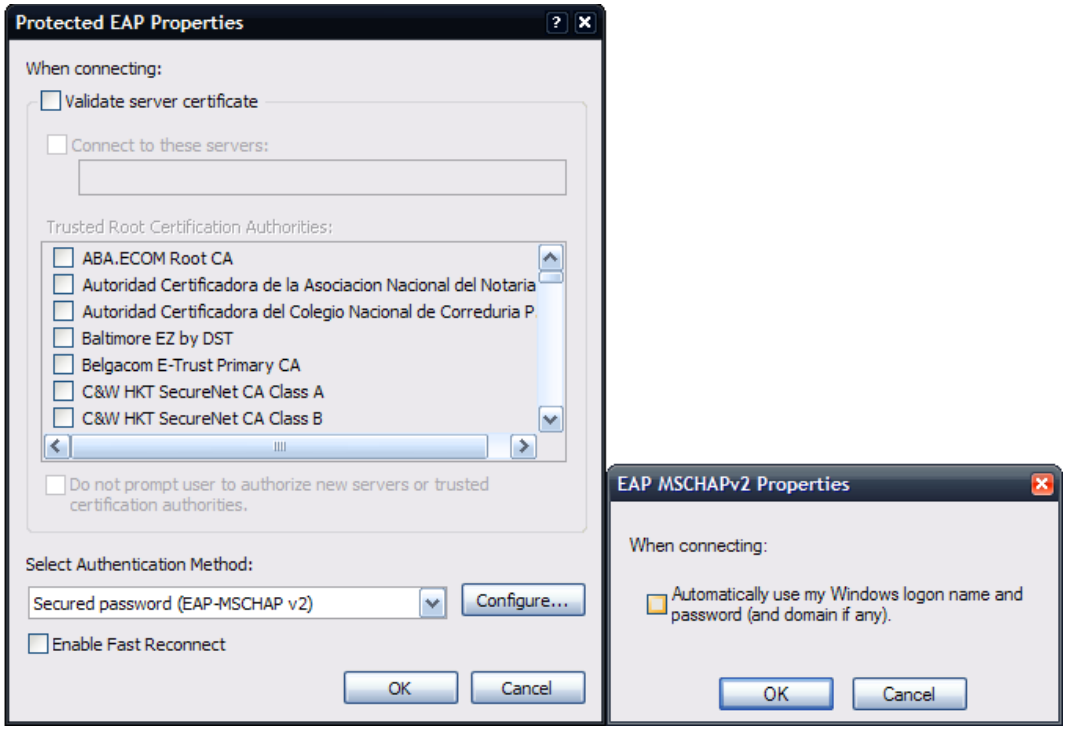
Obrázek 7.5: Zoznam dostupných sietí



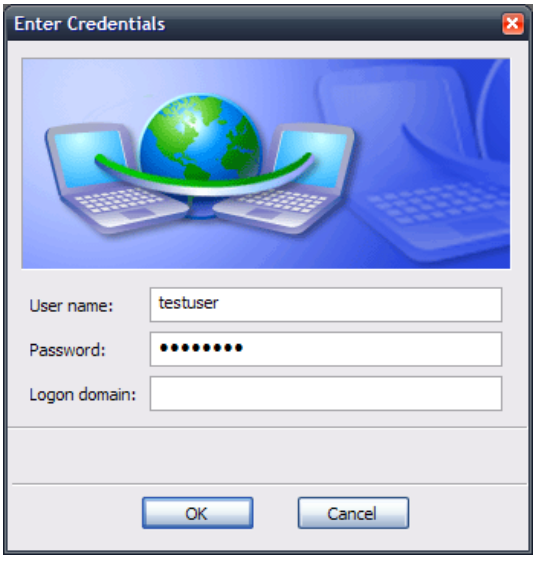
Obrázek 7.6: Konfigurácia klienta

7.2 Zhrnutie autentizácie

Autentizácia užívateľov bezdrôtových sietí je nutnou súčastou zabezpečenia pre rozsiahle bezdrôtové siete so stálymi užívateľmi. Túto možnosť je ale možné využiť len v spojení s mechanizmami WPA a WPA2. Prvotná špecifikácia WPA zahŕňala len jednu možnosť overovania a to pomocou protokolu EAP-TLS. Ten je ale veľmi náročný na nasadenie, pretože vyžaduje klientské certifikáty, čo predstavuje extra úsilie administrátora siete ako ak extra náklady na zakúpenie týchto certifikátov, resp. založenie vlastnej certifikačnej autority. Niekoľko rokov neskôr boli štandardizované aj ďalšie autentizačné metódy. Sieťové adaptéry, ktoré podporujú túto rozšírenú autentizačnú schému takisto väčšinou podporujú aj kompletnú schému WPA2. Použitie niektorého z protokolov z rozšírenej schémy tak vyžaduje novšie sieťové adaptéry, čo ale dnes spĺňajú takmer všetky používané karty a AP. Z hľadiska typu AP, postačí ak tento umožňuje preposielať EAP komunikáciu na RADISU server. Presný typ použitého protokolu je pre AP transparentný. S týmto komponentom by teda nemal byť vo všeobecnosti problém. Z pohľadu klientských staníc musíme výber overovacieho protokolu zvážiť lepšie. Podpora je v tomto prípade nutná na HW aj SW úrovni. Zvážime fakt, že najpoužívanejšie WiFi adaptéry sú od výrobcov Intel, Broadcom a IBM, a overíme si stupeň certifikácie pre jednotlivé autentizačné protokoly na stránkach www.wi-fi.org. Tie patria organizácii WiFi Alliance, ktorá udeľuje certifikáty bezdrôtovým sieťovým zariadeniam. Niekoľko posledných generácií adaptérov od týchto popredných výrobcov je certifikovaných pre všetky autentizačné protokoly ako EAP-TTLS, EAP-PEAP, LEAP, ... Ak sa pozrieme na podporu týchto protokolov