UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Principy funkce bezdrátových sítí, jejich využití a bezpečnost

Michal Mojžíš

Bakalářská práce
2012

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michal Mojžíš**
Osobní číslo:	**I08117**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Principy funkce bezdrátových sítí, jejich využití a bezpečnost**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je popsat principy fungování a využití bezdrátových sítí a jejich zabezpečení. Dalším cílem je otestovat odolnost zabezpečení bezdrátové sítě pomocí běžně dostupných technologií a útoků.
Autor práce představí základní principy fungování bezdrátových sítí. Dále představí principy fungování nejpoužívanějších zabezpečení bezdrátových sítí. Autor provede analýzu těchto zabezpečení a na jejich základě se pokusí provést simulaci prolomení zabezpečení s využitím open source nástrojů.
Předpokládaný rozsah textu je 30 stran.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: tištěná/elektronická

Seznam odborné literatury:

Yang Xiao,Xuemin Shen,Dingzhu Du: Wireless network security, Springer 2007
Georgios I. Papadimitriou , Andreas S. Pomportsis P. Nicopolitidis, Mohammed S. Obaidat : Wireless Networks , Wiley 2003
Rita Pužmanová Bezpečnost bezdrátové komunikace, Computer Press 2005

Vedoucí bakalářské práce: Mgr. Josef Horálek
Katedra softwarových technologií

Datum zadání bakalářské práce: 16. prosince 2011
Termín odevzdání bakalářské práce: 11. května 2012

Univerzita Pardubice
Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Ozgan, Ph.D.
vedoucí katedry

V Pardubicích dne 30. března 2012

Prohlášení autora

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

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

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne

Poděkování

Na tomto místě bych rád poděkoval vedoucímu své bakalářské práce Mgr. Josefu Horálkovi za vynaložený čas, který mi věnoval.

Anotace

Bakalářská práce se zaobírá bezdrátovými sítěmi, k čemu se v běžném životě používají a jak fungují. Dále obsahuje testování protokolů WEP, WPA a WPA2 a zabezpečení proti vnějším útokům.

Klíčová slova

IEEE 802.11, Wi-Fi, WEP, WPA, WPA2, RC4, AES, TKIP, CCMP, MIC

Title

Principles of operation wireless networks, their availability and security.

Annotation

Bachelor's theses on wireless networks to use in daily life and how they operate. Also includes the testing protocols, WEP, WPA and WPA2, and security against external attacks.

Keywords

IEEE 802.11, Wi-Fi, WEP, WPA, WPA2, RC4, AES, TKIP, CCMP, MIC

Obsah

Seznam zkratek **9**

Seznam obrázků **10**

Seznam tabulek **11**

1 Úvod **12**

2 Bezdrátová síť **13**

2.1 Bezdrátová síť obecně 13

2.2 Antény 13

2.2.1 Rozdělení 13

2.2.2 Zisk 15

2.2.3 Decibel 15

2.2.4 Polarizace 16

2.2.5 Vzhled 16

2.2.6 Šíření radiového signálu 17

3 Standardy IEEE 802.11 ..... **18**

3.1 IEEE 802.11 obecně 18

3.1.1 Popis jednotlivých standardů 18

3.1.2 Popis modulací 19

4 BackTrack **21**

4.1 BackTrack obecně 21

4.2 Důležité aplikace 21

4.2.1 Aircrack-ng 21

4.2.2 Airodump-ng 22

4.2.3 Aireplay-ng 23

5 Autentizační protokol 802.1x **25**

5.1 Autentizační mechanismy 26

5.2 Výhody a nevýhody 26

6 Bezpečnostní protokoly používané ve Wi-FI **27**

6.1 WEP (Wired Equivalent Privacy) 27

6.1.1 Autentizace 27

6.1.2 Šifrování 27

6.2 WPA (Wi-Fi Protected Access) 28

6.2.1 Čtyři fáze pro bezpečnou komunikaci 29

6.3 WPA2 (Wi-Fi Protected Access 2) 38
6.3.1 Čtyři fáze pro bezpečnou komunikaci 38
6.4 Přehled WEP, WPA a WPA2 42
7 Doporučené zabezpečení 43
8 Ukázka prolomení protokolu WEP 44
9 Ukázka prolomení protokolu WPA (802.1X) 46
10 Ukázka prolomení protokolu WPA2 52
11 Závěr 58
12 Literatura 59

Seznam zkratek

IEEE - Wi-Fi standard pro lokální bezdrátové sítě

Wi-Fi – Bezdrátová síť

RC4 – Šifra, která generuje pseudonáhodný proud bajtů

CRC-32 – Kontrolní součet

PSK – Před-sdílený klíč

MIC – Algoritmus Michael

TKIP – Šifrovací protokol založený na RC4

AES – Bloková šifra

CCMP – Šifrovací protokol založený na AES

Seznam obrázků

Obr. 2.1 - Všesměrové vysílání [4] 13
Obr. 2.2 - Sektorové vysílání [10] 14
Obr. 2.3 - Směrové vysílání signálu [5] 14
Obr. 3.1. – FHSS (přepracováno dle [12]) 19
Obr. 3.2 – DSSS (přepracováno dle [12]) 20
Obr. 3.3 – OFDM (přepracováno dle [12]) 20
Obr. 5.1 - Žádání o autentizaci klientem (přepracováno dle [12]) 25
Obr. 6.1 - Šifrovací algoritmus (přepracováno dle [12]) 28
Obr. 6.2 - Komunikace založená na čtyřech fázích (přepracováno dle [12]) 29
Obr. 6.3 – Architektury ve WLAN (přepracováno dle [24]) 30
Obr. 6.4 - Před-Sdílený klíč (přepracováno dle [12]) 31
Obr. 6.5 - Ukázka odvozování klíčů (přepracováno dle [12]) 32
Obr. 6.6 - Hierarchie párového klíče WPA (přepracováno dle [12]) 33
Obr. 6.7 - 4-Way Handshake (přepracováno dle [12]) 34
Obr. 6.8 - Hierarchie skupinového klíče u WPA (přepracováno dle [12]) 35
Obr. 6.9 - Group key Handshake (přepracováno dle [12]) 36
Obr. 6.10 - Algoritmus Michael (přepracováno dle [12]) 37
Obr. 6.11 - Mixování a šifrování TKIP (přepracováno dle [12]) 38
Obr. 6.12 - Odsouhlasení bezpečnostních zásad (přepracováno dle [12]) 39
Obr. 6.13 - Hierarchie párového klíče WPA2 (přepracováno dle [12]) 40
Obr. 6.14 - Hierarchie skupinového klíče WPA2 (přepracováno dle [12]) 41
Obr. 6.15 – CCMP (přepracováno dle [12]) 42
Obr. 8.1 - Odposlouchávání přenášených inicializačních vektorů 44
Obr. 8.2 - Hledání hesla 45
Obr. 9.1 – Odposlech 46
Obr. 9.2 - Ukládání do souboru 47
Obr. 9.3 – Deautentizace 48
Obr. 9.4 - Získaný handshake 49
Obr. 9.5 - Neúspěšný slovníkový útok 50
Obr. 9.6 - Úspěšný slovníkový útok 51
Obr. 10.1 – Odposlech 52
Obr. 10.2 - Ukládání do souboru 53
Obr. 10.3 – Deautentizace 54
Obr. 10.4 - Získaný handshake 55
Obr. 10.5 - Neúspěšný slovníkový útok 56
Obr. 10.6 - Úspěšný slovníkový útok 57

Seznam tabulek

3.1 - Přehled standardů IEEE 802.11 19
4.1- Klasické nastavení 21
4.2 - WEP nastavení 22
4.3 - WEP a WPA - PSK nastavení 22
4.4 – Klasické nastavení 22
4.5 - Nastavení filtru 23
4.6 – Typ útoku 23
4.7 – Klasické nastavení 23
4.8 - Nastavení Replay, ARP a Fragmentačního útoku 24
5.1 - Přehled autentizačních mechanismů 26
6.1 - Dočasné klíče 32
6.2 - Dočasné klíče 35
6.3 - Přehled bezpečnostních protokolů 42

1 Úvod

Pro běžný život drtivé většiny lidí je Wi-Fi připojení důležitým faktorem. Bez něho neudělají ani krok. Vše má své výhody a nevýhody. U Wi-Fi převládají výhody a to takové jako například mobilita. To znamená, že se můžeme připojit, kdekoli kde je přístupový bod. Například kavárny, obchodní centra atd.

Většina firem využívá internet na připojení k němu, pro provoz webových stránek nebo dokonce i provozu e-shopu. E-shop je velmi oblíbený, protože si v klidu ze svého domova vyberete např. lampičku nebo nějaké oblečení a následným objednáním vám to přijde až domu a to bez většího vynaloženého úsilí. Pomocí přístupových bodů (Wi-Fi router, AP) se může kdokoli, kdo je v dosahu signálu a zná přístupová hesla, připojit. S Wi-Fi přichází i velké riziko vniknutí do sítě nežádanou osobou a ztráty citlivých dat. A proto bychom měli klást velký důraz na bezpečnost sítě a věnovat tomu více peněz.

První část je teoretická a v ní budu popisovat princip bezdrátové sítě a vše, co se Wi-Fi týče.

V druhé kapitole se budu věnovat bezdrátovým sítím obecně. Budu tu popisovat i antény, které jsou potřebné pro provozování bezdrátové sítě, a to jak by měli vypadat, jakým směrem se šířit a hlavně na jak velkou vzdálenost dokáží vysílat.

V třetí kapitole se budu věnovat standardům Wi-Fi. Jaké známe a co v sobě obsahují.

Ve čtvrté kapitole budu rozebírat a věnovat se operačnímu systému BackTracku. K čemu se dá využít a jaké užitečné nástroje v sobě obsahuje.

Ve zbývajících kapitolách se budu věnovat autentizačnímu serveru 802.1x a bezpečnostním protokolům WEP, WPA a WPA2. Popíšu, jak fungují, jaké využívají algoritmy pro šifrování dat a rozdíly mezi nimi. Jaký protokol je nejsilnější a který na druhou stranu nejslabší.

Druhá část je praktická a v ní se budu snažit dokázat chyby, které bezpečnostní protokoly mají. Mým úkolem je skenovat sítě v mém okolí, zjišťovat jejich sílu zabezpečení a poté se pokusit do dané sítě vniknout.

2 Bezdrátová síť

2.1 Bezdrátová síť obecně

Bezdrátová síť neboli Wi-Fi je typ počítačové sítě, ve které komunikují účastníci prostřednictvím elektromagnetických vln. Výhoda mobility na rozdíl od drátové komunikace. Více informací nalezneme na [1][21][23].

2.2 Antény

Antény jsou velmi důležitým faktorem v bezdrátových sítích. Závisí na nich ve velké míře překonávání dvou a více od sebe vzdálených míst neboli přístupových bodů.

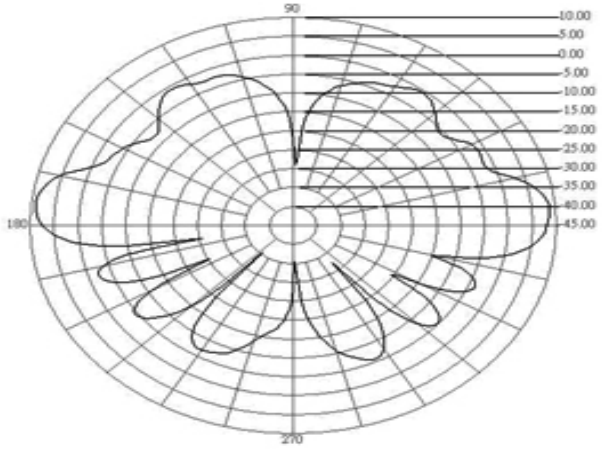
Antény dodávané např. v notebooku nemají velký dosah. Můžeme vidět síť v dosahu desítek metrů. Viditelnost bezdrátových sítí je ovlivněna několika faktory např. prostředím. Interní neboli zabudované antény v bezdrátových zařízeních by měly postačovat pro připojení v budově, ale pro překonávání větších vzdáleností je potřeba kvalitnější externí anténa.

2.2.1 Rozdělení

U antén není rozhodující barva, ale kvalitní vysílání a přijímání signálu. Antény bychom měli vybírat hlavně podle kvality a podle toho jakým směrem vysílají.

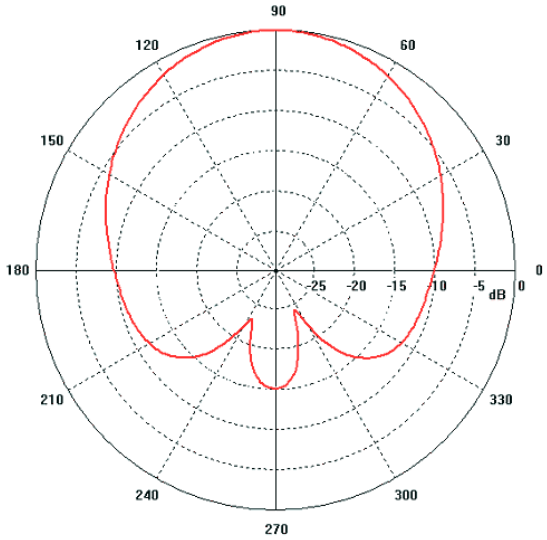
Směrovost antén:

- **Všesměrové** – šíření signálu je všemi směry, což znamená, že vykrývají 360°. Přímo od výrobce dodávané k jednotlivým zařízením, protože jsou nejběžněji používané. Souvislé pokrytí viz Obr. 2.1.



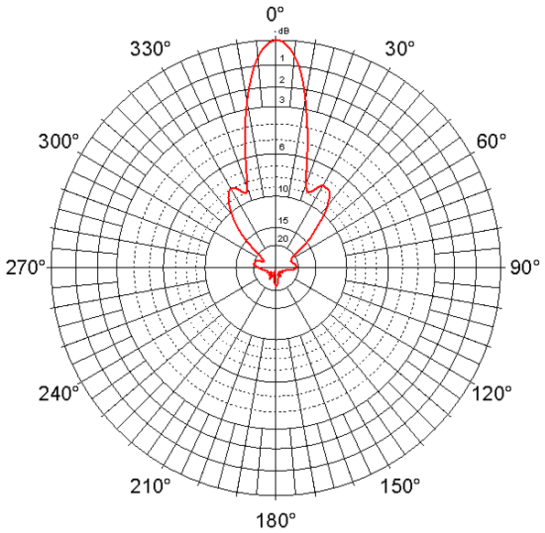
Obr. 2.1 - Všesměrové vysílání [4]

- **Sektorové** - šíření signálu je v takzvaných sektorech, což znamená, že mohou vykrývat např. 180°. Vhodné pro použití v oblasti, kde potřebujeme vykrýt jen jeden směr (např. 180°) a zabránit vysílání jiným směrem viz Obr. 2.2.



Obr. 2.2 - Sektorové vysílání [10]

- **Směrové** – šíření signálu jedním směrem. Tento typ antény, jelikož vysílá jen jedním směrem, tak má kvalitnější vysílání a větší dosah viz Obr. 2.3.



Obr. 2.3 - Směrové vysílání signálu [5]

2.2.2 Zisk

Při výběru antény musíme klást velký důraz na zisk. Čím vyšší zisk, tím vzdálenější signál anténa zachytí. Zisk je poměr mezi intenzitami vyzařování. Více informací nalezneme na [5].

Vlnovou délku můžeme spočítat podle vzorce

$$\mathbf{l = C / f} \qquad (2.1)$$

Vysvětlivky:

l – vlnová délka v metrech

C – rychlost světla v metrech za sekundu (2,997 x 10 m/s)

f – frekvence záření v hertzech

čili pro pásmo 2,4 GHz uvažujeme vlnovou délku 12,48 cm, půlvlna je pak dlouhá 6,24 cm

Zisk antény se udává v dBi, tedy v decibelech na isotrop.

