TECHNICKÁ UNIVERZITA V LIBERCI

Fakulta mechatroniky, informatiky a mezioborových studií

Studijní program: B2612 – Elektrotechnika a informatika
Studijní obor: 1802R022 – Informatika a logistika

Zabezpečení bezdrátových sítí Wi-Fi

Wireless network security

Bakalářská práce

Autor: Aleš Kabátek

Vedoucí práce: Mgr. Milan Keršláger

V Liberci 28. 5. 2009

Originál zadání práce

ORIGINAL PRACE

ORIGINAL PRACE

ORIGINAL PRACE

ORIGINAL PRACE

ORIGINAL PRACE

ORIGINAL PRACE

ORIGINAL PRACE

ORIGINAL PRACE

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 o právu autorském, zejména § 60 (školní dílo).

Beru na vědomí, že TUL má právo na uzavření licenční smlouvy o užití mé bakalářské práce a prohlašuji, že **s o u h l a s í m** s případným užitím mé bakalářské práce (prodej, zapůjčení apod.).

Jsem si vědom toho, že užít své bakalářské práce či poskytnout licenci k jejímu využití mohu jen se souhlasem TUL, která má právo ode mne požadovat přiměřený příspěvek na úhradu nákladů, vynaložených univerzitou na vytvoření díla (až do jejich skutečné výše).

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce.

Datum

Podpis

Poděkování

Tímto bych chtěl poděkovat všem, kteří přispěli ke vzniku této bakalářské práce. Především panu Mgr. Milanu Keršlágerovi za odborné rady a poskytnutí všech potřebných materiálů.

Abstrakt

Tato bakalářská práce postihuje problematiku sítí od jejich počátku. Sleduje jejich vývoj, strukturu a topologii. Jsou zde zmíněny mezinárodní organizace, které stály nejen při vzniku standardů pro bezdrátové komunikace a její zabezpečení, ale podílely se i na jejich definování v rozsáhlé řadě disciplín, zahrnujících elektrickou energii, lékařské technologie, zdravotní péči, informační technologie, telekomunikace, spotřebitelskou elektroniku a dopravu.

Hlavní náplň tvoří zabezpečení bezdrátových sítí spolu s popisem jednotlivých metod. Jeho úkolem je zabraňovat využívání služeb těm uživatelům, kteří za službu nezaplatili, či jsou nežádoucí.

Demonstrativně je předvedeno, že i pro středně znalého uživatele výpočetní techniky není velký problém připojit se k dostupné Wi-Fi síti „ilegálně“.

V poslední části je rozebrán nástroj, který vznikl za účelem automatizovaného zhodnocení bezpečnosti bezdrátových sítí.

Abstract

This bachelor thesis cover the network issue from their beginning. It monitors the development, structure and topology. There are mentioned international organizations which figured not only at the development of standards for wireless communications and its security, but also participated on their definition of a large number of disciplines, including electrical energy, medical technology, health care, information technology, telecommunications, consumers' electronics and transport .

The main subject of this thesis is the wireless security problems together with description of various methods. The security prevent the use of services to those users who have not paid for the service, or who are undesirable.

It is shown demonstratively that even for users with moderate knowledge of information technologies there is not a big problem to connect to available Wi-Fi networks "illegally".

In the last part of the work there is analysed an instrument which was created for the purpose of the automated assessment of the wireless networks security.

Obsah

Použité zkratky

AES	Advanced Encryption Standard
AP	Acces Point
BSS	Basic Service Set
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standards
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IrDA	Infrared Data asociation
ISM	Industrial, Scientific and Medical
IV	Inicializační Vektor
MIC	Message Integrity Code
MSDU	Mac Service Data Unit
OFDM	Orthogonal Frequency Division Multiplexing
PPP	Point-to-Point Protocol
PPPoA	Point-to-Point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier
TFTP	Trivial File Transfer Protocol
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
XOR	eXklusive OR

1. Úvod

V současné době jsme svědky mohutného a především rychlého rozvoje technologií. Tomuto vývoji se nevyhnuly ani počítače a k nim patřící počítačové sítě. Informace mají v dnešním světě obrovskou hodnotu. Potřebujeme je dnes a denně ke svému životu, práci, zábavě atd.

Jedním z médií pro šíření informací jsou rádiové vlny. Za prvního člověka, který prolomil bránu do tajů radiokomunikací je považován italský fyzik, vynálezce a podnikatel Marchese Guglielmo Marconi, který 2. června 1896 vynalezl bezdrátový telegraf (první způsob radiového spojení). Tímto vynálezem způsobil průlom v dosavadních možnostech přenosu informací a tak byla započata nová éra možností v oblasti přenosu informací [1].

Bezdrátové komunikační technologie jsou v dnešní době naprosto běžnou součástí našich životů. Jejich masové rozšíření nastalo především díky „volnosti“, kterou s sebou přinesly. Tím je myšleno především zbavení se závislosti na kabelech a patřičná mobilita. Umožňuje uživateli se přesouvat společně se zařízením a přitom plně využívat danou technologii (např.: GSM1[1], GPS[2], Bluetooth[3], IrDA[4], satelitní televizi, apod.).

Bakalářská práce se zaobírá oblastí bezdrátových sítí, konkrétně jejich možnostmi zabezpečení.

1 GSM (Global System for Mobile Communications) je standard pro mobilní telefony na světě.
2 GPS (Global Positioning System) je družicový systém umožňující zjistit přesnou poloho kdekoliv na Zemi.
3 Bluetooth pracuje v ISM pásmu 2,4 GHz, slouží k bezdrátovému propojení mezi jednotlivými zařízeními.
4 IrDA(Infrared Data asociation) je komunikační infračervený port sloužící k bezdrátové komunikaci.

2. Bezdrátové přenosy

2.1. Historie a vývoj

V dobách před zavedením standardu IEEE 802.11 se bezdrátové přenosy používaly pro specializované účely. Chybějící standardizace přenosů vedla ke vzniku velkého množství pomalých a proprietárních protokolů, drahých zařízení, které byly vzájemně nekompatibilní.

Typickým příkladem realizace bezdrátových přenosů z dob před protokolem IEEE 802.11 byly bezdrátové pokladny. Marketingoví specialisté z velkých obchodních středisek přišli na to, že lze zvýšit zisky za předpokladu, že u různých malých stánků a pultíků bude možné platit platebními kartami. Bezdrátové zpracování plateb bylo možné zakomponovat do stávajících platebních účetních procesů. Výhodou on-line transakcí byla nejen minimalizace rizika zneužití karet a snadnější účetní zpracování, ale také zmenšení šance zpronevěření peněz v hotovosti. Ovšem v dnešní době se může tento názor brát lehce s úsměvem, poněvadž připravit někoho o peníze je daleko snazší právě on-line. Úsměvné bylo též zabezpečení. Z unikátnosti jednotlivých řešení vycházela i obecná neznalost použitých protokolů. Většina společností tedy spoléhala na „security by obscurity“[1] a bezpečnost zajišťovala pouze přísným utajením technických podrobností použitého řešení, což je na aktuální poměry naprosto neakceptovatelná věc.

2.1.1. IEEE

IEEE (*Institute of Electrical and Electronics Engineers*), jejíž český ekvivalent se nazývá *Institut pro elektrotechnické a elektronické inženýrství,* je mezinárodní nezisková profesionální organizace. Její členská základna obsahuje na 360 000 členů ve 175 zemích. Jedná se o celosvětově uznávanou a všestrannou organizaci, která tvoří a vydává standardy v rozsáhlé řadě disciplín, zahrnujících elektrickou energii, lékařské technologie, zdravotní péči, informační technologie, telekomunikace, spotřebitelskou elektroniku, dopravu, letectví a nanotechnologie [2].

[1] Pojmem „security by obscurity“ rozumějme zabezpečení založené na utajení použitých protokolů a principů.

2.1.2. Rozprostřené spektrum

Technologie rozprostřeného spektra (SS – Spread Spectrum) se využívá v pásmu ISM[1] pro dosažení rychlých přenosů dat. Tradiční rádiové technologie se soustředí na vměstnání co největšího množství signálů do relativně úzkého pásma. Výše zmíněné rozprostřené spektrum oproti tomu využívá matematické funkce pro rozptýlení síly signálu do širokého frekvenčního bloku.

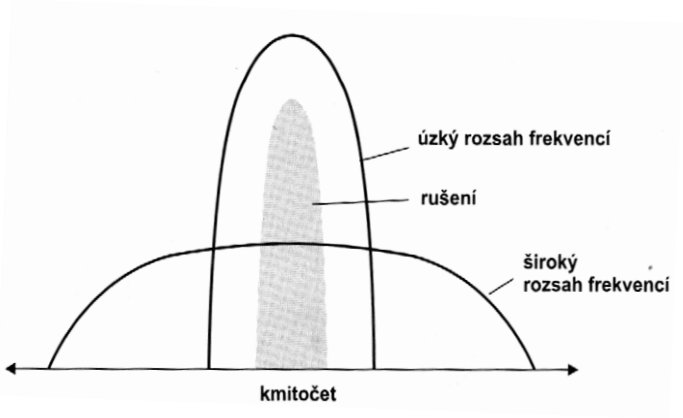
Přijímač provede opačnou operaci a složí takovýto rozprostřený signál do klasického úzkopásmového signálu, se kterým pak dále pracuje. Používání rozprostřeného spektra u určitého úhlu pohledu vede k neefektivnímu využití frekvenčního pásma, zvyšuje však odolnost k interferencím a rušení. Výsledkem jsou ovšem spolehlivější přenosy.

Důležité je, že aplikace rozprostřeného spektra je požadavkem pro provoz nelicencovaných zařízení a vyplývá z nařízení regulátora. V pásmu ISM nelze tedy jiný typ přenosu využívat. Pro doplnění je na obr. 2.1 uveden frekvenční rozsah bezlicenčního pásma ISM.

Obr. 2.1: Pásmo ISM

Použití SS přináší vyšší odolnost k rušení, ale nepřináší řešení k její eliminaci. Rušení mohou způsobovat obdobná zařízení, ale i klasické vysílače pracující s úzkým radiovým pásmem. Na obr. 2.2 je vidět, jak může rušení na úzkém rozsahu frekvencí výrazně ovlivnit úzkopásmový signál. Stejné rušení však signál rozprostřeného spektra ovlivní o značnou část méně. Problémům se též z části snaží předcházet regulační orgány předpisem, omezující maximální vyzářený výkon.

[1] ISM (Industrial, Scientific and Medical) je bezlicenční pásmo na frekvenci 2,4 GHz.



Obr. 2.2: Diagram rozprostřeného spektra [5]

FHSS

Technika přeskokových zařízení se poprvé objevila v období 2. světové války roku 1942 v patentu pod jménem „Bezpečný komunikační systém“. Cílem byla tvorba systému umožňující udržet rádiově naváděná torpéda na správném kurzu a zabránit nepříteli v rušení naváděcího systému.

Princip byl postaven na neschopnosti rušičky měnit vysílanou frekvenci stejně rychle jako vysílač. Na základě tohoto systém skákal z jednoho kmitočtu na druhý. Tyto změny probíhaly velice rychle a než rušící strana zachytila frekvenci vysílání a zahájila rušení, naváděcí signál již pracoval na jiném kmitočtu.

Tato technika vedla ke vzniku FHSS (Frequency Hopping Spread Spectrum). Využívá frekvenční šířku 83,5 MHz, čímž je vykryt celý dostupný rozsah 2,4 GHz pásma (tj. od 2,4 do 2,4835 GHz). Toto pásmo je rozděleno do 75 kanálů o šířce 1 MHz. Zbývajících cca 8,5 MHz je vyhrazeno jako „ochranné pásmo“ proti interferencím ze sousedního frekvenčního pásma. Radiový signál skáče v náhodném pořadí (tzn. na základě náhodné posloupnosti) po jednotlivých kanálech. Každých 30 vteřin vystřídá alespoň 75 kanálů a na každém vysílá max. 400 milisekund.