v SW, tak sa môžeme spoľahnúť buď na zabudovanú podporu v OS alebo môžeme použiť SW modul, tzv. "supplicant" pre zavedenie podpory daného protokolu na stranu klienta. Supplicant môže byť poskytovaný od konkrétneho výrobcu pre podporu proprietárneho protokolu, napr. od firmy CISCO. Je ale možné nasadiť aj supplicant pre zavedenie podpory otvorených protokolov. Napríklad modul "Xsupplicant" pre OS Linux. Tieto moduly ale predstavujú extra úsilie, ktoré musí vynaložiť administrátor siete ako aj samotný užívateľ a často nie sú prijateľné. Tento fakt musíme zohľadniť pri výbere riešenia, ktoré nasadíme a preto je najistejšie, aj keď trochu obmedzujúce, spoľahnúť sa na podporu zabudovanú v OS. V OS Windows 2000 a XP nájdeme podporu protokolu PEAP. Jeho použitie nevyžaduje od užívateľov žiadnu inštaláciu dodatočného SW. Je ale potrebná manuálna konfigurácia a výber tých správnych nastavení. Postup je pre bežného používateľa trochu komplikovaný. Preto je vhodné poskytnúť mu stručný návod. Tento by mohol byť ku koncovým užívateľom distribuovaný niekoľkými možnými kanálmi. Medzi patria vystavenie návodu na WWW server, ktorý je dostupný aj bez autentizácie alebo rozoslanie návodu v papierovej podobe klasickou poštou, v prípade, že sieť pozostáva zo stálych zákazníkov.



Obrázek 7.7: Ďalšia konfigurácia klienta



Obrázek 7.8: Zadanie mena a hesla

Kapitola 8

Záver

Záver tejto práce zhrňuje a rekapituluje všetky zistenia a pozorovania, ktoré vyplývajú z predchádzajúcich kapitol. Cieľom tejto diplomovej práce bolo vypracovať prehľad jednotlivých štandardizovaných možností zabezpečenia WiFi sietí, ich porovnanie, vplyv na rýchlosť prenosu dát. Rovnako demonštrovať slabé miesta zabezpečovacích schém a vypracovať štúdiu nasadenia centrálnej autentizácie. Výsledkom týchto snáh je odporúčanie vhodnosti nasadenia určitého typu zabezpečenia v závislosti na situácii.