2.2.3 Decibel

Základní jednotka bel (Alexandr Graham Bell[1]), která vznikla jako poměr 10:1 mezi intenzitami (výkony) dvou různých zvuků. Tento poměr je ze dvou stejných veličin, tím pádem je fyzikálně bezrozměrný a vyjadřuje kolikrát je jedna hodnota větší než druhá. Více informací nalezneme na [7].

Výkonový poměr je 10:1 = 1B, 100:1 = 2B, 1 000:1 = 3B

Zisk v belech je dán vztahem:

$$\boldsymbol{G_{Bel} = \log(\frac{P_2}{P_1})} \qquad \mathbf{(2.2)}$$

Vysvětlivky:

- $\mathbf{P_2}$ a $\mathbf{P_1}$ - výkony

Základní jednotka bel je řádově malá, proto se přistoupilo k jednotce decibel.

Výkonový poměr 10:1 = 10dB, 100:1 = 20dB, 1 000:1 = 30dB

[1] Americký profesor fyziologie orgánů řeči, fyziky a vynálezce. Narozen 1847 a zemřel v roce 1922.

Zisk v decibelech je dán vztahem:

$$G_{Decibel} = 10 \times \log(\frac{P_2}{P_1}) \quad (2.3)$$

$\mathbf{P_2}$ a $\mathbf{P_1}$ - výkony

Mohou nastat čtyři možnosti:

- $P_2 > P_1$ - výsledek je kladná hodnota - log(100/ 1) = 2
- $P_2 < P_1$ - výsledek je záporná hodnota - log(0,01/ 1) = -2
- $P_2 = P_1$ - výsledek je roven 0
- $P_2 = 0$ - pro nulovou a zápornou hodnotu není log definován

Podle výsledku můžeme říci, jestli se jedná o zisk čí ztrátu (např. útlum na vedení).

2.2.4 Polarizace

Dva typy polarizace elektromagnetického vlnění:

- **Lineární** – horizontální a vertikální
- **Kruhová** – může být pravotočivá nebo levotočivá.

Pro optimální provoz datového spoje, musí mít obě stanice stejnou polarizaci. Při rozdílné polarizaci dochází ke ztrátám a zmenšení dosahu.

V bezdrátových sítích se používá více horizontální a vertikální polarizace než kruhová.

Vyzařovací úhel

Důležitým prvkem popisu každé antény je vyzařovací úhel, což znamená do jakého směru a pod jakým úhlem anténa vyzařuje. U každé antény bychom měli znát dva vyzařovací úhly a to vertikální a horizontální (viz kapitola 2.2.1).

Vertikální úhel vyzařování vlastně omezuje výšku vyzařovaného kužele.

2.2.5 Vzhled

Důležitým parametrem venkovní antény je váha a rozměr. Při výběru antény bychom si tyto parametry měli zjistit, protože je potřeba vědět jak pevně anténu upevnit, aby nám při větším větru neodlétla, a hlavně musí být z materiálu, který neoxiduje.

2.2.6 Šíření radiového signálu

Rušení jinými systémy ve stejném frekvenčním pásmu

Systémy používající modulaci FHSS (viz kapitola 3.1.2) např. BreezNet. Tato technologie vysílá krátké signály do celého pásma. Pokud na sebe narazí tyto technologie, tak dochází k několikavteřinovému výpadku.

Wi-Fi zařízení kvůli šířce kanálu 22MHz a odstupu mezi jednotlivými kanály poskytuje Wi-Fi pásmo pouhé tři zcela oddělené fyzické kanály, a to kanály 1, 6 a 11. V 2,4 GHz pásmu si může vysílat každý, jak chce, ale musí dodržet výkonnostní limity stanovené ČTÚ[2].

Přímá viditelnost

Pod přímou viditelností si představme, že vidíme z jedné antény na druhou pouhým pohledem oka nebo s použitím dalekohledu. Pokud tomu tak není, musíme počítat se ztrátami. Pro signál 2,4 GHz je jistou smrtí železobetonová zeď. U cihlové zdi může být dosah do 15 m a u sádrokartonu to může být i několik desítek metrů.

Vliv stromů - představují velký problém, který je velmi často podceňován. Lepší je vyhnout se stromům nebo šířit signál nad korunami stromů.

Vliv Počasí - způsobuje při provozu Wi-Fi jen drobné výchylky, ale na delší vzdálenosti je lepší je do kalkulací zahrnout.

Voda - pro signál v pásmu 2,4 GHz problém. Mikrovlny o této frekvenci totiž mají schopnost excitovat molekuly vody a tím vodu ohřívat. Ostatně na tomto principu pracuje mikrovlnná trouba, ta ohřívá pokrmy několika sty watty radiových signálů na frekvenci 2,45 GHz.

[2] Český telekomunikační úřad. Výkonnostní limit je 100 mW.

3 Standardy IEEE 802.11

3.1 IEEE 802.11 obecně

Wi-Fi standard pro lokální bezdrátové sítě. Standard 802.11 obsahuje různé druhy modulací pro vysílání radiového signálu, přičemž tyto modulace používají jeden protokol.

Standardy 802.11b, g používají 2,4 GHz pásmo. V tomto pásmu pracují bezdrátové telefony, bluetooth i mikrovlnné trouby. Standard 802.11a používá 5 GHz pásmo a ten nemůže pracovat se zařízeními, které pracují v 2,4 GHz pásmu.

Nový standard 802.11ac používá 2,4 GHz i 5 GHz. Je kompatibilní pro obě pásma.

Více informací nalezneme na [3].

3.1.1 Popis jednotlivých standardů

IEEE 802.11a

Využívá Wi-Fi pásmo 5GHz. Používá modulaci OFDM. Je stabilnější, vyspělejší a lze ho použít na delší vzdálenosti oproti standardu IEEE 802.11b/g.

IEEE 802.11b

Schválen v roce 1999. Přenosová rychlost 11 Mbit/s v přenosovém pásmu 2,4 GHz. Dosah až 12 km ve volném prostředí. Modulace DSSS.

IEEE 802.11g

Rozšiřuje standard IEEE 802.11b. Je zpětně kompatibilní, vysílá v pásmu 2,4 GHz a jeho nominální rychlost je 54 Mbit/s. Modulace OFDM mimo rychlostí 1, 2, 5,5 a 11 Mbit/s, protože ty používají DSSS.

IEEE 802.11n

Úprava fyzické vrstvy a pod části linkové vrstvy, takzvané MAC[3] podvrstvy tak, aby se docílilo reálných rychlostí přes 100 Mbit/s.

Zvýšení rychlosti se dosahuje použitím MIMO[4] technologie, která využívá více vysílacích a přijímacích antén. Více informací nalezneme na [8][22].

[3] Media Access Control
[4] Multiple Input Multiple Output

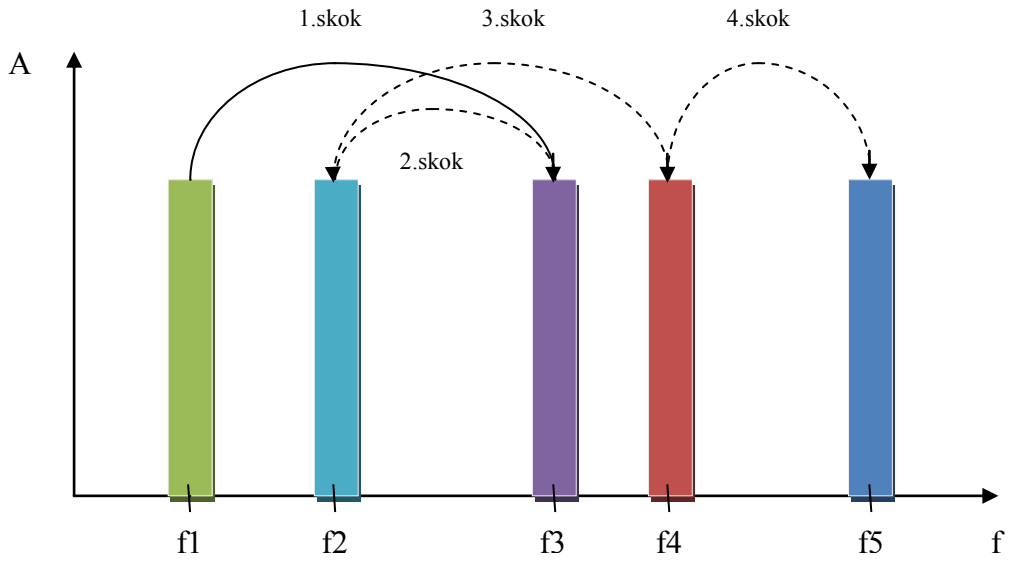
3.1 - Přehled standardů IEEE 802.11

Standard	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva
původní IEEE 802.11	1997	2,4	2	DSSS a FHSS
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM
IEEE 802.11n	2009	2,4 nebo 5	600	MIMO OFDM

3.1.2 Popis modulací

FHSS (Frequency Hopping Spread Spectrum)

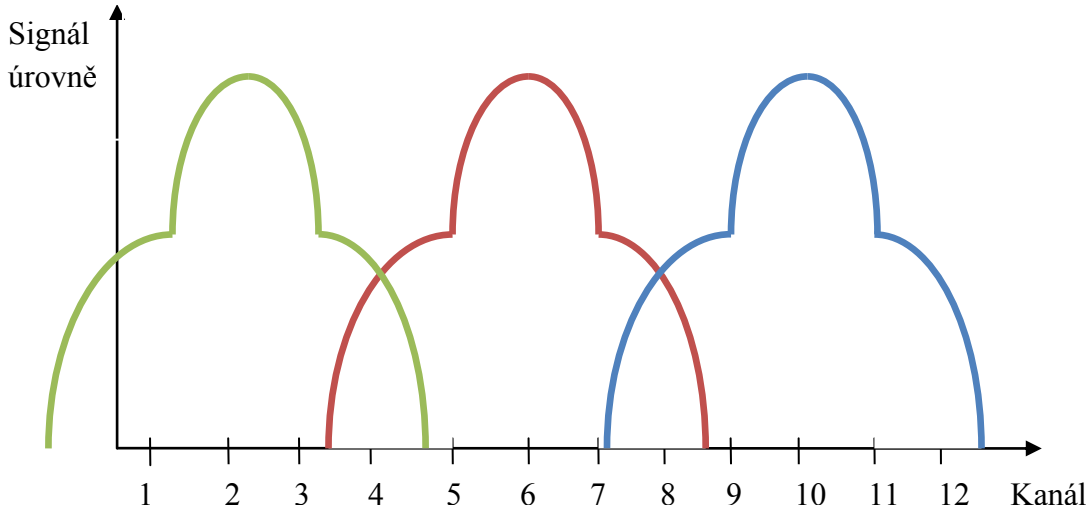
K dispozici 22 skokové sekvence. 79 kanálů v okolí frekvence 2,4 GHz. Šířka pásma každého z nich je 1 MHz a "přeskakuje" minimálně 2,5krát za vteřinu (typicky 20krát). Má vysokou odolnost proti rušení, ale také nízkou propustnost (max. 2 Mbps). Znázorněno na Obr. 3.1.



Obr. 3.1. – FHSS (přepracováno dle [12])

DSSS (Direct Sequence Spread Spectrum)

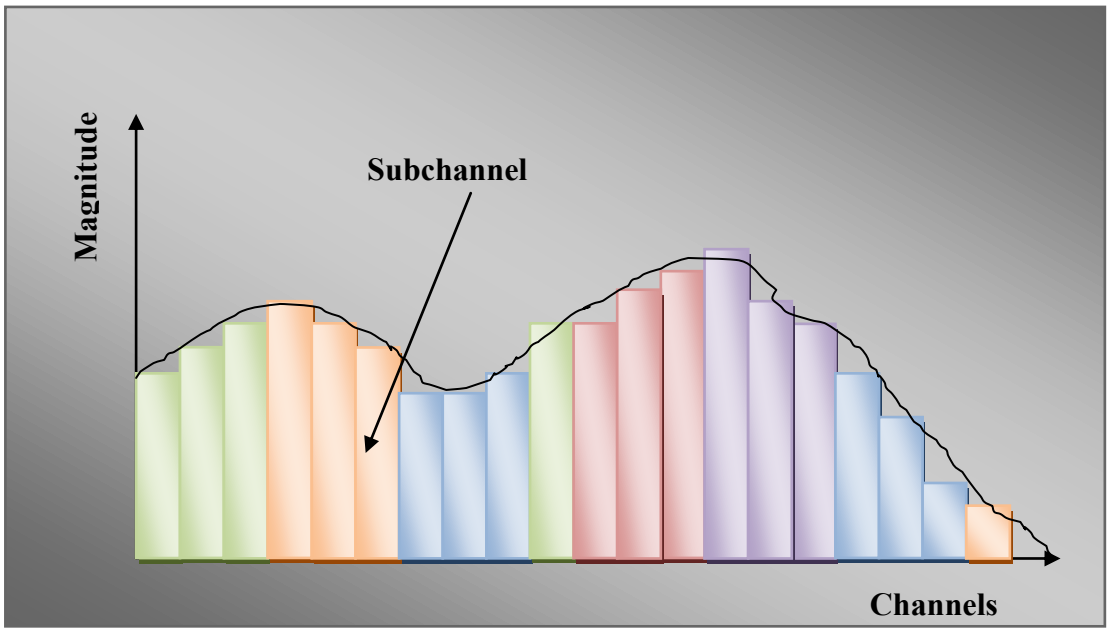
Náročnější na zpracování signálu viz Obr. 3.2. Všechna data jsou přenášena v jednom 22 MHz širokém kanálu, což znamená čím větší rychlost, tím větší šířka pásma. Více informací nalezneme na [9].



Obr. 3.2 – DSSS (přepracováno dle [12])

OFDM (Orthogonal Frequency Division Multiplexing)

Kmitočtové dělení kanálu pro komunikaci. Ve virtuálních kanálech, které jsou vytvořené ve frekvenčním pásmu, se data přenášejí najednou, ale pomalu. Díky tomu je přenos rychlejší, ale odolnost proti rušení je nízká. Znázornění na Obr. 3.3.



Obr. 3.3 – OFDM (přepracováno dle [12])

4 BackTrack

4.1 BackTrack obecně

Operační systém, ve kterém jsou nainstalované aplikace (viz kapitola 4.2) nebo skripty pro zjišťování bezpečnosti sítě. BackTrack nám usnadňuje práci k prolomení bezpečnostních protokolů WEP, WPA nebo WPA2, protože má v sobě všechny potřebné aplikace nainstalované a nemusíme je pracně stahovat a instalovat. Ušetří nám to hodně práce. Více informací nalezneme na [6].

Linux distribuce odvozená od Auditor a WHAX.

Vydavatelé Mati Aharoni a Max Moser. Na Ubuntu Linux pracuje až 4. verze, která má vlastní balíčkovací systém a strukturu.

4.2 Důležité aplikace

4.2.1 Aircrack-ng

Balíček aplikací, který obsahuje implementace útoků na šifrování WEP a WPA. Pracuje s Wi-Fi kartou, která umožňuje tzv. raw monitoring mode. Nástroj se dá použít na všech operačních systémech.

4.2.1.1 Popis

aircrack-ng [nastavení] <.cap / .ivs soubor>

4.1- Klasické nastavení

Parametr	Vysvětlení
-a	zvolení útoku WEP / WPA
-e	síťová identifikace
-b	MAC adresa AP
-C	MAC adresa PC
-l	zápis klíče do souboru

4.2 - WEP nastavení

Parametr	Vysvětlení
-c	hledej jen alfanumerické kombinace
-t	hledej jen binární kód
-h	hledej čísla pro Fritz!BOX[5]
-d	použití masky z klíče (A1:XX:CF:YY)
-m	MAC adresa pro filtrování paketů
-n	velikost WEP klíče

4.3 - WEP a WPA - PSK nastavení

Parametr	Vysvětlení
-w	cesta k slovníku
-r	cesta k airolib-ng

4.2.2 Airodump-ng

Nástroj dokáže detekovat všechny Wi-Fi sítě v dosahu síťové karty, kterou používá a následně chytit a uložit provozní data nebo inicializační vektory do souboru. Zachycení inicializačních vektorů pro následné rozluštění WEP klíče. Tento nástroj je jen v balíčku. Je použitelný pro Linux a Windows.