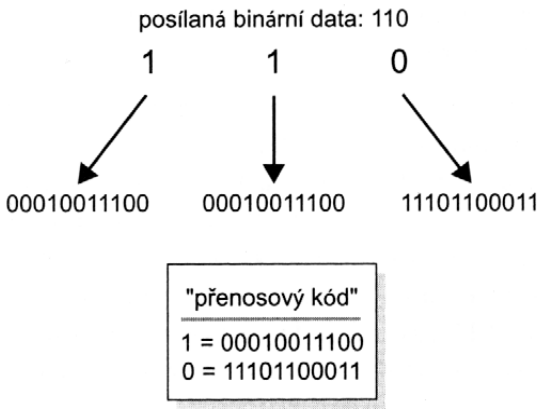
Výhodou FHSS je větší počet pracujících systémů v pásmu 2,4 GHz. Teoreticky je to kolem 26, prakticky kolem 15 přístupových bodů.

Metoda frekvenčních poskoků je v dnešní době využívána minimálně, byla nahrazena úspěšnějším DSSS. Tím vzniká využití FHSS jako „security by obscurity“.

Převážná většina nástrojů pro detekci sítí je založená na DSSS (např. NetStumbler[1]) a systémy používající FHSS jsou poměrně neznámé a potencionálním útočníkům skryté.

DSSS

Systémy využívající přímé sekvence mají oproti FHSS výhodu podpory vyšších přenosových rychlostí. Technologie DSSS (Direct Sequence Spread Spectrum) funguje tak, že se vezme jeden přenášený datový bit a transformuje se do 11 bitového přenosového kódu (tzv. chipping code), což je vidět na obr. 2.3.

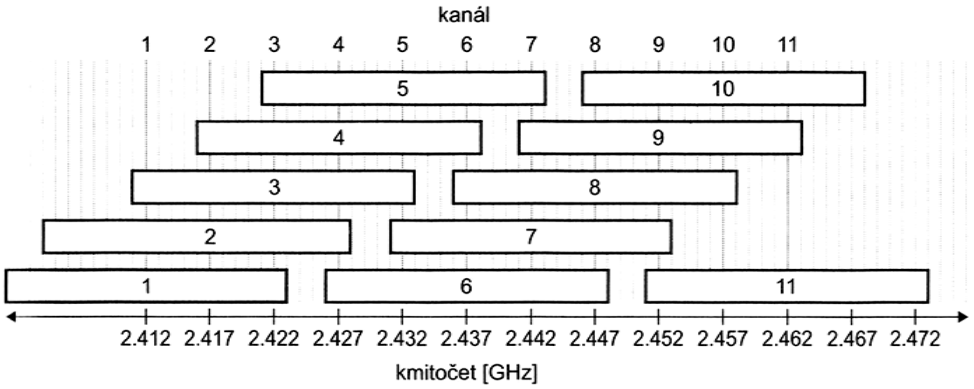


Obr. 2.3: Technologie DSSS

Inverznost přenosového kódu není náhoda. Díky této skutečnosti má DSSS velkou odolnost vůči rušení. V případě poškození přenášených dat dokáží opravné techniky tyto data zrestaurovat do původní podoby.

DSSS používá 11 kanálů o šířce 22 MHz. Povolené pásmo na 2,4 GHz má však šířku pouze 83,5 MHz. Tento paradox je vyřešen tím, že střední kmitočty jednotlivých kanálů jsou od sebe posunuty o pouhých 5 MHz. Sice je tímto způsobem získáno více kanálů, ale za cenu překrývání. Tím pádem se za použitelné (vzájemně se nepřekrývající) dají považovat pouze tři (viz obr. 2.4).

[1] NetStumbler je volně dostupný nástroj na zjištění dostupných bezdrátových sítí.



Obr. 2.4: Rozložení kanálů technologie DSSS

OFDM

Přenosová technika OFDM, neboli *ortogonální multiplex s kmitočtovým dělením,* pracuje stejně jako výše zmíněně systémy s rozprostřeným spektrem.

Princip OFDM spočívá v použití několika stovek až tisíců nosných kmitočtů, které jsou dále dle potřeby konkrétní aplikace modulovány různě robustními modulacemi (QPSK, 16-QAM, či 64-QAM).

Jednotlivé nosné frekvence jsou vzájemně ortogonální, takže maximum každé by se mělo překrývat s minimy ostatních. Datový tok celého kanálu se tak dělí na stovky dílčích datových toků jednotlivých nosných. Poněvadž jsou ve výsledku toky na jednotlivých nosných frekvencích malé, je možné vkládat ochranný interval (GI) – čas, kdy se nevysílá žádná nová informace. Na přijímací straně je tak možné nerušeně přijmout (právě) vysílaný symbol, i když přichází k přijímači více cestami a s různým zpožděním. Stejný symbol přijatý vícekrát s různým zpožděním tak může odpovídat i více vysílačům. Přijímané výkonové úrovně více vysílačů resp. odrazů se tak na přijímací straně do jisté míry sčítají.

Díky vysílání signálu na více nezávislých frekvencích se zvyšuje odolnost vůči interferencím. OFDM nachází uplatnění pro přenos signálu nejen v bezdrátových sítích standardu IEEE 802.11a/g, ADSL a WiMAX, ale také ve standardech pro digitální televizi DAB a DVB-T [13].

3. IEEE 802.11

Řada diskuzí a debat, které byly vedeny od počátku 90. let vyvrcholila v přijetí specifikace IEEE 802.11. Původním cílem bylo vytvořit vzájemné bezdrátové propojení přenosných zařízení a dále jejich připojování na lokální (např. firemní) sítě LAN. Postupem času začala být technologie využívána i k bezdrátovému připojení do sítě Internet v rámci rozsáhlejších lokalit a tzv. HotSpotů[1].

Produkty z řady IEEE 802.11 jsou dnes implementovány v podstatě ve všech přenosných počítačích i mobilních telefonech. Masivní rozšíření přineslo využívání pásma ISM, což má negativní důsledky ve formě silného zarušení příslušného frekvenčního spektra.

Tento „původní“ standard definoval přenosové rychlosti 1 nebo 2 megabity za sekundu a pokrýval první (fyzickou) a druhou (linkovou) vrstvu modelu OSI[2].

Na fyzické vrstvě byly definovány metody:

DSSS (Direct Sequence Spread Spectrum)

FHSS (Frequency Hopping Spread Spectrum)

Infračervený přenos

Na spojové vrstvě byly definovány služby:

Autentizace a deautentizace

Asociace, disasociace a reasociace

Privátnost (WEP)

Doručování MSDU (Mac Service Data Unit)

Velkou zajímavostí, která rozhodně stojí za zmínku, je infračervené světlo, které je definováno jako možná fyzická vrstva.

V době vzniku se vyskytovaly obavy týkající se rozšíření založené na vysoké výrobní ceně bezdrátových adaptérů vůči infračerveným. Právě bezdrátové adaptéry znevýhodňovala cena až padesátinásobně. Vycházelo se z představ, že pro technologii by bylo možné využít infračervené porty, které v již v této době byly běžně obsazené

[1] HotSpot je místo, či oblast s možností bezdrátového připojení k Internetu.

[2] Referenční model OSI byl přijat v r. 1984 jako nosný prvek pro standardizaci architektury počítačových sítí. Vrstev je sedm. Fyzická, spojová, síťová, transportní, relační, prezentační a aplikační.

v noteboocích formou standardní výbavy. Po pouhé úpravě ovladačů by bylo možné počítače propojovat pomocí infračervených portů.

Výhodou též byla odolnost vůči radiovému rušení. Přenos IR operuje v okolí pásma 200 THz a celosvětově je absolutně neregulovaný, takže byla očekávaná bezproblémová světová adaptace.

Nakonec, jak je vidět, věc dopadla jinak. Díky masové produkci spolu s jdoucím pádem cen, se staly bezdrátové adaptéry dostupné a revoluce v infračerveném světle nenastala. Nebylo by to poprvé, co silná lobby „horší technologie“ zvítězila nad lepším a funkčnějším řešením, ale v tomto případě se tak naštěstí nestalo. Velkou roli zde hrály nevýhody, jež IR mělo (zejména malý dosah a neprůchodnost skrze zdi).

3.1.1. Wi-Fi Alliance

Nedlouho po zavedení standardu IEEE 802.11, vznikly dva doplňky: 802.11a a 802.11b. Vzhledem k rychlému vývoji bezdrátových technologií se objevilo na trhu velké množství firem, jež měly zájem produkty vyrábět. Ovšem nastal problém s kompatibilitou.

Z tohoto důvodu roku 1999 vzniká globální nezisková organizace s úkolem správy a dohlížení nad standardy a kompatibilitou hardwaru použitého u vysokorychlostních bezdrátových sítí. U jejího zrodu stálo několik velkých firem z oboru.

Dnes je tato organizace známá pod názvem Wi-Fi[1] Alliance (logo aliance je na obr. 3.1). Sdružuje přes 300 výrobců a vývojářů z 20 zemí světa, kteří spolurozhodují o nejdůležitějších aspektech a standardech Wi-Fi sítí. Ve svých laboratořích testuje jednotlivá zařízení založená na specifikaci IEEE 802.11 a v případě jejich kompatibility a interoperability dochází k certifikaci.

Obr. 3.1: Logo Wi-Fi Alliance

[1] Wi-Fi vychází z anglických slov „Wireless Fidelity“, což v překladu znamená „bezdrátová věrnost“.

3.1.2. IEEE 802.11b

Pod hlavičkou IEEE vyšel v roce 1999 standard 802.11b, který umožňoval díky novým modulačním technikám přenášet rychlostmi až 11Mb/s při využití technologie DSSS.

Specifikace:

Kmitočet:	2,4 GHz
Kanály:	14
Rychlost:	11 Mb/S
Kódování:	DSSS
Modulace:	DBPSK (1 Mb/S)
	DQPSK (2 Mb/S)
	CCK (5,5 a 11 Mb/s)

Standard IEEE 802.11b pracuje v kmitočtovém pásmu 2,4000-2,4835 GHz, jež je součástí bezlicenčního pásma ISM. Každý stát má vlastní standardizační instituci, která toto pásmo spravuje (v ČR Český telekomunikační úřad).

Standard se v jednotlivých oblastech odlišuje počtem povolených kanálů. (tab. 3.1)

Místo	**Počet kanálů**
Severní Amerika	11
Evropa	13
Španělsko	2
Francie	4
Japonsko	1

Tab. 3.1: Přehled povolených kanálů v jednotlivých oblastech

3.1.3. IEEE 802.11a

Tento standard vznikl ve stejné době jako IEEE 802.11b, ovšem na rozdíl od něj pracuje v jiném kmitočtovém pásmu – pásmu 5 GHz. Následkem toho nejsou navzájem kompatibilní a mohou být provozovány ve stejné oblasti, aniž by nastal problém vzájemného rušení.

Specifikace:

Kmitočet:	5 GHz
Kanály:	12
Rychlost:	54 Mb/s
Kódování:	OFDM
Modulace:	BPSK (6 a 9 Mb/s) QPSK (12 a 18 Mb/s) 16-QAM (24 a 36 Mb/s) 64-QAM (48 a 54 Mb/s)

Standard IEEE 802.11a zavádí na rozsahu 5,15-5,825 GHz 12 nepřekrývajících se kanálů a pracuje s přenosovou rychlostí až 54 Mb/s.