Pri výbere zabezpečenia musí každý správca siete zobrať do úvahy aká je cena toho, čo potrebujeme zabezpečiť a aká je cena nasadenia daného zabezpečenia. Tá by v žiadnom prípade nemala prekročiť cenu toho, čo môžeme stratiť pri podľahnutí útoku. Stratou sa myslí odcudzenie utajených informácii, neoprávnené využívanie siete či prístup na Internet pomocou tejto siete, neoprávnené používanie SW, či HW vybavenia, alebo poškodenie HW, prípadne dobrého mena spoločnosti následkom nekalých aktivít.

Pri výbere a nasadení zabezpečenia musí toto zabezpečovať základné 3 vlastnosti ako: utajenie, integritu a dostupnosť. Vo väčšine prípadoch sa ale po?adujú aj niektoré ďalšie ako autentizácia, či možnosť auditu. Pri nasadení konkrétneho mechanizmu musíme tento zvažovať z niekoľkých hľadísk. Medzi ne patrí okrem kvalita utajenia a integrity aj možnosť autentizácie, ale aj cena a čas potrebný na nasadenie. Nesmieme zabudnúť ani na podporu daných mechanizmov v HW a SW, čo môže nepriaznivo zvýšiť výslednú cenu a potrebný čas. Často sa zabúda na hľadisko ergonomické, čiže zabezpečenie by malo čo najmenej ovplyvňovať pohodlie a kvalitu práce užívateľov a nemali by na nich byť kladené nadmerné požiadavky. Tie v krajnom prípade môžu vyústiť v podobe potreby školenia užívateľov. Inými slovami dôvernosť, integrita a autentizácia by nemala nepriaznivo ovplyvňovať dostupnosť.

Bez ohľadu na situáciu v ktorej dané zabezpečenie nasadzujeme, môžeme vyvodiť niekoľko záverov:

WEP Tento mechanizmus by sa vzhľadom na množstvo známych útokov, voči implementačným chybám prakticky nemal vôbec používať. Ochrana utajenia aj integrity je veľmi ľahko prelomiteľná, bez ohľadu na to, či použijeme 64 alebo 128 bitový šifrovací kľúč. WEP nie je použiteľný ani pre účely plnohodnotnej autentizácie. Pre jeho prípadné použitie hraje snáď len fakt že je podporovaný praktický vo všetkých sieťových zariadeniach a SW.

WPA1 PSK WPA1 v móde so zdieľaným kľúčom je pomerne bezpečná metóda, ktorá ale v sebe pri nesprávnom použití obsahuje skrytú hrozbu. Z hľadiska poskytovania utajenia a integrity sa jedná a bezpečné riešenie. Z pohľadu autentizácie je situácia

prakticky rovnaká ako pri WEP. Navyše použitie slovníkového hesla predstavuje bezpečnostnú dieru. Nasadenie spolu s netriviálnym heslom ale môže predstavovať náhradu za WEP, k čomu prispieva aj podpora WPA1 PSK aj pomerne starých klientských adaptéroch.

WPA1 Enterprise Predstavuje vysoký stupeň utajenia a integrity spolu s najvyšším stupňom autentizácie. Vzhľadom k podpore v HW môžeme pri kartách s podporou WPA1 bezpečne počítať aj s podporou EAP-TLS. Podpora ostatných metód je otázna. Nebezpečenstvo nastáva jedine v kombinácií s LEAP overovaním. Úzkym hrdlom tohto riešenia ale môžu by? AP s nízkym výpočtovým výkonom, ktoré takto môžu negatívne ovplyvniť celkovú priepustnosť siete. Tento problém sa vzťahuje aj na mód PSK.