4.2.2.1 Popis

airodump-ng <nastavení> <rozhraní>[,< rozhraní >,...]

4.4 – Klasické nastavení

Parametr	Vysvětlení
--ivs	ukládání jen IV
--gpsd	použití GPS
--beacons	nahrávání beacons do souboru
--update	aktualizace času
--showack	vypsání ack/cts/rts statistiky
-r	čtení souboru
-w	ukládání do souboru

[5] Fritz!BOX - univerzální komunikační zařízení (router)

4.5 - Nastavení filtru

Parametr	Vysvětlení
--encrypt	podle šifrovací sady
--netmask	podle masky
--bssid	podle BSSID
-a	podle neasociovaných klientů

4.2.3 Aireplay-ng

Hlavním úkolem je generování trafiku pro pozdější použití v 4.2.1 pro rozšifrování klíčů. Nástupce staršího Aireplay a implementuje nové typy útoků. Například deautentizaci a falešnou autentizaci.

4.2.3.1 Popis

aireplay-ng <volba> <replay rozhraní>

4.6 – Typ útoku

Parametr	Typ útoku
0	Deautentizace
1	Falešná autentifikace
2	Interaktivní přehrávání paketu
3	ARP požadavek replay útok
4	KoreK chopchop útok
5	Fragmentační útok
9	Test injekce

4.7 – Klasické nastavení

Parametr	Vysvětlení
-b	BSSID
-d	MAC adresa cíl
-s	MAC adresa zdroj
-m	minimální délka paketu
-n	maximální délka paketu
-w	kontrola rámce, WEP bit

4.8 - Nastavení Replay, ARP a Fragmentačního útoku

Parametr	Vysvětlení
-x	počet paketů za sekundu
-a	nastav MAC adresu AP
-c	nastav MAC adresu cíle
-h	nastav MAC adresu zdroje
-e	nastav cílové SSID AP
-j	útok ARP
-k	nastav cílovou IP při fragmentačním útoku
-l	nastav zdrojovou IP při fragmentačním útoku
-y	proud klíčů pro autentizaci PSK

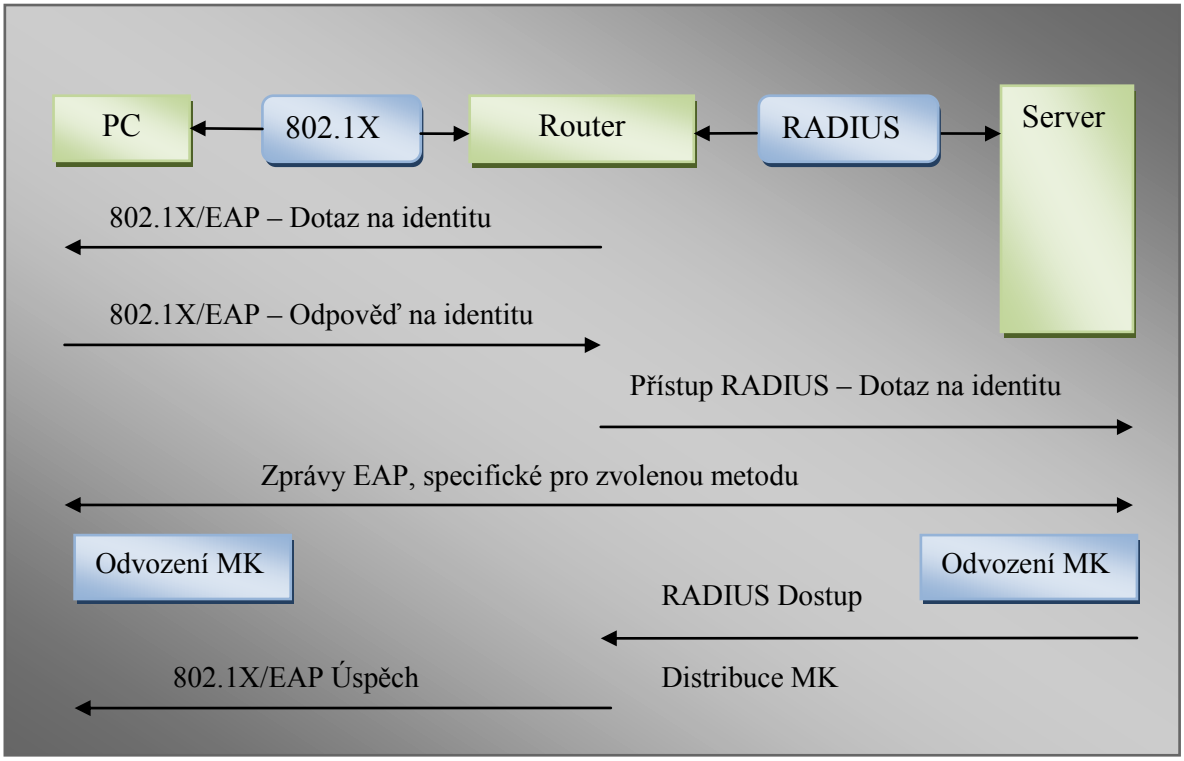
5 Autentizační protokol 802.1x

IEEE 802.1x je norma týkající se řízením přístupu do sítě pomocí autentizace. Je určena hlavně pro metalické sítě, ale využívá se i v bezdrátových sítích kvůli zlepšení bezpečnosti. Umožňuje silnou autentizaci uživatelů, integritu šifrované zprávy a distribuci klíčů. Snaží se blokovat přístup nežádoucím klientům.

802.1x využívá protokol EAPOL (EAP over LAN). EAPOL zapouzdřuje zprávy protokolu EAP do EAPOL rámců. EAP byl zamýšlen pro PPP (Point to Point Protocol).

Jestli bude nebo nebude klient moci komunikovat s AP (autentizátor) záleží na autentizaci s AS (autentizační server). Navázání spojení viz Obr. 2.1. AP využívá dvou virtuálních portů tzv. řízený a neřízený port.

- **řízený port** – nejdříve klient zablokován od veškerého síťového provozu, protože je v neautorizovaném stavu. A po autentizaci je klientovi povolen síťový provoz.
- **neřízený port** – tento port nejdříve blokuje vše mimo EAP rámců, které slouží ke komunikaci mezi AP a AS.



Obr. 5.1 - Žádání o autentizaci klientem (přepracováno dle [12])

5.1 Autentizační mechanismy

Obě strany musí mít stejný způsob autentizace. Autentizace probíhá na dohodě ověřovacího mechanismu a vlastní autentizace.

Existuje několik druhů autentizací:

- **EAP-TLS** – nejsilnější autentizační mechanismus z pohledu bezpečnosti. Vzájemná autentizace pomocí digitálních certifikátů podepsaných certifikační autoritou (metoda TLS). Dynamické generování klíčů.
- **EAP-TTLS** – rozšíření modifikace EAP-TLS. Jedná se o vzájemnou autentizaci pomocí digitálního certifikátu, který je na straně AS a slouží k autentizaci klientů. A jako u TLS je přenos přes šifrovaný tunel, který je odolný vůči odposlechu.
- **EAP-PEAP** – obdobná autentizace jako u EAP-TTLS. Šifrovaný tunel pro vzájemnou autentizaci. Autentizace probíhá pomocí hesla, které může být zahašováno pomocí MD5.
- **EAP-LEAP** – vzájemná autentizace pomocí uživatelského jména a hesla. Dynamické generování klíčů. Určen pro sítě s Cisco zařízením.
- **EAP-MD5** – jednocestné ověřování, při kterém je používáno uživatelské jméno a heslo. Ale nevíme, jestli komunikujeme se správným AP. Údaje o klientovi jsou hašovány pomocí MD5. Nejslabší autentizační mechanismus, protože je náchylný na slovníkové útoky. Neumožnuje dynamické generování klíčů.

Více informací nalezneme na [2][24][25].

5.1 - Přehled autentizačních mechanismů

Autentizační mechanismy	Bezpečnost	Autentizace	Náročnost Implementace
EAP-TLS	nejsilnější	vzájemná	vysoká
EAP-TTLS	silná	vzájemná	střední
EAP-MD5	nejslabší	jednocestná	nízká
EAP-LEAP	slabší	vzájemná	střední
EAP-PEAP	silná	vzájemná	střední

5.2 Výhody a nevýhody

Výhody:

- zablokování nežádoucím klientům do sítě.

Nevýhody:

- pro vzdálenou správu v případě, že je počítač připojený k neautorizovanému portu.

6 Bezpečnostní protokoly používané ve Wi-FI

6.1 WEP (Wired Equivalent Privacy)

Výchozí šifrovací protokol, který byl poprvé uveden v roce 1999 ve standardu IEEE 802.11. Používá šifru **RC4** pro utajení a kontrolní součet **CRC-32** pro ověření integrity. WEP 64 bit používá 40. bitový klíč a 24. bitový inicializační vektor IV pro vytvoření RC4 klíče. WEP 128 bit používá 104. bitový klíč a 24. bitový inicializační vektor. Více informací nalezneme na [11][14][20].

6.1.1 Autentizace

Autentizace je pouze jednocestná, ověřuje se pouze klient, ale nikoliv AP.

- **Open Systém autentizace**

  Klient neprovádí autentizaci a nezáleží na jeho WEP klíči.

- **Před-Sdílený Key autentizace**

  Klient se autentizuje a jeho WEP klíč je použit pro šifrování dat.

6.1.2 Šifrování

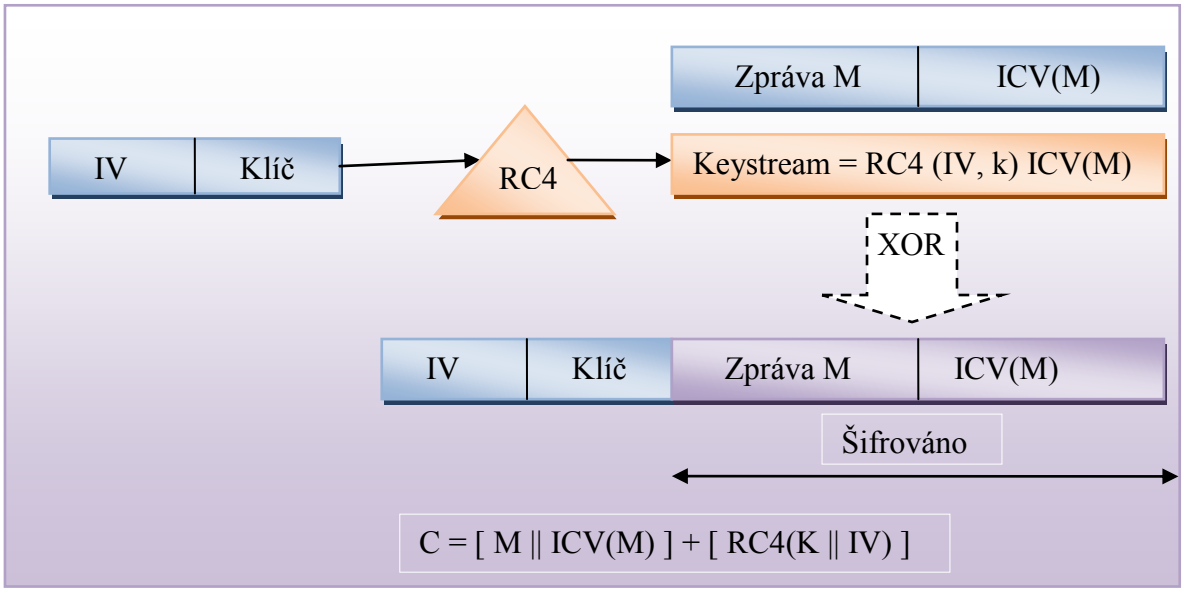
Rovnice pro zašifrování zprávy (viz rovnice $\boldsymbol{C} = [\boldsymbol{M}||\boldsymbol{ICV}(\boldsymbol{M})] + [\boldsymbol{RC4}(\boldsymbol{K}||\boldsymbol{IV})]$ (6.1)).

$$\boldsymbol{C} = [\boldsymbol{M}||\boldsymbol{ICV}(\boldsymbol{M})] + [\boldsymbol{RC4}(\boldsymbol{K}||\boldsymbol{IV})] \quad \textbf{(6.1)}$$

Vysvětlivky:

- **C** – šifrovaná zpráva
- **M** – zpráva
- **ICV** – kontrolní součet
- || - operátor zřetězení
- + - XOR

RC4 (K || IV) – šifrovací algoritmus s tajným klíčem o velikosti 40 nebo 104 bitů kombinovaných s 24. bitovým inicializačním vektorem



Obr. 6.1 - Šifrovací algoritmus (přepracováno dle [12])

RC4

Hlavním faktorem úspěchu RC4 je široký rozsah použitelnosti v aplikacích, jeho rychlost a jednoduchost: efektivní a snadná implementace v softwaru i hardwaru.

Popis:

Šifra RC4 generuje pseudonáhodný proud bajtů. Používá k šifrování spojení náhodných bajtů spolu s čistým textem (operací XOR) viz Obr. 6.1 a dešifrování probíhá podobným způsobem, ale inverzně.

Typy útoků:

- **Brute-Force –** slovníkový útok - neefektivní
- **Injekce rámců –** libovolný zachycený rámec znovu pošleme a tím docílíme toho, že nebude identifikovaný jako zdvojený

Shrnutí:

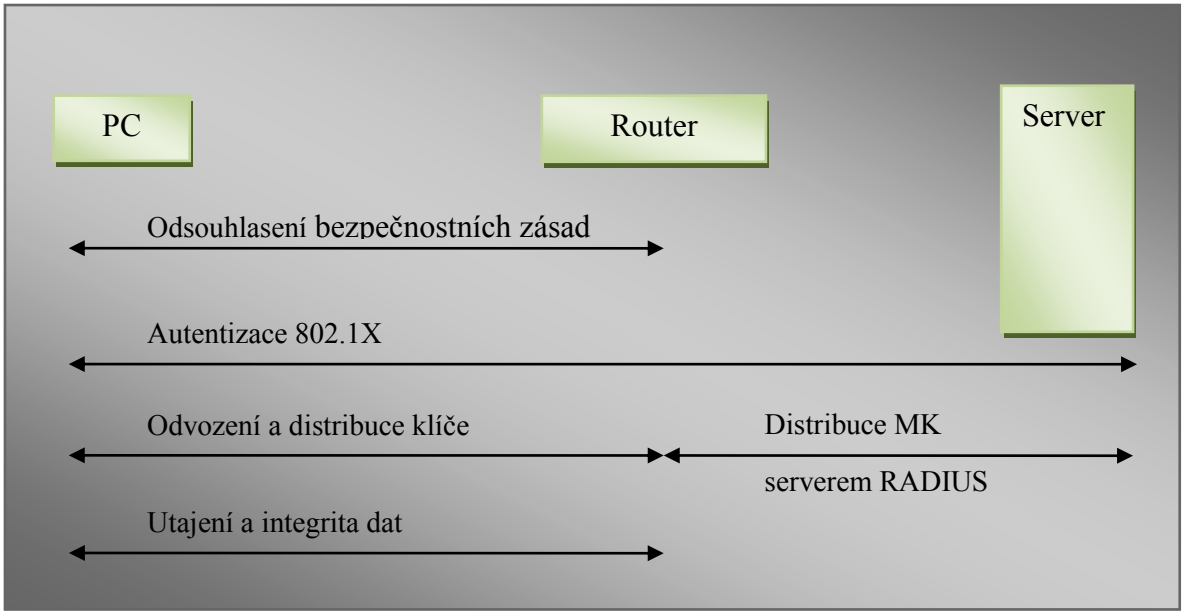
- IV jsou příliš krátké a není žádná ochrana proti opakování zprávy
- Kontrola integrity není dostačující (CRC32 slouží k detekci chyb a tím pádem není kryptograficky bezpečný)
- Žádná aktualizace klíčů

6.2 WPA (Wi-Fi Protected Access)

Roku 2001 byl započat vývoj pro zlepšení zabezpečení bezdrátových sítí pod označením 802.11i, jelikož tato norma byla schválena až roku 2004, tak do té doby Wi-Fi Aliance na dočasné řešení bezpečnostních problémů uvedla bezpečnostní protokol WPA.