3.1.4. IEEE 802.11g

V roce 2003 schválilo IEEE specifikaci 802.11g, která měla řešit některé z problémů standardu 802.11a.

V podstatě je 802.11g přepracovaný standard 802.11b pracující s rychlostí až 54 Mb/s. IEEE použilo modulační techniku OFDM ze standardu 802.11a a použilo ji v pásmu 2,4 GHz. Velikým pozitivem tohoto standardu je plná zpětná kompatibilita s 802.11b. Ovšem stále zůstávají negativa známé ze standardu 802.11b. Stále jsou k dispozici pouze tři nepřekrývající se kanály a stále jsou problémy s rušením od jiných zařízení pracujících v pásmu 2,4 GHz.

Specifikace:

Kmitočet:	2,4 GHz
Kanály:	14
Rychlost:	54 Mb/S
Kódování:	OFDM
Modulace:	DBPSK (1 Mb/s) DQPSK (2 Mb/s) CCK (5,5 a 11 Mb/s) OFDM (6,12,18, 36, 48 a 54 Mb/s)

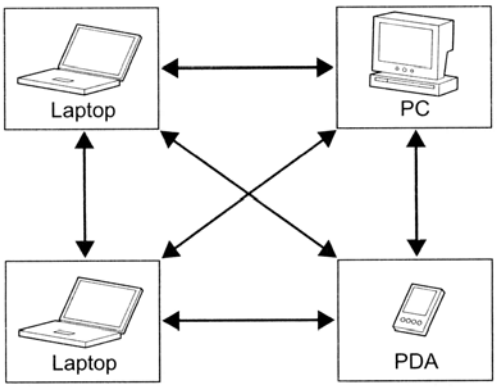
3.2. Topologie bezdrátových sítí

Bezdrátové sítě je možno nastavit dvěma základními způsoby. V jednom případě se klienti propojují přímo navzájem (ad-hoc sítě), ve druhém se připojují k centrálnímu přístupovému bodu (infrastrukturní sítě).

3.2.1. Ad-hoc sítě

Ad-hoc sítě jsou specifické absencí „prostředníka“, jsou složeny pouze z jednotlivých klientů. Každý klient je ve své podstatě malým samostatným přístupovým bodem. Pracuje v režimu peer-to-peer a nepotřebuje ke své činnosti AP[1]. Takto nezávislá síť se nazývá IBSS (Independent Basic Service Set).

Režim ad-hoc se využívá především u sítí budovaných „improvizovaně“. Například při různých zasedáních a konferencích, kde se vyskytuje několik počítačů a krátkodobě potřebují vzájemnou síťovou konektivitu. Pokud nejsou k dispozici adekvátní síťové prvky na propojení, je tato topologie řešením (obr. 3.2).



Obr. 3.2: IBSS [6]

3.2.2. Infrastrukturní sítě

Použití Infrastrukturních sítí převažuje nejen díky přenášení komunikační zátěže z klientských stanic na AP, ale také snazší konfiguraci i pro málo zběhlé uživatele v práci s počítačovými sítěmi.

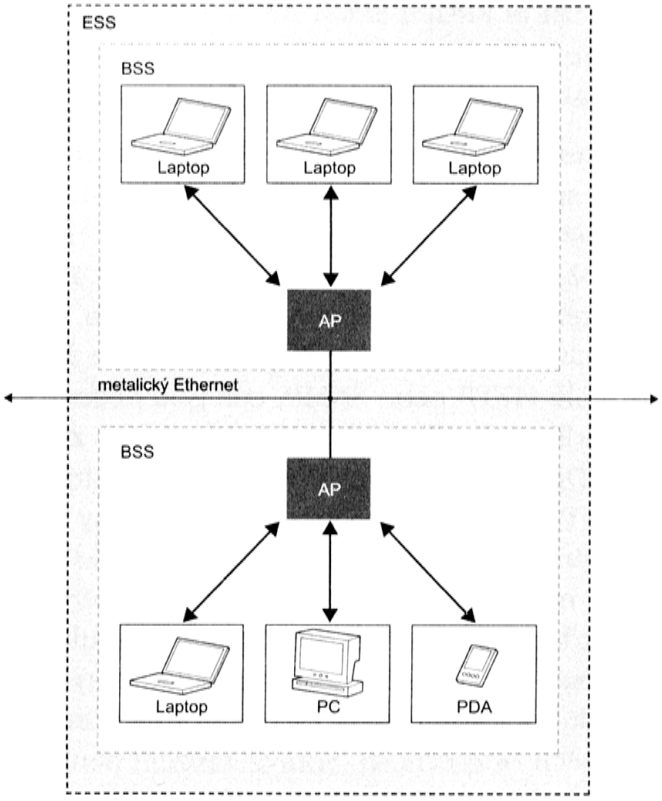
[1] AP (Acces Point) je přístupový bod, ke kterému se klienti v bezdrátových sítích připojují.

BSS (Basic Service Set)

Tyto sítě mají přesně vymezenou infrastrukturu v podobě síťové komponenty AP. Má význam jako rozhraní mezi drátovou a bezdrátovou sítí. Jednotlivé bezdrátové stanice se připojují k centrálnímu přístupovému bodu (AP) a veškerý provoz (dokonce i přímý provoz mezi klienty) se směruje přes něj.

ESS (Extended Service Set)

ESS vytvoříme propojením dvou a více BSS skrze páteřní síť. Na obr. 3.3 je vidět jak taková ESS může vypadat. V tomto případě se jedná o propojení dvou BSS a dvou přístupových bodů. Stanice uvnitř ESS mohou mezi sebou komunikovat, ačkoliv jsou v rozdílných BSS a mohou se pohybovat i mezi jednotlivými BSS.



Obr. 3.3: BSS/ESS [6]

4. Zabezpečení bezdrátových sítí

Bezdrátová síť má proti kabelové jednu nevýhodu vycházející z jejího principu: nelze dostatečně přesně omezit prostor kde je její signál dostupný.

Chceme-li odposlouchávat prostor v kabelové síti, je potřeba se fyzicky dostat k její kabeláži. Máme-li dosáhnout toho samého u bezdrátové sítě, stačí se pohybovat v oblasti, kde lze její signál zachytit.

Mylně se lidé domnívají, že není potřeba sítě zabezpečovat, pokud se v nich neoperuje s citlivými a tajnými daty. Zabezpečení ovšem řeší i přístup do sítě Internet a logicky eliminuje ty, kteří za službu nezaplatili, nebo jsou nežádoucí. Snad jedinou výjimkou je případ, kdy máme v úmyslu provozovat veřejný přístupový bod k Internetu zdarma.

4.1. SSID

Každý přístupový bod neboli AP (Access Point) vysílá každých několik sekund implicitně identifikátor SSID (Service Set Identifier) v tzv. majákovém rámci (beacon frame). Takto můžou síť snadno najít oprávnění uživatelé, ale zároveň do ní proniknout i nežádoucí. Právě díky této funkci dokáže většina softwarových detekčních nástrojů najít bezdrátovou síť bez znalostí SSID.

Konfigurace přístupového bodu umožňuje i vypnutí pravidelného vysílání beacon frame s SSID. Tím docílíme „skrytí“ sítě před běžnými uživateli, ale ne před všemi. Pokaždé, když se někdo připojí k síti, odesílá SSID nekódovaným textem, i když síťové spojení může být jiným způsobem zakódované. Na základě toho je možnost síť zachytit, a pokud není dalším způsobem zabezpečená, je možné se k ní bez problému připojit.

Vypínání vysílání SSID tedy není považováno za úroveň zabezpečení, ale lze ho brát pouze jako ztížení.

4.2. WEP

Protokol WEP (Wired Equivalent Privacy) pracuje jako volitelný doplněk. Vzhledem k tomu, že ho Wi-Fi Alliance pro certifikaci Wi-Fi produktů vyžaduje povinně, je dnes implementován v každém zařízení.

Záměrem protokolu je zajistit uživatelům stejnou míru bezpečnosti, jako mají metalické sítě (což ovšem není příliš mnoho). Jeho úlohou nebylo zaujmout místo jako šifrovací algoritmus. Především měl za úkol zajistit uživatelům přechodem z pevné sítě do „vzduchu“ standard bezpečnosti dat, na něž byli zvyklí. Wired Equivalent Privacy se vykládá jako „míra soukromí, ekvivalentní pevné síti“. Mnozí lidé mylně vidí ve zkratce „E“ význam „Encryption“.

Úkolem WEP je vyřešit slabší zabezpečení bezdrátového přenosu proti klasické síti. S protokolem WEP jsou data stejně bezpečná, jako na pevné nešifrované síti typu Ethernet.

RC4

Standard WEP používá jako šifru symetrickou streamovou šifru RC4, tedy šifru s tajným klíčem. Podstatou této šifry je že se odesílaná zpráva šifruje podle klíče a na cílové straně se dle něho dešifruje.

Klíč (v podobě slova, nebo sekvence znaků) se expanduje v pseudonáhodný klíčovací stream o stejné délce, jako má šifrovaná zpráva. O „pseudonáhodnost“ se stará generátor pseudonáhodných čísel PRNG, což je sestava pravidel, podle nichž se klíč rozšíří na délku zprávy klíčovacího streamu. Šifrování probíhá tak, že na šifrované hodnotě se provede logická operace XOR[1] s klíčovacím streamem, rozšifrování probíhá stejným způsobem. Obě zařízení, mezi nimiž má být provoz šifrován, tedy musí obsahovat stejná pravidla PRNG a musí znát tajný klíč. Problémem tajného klíče ve WEP je fakt, že standard nijak neřeší jeho automatickou distribuci a je na jednotlivých výrobcích, jak distribuci klíče realizují. Jelikož Wi-Fi zařízení většinou

[1] Hradlo XOR je druh logického digitálního elektronického obvodu ze skupiny kombinačních obvodů (hradel).

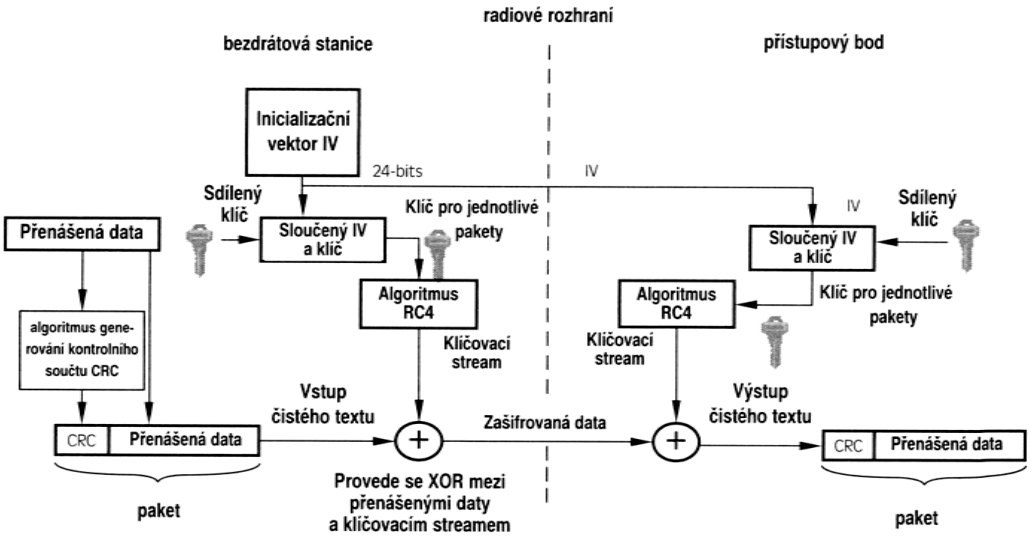
umí klíč přijmout pouze ve formě zápisu do konfigurace zařízení, a tedy nikoliv bez účasti lidského faktoru, čelíme problému jménem „bezpečný přenos klíče“.