WPA2 PSK WPA2 v móde so zdieľaným kľúčom poskytuje veľmi vysoký stupe? utajenia a integrity dát. Ten je zabezpečený použitím algoritmu AES. V samotnom algoritme ani v jeho implementácií pre WPA2 sa zatiaľ nikomu nepodarilo nájsť zneužiteľnú chybu, resp. táto skutočnosť nie je všeobecne známa. Z hľadiska autentizácie je situácie rovnaká ako pri WPA1 PSK. Opäť je teda nutné použiť netriviálne zdieľané heslo. Podporu nájdeme len v pomerne nových sieťových adaptéroch a AP, ktoré sú u? dnes ale vcelku bežne používané a rozšírené.

WPA2 Enterprise Je to zastupiteľ dnes zrejme najvyššieho dostupného stupňa zabezpečenia. Predstavuje veľmi vysoký stupeň utajenia aj integrity a rozsiahle možnosti autentizácie. Za jeho nasadenie hovorí aj efektívna rýchlosť sieťového prenosu, ktorá nie je jeho použitím negatívne ovplyvnená. Jeho nasadenie ale môže skomplikovať fakt, že je nutné použiť novšie klientské karty ako aj AP. Podporu do OS Windows XP SP2 je možné doplniť po manuálnej inštalácii rozširujúceho balíčka. Vo Windows Vista je ale podpora natívna.

8.1 Modelové situácie

Nie je možné vyvodiť jeden záver o odporúčanom spôsobe zabezpečenia bezdrôtovej siete, ktorý by bol všeobecne platný. Predkladám tak niekoľko typických modelových situácií, s ktorými sa často stretávame v bežnom živote.

8.1.1 Hotel / Hostel

Hotel, resp. hostel môže mať v portfóliu svojich služieb aj poskytnutie bezdrôtovej konektivity pre svojich hostí. Musíme vziať do úvahy niekoľko dôležitých skutočností, ktoré ovplyvnia výsledný vyber zabezpečenia. Je to vysoký stupeň výmeny zákazníkov, nepredpovedateľná rôznorodosť bezdrôtových adaptéroch v mobilných zariadeniach hostí a často nízka hodnota prenášaných informácií. Tieto fakty znamenajú v prvom rade nemysliteľný prístup vo forme plnohodnotnej autentifikácie každého zákazníka unikátnym menom a heslom. V druhom rade nutnosť podpory čo najširšieho spektra WiFi adaptérov. V treťom rade je to fakt, že maximálna ochrana dát nie je zvyčajne nevyhnutná. To znamená vyradenie z hry WPA2 a pokročilých autentizačných mechanizmov. WPA s TLS overovaním je nepoužiteľné z hľadiska náročnosti na správu. WPA-PSK je teoreticky použiteľné. Na zabezpečenie maximálnej konektivity pre všetkých klientov teda vychádza ako najlepšie

riešenie WEP so 128bit kľúčom. Keď navyše vezmeme do úvahy fakt, že jeho prelomenie môže pri nízkom vyťažení siete trvať aj pol dňa, tak je to ideálne riešenie spolu s každodennou zmenou šifrovacieho kľúča.

8.1.2 Domáca sieť / Malá firma

V tejto modelovej situácii vstupuje na scénu niekoľko skutočností. Je to pomerne malý počet užívateľov s nízkou frekvenciou ich výmeny. Zároveň je to skutočnosť pravdepodobnej absencie úplne najnovšieho HW a SW vybavenia. Tiež nemôžeme predpokladať existenciu centrálneho serveru. Prenášané dáta môžu byť často citlivé. Z týchto dôvodov je nemysliteľné nasadenie WEP ani WPA, či WPA2 v Enterprise móde. Na výber nám zostáva WPA-PSK a WPA2-PSK. Pripomeniem to, že pri použití komplexného hesla sú považované sa rovnako bezpečné. Zvážime fakt, že sú zrejme použité prístupové body nižšej kategórie, prípadne staršieho dátumu výroby, tak ako optimálne riešenie vychádza WPA-PSK (s použitím netriviálneho zdieľaného hesla). Eventuálne menšie zníženie priepustnosti siete, je prijateľné.