Reaguje na nedokonalosti v zabezpečení bezdrátových sítí protokolem WEP (viz 6.1). WPA byl vytvořen tak, aby byl kompatibilní s dosavadním hardware vybavením. Tím pádem stačí jen aktualizace daného hardwaru a nemusí se vyměňovat za jiný. To je finančně náročné. WPA je kompatibilní i pro následující WPA2. Přináší nám dvě možnosti pro využití WPA (viz kapitola 6.4) a to pod názvem WPA Enterprise (pro velké sítě) a WPA Personal (pro malé sítě). Více informací nalezneme na [12][13][14][15].

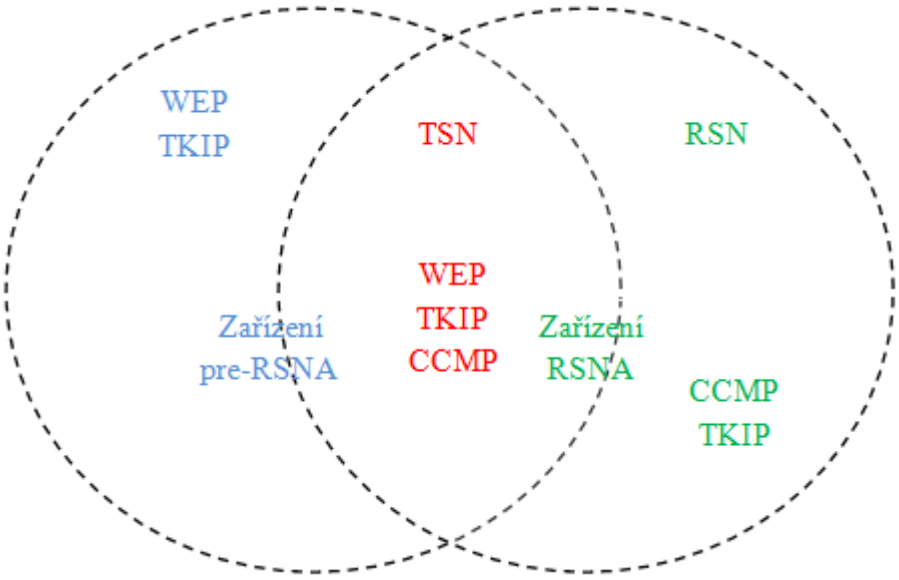
6.2.1 Čtyři fáze pro bezpečnou komunikaci



Obr. 6.2 - Komunikace založená na čtyřech fázích (přepracováno dle [12])

1. **Odsouhlasení bezpečnostních zásad**

Pokud např. klient chce komunikovat s AP, tak se musí dohodnout na bezpečnostních zásadách, které budou používat. V Beacon nebo Probe Respond jsou obsaženy bezpečnostní zásady, které podporují. Dále následuje otevřená autentizace.



Obr. 6.3 – Architektury ve WLAN (přepracováno dle [24])

Informace o bezpečnostních zásadách se zašlou v poli RSN:

- Podporované autentizační metody (PSK, 802.1X)
- Bezpečnostní protokoly pro unicast (TKIP)
- Bezpečnostní protokoly pro multicast (TKIP)
- Možnost před-autentizace před přepnutím na přístupový bod stejné sítě

2. Autentizace (PSK a 802.1x)

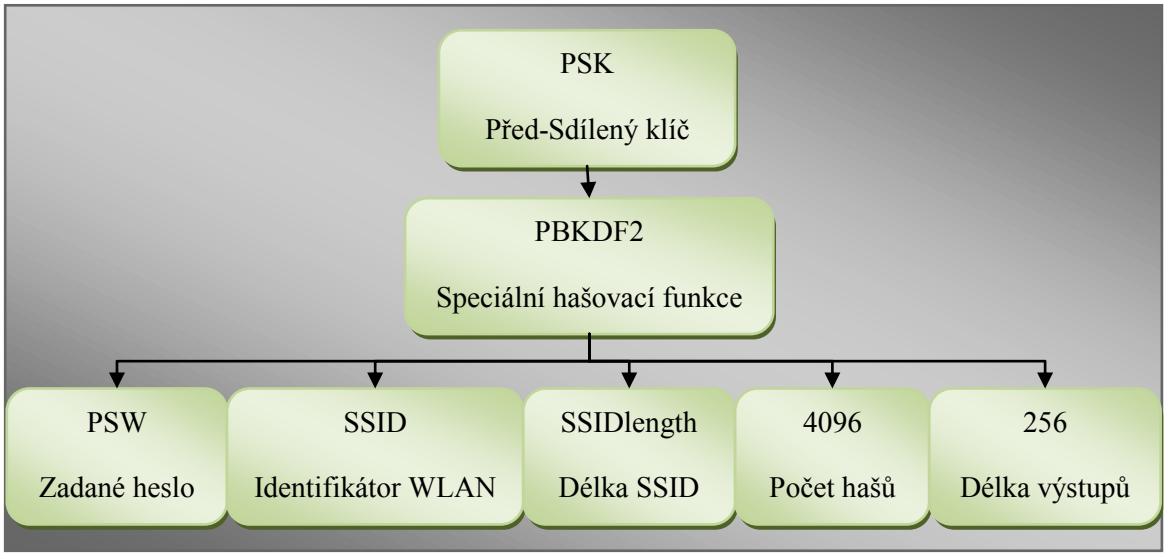
A. Před-Sdílený klíč

Autentizace použitelná ve WPA Personal (v malé síti bez autentizačního serveru). Probíhá pomocí hesla, které musí být nastaveno jak u AP, tak i u stanice. Toto heslo musí být na obou stranách stejné a musí se držet v tajnosti.

Autentizace probíhá následovně:

- Stanice se autentizuje z druhé zprávy z 4-Way Handshake si přístupový bod vypočte MIC[6] a ověří s MIC přijaté zprávy
- AP se autentizuje stejným způsobem a to vypočtením MIC z třetí zprávy z 4-Way Handshake a porovná s přijatým MIC

[6] MIC (Message Integrity Code) – datové pole připojené k nešifrovaným datům pro integritu (pomocí algoritmu Michael)



Obr. 6.4 - Před-Sdílený klíč (přepracováno dle [12])

B. Autentizace 802.1x

Popsána v kapitole (viz kapitola 5).

3. Hierarchie a distribuce klíčů

Bezpečnost připojení závisí na bezpečnosti klíčů. V této fázi se generují a obnovují klíče.

Odvození PMK (viz Obr. 6.5)**:**

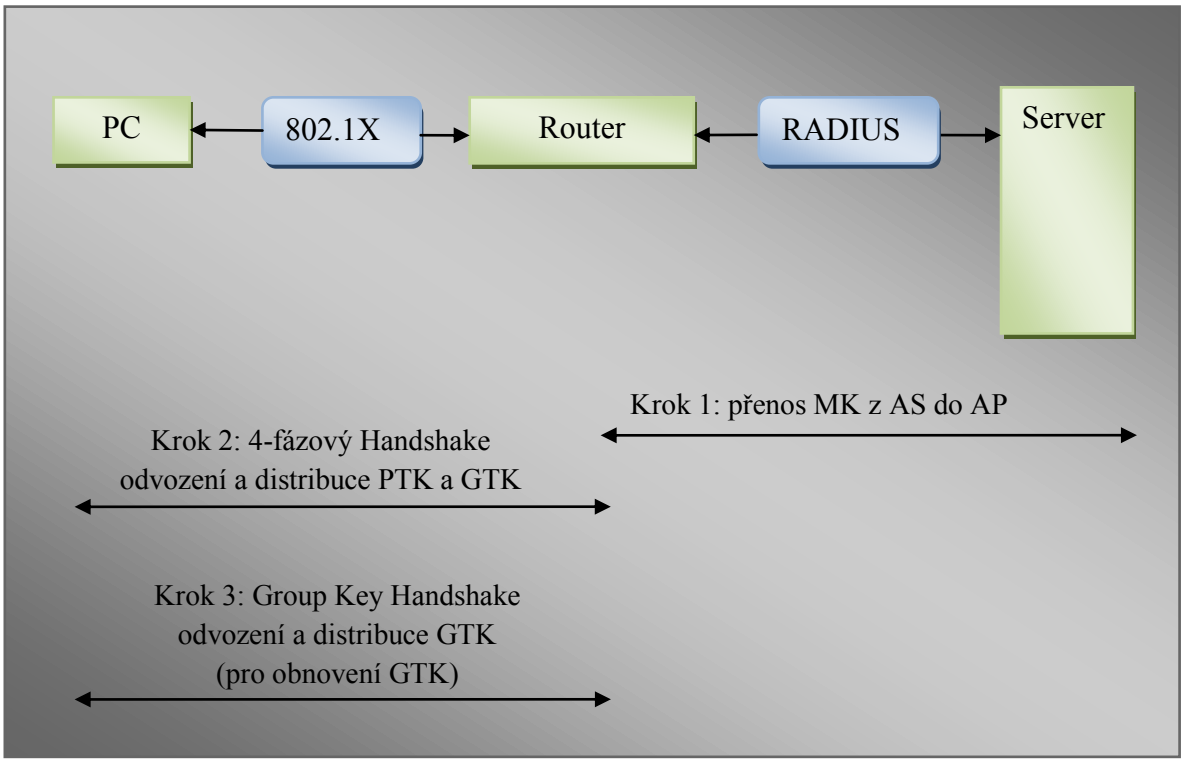
- Autentizace PSK - PMK=PSK. Pro domácí sítě a malé podniky, které nemají autentizační server
- Autentizace 802.1x – PMK se odvodí z MK[7].

PMK slouží pro generování dočasného klíče a v tom případě kvůli bezpečnosti nemůže být použit sám ke šifrování nebo kontrole integrity. Proto u unicast provozu je použit PTK.

[7] MK (Master Key) – hlavní klíč, který se získá po autentizaci 802.1x mezi AP a klientem

Vznikají dva handshake při odvozování klíčů (viz Obr. 6.6)**:**

A. 4-Way Handshake pro obnovení PTK[8] a GTK[9]



Obr. 6.5 - Ukázka odvozování klíčů (přepracováno dle [12])

Délka PTK závisí na použití šifrovacího protokolu:

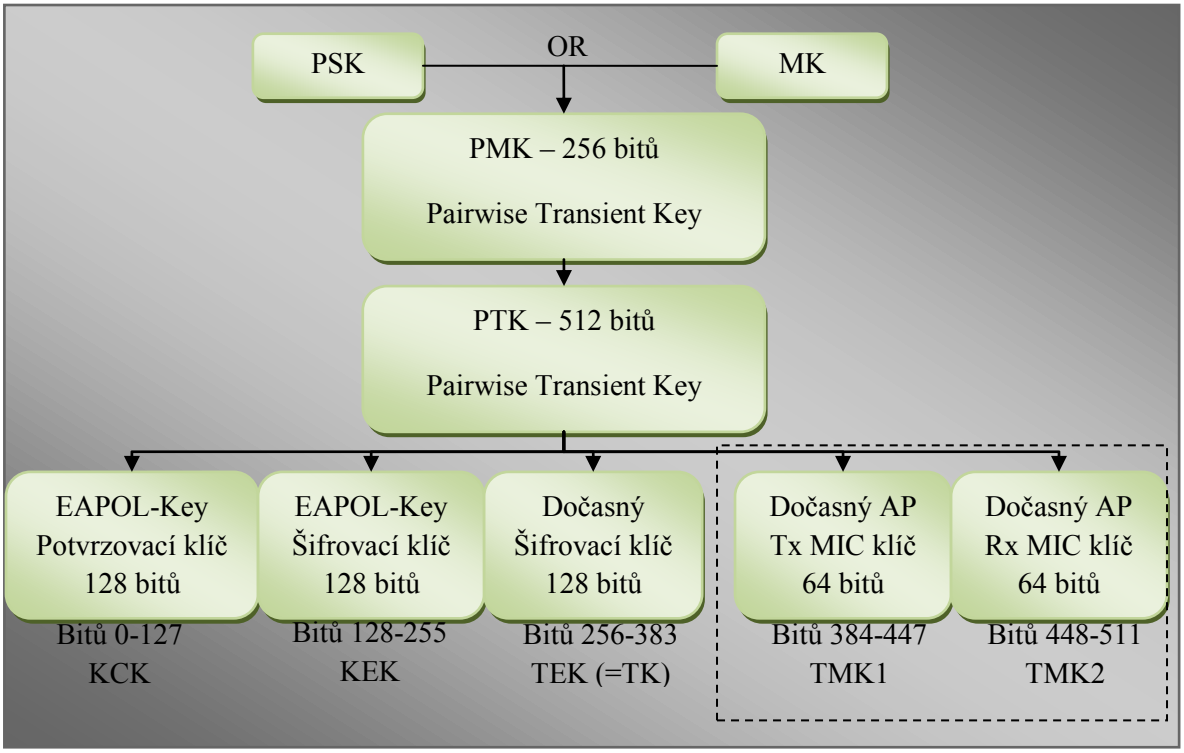
- 512 bitů u TKIP

Přidělené dočasné klíče k PTK:

6.1 - Dočasné klíče

Zkratka	Celý název	Velikost	Vlastnosti
KCK	Key Confirmation Key	128 bitů	klíč pro autentizační zprávy (MIC)
KEK	Key Encription Key	128 bitů	klíč pro zjištění utajených dat
TK	Temporary Key	128 bitů	klíč pro šifrování dat (používaný TKIP)
TMK	Temporary MIC Key	2x 64 bitů	klíč pro autentizaci dat

[8] PTK (Pairwase Transient Key) – klíč odvozený z hlavních párových klíčů (PMK (Pairwase Master Key))
[9] GTK (Group Transient Key) – klíč odvozený z hlavních skupinových klíčů (GMK (Group Master Key))



Obr. 6.6 - Hierarchie párového klíče WPA (přepracováno dle [12])