Inicializační vektor je 24bitová hodnota, která slouží spolu s “tajným klíčem” k šifrování pomocí RC4. Díky jeho použití dochází k zmírnění statičnosti šifrovaní pomocí WEP. Unikátnost inicializačního vektoru je zcela základním požadavkem šifry RC4. V samotném návrhu WEPu však není specifikováno, jakým způsobem se má inicializační vektor generovat, což je zpětně považováno za ohromnou chybu. Rovněž se ukázalo, že délka inicializačního vektoru zdaleka nedostačuje. Po několika hodinách provozu i ve středně vytížené síti dojde k vyčerpání všech možných inicializačních vektorů a musí se použít znovu. Tím je ale porušena již zmiňovaná nutnost unikátnosti inicializačního vektoru.

Pravidla pro generátor pseudonáhodných čísel jsou velmi důležitá, protože klíč pro šifrování je relativně krátký. Zpočátku byl popis této „pseudonáhodnosti" držen v tajnosti, jenže s volbou RC4 jakožto šifry pro WEP a Wi-Fi sítě vystupňoval touhu hackerů PRNG rozlousknout. A to se také později stalo.

Bezpečnost RC4 šifry záleží především na délce klíče a na četnosti jeho obměny. Čím častěji se mění, tím větší problémy mají potenciální hackeři, protože se jim nepodaří rozluštit celý klíč, nebo je rozluštěný klíč nefunkční. Problém se nalézá v tom, že samotný WEP ani RC4 neřeší způsob bezpečné distribuce tajného klíče, takže musí být uživatelům distribuován jinak, což je právě bezpečnostní riziko jeho odhalení.

Problémem je také jeho délka - WEP definuje délku klíče 40 bitů. Není to mnoho, proto někteří výrobci začali používat vlastní delší šifry, 128 bitů a někteří i 256 bitů. Bohužel to není ve standardu podporováno, může tedy nastat situace, kdy produkty od různých výrobců nemusejí být schopny vzájemné komunikace. Na obr. 4.1 je demonstrováno, jak šifrování podle RC4 probíhá.



Obr. 4.1: WEP zabezpečení pomocí algoritmu RC4

Krátký šifrovací klíč se v počátku prosadil především proto, že USA nepovolovaly „vývoz“ náročnějších šifer a IEEE chtělo Wi-Fi standardizovat tak, aby bylo dostupné po celém světě. Proto nezbylo než se smířit s omezením šifrovacího WEP klíče na 40 bitů. Později se sice pravidla uvolnila, ale to už se začalo pracovat na standardu 802.11i v rámci něhož se řeší právě šifrování a autentizace. Výrobky podporující tento standard začaly plnit trh a vývoj WEP se zastavil.

4.3. Filtrování MAC adres

Metoda filtrování MAC adres[1] představuje další z možností zabezpečení bezdrátových sítí.

Každá bezdrátová karta sítě Ethernet má svoji MAC adresu. Administrátor může do každého přístupového bodu zadat seznam MAC adres, jimž byl povolen přístup do bezdrátové sítě. Žádosti ostatních klientských adaptérů jsou automaticky zamítnuty. Vznikly i četné sofistikovanější varianty tohoto přístupu k autentizaci uživatele, bylo možno vytvořit seznam adres, které mají přístup zakázaný a ostatním adresám přístup povolit. Některá zařízení umožňují přístup na MAC adresy omezit i časově nebo

[1] MAC adresa je unikátní 48 bitový identifikátor síťového rozhraní nejčastěji zapisovaný jako šestice dvojciferných hexadecimálních čísel (např. 01:23:45:67:89:ab)

jim umožnit využívat pouze určitou šířku pásma. Možnosti jsou téměř neomezené a záleží jen na ochotě výrobce takové autentizace implementovat do firmwaru či softwaru.

Toto řešení vypadá na první pohled velice rozumně. Přístup na základě jedné unikátní adresy by bylo velmi dobré řešení. Ovšem narušitelé mohou pomocí odposlouchávání provozu na síti zjistit, které MAC adresy jsou v síti povoleny. Obvykle ani není nutné vyčkat, než se některý z klientů odpojí, aby si útočník mohl jeho adresu „přivlastnit“ a úspěšně projít filtrem.

Slabinou je právě oblast filtrování. Adresa je totiž nastavitelná a ukládá se do firmware zařízení, přičemž je možné ji změnit. U produktů určených pro koncové uživatele v domácí sféře šla situace tak daleko, že možnost změny MAC adresy zařízení přidali výrobci přímo do webového rozhraní. Změnu je možné provést velmi snadno (viz obr. 4.2).

Obr. 4.2: Změna MAC adresy (TP-LINK TL-WR340GD)

Pravdou je, že zde to má své opodstatnění a nejde ani tak o nástroj pro hackery. Společnosti poskytující širokopásmové připojení jako ADSL ve většině případů dodávají svoje síťové prvky a uživatelův účet svazují s MAC adresou dodaného zařízení. Uživatel má takto možnost pořídit si lepší a vhodnější směrovač (např. s více ethernetovými porty, Wi-Fi rozhraním,…) dle svého uvážení a zprovoznit ho nastavením MAC adresy povoleného zařízení. Společnosti také ale vědí, proč to dělají –

uživatelé si většinou tyto směrovače kupují především proto, aby mohli více využívat linku, kterou si pronajali. To logicky není v zájmu společností nabízející širokopásmové připojení, resp. ano - za předpokladu, že si uživatel za připojení dalšího počítače zaplatí.

V každém případě ale výše uvedená možnost změnit MAC adresu znamená také možnost obejít filtrování podle MAC adres. I proto se více uplatňuje seznam povolených MAC adres než seznam vyloučených MAC adres, neboť zjistit povolenou MAC adresu je složitější, než ji změnit a tím se dostat mimo listinu zakázaných.

Druhým a souvztažným problémem filtrace dle MAC adres je distribuce seznamu MAC adres. Standardně není distribuce seznamu nijak řešena. Většině výrobků chybí jakýkoliv systém centrální správy a většina přístupových bodů to řeší prostým vstupním okénkem, kde lze přidávat a ubírat MAC adresy, v lepším případě možností uploadu seznamu přes webový prohlížeč. Jen výjimečně je možné tyto seznamy nahrávat pomocí TFTP (Trivial File Transfer Protocol) - to má ale samo o sobě dostatek bezpečnostních problémů, aby bylo možno mu zcela důvěřovat.

4.4. 802.1X

802.1X je protokol umožňující autentizaci na portech. V tomto kontextu chápeme porty jako součást první síťové vrstvy, tedy fyzické porty na přepínači. Nejde o TCP porty na čtvrté vrstvě modelu OSI (například port 80 služby http).

I když tento standard nebyl původně určen pro bezdrátové sítě, lze jej použít i k významnému zlepšení bezpečnosti v prostředí 802.11 a samozřejmě jím můžete chránit i fyzické porty na metalické síti. Vezmeme si za příklad útočníka, který se fyzicky dostane do budovy a připojí svůj přenosný počítač do ethernetové zásuvky. Je-li zapnut protokol DHCP, útočník dostane přidělenu IP adresu a může pracovat a pohybovat se interní síti. V souvislosti s 802.11 lze každého bezdrátového klienta chápat jako virtuální metalické připojení, kde 802.1X blokuje veškerý provoz na daném portu až do doby, než se klient autentizuje prostřednictvím údajů, které jsou uloženy na back-end serveru, kterým je typicky RADIUS (Remote Authentication Dial In User Service).

4.4.1. Vývoj

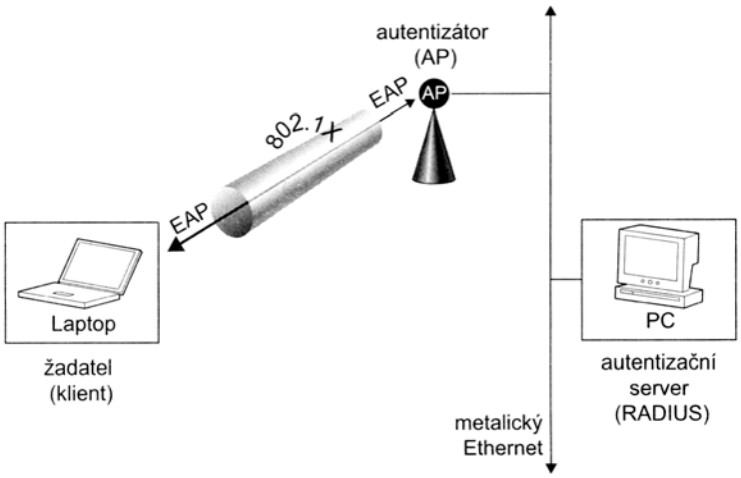
Protokol 802.1X vychází z protokolu PPP (Point-to-Point Protocol). Tento protokol se původně používal u vytáčených připojení a později našel využití u některých DSL modemů a kabelových modemů (tentokrát jako protokol PPPoE, či PPPoA). Postupem času nastalo jeho nemalé rozšíření. Jediným omezením jdoucím nazvat slabinou, se stala autentizace. Je založená pouze na kombinaci uživatelského jména a hesla.

Za cíl vývoje bylo dáno vytvoření obecné platformy pro různé autentizační metody. Vznikl protokol EAP. Ve stručnosti ho lze charakterizovat jako PPP se „zásuvnými" autentizačními moduly. Díky tomu je možno uživatele autentizovat různými způsoby. Máme možnost použít hesla, certifikáty, tokeny, PKI, čipové karty, Kerberos, biometriky, atd.

Otevřený standard zajišťuje, že kdykoliv v budoucnu bude možno metody zabezpečení zlepšit. Jako nový typ bude moci využít mechanismy, které dnes ještě nejsou známy.

4.4.2. Princip

802.1X je jednoduše protokol, který umožňuje používat EAP na metalických nebo bezdrátových sítích. Pro pochopení funkčnosti tohoto protokolu se musíme seznámit se třemi jeho základními komponentami (obr. 4.3):



Obr. 4.3: 802.1X [6]

Žadatel (suplikant): Uživatel nebo klient, požadující přístup k síti.

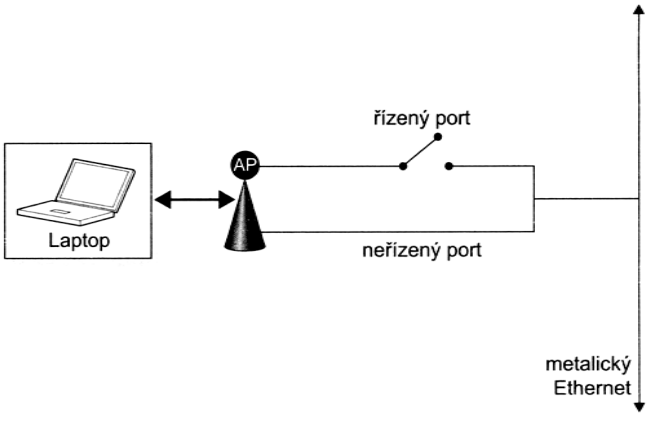
Autentizátor: „Muž uprostřed" (typicky přepínač nebo AP), povolující nebo blokující provoz.

Autentizační server: Systém udržující autentizační informace, typicky server RADIUS.

Proceduru protokolu 802.1X si lze ilustrativně představit na situaci, kdy se chceme dostat do nového exkluzivního klubu či baru. Žadatel je osoba, která chce dovnitř. Autentizátor je vyhazovač u dveří, který někoho pustí a někoho ne. Autentizační server je pak seznam členů, kteří mají povolen vstup.