8.1.3 Univerzitná sieť / Veľká firma

V poslednom modelovom prípade pred nás opäť predstupuje niekoľko typických faktorov. Medzi ne patrí väčšie množstvo užívateľov, avšak s pomerne málo častou zmenou osadenstva. Je tu aj faktor citlivosti a dôležitosti prenášaných dát. Môžeme tu počítať s prezenciou pomerne nového HW a SW vybavenia, resp. s pravdepodobnou ochotou do jeho investície. Vyplýva z toho možnosť a nutnosť čo najvyššieho stupňa zabezpečenia utajenia a integrity ako aj autentizácie a auditu. Vo výsledku teda dostaneme nasadenie WPA2 spolu s EAP autentizáciou pomocou RADIUS serveru. Možnou alternatívou je aj WPA1 s použitím AES šifrovania. Táto kombinácia síce nie je štandardizovaná, ale je široko podporovaná na rôznych AP ako aj v OS Windows XP SP2 bez nutnosti manuálnej inštalácie balíku pre WPA2. Táto možnosť je ale na zvážení správcu a vyžaduje predchádzajúce testovanie.

8.2 Súčasnosť a budúcnosť

Bezdrôtové počítačové siete spolu s ich zabezpečením je oblasť, ktorá sa rozvíja veľmi dynamicky a niekdy až takmer nekontrolovateľne. Neblahým následkom je spleť rôznych bezpečnostných algoritmov, mechanizmov a schém. Verím, že táto práca poskytla ich použiteľný prehľad a popis. Spolu s niekoľkými praktickými úlohami tak demonštruje súčasný stav možností zabezpečenia sietí typu WiFi. Čitateľovi by mala pomôcť pri výbere spôsobu, ako ochrániť svoju bezdrôtovú sieť.

Do budúcnosti si môžeme želať kontrolovaný vývoj v tejto sfére a rešpektovanie súčasných i budúcich štandardov. Len tak je možné zaručiť vzájomnú interoperabilitu všetkých zariadení a bezproblémové a hlavne bezpečné používanie našich WiFi sietí.

Prílohy

Príloha A

```
#
# clients.conf - client configuration directives
#
#########################################################################

#########################################################################
#
#  Definition of a RADIUS client (usually a NAS).
#
#  The information given here over rides anything given in the
#  'clients' file, or in the 'naslist' file.  The configuration here
#  contains all of the information from those two files, and allows
#  for more configuration items.
#
#  The "shortname" is be used for logging.  The "nastype", "login" and
#  "password" fields are mainly used for checkrad and are optional.
#

#
#  Defines a RADIUS client.  The format is 'client [hostname|ip-address]'
#
#  '127.0.0.1' is another name for 'localhost'.  It is enabled by default,
#  to allow testing of the server after an initial installation.  If you
#  are not going to be permitting RADIUS queries from localhost, we suggest
#  that you delete, or comment out, this entry.
#
client 127.0.0.1 {
#
#  The shared secret use to "encrypt" and "sign" packets between
#  the NAS and FreeRADIUS.  You MUST change this secret from the
#  default, otherwise it's not a secret any more!
#
#  The secret can be any string, up to 31 characters in length.
#
secret = testing123
```