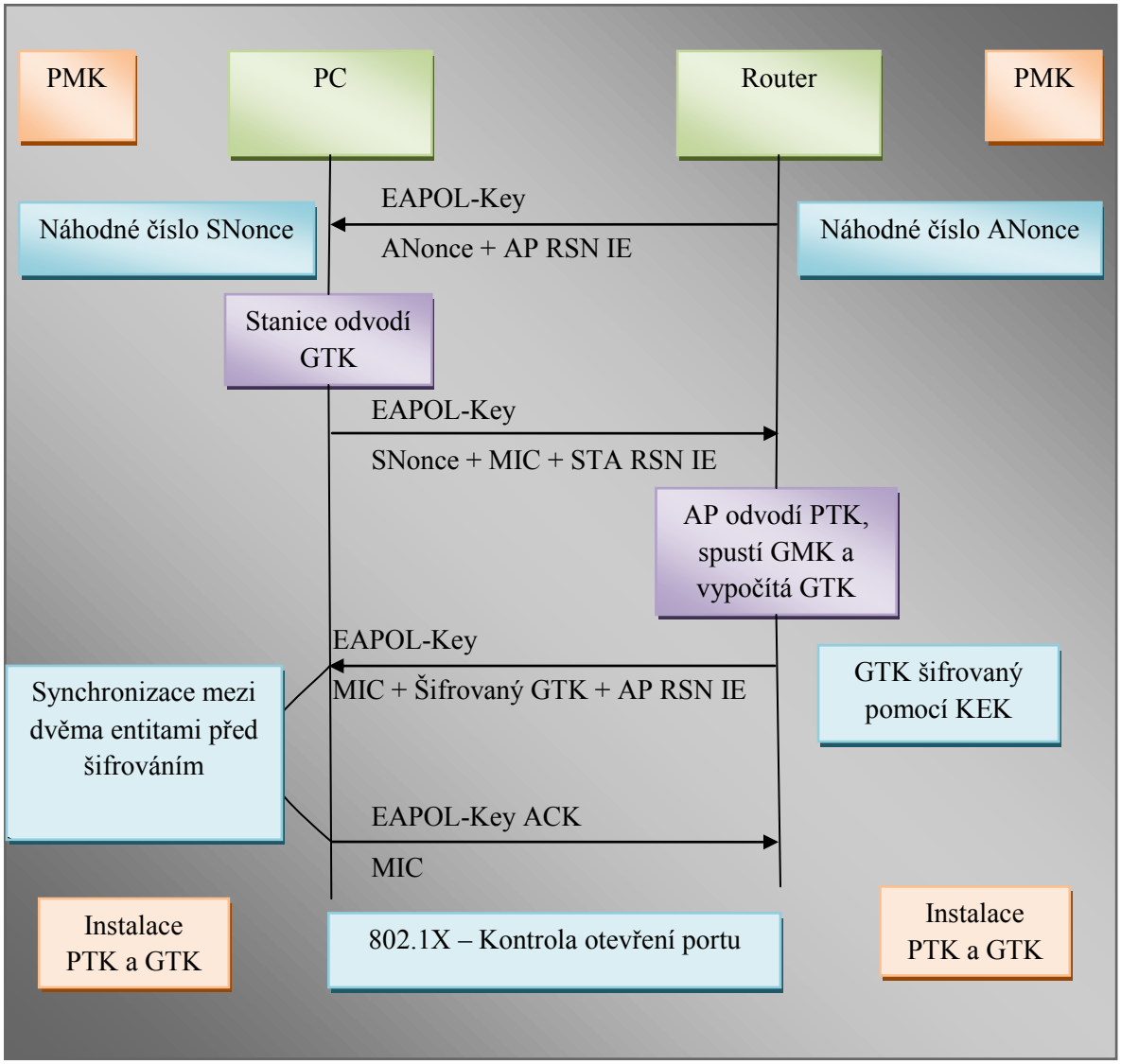
Popsání procesu 4-Way Handshake:

AP si vygeneruje náhodné číslo Anonce a pošle ho v nezašifrované podobě. Stanice si vytáhne z přijaté nezašifrované zprávy ANonce, MAC adresu AP a ze svého PMK, své MAC adresy a náhodně vygenerovaného čísla SNonce si vypočítá klíč PTK. Dále si vypočítá odvozené klíče.

Za pomoci klíče KCK zašle SNonce a MIC vypočítaný z druhé zprávy směrem k AP. AP při obdržení druhé zprávy dozví hodnotu SNonce a vypočítá stejným způsobem klíč PTK a odvozené klíče. A porovná MIC z přijaté zprávy s MIC, kterou AP vypočítalo. Při shodě AP ví, že stanice zná PMK a správně vypočítal PTK a odvozené dočasné klíče.

Třetí zprávu zasílá AP stanici a obsahuje GTK (šifrovaný pomoci KEK) a GNonce spolu s MIC vypočítaným ze třetí zprávy pomocí klíče KCK. Stanice při obdržení třetí zprávy zjistí, že se shoduje PMK, odvozené dočasné klíče i hodnota MIC s AP.

Čtvrtá a zároveň poslední zpráva potvrzuje dokončení 4-Way Handshake a říká, že stanice nyní nainstaluje klíč a spustí šifrování. AP při přijetí instaluje, jakmile ověří hodnoty MIC a klíče. Při shodě stanice a AP získaly, vypočítaly a nainstalovaly šifrovací klíče a jsou schopny komunikovat v zašifrovaném kanálu jak pro provoz unicast tak i multicast (viz Obr. 6.7).



Obr. 6.7 - 4-Way Handshake (přepracováno dle [12])

B. Group Key Handshake pro obnovu GTK

Skupinové vysílání je chráněno klíčem GTK a ten je odvozen z GMK (pevný řetězec + MAC adresa AP + GNonce)

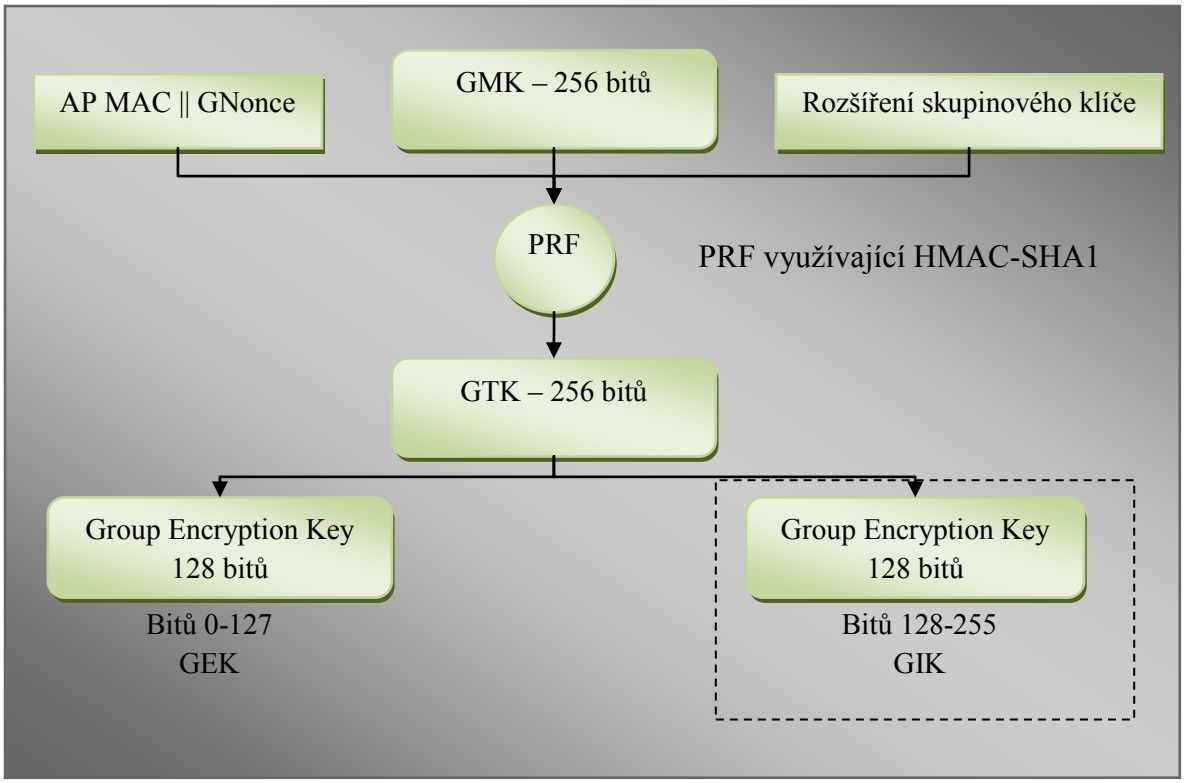
Délka GTK závisí na použití šifrovacího protokolu:

- 256 bitů u TKIP

Přidělené dočasné klíče k PTK:

6.2 - Dočasné klíče

Zkratka	Celý název	Velikost	Vlastnosti
GEK	Group Encryption Key	128 bitů	klíč pro zjištění utajených dat
GIK	Group Integrity Key	128 bitů	klíč pro autentizační zprávy (MIC)

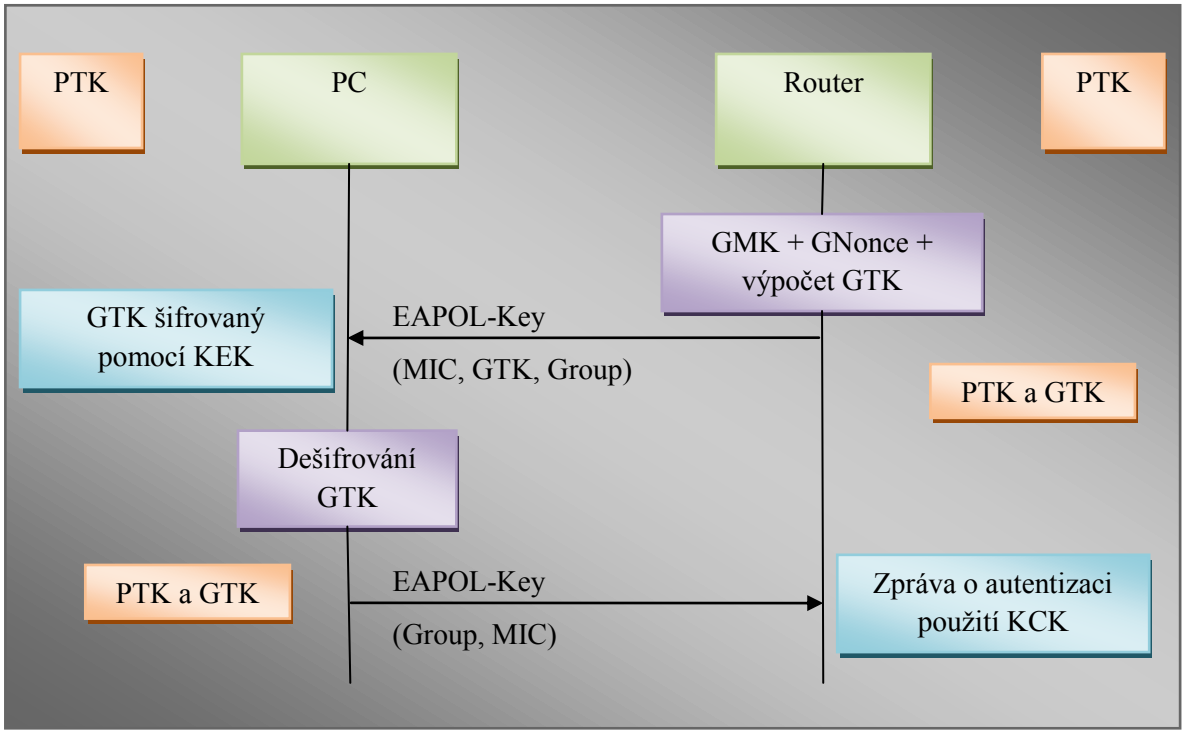


Obr. 6.8 - Hierarchie skupinového klíče u WPA (přepracováno dle [12])

Tento Handshake využívá dočasné klíče generované v průběhu 4-Way Handshake (KCK a KEK). Je potřeba jen k deasociaci hostitele a k obnovení GTK na požadavek stanice.

AP vyšle první zprávu, která obsahuje nově vypočítaný GTK zašifrovaný pomocí KEK, pořadové číslo GTK a MIC vypočítaný pomoci KCK. Stanice po obdržení zprávy si ověří MIC, a pokud se shoduje, tak je možné dešifrovat GTK.

Druhá zpráva ukončuje Group Key Handshake zasláním pořadového čísla GTK a MIC vypočítaný z druhé zprávy. AP při přijetí kontroluje MIC a při shodě instaluje nový GTK (viz Obr. 6.9).



Obr. 6.9 - Group key Handshake (přepracováno dle [12])

4. Utajení a integrita dat RSNA

TKIP je založen na šifrovacím algoritmu RC4 (viz kapitola 6.1.2) a je vytvořen kvůli velkým slabinám protokolu WEP.

Slabiny nahrazené protokolem TKIP jsou:

- Integrita zpráv – nový algoritmus MIC
- Inicializační vektory – k zamezení opětovného použití se zvyšuje velikost IV

Vylepšení:

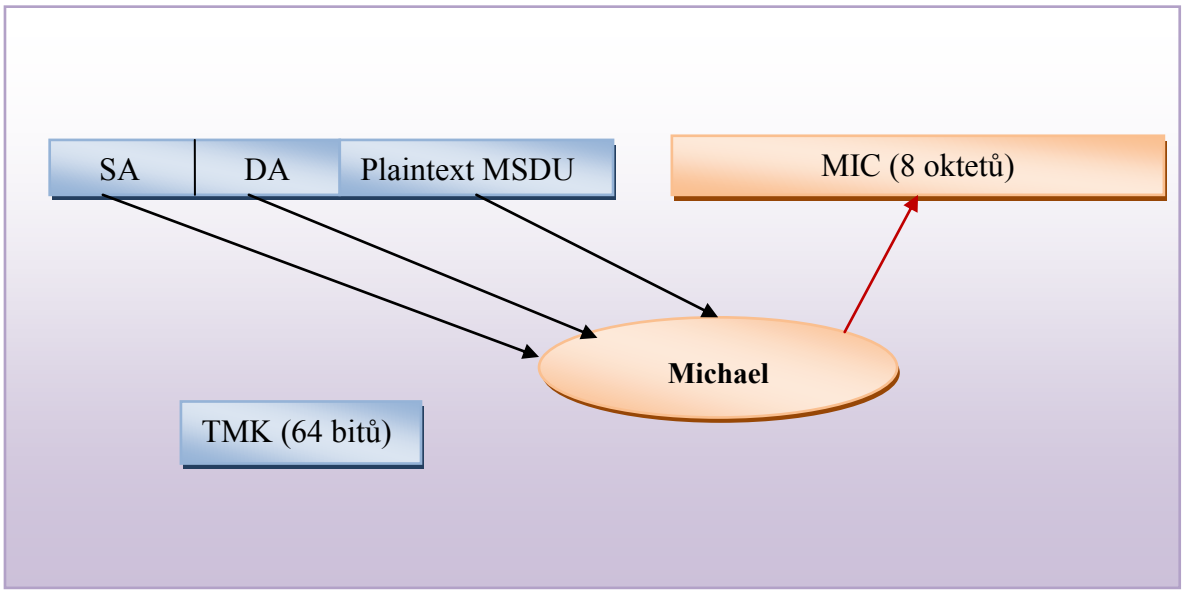
- Správa klíčů – nová metoda pro distribuci a výměnu klíčů
- PPKM[10]

Algoritmus Michael

Vytvořen pro TKIP a úroveň cílové bezpečnosti je 20 bitů. Opatření proti podvržení kódu MIC a to tak, že za jednu minutu nesmí nastat více jak dvě selhání MIC. Pokud nastane více selhání, tak nastane jedno minutový výpadek a poté se musí znovu vytvořit nové klíče (GTK a PTK).

[10] PPKM (Per Packet Key Mixing) – získávání nesouvisejících šifrovacích klíčů

Kód MIC se vypočítá ze zdrojové adresy (SA), cílové adresy (DA), nešifrovaného (plaintext) MSDU[11] a příslušného TMK viz Obr. 6.10.