Aby mohl celý protokol fungovat, musí být jak 802.1X tak zvolený EAP konzistentně podporován na všech třech komponentách. O metodách protokolu EAP bude hovořeno později v další části. Šlo o problém zejména v době, kdy 802.1X podporovaly pouze AP vyšší třídy a jen některé operační systémy. V současnosti už jsou role žadatelů, autentizátorů i autentizačních serverů podporovány téměř univerzálně.

Autentizátor funguje stejně jako dynamický firewall. Dokud neproběhne autentizace, nepropustí žádný provoz kromě zpráv protokolu 802.1X. Po provedení autentizace je povolen libovolný provoz. Dosahuje se toho zavedením dvou virtuálních portů - řízeného portu a neřízeného portu (obr. 4.4). Neřízený port slouží pouze ke komunikaci autentizátora s autentizačním serverem. Řízený port je na počátku v neautorizovaném stavu, kdy je blokován veškerý provoz. Po autentizaci klienta se řízený port přepne do autorizovaného stavu a může jím procházet síťový provoz.

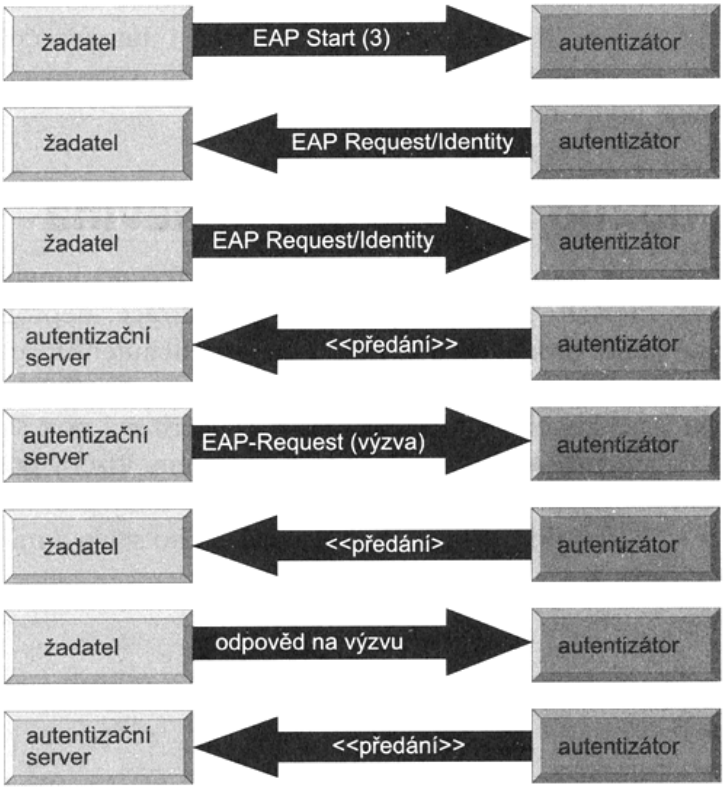


Obr. 4.4: 802.1X [6]

Autentizační konverzace

Žadatel (klient) začíná odesláním rámce EAP Start. Tím se autentizátor dozví, že někdo klepe na dveře a chce jít dovnitř. Autentizátor odpoví rámcem EAP Reguest/Identity, který v zásadě říká: „Kdo je tam?“ Žadatel odpoví rovněž rámcem EAP Request/Identity, ve kterém se identifikuje (uvede uživatelské jméno). Autentizátor tuto informaci předá autentizačnímu serveru. autentizační server pošle autentizátoru rámec EAP-Request, který obsahuje nějakou výzvu nebo požadavek na informaci, například na zadání hesla. Autentizátor tento rámec předá žadateli, který na něj příslušným způsobem odpoví. Autentizátor odpověď převezme a předá ji autentizačnímu serveru.

Následně provede autentizační server ověření a odpoví autentizátoru rámcem EAP-Success (nebo Failure). Pokud autentizátor obdrží rámec EAP-Success, přepne autentizátor řízený port z neautorizovaného stavu do autorizovaného stavu a povolí normální síťovou komunikaci. Obr. 4.5 ukazuje průběh autentizace.



Obr. 4.5: komunikace protokolem 802.1X [6]

Jak vidíme, žadatel a autentizační server spolu nikdy nekomunikují přímo. Veškerou komunikaci přijímá a zprostředkovává autentizátor. Klient může v síti komunikovat až ve chvíli, kdy se úspěšně autentizuje [6].

4.4.3. Perspektiva

Infrastruktura protokolu 802.1X umožňuje dělat věci, které v tradičním prostředí 802.11 nebyly vůbec možné.

První a nejdůležitější možnost je ta, že lze klienty individuálně identifikovat a autentizovat. V původním prostředí metody WEP sdíleli všichni uživatelé stejný klíč. Při autentizaci uživatele jsme získali jedinou informaci, že daný uživatel zná klíč. Nebyla ovšem žádná možnost dozvědět se, o kterého konkrétního uživatele jde. U protokolu 802.1X je každý autentizovaný uživatel jednoznačně identifikován. Máme tedy k dispozici podporu centrálního mechanismu AAA (autentizace, autorizace a účtování). Protože víme, kdo se připojuje, můžeme také nasadit politiku síťového přístupu. Pro jednotlivé uživatele lze např. omezit dny a časy, kdy se mohou k síti připojit. Můžeme dokonce dělat takové věci, jako je nezávislé přiřazení uživatelů do různých VLANů.

No a konečně 802.1X nabízí pokročilejší autentizační metody, než jsou jen jména a hesla. Máme podporu libovolného autentizačního mechanismu – např. vzorky DNA.

4.5. Protokol EAP

Protokol EAP je bezpečnostní protokol, který pracuje ve vrstvě 2 (tedy ve vrstvě adres MAC) a aktivuje se v autentizační fázi celého procesu zabezpečení. 802.1X spolu s EAP představují pouze základnu pro tzv. „zásuvné“ autentizační moduly/metody (zmíněno již výše).

V současné době protokol EAP podporuje desítky těchto metod. Od výběru se bude odvíjet jak náročnost implementace, tak i bezpečnost celého řešení. Některé metody se instalují snáze, jiné jsou zase mnohem bezpečnější. V závěru nelze

opomenout nutnost podpory od všech tří komponent systému – tedy žadatelé, autentizátoři i autentizační server.

4.5.1. Metody autentizace

Autentizace EAP-MD5

Metoda EAP-MD5 se při odesílání autentizačních informací na server RADIUS opírá o hash (otisk) MD5 vytvořený z uživatelského jména a hesla. Tato metoda nezajišťuje žádnou správu klíčů ani nenabízí dynamické generování klíčů WEP, a proto vyžaduje statické klíče WEP; má proto jistá omezení:

- Protože není k dispozici žádné dynamické generování klíče WEP, neznamená protokol EAP oproti WEP žádné vyšší zabezpečení. Útočníci mohou i nadále odposlouchávat síť a snadno dešifrovat klíč WEP.
- EAP-MD5 nenabízí žádné prostředky, kterými by si klientské zařízení ověřilo, že vysílá informace do správného přístupového bodu. Klient tak může mylně vysílat i do pirátského přístupového bodu.

Znamená to, že EAP-MD5 nenabízí oproti samotnému standardu 802.1X žádné funkce navíc, a proto se ze všech metod EAP považuje za nejméně bezpečnou.

Autentizace LEAP

Metodu LEAP vyvinula na základě normy 802.1X firma Cisco (bývá označována též jako EAP-Cisco) a je základem velké části oficiálně schválené verze EAP. Podobně jako EAP-MD5 i metoda LEAP od klientského bezdrátového zařízení přebírá uživatelské jméno a heslo, a předává je k autentizaci na server RADIUS. Firma Cisco doplnila kromě požadavků samotné normy i další podporu a přinesla tak do metody vyšší bezpečnost:

- Metoda LEAP provádí autentizaci klienta tak, že pro každé klientské připojení se dynamicky generují jednorázové klíče WEP. To znamená, že každý klient bezdrátové sítě pracuje

s jiným dynamicky vygenerovaným klíčem, který nikdo nezná - dokonce ani samotný uživatel.

- LEAP podporuje jednu funkci protokolu RADIUS, kterou jsou časové limity komunikačních relací; to znamená, že se klient musí každých několik minut přihlásit znovu. Přidáme-li k této funkci dynamické klíče WEP, budou se v důsledku toho klíče WEP měnit tak často, že se útočníkům nepodaří je včas prolomit.
- LEAP provádí vzájemnou autentizaci, tedy *klienta vůči přístupovému bodu* i naopak *přístupového bodu vůči klientu;* tím se vytváří ochrana proti instalaci pirátských přístupových bodů do sítě.

U autentizační metody LEAP je známo jediné omezení: pro autentizaci klienta i přístupového bodu se používá protokol MS-CHAPv1, který obsahuje známá zranitelná místa.

Autentizace EAP-TLS

Metodu EAP-TLS vyvinula firma Microsoft a její popis je uveden v dokumentu RFC 2176. Namísto kombinace uživatelského jména a hesla provádí tato metoda autentizaci pomocí certifikátů X.509; informace veřejného klíče v PKI se zde do EAP přenášejí pomocí zabezpečení transportní vrstvy. Podobně jako LEAP nabízí i verze EAP-TLS dvě důležité funkce:

- Dynamické generování jednorázového klíče WEP
- Vzájemná autentizace zařízení

Mezi nevýhody metody EAP-TLS patří:

- Pro jeho činnost je nutný protokol PKI, který většina firem neprovozuje.
- Pokud v síti běží adresářové služby Open LDAP nebo Novell Directory Services, je potřeba mít také server RADIUS.
- V případě implementace PKI certifikátu VeriSign nejsou k dispozici všechna pole požadovaná metodou EAP-TLS.

Tuto metodu má smysl uvádět do provozu jen v případě, že se při její implementaci bude přesně dodržovat doporučení firmy Microsoft.

Autentizace EAP-TTLS

Autentizační metodu EAP-TTLS zavedla firma Funk Software jako alternativu k výše popsané EAP-TLS. Bezdrátový přístupový bod se i zde musí autentizovat vůči klientu pomocí serverového certifikátu, ale uživatelé odesílají pro přihlášení jen uživatelské jméno a heslo. Tyto přihlašovací informace (jméno a heslo) pak EAP-TTLS předává k ověření pomocí libovolného mechanismu výzvy a odpovědi, určeného administrátorem (PAP, CHAP, MS-CHAPv1, MS-CHAPv2, PAP/tokenová karta, nebo EAP). Jedinými nedostatky této metody je:

- menší bezpečnost než dvojité certifikáty EAP-TLS,
- stejný způsob práce jako standard firem Microsoft a Cisco – „chráněná“ verze Protected EAP (PEAP).

4.6. WPA

WPA jako dočasné řešení

WEP byl již od roku 2001 považován za zcela nedostatečný mechanismus pro WLAN nesplňující současné požadavky na bezpečnost sítí. Proto se začalo pracovat na jeho vylepšení. Na konci roku 2002 sdružení výrobců *Wi-Fi Alliance* oznámilo momentální řešení pro problémy s bezpečností WLAN pod označením Wi-Fi Protected Access (WPA). WPA bylo přijato jako dočasné řešení do doby, než bude schválen bezpečnostní doplněk normy IEEE 802.11i (k čemuž došlo v polovině roku 2004) a než budou k dispozici slučitelné produkty.

WPA představuje podmnožinu prvků 802.11i. Při jeho vývoji se volily ty prvky, které nevyžadovaly změny v hardwaru, takže modernizace většiny zařízení šla provést pouze prostřednictvím softwarových/firmwarových změn. Proto také WPA používá stejný šifrovací mechanismus RC4 jako WEP. Nicméně protokol použitý ve WPA (TKIP) má kvůli své vyšší složitosti určitý vliv na výkonnost zařízení: ve srovnání

s WEP snižuje výkonnost o 5-15 %. Právě výkonnost již používaného hardwaru bránila návrhu ideálního řešení. Dostupný výkon CPU nedostačoval pro podporu lepších šifrovacích metod (např. AES).