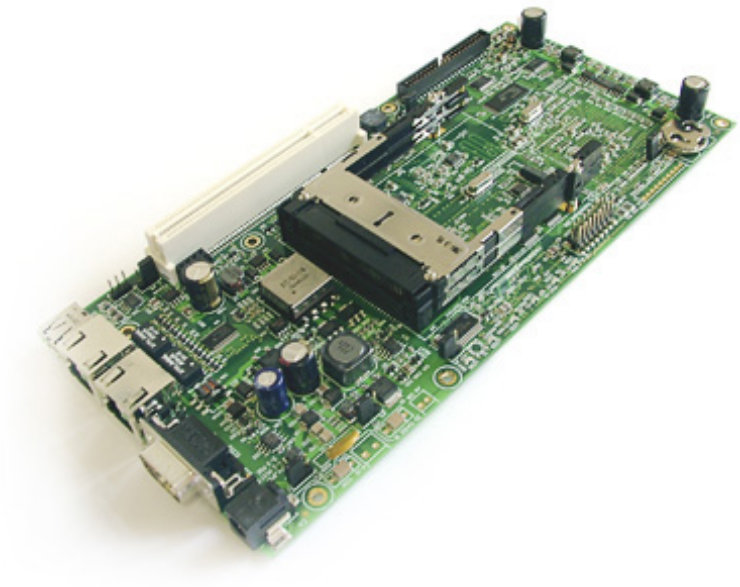
```
#
#  The short name is used as an alias for the fully qualified
#  domain name, or the IP address.
#
shortname = localhost

#
# the following three fields are optional, but may be used by
# checkrad.pl for simultaneous use checks
#

#
# The nastype tells 'checkrad.pl' which NAS-specific method to
#  use to query the NAS for simultaneous use.
#
#  Permitted NAS types are:
#
# cisco
# computone
# livingston
# max40xx
# multitech
# netserver
# pathras
# patton
# portslave
# tc
# usrhiper
# other # for all other types

#
nastype     = other # localhost isn't usually a NAS...

#
#  The following two configurations are for future use.
#  The 'naspasswd' file is currently used to store the NAS
#  login name and password, which is used by checkrad.pl
#  when querying the NAS for simultaneous use.
#
# login       = !root
# password    = someadminpas
}

client 147.229.220.150 {
secret = BUSlab
shortname = AP
}
```

```
#client some.host.org {
# secret = testing123
# shortname = localhost
#}

#
#  You can now specify one secret for a network of clients.
#  When a client request comes in, the BEST match is chosen.
#  i.e. The entry from the smallest possible network.
#
#client 192.168.0.0/24 {
# secret = testing123-1
# shortname = private-network-1
#}
#
#client 192.168.0.0/16 {
# secret = testing123-2
# shortname = private-network-2
#}


#client 10.10.10.10 {
# # secret and password are mapped through the "secrets" file.
# secret      = testing123
# shortname   = liv1
#       # the following three fields are optional, but may be used by
#       # checkrad.pl for simultaneous usage checks
# nastype     = livingston
# login       = !root
# password    = someadminpas
#}
```

Príloha B

Obrázky a technická špecifikácia dosiek RouterBoard použitých v prístupových bodoch firmy MikroTik. Údaje prevzaté z webu spoločnosti RouterBoard [6].

Obrázek 8.1: Router Board 112



Obrázek 8.2: Router Board 230

	RouterBOARD 112	RouterBOARD 153
CPU	MIPS32 4Kc, 175MHz embedded	MIPS32 4Kc, 175MHz embedded
Memory	16MB SDRAM	32MB SDRAM
Boot loader	RouterBOOT, 1Mbit Flash chip	
Data storage	64MB onboard NAND memory chip	
Ethernet ports	One 10/100 Mbit/s Fast Ethernet port supporting Auto MDI/X	Five 10/100 Mbit ethernet ports supporting Auto MDI/X
MiniPCI slot	Two miniPCI Type IIIA/IIIB slots	Three miniPCI Type IIIA/IIIB slots
Speaker	present	
Serial ports	One DB9 RS232C asynchronous serial port	
LEDs	Power, 2 LED pairs for MiniPCI slots, 1 user LED	Power, 3 LED pairs for MiniPCI slots, 1 user LED
Power options	11..60V DC - power jack or IEEE802.3af Power over Ethernet (12V / 48V DC, except power over datalines)	11..60V DC - power jack or IEEE802.3af Power over Ethernet (12V / 48V DC, including power over datalines)
Power Out	Two 3V DC power output headers (only one populated by default), maximal output current - 500mA total	
Power Consumption	3-4W without extension cards. Maximum 10W	3-4W without extension cards. Maximum 13W
Dimensions	140mm x 85mm (5.51in x 3.35in)	160mm x 160mm (6.3in x 6.3in)
Weight	95g (3.4oz)	183g (6.5oz)
Temperature	Operational: -20°C to +70°C (-4°F to 158°F)	
Humidity	Operational: 70% relative humidity (non-condensing)	
Supported OS	RouterOS	RouterOS, GNU/Linux
Documentation	Users Manual Startup Guide	Users Manual Startup Guide
Unit Dimensions	[PDF] [DXF]	[PDF] [DXF]
Case Dimensions	[PDF]	[PDF] [DXF]
Firmware Upgrade	2.7 Changes	2.7 Changes