Obr. 6.10 - Algoritmus Michael (přepracováno dle [12])

TKIP

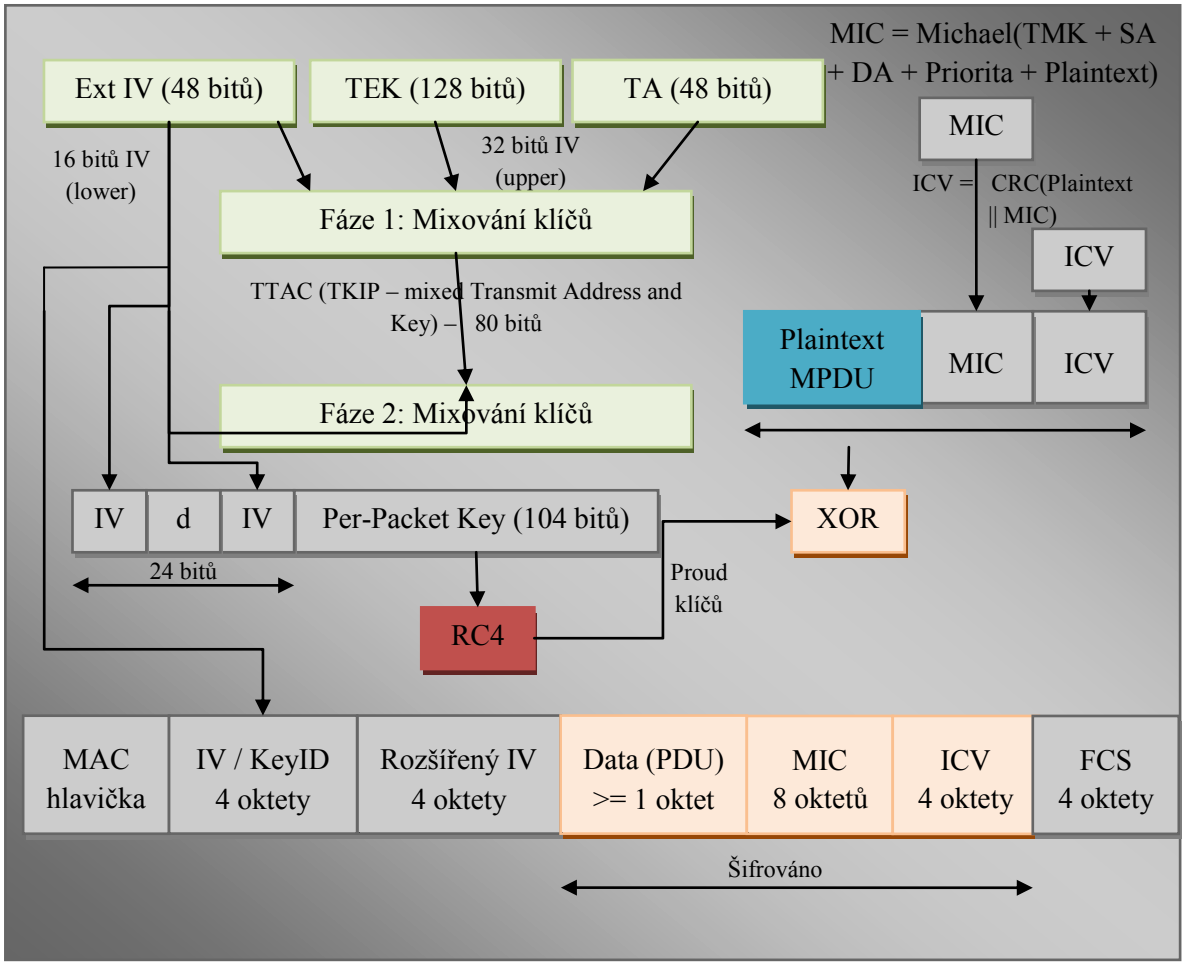
Dva kroky při mixování klíčů:

V prvním jsou statická data (TEK[12] + TA[13] + IV (32 bitů)).

V druhém je (výstup prvního kroku + IV (16 bitů)). Těchto dolních 16 bitů se mění pro každý nový IV a to za pomoci Per Packet Key. Hodnota IV vždy začíná na 0 a zvyšuje se o 1 pro každý zaslaný paket za podmínky, že TSC < TSC (naposledy vyřízené zprávy).

Do RC4 jde výstup druhého kroku, část rozšířeného IV a dummy bajt. Algoritmus RC4 z dat, co k němu přišli, vygeneruje proud klíčů a ten je XOR-ovaný pomocí nešifrované MPDU a starého IV.

[11] MSDU (MAC Service Data Unit) – představuje data před fragmentací
[12] TEK – tajný relační klíč
[13] TA – vysílač MAC adresy, který slouží k zamezení kolizí IV



Obr. 6.11 - Mixování a šifrování TKIP (přepracováno dle [12])

6.3 WPA2 (Wi-Fi Protected Access 2)

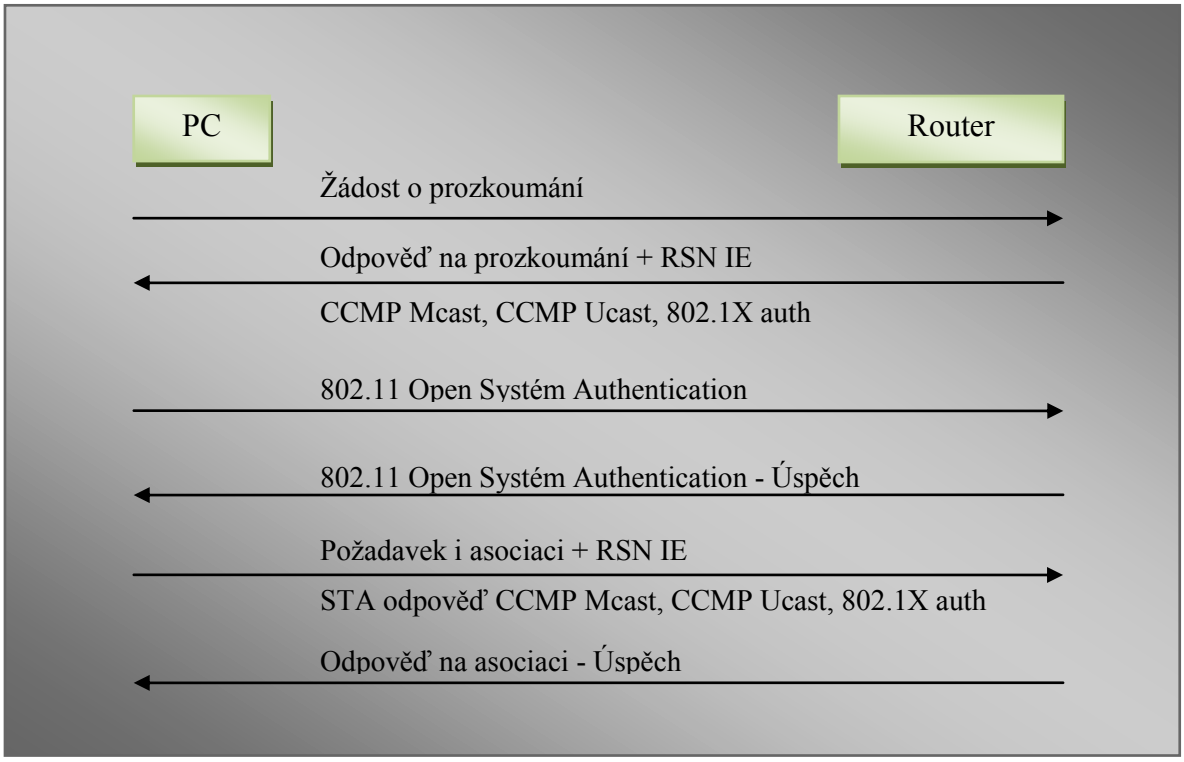
6.3.1 Čtyři fáze pro bezpečnou komunikaci

1. **Odsouhlasení bezpečnostních zásad**

   Podobné jako u WPA (viz kapitola 6.2.1).

   Informace o bezpečnostních zásadách se zašlou v poli RSN Obr. 6.12**):**

   - Podporované autentizační metody (PSK, 802.1X)
   - Bezpečnostní protokoly pro unicast (CCMP)
   - Bezpečnostní protokoly pro multicast (CCMP)
   - Možnost před-autentizace před přepnutím na přístupový bod stejné sítě



Obr. 6.12 - Odsouhlasení bezpečnostních zásad (přepracováno dle [12])

2. **Autentizace**

   Stejná jako u WPA (viz kapitola 6.2.1).

3. **Hierarchie a distribuce klíčů**

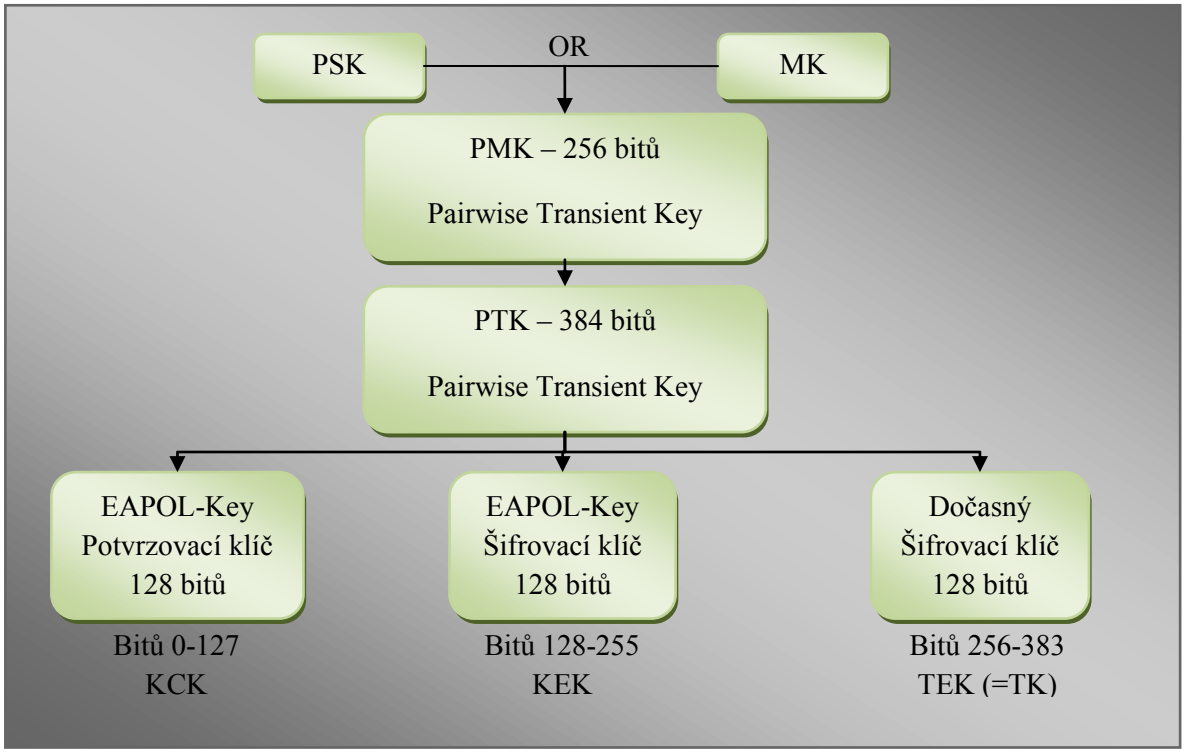
   A. 4-Way Handshake pro obnovení PTK[14] a GTK[15]

   Délka PTK závisí na použití šifrovacího protokolu:

   - 384 bitů u CCMP

   PTK pracuje se všemi dočasnými klíči jako u protokolu WPA mimo TMK.

[14] PTK (Pairwase Transient Key) – klíč odvozený z hlavních párových klíčů (PMK (Pairwase Master Key))
[15] GTK (Group Transient Key) – klíč odvozený z hlavních skupinových klíčů (GMK (Group Master Key))



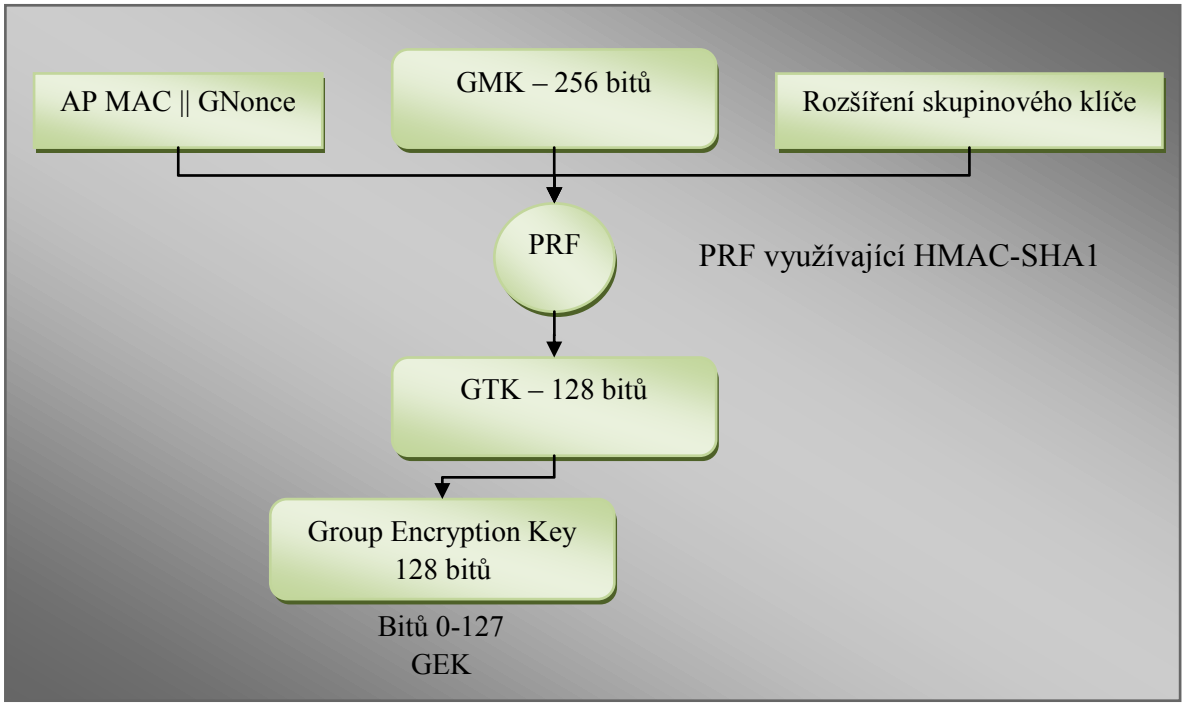
Obr. 6.13 - Hierarchie párového klíče WPA2 (přepracováno dle [12])

B. Group Key Handshake pro obnovu GTK

Funguje stejně jako WPA (viz kapitola 6.2.1), jen nepoužívá dočasný klíč GIK.

Délka GTK závisí na použití šifrovacího protokolu:

- 128 bitů u CCMP



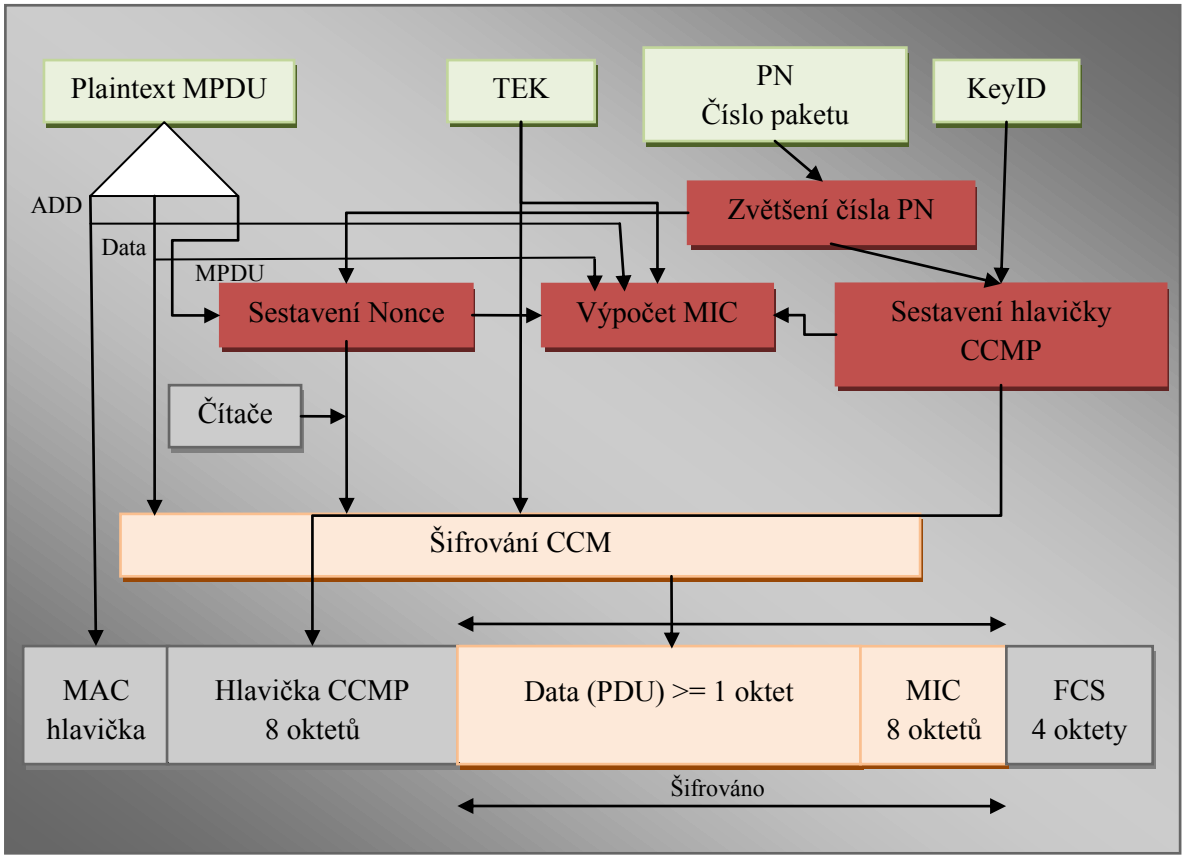
Obr. 6.14 - Hierarchie skupinového klíče WPA2 (přepracováno dle [12])

4. Utajení a integrita dat RSNA

CCMP (Counter Mode with CBC-MAC Protocol) je šifrovací protokol, který nahrazuje TKIP. Protokol využívá šifrovací standard AES. Přidány zajímavé funkcionality, např. použití stejného klíče k šifrování a autentizaci (s různými IV).