WPA je dopředně slučitelné s 802.11i, ale ještě nezahrnuje takové prvky normy jako bezpečné rychlé předávání stanice mezi přístupovými body (secure fast handoff) na základě předběžné autentizace (pre-authentication), bezpečné deautentizace a odpojení nebo rozšířený protokol pro šifrování na bázi AES (Advanced Encryption Standard). Ty totiž již vyžadují hardwarové změny v bezdrátových produktech.

První produkty odpovídající standardu WPA se na trhu objevily v květnu 2003. Vylepšení nabízená protokolem WPA se ovšem nedají použít pro sítě typu ad-hoc a fungují pouze v sítích BSS/ESS s instalovanými AP.

4.6.1. TKIP

Mechanismus TKIP zlepšuje šifrování prostřednictvím tří hlavních prvků:

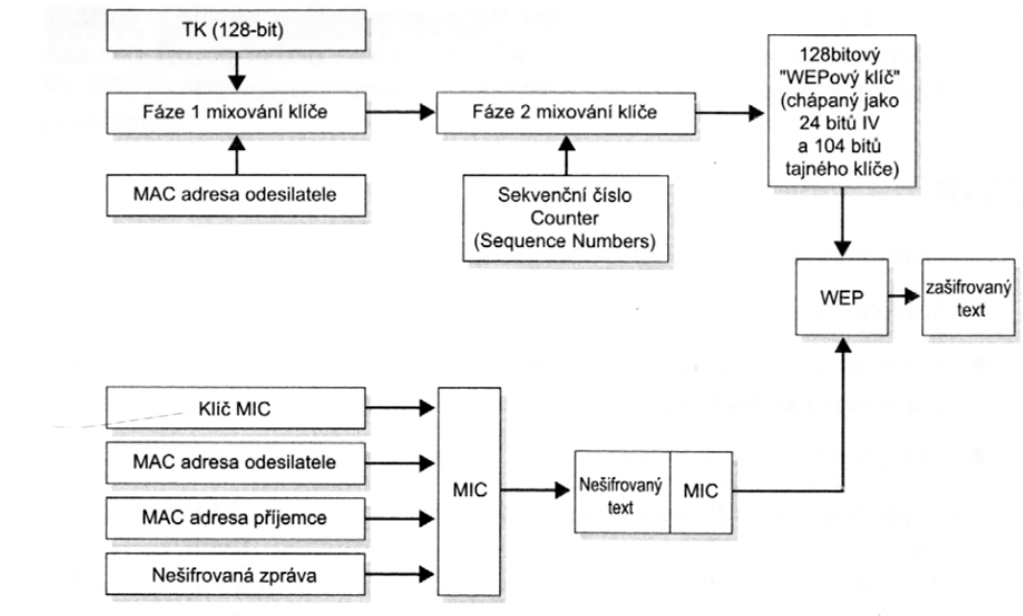
- Funkce mixování klíče pro každý paket.
- Vylepšená funkce kontroly integrity (MIC, Message Integrity Code), pojmenovaná Michael.
- Vylepšená pravidla generování IV včetně sekvenčních pravidel.

V zásadě představuje TKIP pouze dočasnou opravu protokolu WEP, kterou lze implementovat jednoduchým upgradem softwaru/firmwaru. Kvůli zachování zpětné kompatibility s velkým počtem stávajících instalovaných hardwarových zařízení byly při jeho návrhu učiněny různé kompromisy.

Princip funkčnosti

Klient začíná se dvěma klíči - 128bitovým šifrovacím klíčem a 64bitovým klíčem pro zajištění integrity, které získá bezpečnými mechanismy v průběhu iniciální komunikace protokolem 802.1X. Šifrovací klíč se označuje jako TK (Temporal Key - viz obr. 4.6.). Klíč pro zajištění integrity se označuje jako klíč MIC (Message Integrity Code). V první fázi se provede XOR mezi MAC adresou odesilatele a hodnotou TK, čímž vzniká klíč označovaný jako Fáze 1 (někdy též „mezilehlý klíč"). Klíč Fáze 1

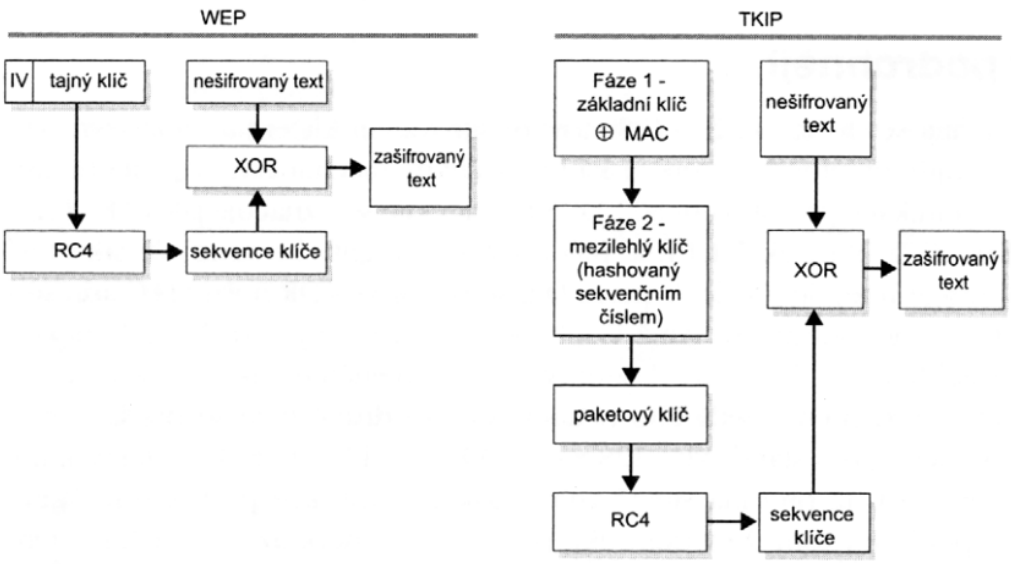
se mixuje se sekvenčním číslem a vzniká tak klíč Fáze 2, pro přenos jediného paketu. Výstup druhé fáze se předává mechanismu WEP jako standardní 128bitový WEPový klíč (tedy IV + tajný klíč). Zbytek procesu už probíhá stejně jako klasická transakce protokolem WEP. Rozdíly spočívají v tom, že v důsledku první fáze už nepoužívají všichni klienti stejný WEPový klíč, a v důsledku druhé fáze už neexistuje korelace mezi hodnotou IV (v tomto případě sekvenčním číslem) a samotnou klíčovací sekvencí.



Obr. 4.6: Šifrování mechanismem TKIP

Mixování paketového klíče

Problém původního návrhu protokolu WEP spočíval v tom, že hodnota IV se jednoduše připojila k tajnému klíči a předala se generátoru RC4. U TKIP první fáze zajistí, že každý klient používá jiný mezilehlý klíč. Ve druhé fázi se tento klíč mixuje se sekvenčním číslem a teprve tento výsledek se následně předává generátoru RC4. Jedná se o propracovanější postup, než je jen prosté připojení hodnoty IV k tajnému klíči. Díky tomuto mechanismu tak TKIP odstraňuje nevhodnou implementaci použití RC4 ve WEP (obr. 4.7).



Obr. 4.7: Mechanismus šifrování

Funkce kontroly Integrity

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

Inicializační vektor

Problém s kolizemi IV je řešen TKIP pomocí dvou jednoduchých pravidel. Prostor inicializačního vektoru se zvětšil z 24 bitů na 48 bitů. Při rychlosti 54 Mbps to znamená, že vyčerpání stavového prostoru bude trvat přes 1000 let. Za další TKIP nařizuje, že hodnota IV roste inkrementálně od nuly a hodnoty mimo pořadí se ignorují.

Z pohledu bezpečnosti znamená rozšíření prostoru IV (respektive sekvenčního čísla) to, že se eliminují kolize IV a na nich založené útoky.

WPA a domácí sféra

Jak už bylo řečeno, TKIP (a WPA) spoléhá při distribuci klíčů na infrastrukturu protokolu 802.1X (jako je například server RADIUS). Ne všichni domácí uživatelé ovšem mají tuto infrastrukturu k dispozici, takže aby mohli využívat šifrovacích funkcí TKIP, zavádí WPA speciální režim, označovaný jako režim s předsdíleným klíčem (PSK - Pre-Shared Key).

V tomto režimu musí všichni uživatelé na všech klientech a AP nastavit sdílenou tajnou hodnotu, takzvaný „master key". Je to trochu podobné tomu, když se u protokolu WEP všude nastavoval WEP klíč. Na rozdíl od WEPu však TKIP používá tento klíč pouze jako výchozí hodnotu, z níž se matematicky odvodí potřebné šifrovací klíče. Na rozdíl od WEPu, kde se stejný klíč používal stále dokola, provádí TKIP změnu šifrovacích klíčů, takže je zaručeno, že stejný klíč nikdy nebude použit dvakrát.

4.7. IEEE 802.11i

Jak už bylo řečeno, WPA je dočasné opatření, které v polovině roku 2003 umožnilo v praxi nasadit část výsledků práce skupiny zabývající se vývojem IEEE 802.11i. WPA je tedy její podmnožinou. Primární komponenta tohoto protokolu, která v té době ještě nebyla úplně hotova, byla šifra AES. Ve specifikaci IEEE 802.11i je AES povinná, zatímco TKIP volitelný.

4.7.1. AES

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

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

Nový šifrovací mechanismus

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

Stejně jako RC4 je i AES šifra se symetrickým klíčem, což znamená, že se text šifruje i dešifruje stejným sdíleným tajným klíčem. Na rozdíl od šifry RC4, která šifruje lineárně každý bajt XORováním s náhodnou sekvencí, AES pracuje s bloky o velikosti 128 bitů, a proto se označuje jako bloková šifra.

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

Inovovaný algoritmus Michael

Stejně jako TKIP i CCMP obsahuje algoritmus MIC zajišťující, že nedošlo k modifikaci přenášených dat. Nicméně mechanismus MIC v CCMP funguje jinak než algoritmus Michael v TKIP. Jeho výpočet je založen na inicializačních hodnotách vycházejících z IV a z dalších hlavičkových informací. Pracuje v 128bitových blocích a počítá se přes jednotlivé bloky až na konec originální zprávy, kdy se vypočte konečná hodnota [5].

5. Ověření bezpečnosti

Pro praktické ověření bezpečnosti byl vybrán protokol WEP. Hlavním důvodem pro výběr byl fakt, že je aplikován ze 70% vyskytujících se zabezpečených přístupových bodů a tím se řadí i přes své dobře známé slabiny mezi nejvíce aplikované prostředky, s kterými se lze v dnešní době setkat.

5.1. Metody průniku

Odrazovým můstkem pro prolomení WEPu se stal dokument s názvem *„Weakness in the Key Scheduling Algorithm of RC4“*, který v srpnu roku 2001 publikovali Scott Fluhrer, Itsik Mantin a Adi Shamir. Dokument poukazoval na slabá místa a popisoval, jakým způsobem lze úspěšně útok na WEP provést. Uchytil se pro něj název „FMS“ odvozený od prvních písmen příjmení autorů.

Slabina zabezpečení tkví především v přibližné známosti vzhledu inicializačního vektoru IV, tedy v možnosti rozluštit klíč. Navíc prodloužení klíče má k délce jeho luštění lineární a nikoliv exponenciální závislost, a tedy prodloužení klíče na dvojnásobek znamená pouze prodloužení potřebného času jeho luštění na dvojnásobek, nikoliv na mnohonásobek, jako je tomu u jiných šifer.