Obrázek 8.3: Router Board 230

	RouterBOARD 230
CPU	266 Mhz NSC SC1100 system on a chip CPU (Pentium MMX architecture)
Memory Slot	SoDIMM (up to 512MBytes SDRAM)
BIOS	2 Mbit Flash BIOS on board
Harddrive connectors	CompactFLASH I/II socket (support for standard CF and IBM Microdrive) 44 pin boxhead IDE connector for Laptop Hard Drive (2.5 inch)
Ethernet ports	Two 10/100 Mb/s Ethernet using the NSC DP83816 (DP83815 driver compatible) one of them with Power over Ethernet 802.3af standard
Serial ports	One port with DB9 standard
USB port	One port with USB 1.1 standard
Mini PCI slot	One slot with Type III standard
PCI slot	One slot with universal support (+/-12v, 5v, 3.3v)
PCMCIA slot	Dual PCMCIA/CardBUS
LEDs	Power, miniUPS, 4 user LEDs
LCD	LCD out header
Temperature Sensors	CPU area, PCI area, LM87 health monitor chip area
Voltage monitor	Monitor for CPU, 12v, 5v, and 3.3v supplies
Intrusion Detector	Enclosure intrusion detector header
Dimensions	10.5 cm x 21.5 cm (4.13 inch by 8.46 inch)
Temperature	-20°C to +70°C (-4°F to 158°F)
Watchdog	Two separate watchdog controllers
Power connections	Onboard power jack 20-56vDC in Onboard power header 48v in (to connect telecom 48v power wires) 3.3v out power header 5v out power header
Extra Features	PC mini-speaker Nine GPIO
Currently supported OS	Linux FreeBSD OpenBSD RouterOS Most DOS versions

Obrázek 8.4: Router Board 230

Literatura

[1] J. Hassell. *Radius*. O'Reilly Media, 2002. ISBN 0596003226.

[2] W.A. Arbaugh J. Edney. *Real 802.11 Security*. Addison-Wesley, 2004. ISBN 0-321-13620-9.

[3] WWW stránky. Extensible authentication protocol - wikipedia. http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol.

[4] WWW stránky. Ieee 802.11 - wikipedia. http://en.wikipedia.org/wiki/IEEE_802.11.

[5] WWW stránky. Navrcholu.cz: Ms windows. http://www.iinfo.cz/tiskove-centrum/tiskove-zpravy/windows-nejuzivanejsim-operacnim

[6] WWW stránky. Router board. http://www.routerboard.com/.

[7] WWW stránky. Wi-fi protected access 2 data encryption and integrity. http://www.microsoft.com/technet/community/columns/cableguy/cg0805.mspx.

[8] WWW stránky. Wi-fi protected access data encryption and integrity. http://www.microsoft.com/technet/community/columns/cableguy/cg1104.mspx.

[9] WWW stránky. Wired equivalent privacy - wikipedia. http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy.

[10] Mikhailovsky Vladimirov, Gavrilenko. *WI-FOO*. Addison-Wesley, 2004. ISBN 0-321-20217-1.