CCMP přidává k MPDU 16 bajtů a to 8 pro hlavičku a 8 pro MIC. Nešifrované pole obsažené mezi hlavičkou MAC a šifrovanými daty obsahující 48. bitové PN a Group Key KeyID se nazývá hlavička CCMP. MPDU s každým následným cyklem zvýší PN o jedničku. Konečný MIC kód o velikosti 64 bitů (MIC je 128. bitový blok, od kterého se dolních 64 bitů oddělí a následně vyřadí) využívá pro výpočet CBC-MAC algoritmus, který šifruje počáteční Nonce blok (výpočet proveden ze zdrojové adresy MPDU, zvýšeného PN a z polí priorit) a XORy následných bloků. Poté se MIC kód připojí k nešifrovaným datům pro šifrování AES v režimu čítače. Čítač tvoří nonce, který se podobá Mic nonce, ale má pole s hodnotou 1, které se zvyšuje o jedničku každým provedeným cyklem.

AES (Advanced Encryption Standard) je bloková šifra. AES používá symetrický klíč, což znamená, že šifruje i dešifruje pomocí stejného sdíleného klíče. Délka klíče může být 128, 192 nebo 256 bitů. AES šifruje celé 128. bitové bloky (RC4 šifruje lineárně operací XOR každý bajt) a proto ji nazýváme bloková šifra. Hlavní výhodou je veliká rychlost a snadná implementace.



Obr. 6.15 – CCMP (přepracováno dle [12])

U CCMP se MIC vypočítává z MPDU[16].

6.4 Přehled WEP, WPA a WPA2

V tabulce 6.3 - Přehled bezpečnostních protokolů máme možnost si prohlédnout autentizaci a šifrování u jednotlivých bezpečnostních protokolů.

6.3 - Přehled bezpečnostních protokolů

Bezpečnostní protokoly	Autentizace	Šifrování
WEP	Open System nebo Shared key	RC4
WPA Enterprise	802.1x / EAP	TKIP / Michael
WPA Personal	PSK	TKIP / Michael
WPA2 Enterprise	802.1x / EAP	AES / CCMP
WP2 Personal	PSK	AES / CCMP

[16] MPDU (MAC Protocol Data Unit) – představuje více datových jednotek po fragmentaci

7 Doporučené zabezpečení

Nejdříve bychom si měli promyslet pár důležitých věcí, než se pustíme do zabezpečení. O jaký typ sítě se jedná (domácí x firemní). A dalším důležitým faktorem je finanční náročnost na pořízení potřebných prvků atd.

Pokud chceme zabezpečit domácí síť (neboli LAN), tak nám stačí Wi-Fi router, který umí bezpečnostní protokol WPA2, protože ten je v této době nejlepší. Nedoporučuji protokol WPA nebo dokonce WEP. Routerem se zabezpečením WEP nepřímo říkáme hackerovi: „Pojď se připojit“! Což samozřejmě nechceme. Sice doporučuji WPA2, ale jestli si nastavíme krátké, smyslné nebo dokonce jen číselné heslo, tak to nemá víceméně význam si dávat WPA2. Důležité je si nastavit dostatečně dlouhé heslo. Například Adg369jLvMP689D@)#…., čím delší a čím více kombinací velkých a malých písmen s čísly a různými znaky má naše heslo, tím lépe pro nás. Heslo bychom měli měnit alespoň jednou za měsíc a tím znemožníme hackerovi přístup do naší sítě. Na druhou stranu není dobré si nastavené heslo zapisovat kamkoli do počítače nebo dokonce nalepit na pracovní stůl nebo na monitor. To by byla obrovská chyba a té hackeři často využívají.

Ještě můžeme síť zabezpečit pomocí MAC adresy, a to tak, že si na routeru nastavíme MAC adresy, kterým umožníme přístup do naší sítě.

Neměli bychom zapomenout na změnu přístupového hesla k routeru, protože každý výrobce má defaultní nastavení např. jméno: admin a heslo: 1234. Když by se útočník dostal i přes přihlášení na router, tak nám může vše přenastavit a to mu nesmíme dovolit!

A teď se dostáváme k té druhé možnosti a to je velká firemní síť, která pro své zabezpečení může použít autentizační server. S použitím autentizačního serveru se dostáváme i k otázce finanční náročnosti. Jak nás může napadnout, tak tato možnost stojí více finančních prostředků, ale k ochraně svých dat se to rozhodně vyplatí!

Pokud pracujeme s citlivými daty a nechceme o ně přijít, tak bychom měli obětovat dostatečný počet financí, pro zabezpečení těchto dat.

8 Ukázka prolomení protokolu WEP

Nejdříve si zjistíme název naší externí antény.

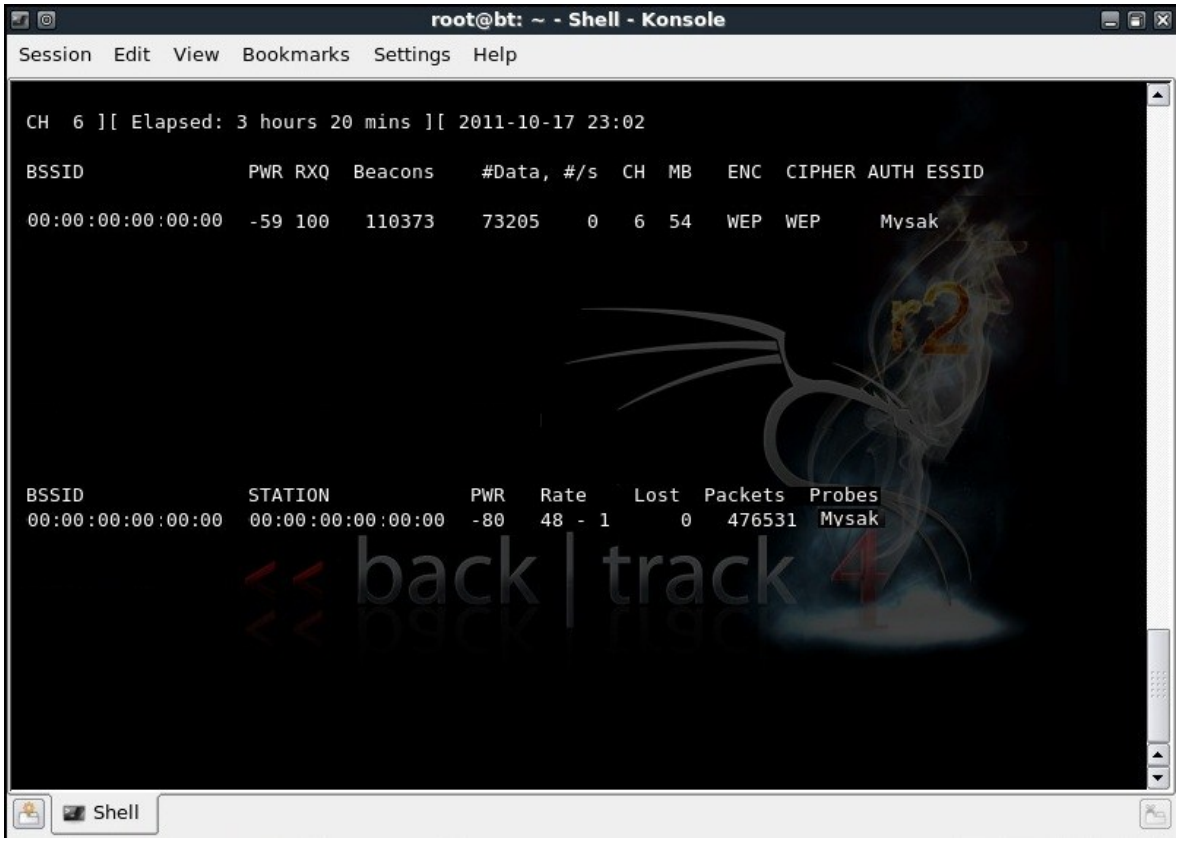
airmon-ng

V mém případě je to wlan0. Poté můžeme tímto příkazem shlédnout všechny dostupné sítě okolo nás a vybrat si síť se zabezpečením WEP.

airodump-ng wlan0

Zjistili jsme si, na jakém kanálu námi vybraný cíl komunikuje (viz Obr. 8.1 - Odposlouchávání přenášených) a následně tímto příkazem ho začneme odposlouchávat a zapisovat si do souboru inicializační vektory (iv).

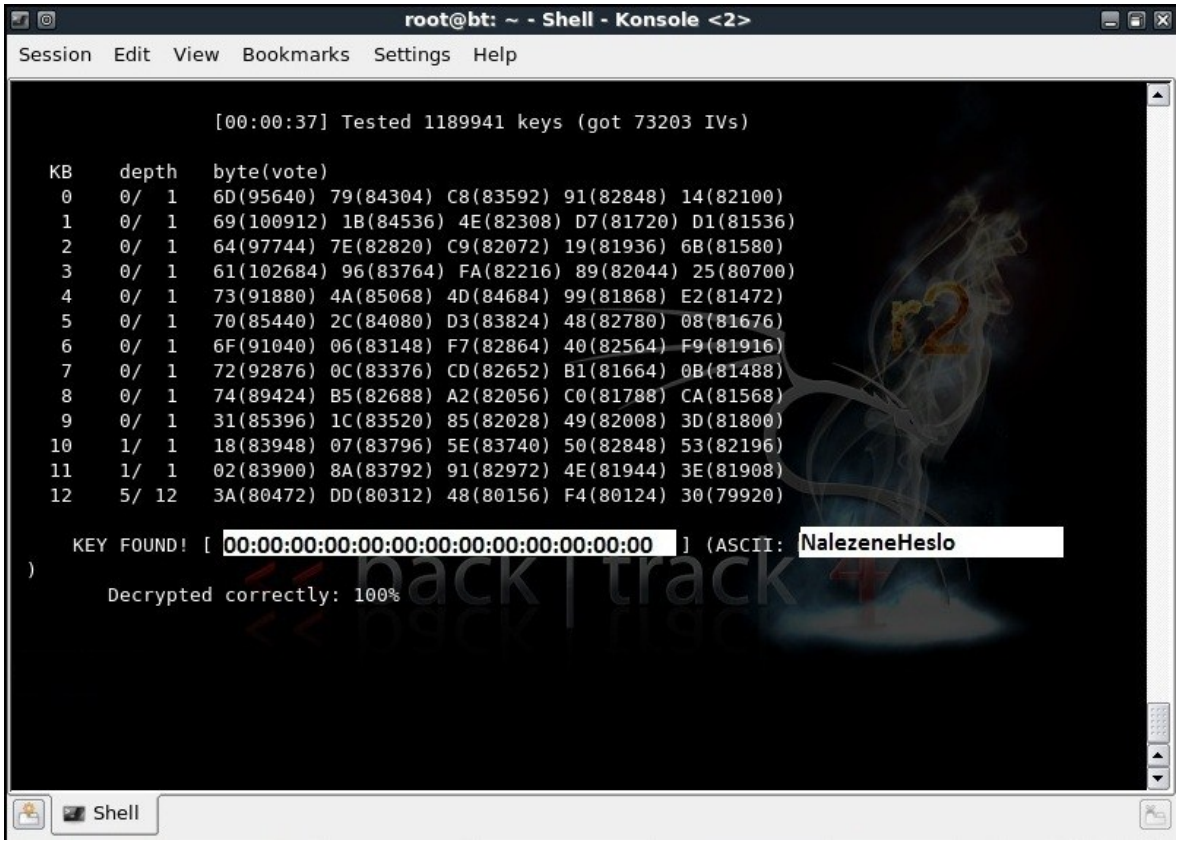
airodump-ng wlan0 –channel 6 –w WEP.txt –ivs



Obr. 8.1 - Odposlouchávání přenášených inicializačních vektorů

Po dostatečném počtu odposlechnutých iv (počet záleží na délce hesla, které se snažíme rozluštit). V mém případě jsem zadal tento příkaz pro rozluštění hesla a pokaždé, kdy byl nedostačující počet odposlechnutých iv, tak skončil a čekal na dalších pět tisíc iv. Znázornění na Obr. 8.2 - Hledání hesla

airecrack-ng WEP.txt-01.ivs



Obr. 8.2 - Hledání hesla

Po zjištění hesla se můžeme přihlásit do sítě a připojit k internetu.

Pro úspěšný útok je potřeba, aby na dané síti byli uživatelé a byl velký trafik, protože čím větší, tím rozluštíme heslo rychleji. Bez trafiku, či dokonce uživatele nemáme šanci se do této sítě dostat i přesto, že protokol WEP je nejslabší.