Nedlouho po uvedení FMS se na svět dostává AirSnort. Jedná se o jeden z prvních nástrojů určených k rekonstrukci WEP klíčů v sítích IEEE 802.11 šířených pod licencí GPL[1] na platformě Linuxu. Postupem času se objevily programy i pro platformu Windows.

[1] GPL (General Public License) je nejpopulárnějším a dobře známým příkladem silně copyleftové licence, která vyžaduje, aby byla odvozená díla dostupná pod totéž licencí. Poskytuje uživatelům počítačového programu práva svobodného softwaru a používá copyleft k zajištění, aby byly tyto svobody ochráněny, i když je dílo změněno nebo k něčemu přidáno.

5.2.Praktická ukázka prolomení WEP

5.2.1. Právní aspekty

Nutností je uvést, že neuváženou činností v této oblasti je možné se dostat na pomezí zákona. Za právně obhajitelnou lze považovat skutečnost pouhého monitoringu okolních přístupových bodů (za předpokladu využití např. k vědeckým či studijním účelům). Případ, kdy se jedná o dlouhodobé užívání, resp. připojení k síti (jakékoli interní či např. k Internetu), a to nikoli pouze jednou osobou, ale někdy i výrazně početnější skupinou, která toto připojení pak navíc ještě dále sdílí, dochází k jednání protiprávnímu a trestně postižitelnému. Za trestně postižitelné se považuje i případ, připojujeme-li se k bezdrátové síti, jež nemá zabezpečení aktivované.

5.2.2. Realizace

Aby se předešlo právním důsledkům, postup byl demonstrován na vlastním přístupovém bodě (model TP-LINK TL-WR340GD).

Konfigurace:

SSID:	TP-LINK
Region:	Czech Republic
Kanál:	6
Mód:	54Mbps (IEEE 802.11g)
Zabezpečení:	WEP
Formát WEP klíče:	ASCII
Typ klíče:	128bit
WEP klíč:	popokatepetl1
LAN IP adresa	192.168.2.1
DHCP server:	192.168.2.101 - 192.168.2.200
Wireless MAC filtering:	00:1B:77:78:66:97 (povolena)

K výše popsanému AP byl připojen notebook Acer Aspire 5720 s integrovanou bezdrátovou kartou Intel PRO/Wireless 3945ABG (MAC: 00:1B:77:78:66:97). Pro odposlouchávání vzájemné komunikace sloužila bezdrátová PCI karta TP-LINK TL-WN551G nainstalovaná do stolního počítače.

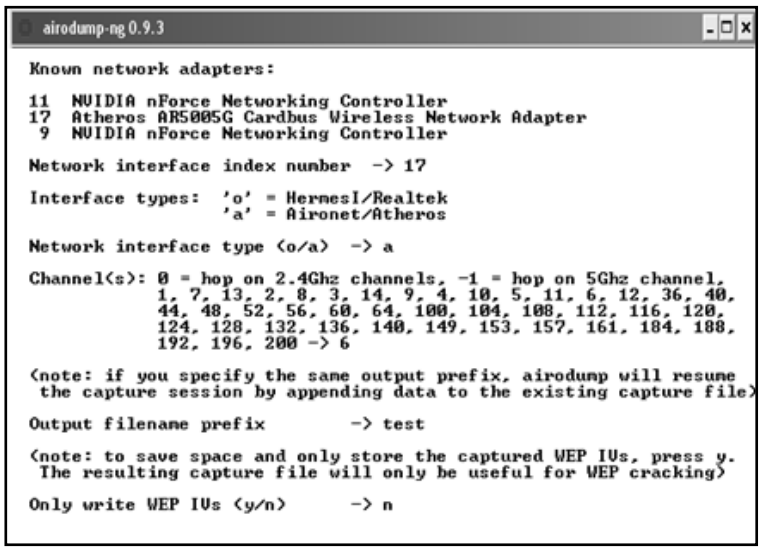
Pro ukázkové prolomení WEPu byla zvolena platforma Windows a nikoliv Linux z důvodu, že MS Windows je brán jako naprosto běžný systém pro laického uživatele. Snahou bylo poukázat na jednoduchost řešení.

Zvolen byl programový balík Aircrack-ng 0.9.3, kompatibilní s MS Windows a námi použitou PCI Wi-Fi kartou. Pro aktivaci „promiskuitního režimu“ byly staženy ovladače, které umožnily naslouchání komunikace v dosahu karty (bez speciálních ovladačů program není schopen pracovat).

Po úspěšném nainstalování ovladačů byl spuštěn nástroj Airodump-ng, který má za primární úkol zachycovat a ukládat kompletní (nebo pouze IV) provozní data na konfigurovaném kanálu/kanálech.

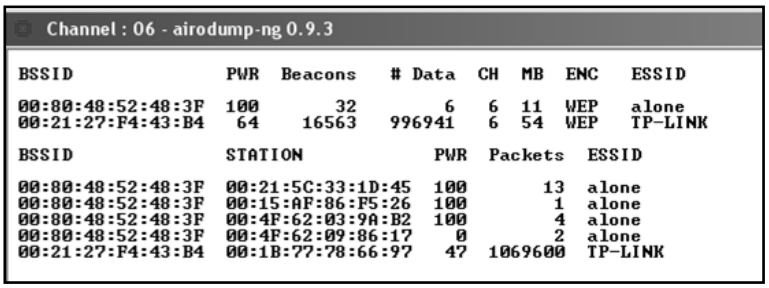
Airodump-ng nabídne stahování paketů z jednotlivého kanálu (1-14), nebo všech najednou (0). Doporučuje se prvně zjistit, na jakém kanálu vysílá cílové AP a až poté zadat jeho kanál. Jsou tím omezeny ztráty, které vznikají zaznamenáváním paketů z kanálů nepotřebných pro tento případ. Pro detekci dostupných bezdrátových sítí je použit program *CommView for WiFi.*

Dále se uvede název výstupního souboru a provede rozhodnutí, zda stahovat všechny pakety nebo pouze ty, které jsou potřebné pro rozšifrování WEP klíče. Naprostá většina přístupových bodů je nastavena „komfortně“. Výrazem „komfortností“ se rozumí dynamické přidělování konfigurace síťové karty (IP adresa, maska podsítě, výchozí brána, DNS server). Na základě toho bylo zvoleno stahování paketů, které jsou potřebné pro rozšifrování WEP klíče. Ve výjimečných případech je nastavení „nekomfortní“ - to však není překážkou. Stačí využít paket analyzéry, které dokáží pomocí analýzy odposlechnuté komunikace potřebné údaje získat. Průběh konfigurace je zobrazen na obr. 5.1.



Obr. 5.1: průběh konfigurace

Po potvrzení se zobrazí okno s nalezenými sítěmi, MAC adresami vysílačů, klientů atd. Společně s tím vším se zobrazí i sloupec "Packets" (obr. 5.2), který je v tomto případě klíčový. K úspěšnému a téměř okamžitému rozluštění klíče je potřeba nejméně 250 - 800 tisíc paketů, což se váže k délce klíče. Pravdou je, že ve výjimečných případech se klíč podaří získat už i z jednoho tisíce paketů.



Obr. 5.2: průběh sledování

Po stažení potřebného množství paketů je program ukončen a spuštěn Aircrack-ng do něhož se načte soubor s nasbíranými pakety a zahájí proces zjišťování šifrovacího klíče. Na obr. 5.3 je uveden výstup programu s nalezeným WEP klíčem „popokatepetl1“.

Obr. 5.3: výstup programu

Po podvržení MAC adresy (v registrech systému, nebo pomocí utility, např. SMAC), která byla vyčtena z komunikace na obr 5.2 (MAC: 00:1B:77:78:66:97). Asociací k SSID „TP-LINK“ a vložením WEP klíče „popokatepetl1“ bylo pomocí protokolu DHCP automaticky provedeno síťové nastavení, na základě něhož byl získán přístup do sítě.

5.3. Zvýšení bezpečnosti pomocí dostupných prostředků

Dle většiny odborníků by bylo nejlepším řešením přestat protokol WEP používat a nahradit ho novějšími a odolnějšími metodami. Vzhledem ke konzervativnosti uživatelského portfolia, není vůle k inovacím a tak by se při jeho aplikaci měly alespoň dodržovat jisté bezpečnostní zásady a opatření:

- **Změna implicitního identifikátoru SSID**
  Vyvarovat se výskytu údajů, jako jméno firmy, adresa, jméno, či defaultní názvy produktů (např. MyWlan).
- **Deaktivace vysílání SSID**
- **Změna přístupového hesla**
  Každý hacker hodný toho jména zná implicitní hesla výrobců a vyzkouší je jako první. Programy typu NetStumbler dokáží identifikovat výrobce podle MAC adresy.
- **Změna umístění přístupových bodů**
  Pokusit se soustředit na umístění přístupových bodů blíže středu budovy, než poblíž oken.
- **MAC filtry**
  Snaha o řízení přístupu podle MAC adres síťových karet.
- **Deaktivace DHCP**
  Zvážit přiřazení statických IP adres bezdrátovým síťovým kartám a deaktivace DHCP.
- **Změna podsítě adres**
  V případě deaktivace DHCP změnit třídu IP adres na méně obvyklou (např. na třídu B – 172.16.1.15)

6. Nástroj pro automatizované zhodnocení bezpečnosti

6.1. Možnost využití

6.1.1. Nezávislé průzkumy

Před dvěma lety představila poradenská firma Ernst & Young na tiskové konferenci výsledky průzkumu z oblasti bezdrátových sítí. Vyhodnocování probíhalo ve dvou pražských městských částech a jedním z bodů zájmu bylo zabezpečení.

Výsledek byl tristní, při počtu cca 1400 detekovaných přístupových bodů (po odečtení bodů typu HotSpot) bylo zabezpečeno pouze 64%. Pro Prahu jako velkoměsto je tento výsledek velice znepokojivý. Vzhledem k tomu, že inovace a využívání nových technologií bývá ve velkých městech napřed, stav v menších městech je pravděpodobně ještě více zneklidňující.

6.1.2. Nástroj pro sledování

Při snaze začít podnikat a proniknout na jakýkoli trh v dnešní době skýtá spoustu hrozeb. Proto je velmi důležité provádět analýzu trhu a i nadále po úspěšném začátku a monitorovat konkurenční prostředí.

Každý poskytovatel bezdrátového připojení k Internetu se snaží budovat svou síť páteřních spojů a přístupových bodů konzistentně. Pro pokrytí oblasti velikosti Liberce jich jsou zapotřebí desítky. Každý poskytovatel používá ve své síti totožné názvy SSID, způsoby zabezpečení a snaží se nakupovat podobné typy zařízení. Činí tak z důvodu zjednodušení údržby sítě, zmenšení režijních nákladů (více typů zařízení – nutnost školení personálu, z toho vyplývající vyšší náklady), ale také z důvodů marketingových a reklamních. Tím se myslí identifikátor SSID, v němž může být vepsán název poskytovatele, či přímo adresa jeho internetových stránek (např. www.poskytovatel.cz), čímž se otvírá cesta pro mapování konkurence, konkrétně jeho přístupových bodů a úrovně technické vyspělosti. Příkladem je program, jenž byl v rámci praktické části vytvořen.

6.2. Modelové řešení

Webová aplikace vznikla na platformě operačního systému Linux, konkrétně distribuci Ubuntu verze 9.04. Bylo nutné doinstalovat moduly PHP5 a softwarový webový server Apache.

6.2.1. Programová část

Program vychází z výpisu příkazu iwlist wlanX scan (viz obr. 6.1). Výstup tohoto příkazu je načten pomocí funkce shell_exec. Získaná data se poté pomocí funkce

```
Cell 01 - Address: 00:21:27:F4:43:B4
          ESSID:"TP-LINK"
          Mode:Master
          Channel:6
          Frequency:2.437 GHz (Channel 6)
          Quality=62/100  Signal level:-70 dBm  Noise level=-68 dBm
          Encryption key:on
          IE: Unknown: 000754502D4C494E4B
          IE: Unknown: 010882848B960C183048
          IE: Unknown: 030106
          IE: Unknown: 0706435A2001 0D14
          IE: Unknown: 2A0102
          IE: Unknown: 320412246 06C
          IE: WPA Version 1
              Group Cipher : CCMP
              Pairwise Ciphers (1) : CCMP
              Authentication Suites (1) : PSK
          Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
                    12 Mb/s; 24 Mb/s; 36 Mb/s; 9 Mb/s; 18 Mb/s
                    48 Mb/s; 54 Mb/s
          Extra:tsf=00000001b0387181
          Extra: Last beacon: 1292ms ago
```

Obr. 6.1: ukázka sítě vypsané příkazem *iwlist wlan0 scanning*

explode rozdělí na jednotlivé řádky a následuje postupné zpracovávání. Rozdělení se provádí podle znaku ":" na dvě části. První část je brána jako označení hodnoty a část druhá jako hodnota sama. U takto získaných dat se prověřuje označení hodnot. Hodnoty žádoucí se uloží do pole nalezených sítí.

Některé položky jsou specifické a vyžadují individuální přístup, mezi ně patří: *quality*, *signal*, *noise*. Vyskytují se na jednom řádku společně a je nutné jejich rozdělení na části oddělené mezerami, či rovnítky. Následně jsou načteny. Podobné je to i u položek *channel* a *frequence*, kde je využito opět rozdělení pomocí mezer. Zbavení se u kanálu ohraničení závorkami učiníme ořízntutím první a posledního znaku hodnoty.

Položka *bit rates* vrací hodnotu na více řádků. Pro její správné načtení je třeba číst několik dalších řádků pro složení celého řetězce. Kompletnost se pozná podle

načtení další hodnoty s označením *Extra*. Podobný algoritmus se volí i v případě detekce zabezpečení *WPA*.

V případě výskytu zaměření pozornosti na klíče: *Group Cipher, Pairwise Ciphers, Authentication Suites*. V případě absence *WPA* nejsou prvkem zájmu.

Poslední fáze programu vyhodnotí šifrování a jeho typ vypíše. Jedná-li se o nezabezpečenou síť, označí ji jako *none*.

V závěru se veškeré nalezené údaje vypíší do přehledné tabulky (viz příloha B). Položky nadpisu, stejně jako „detekované typy“ šifrování jsou koncipované jako odkazy, které vyvolají html stránku a adekvátním popisem.

6.3. Možnost zlepšení

Vyšší forma programu se musí odvíjet dle reálných potřeb praktického řešení. Další vývoj by byl možný v podobě nástroje realizovaného na míru konkrétnímu poskytovateli pro monitorování vývoje konkurence.

Na centrálním místě / serveru by docházelo ke sběru dat z požadované oblasti a jejich následné vyhodnocování. Poskytovatel takto získá plně automatizovaný systém, jenž mu umožní poznat kompletní infrastrukturu konkurence a spolu s pomocí triangulačních procesů vytvořit interaktivní mapu pokrytí bezdrátových sítí. Vhodně zvolená strategie, podložená skvělou informovaností o každém tahu konkurence by umožnila být vždy o krok napřed.

7. Závěr

Cílem bakalářské práce bylo postihnout problematiku zabezpečení bezdrátových sítí od jejich počátku. Po teoretickém úvodu, kde byly představeny bezdrátové sítě jako celek, následoval obecný popis jednotlivých doplňků a autorit, které se podílely na jejich vývoji a certifikaci.

Hlavní náplň je tvořena popisem jednotlivých metod zabezpečení, jejich strukturou a možnostmi uplatnění. Demonstrativně je předvedeno, že není velký problém připojit se k dostupné Wi-Fi síti „ilegálně“.

Úmyslně nebyl výchozí platformou zvolen Linux, jako prostředí pokročilých „uživatelů“ s chutí poznávat a zkoušet, ale systém Microsoft Windows, operační systém běžného uživatele. Snahou je poukázat, že připojení do zabezpečené sítě bez znalosti přístupových údajů není záležitost pouze pro hackera, či odborníka na informační technologie, ale není problémem ani pro středně pokročilého uživatele.

V poslední části jsou rozebrány možnosti automatizovaného zhodnocení bezpečnosti bezdrátových sítí.

Práce nemá působit jako návod na obcházení jednotlivých úrovní zabezpečení, ale spíše jako „nástroj“ na zvýšení povědomí ohledně bezpečnostních rizik.

Seznam použité literatury

[1] Guglielmo Marconi. Wikipedia.org [online]. Poslední aktualizace 1. 5. 2009. URL: <http://cs.wikipedia.org/wiki/Guglielmo_Marconi>.

[2] IEEE. Wikipedia.org [online]. Poslední aktualizace 11. 2. 2009. URL: <http://cs.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers>.

[3] IEEE 802.11 [online]. Wikipedia.org. Poslední aktualizace 11. 4. 2009. URL: <http://cs.wikipedia.org/wiki/IEEE_802.11>.

[4] Wi-Fi Alliance. Wi-Fi.org [online]. Poslední aktualizace 2009. URL: <http://www.wi-fi.org/about_overview.php>.

[5] Pužmanová, Rita. Bezpečnost bezdrátové komunikace: Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. Vydání 1. Brno, Computer Press, 2005. 184 s. ISBN: 80-251-0791-4.

[6] Barken, Lee. Wi-Fi: jak zabezpečit bezdrátovou síť. Vydání 1. Brno, Computer s. ISBN 80-251-0346-3.

[7] Thomas, Thomas M. Zabezpečení počítačových sítí bez předchozích znalostí. Vydání 1. Brno, CP Books, 2005. 338 s. Cisco systems. ISBN 80-251-0417-6.

[8] Zandl, Patrick. Bezdrátové sítě WiFi : praktický průvodce. Vydání 1. Brno, Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

[9] Köhre, Thomas. Stavíme si bezdrátovou síť Wi-Fi. Vydání 1. Brno, Computer Press, 2004. 296 s. ISBN 80-251-0391-9.

[10] Davis, Harold. Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě: není zapotřebí žádných předchozích zkušeností! Vydání 1. Praha, Grada, 2006. 334 s. ISBN 80-247-1421-3.

[11] Anonymous. Maximální bezpečnost: Svazek II. Vydání 4. Praha, Softpress, 2004. 544 s. ISBN 80-86497-65-8.

[12] Php.net [online]. Poslední aktualizace 28. 5. 2009. URL: < http://www.php.net/manual/en/>.

[12] Ernst & Young. www.ey.com/cz [online]. 2. 10. 2007. URL: <http://www.ey.com/CZ/cs/Newsroom/News-releases/2007-WiFi-survey-CZ>.

[13] OFDM [online]. Wikipedia.org. Poslední aktualizace 16. 5. 2009. URL: <http://cs.wikipedia.org/wiki/OFDM>.

Příloha A - Dodatky ke standardu IEEE 802.11 [3]

IEEE 802.11	Původní standard pro 1 a 2 Mbit/s rychlost s frekvencí 2.4 GHz (r.1999)
IEEE 802.11a	54 Mbit/s, 5 GHz standard (vydáno r.1999, produkty od r.2001)
IEEE 802.11b	Vylepšení 802.11 s podporou 5.5 a 11 Mbit/s (r.1999)
IEEE 802.11c	Bezdrátové přemostění (bridge); obsaženo v IEEE 802.1D standardu (r.2001)
IEEE 802.11d	Mezinárodní roamingový dodatek (r.2001)
IEEE 802.11e	Vylepšení QoS, včetně dlouhých (burst) paketů (r.2005)
IEEE 802.11F	Komunikace mezi bezdrátovými přístupovými body (r.2003, stažen v březnu r.2006)
IEEE 802.11g	54 Mbit/s, 2.4 GHz standard (zpětně kompatibilní s 802.11b) (r.2003)
IEEE 802.11h	Správa spektra 802.11a (5 GHz) pro Evropu (r.2004)
IEEE 802.11i	Vylepšený autentifikační a šifrovací algoritmus (WPA2) (r.2004)
IEEE 802.11j	Dodatek pro Japonsko; nová frekvenční pásma pro multimedia (r. 2004)
IEEE 802.11k	Vylepšení správy rádio zdrojů pro vysoké frekvence. (Navazuje na IEEE 802.11j)
IEEE 802.11l	(rezervováno a nebude použito)
IEEE 802.11m	Správa standardu: přenosové metody a drobné úpravy.
IEEE 802.11n	Vylepšení pro vyšší datovou propustnost
IEEE 802.11o	(rezervováno a nebude použito)
IEEE 802.11p	Bezdrátový přístup pro pohyblivé prostředí (auta, vlaky, sanitky)
IEEE 802.11q	(rezervováno a nebude použito, aby se nepletlo s 802.1Q)
IEEE 802.11r	Rychlé přesuny mezi přístupovými body (roaming) (r. 2008)
IEEE 802.11s	Samoorganizující se bezdrátové sítě (ESS Mesh Networking)
IEEE 802.11T	Předpověď bezdrátového výkonu - testovací metody
IEEE 802.11u	Spolupráce se sítěmi mimo 802 standardy (například s mobilními sítěmi)
IEEE 802.11v	Správa bezdátových sítí (konfigurace klientských zařízení během připojení)
IEEE 802.11w	Chráněné servisní rámce
IEEE 802.11x-	(rezervováno a nebude použito)
IEEE 802.11y	Pro běh ve frekvenčním pásmu 3650 - 3700 MHz (veřejné pásmo v USA)

Příloha B – Výstup nástroje na zhodnocení bezpečnosti bezdrátových síti

ESSID	MAC address	Frequency (channel)	Signal / Noise	Mode	Max rate	Encryption key	Encryption type
M-Net	00:19:E0:F9:BA:DC	2.412 GHz (1)	-53 dBm / -92 dBm	Master	54 mb/s	on	WPA Version 1 GC:TKIP PC:TKIP CCMP AS:PSK
Home	00:13:92:09:64:FE	2.437 GHz (6)	-82 dBm / -127 dBm	Master	54 mb/s	off	none
anetliberec.cz	00:4F:62:0A:5C:97	2.437 GHz (6)	-86 dBm / -127 dBm	Master	11 Mb/s	on	WEP
straightcore	00:0A:59:F3:9A:BD	2.452 GHz (9)	-80 dBm / -127 dBm	Master	11 Mb/s	on	IEEE 802.11i/WPA2 Version 1 GC:CCMP PC:CCMP AS:PSK
letnax	00:0B:6B:80:EF:58	2.472 GHz (13)	-87 dBm / -127 dBm	Master	11 Mb/s	on	WEP
net150d	00:0B:6B:80:EF:58	2.467 GHz (12)	-90 dBm / -127 dBm	Master	11 Mb/s	on	WEP
JUL-LSB2	00:1E:E5:A9:DB:F0	2.472 GHz (13)	-87 dBm / -127 dBm	Master	54 mb/s	on	IEEE 802.11i/WPA2 Version 1 GC:CCMP PC:CCMP AS:PSK
juf2h	00:4F:67:03:53:AC	2.467 GHz (12)	-90 dBm / -127 dBm	Master	54 mb/s	on	IEEE 802.11i/WPA2 Version 1 GC:TKIP PC:TKIP CCMP AS:PSK