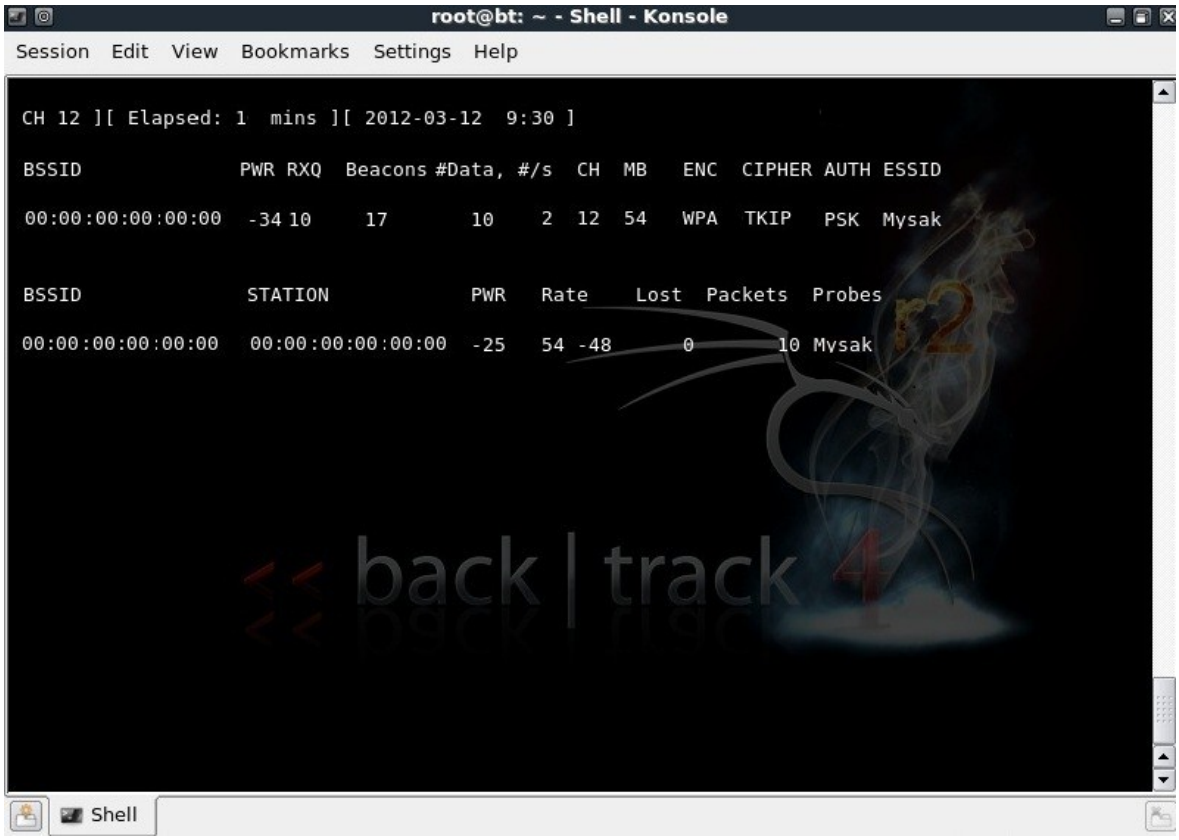
9 Ukázka prolomení protokolu WPA (802.1X)

Nejdříve si zjistíme název naší externí antény. Více informací nalezneme na [17][18].

airmon-ng

V mém případě je to wlan0. Poté můžeme příkazem níže shlédnout všechny dostupné sítě okolo nás a vybrat si síť se zabezpečením WPA.

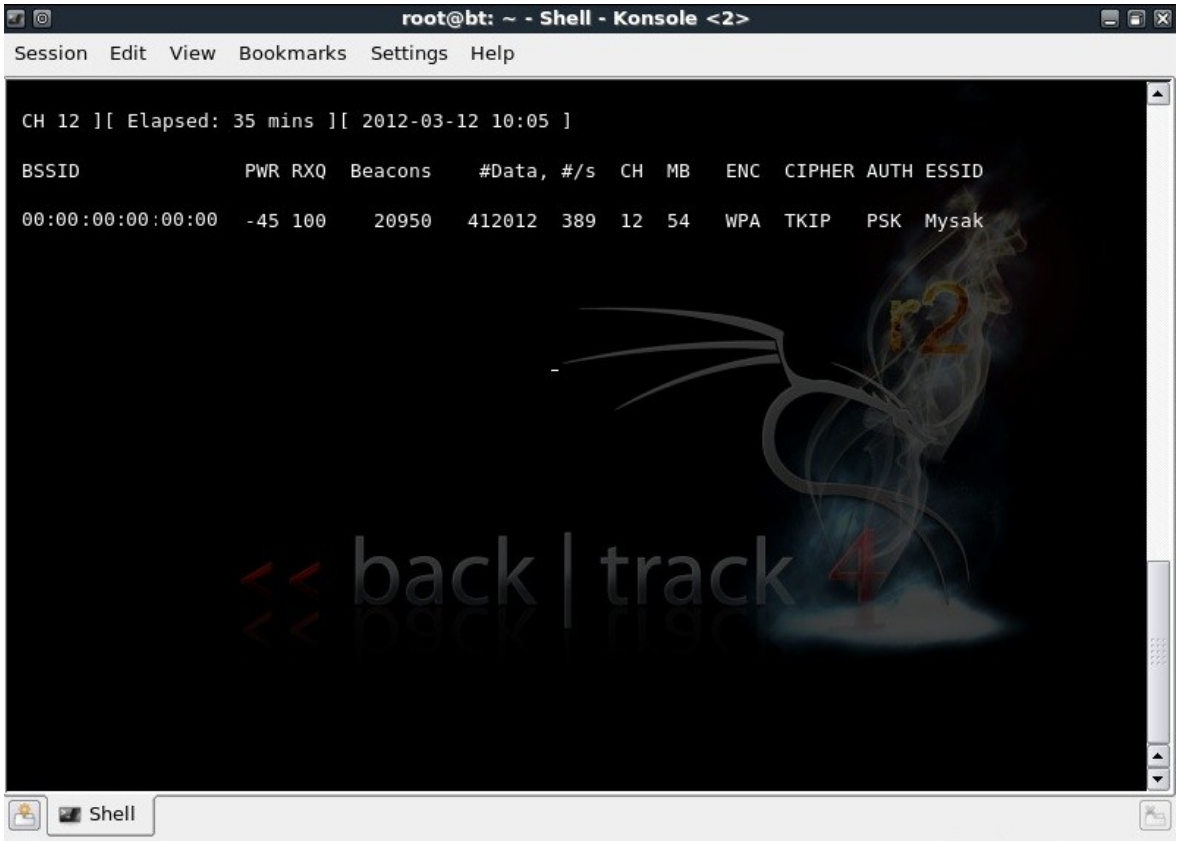
airodump-ng wlan0



Obr. 9.1 – Odposlech

Zjistili jsme si, na jakém kanálu námi vybraný cíl komunikuje (viz Obr. 9.1) a následně tímto příkazem ho začneme odposlouchávat a zapisovat si do souboru.

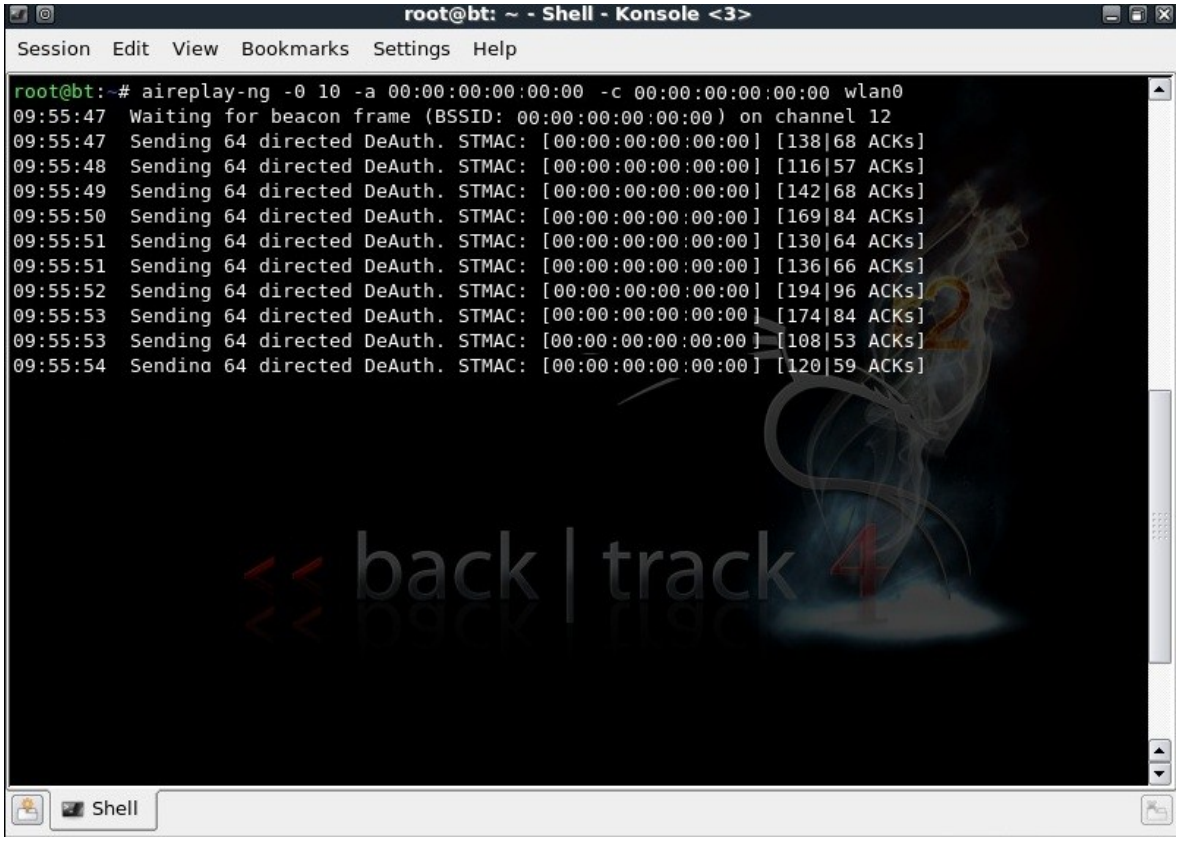
airodump-ng --bssid 00:00:00:00:00:00 –w hackMysak –c 12 wlan0



Obr. 9.2 - Ukládání do souboru

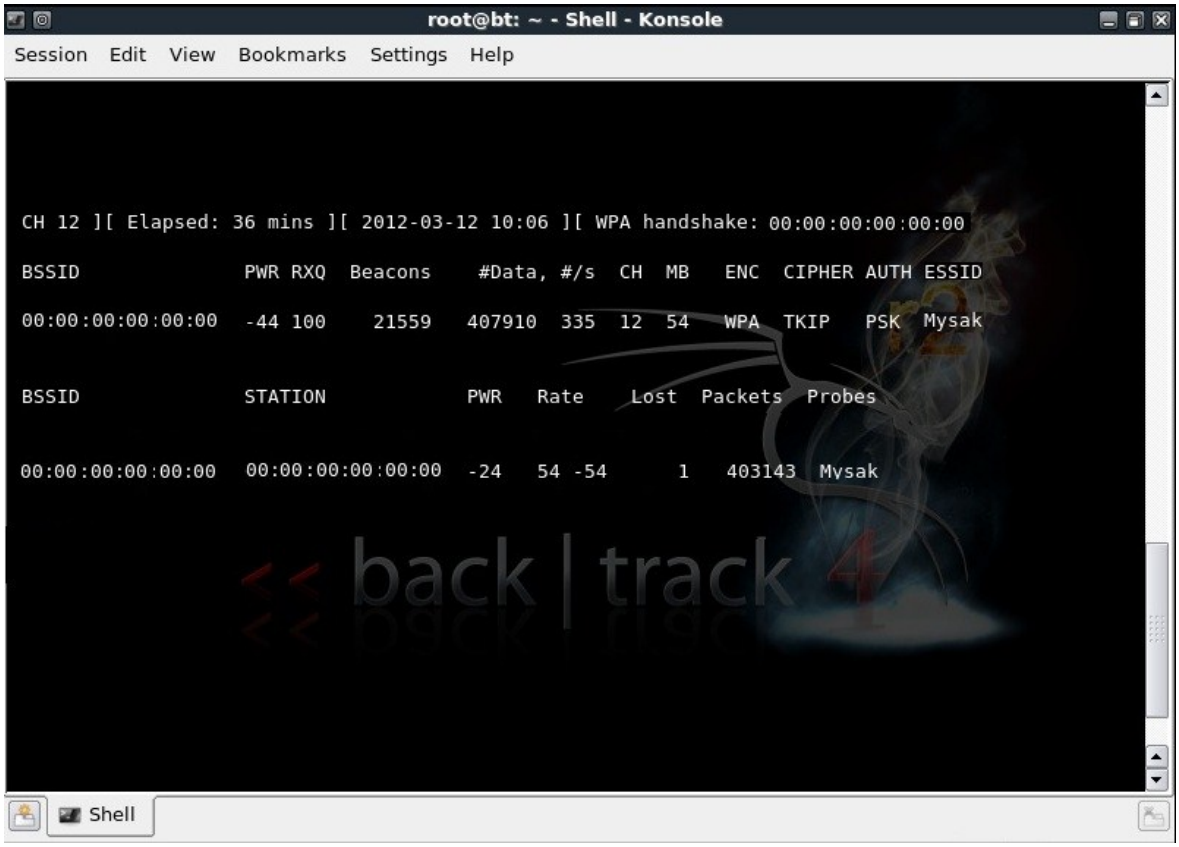
Použita deautentizace a to za pomoci příkazu, který se nachází níže.

aireplay-ng -0 10000 -a 00:00:00:00:00:00 -c 00:00:00:00:00:00 wlan0



Obr. 9.3 – Deautentizace

Tento příkaz v mém případě nefungoval a musel jsem čekat, dokud se nějaký uživatel nepřipojí. Jestli jsme získali handshake, zjistíme sledováním viz Obr. 9.4. Bude zobrazen v pravém horním rohu.

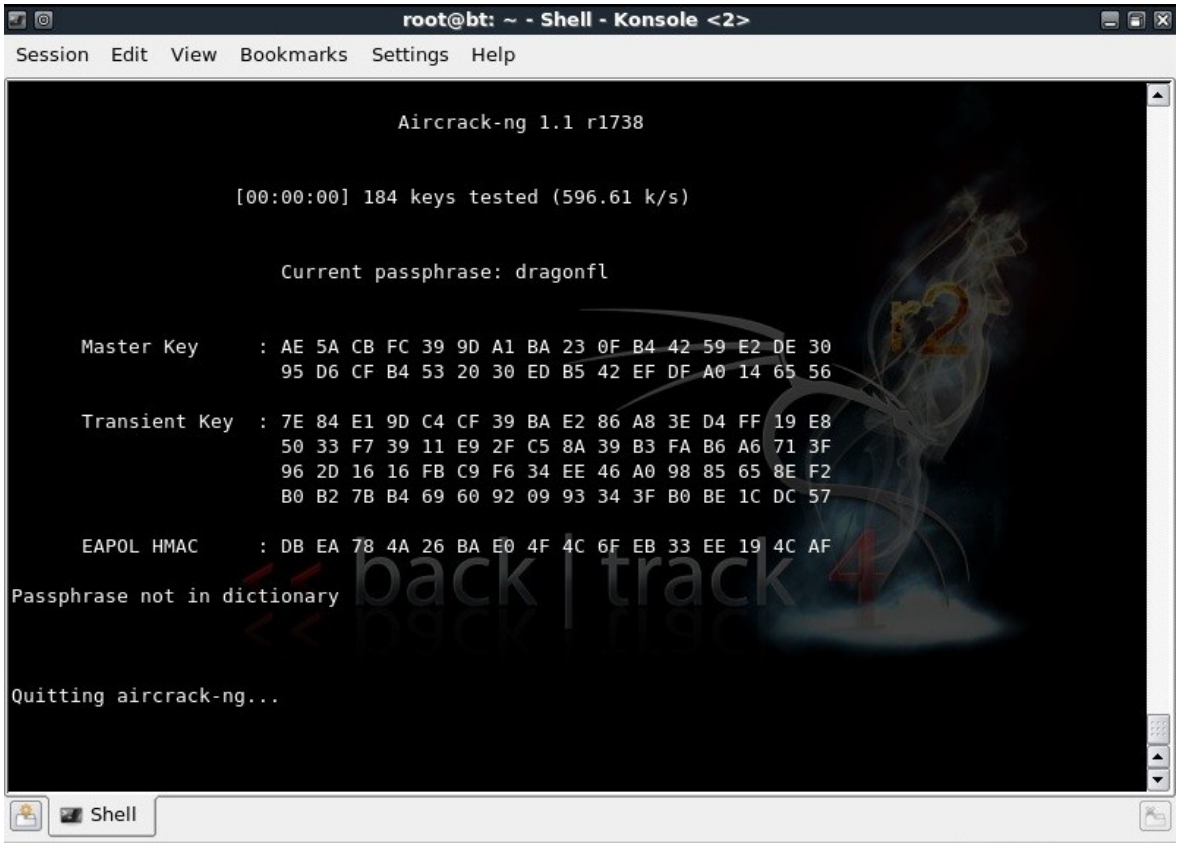


Obr. 9.4 - Získaný handshake

A teď už jen spustit nástroj aircrack a doufat, že heslo bude ve slovníku. Více informací nalezneme na [16].

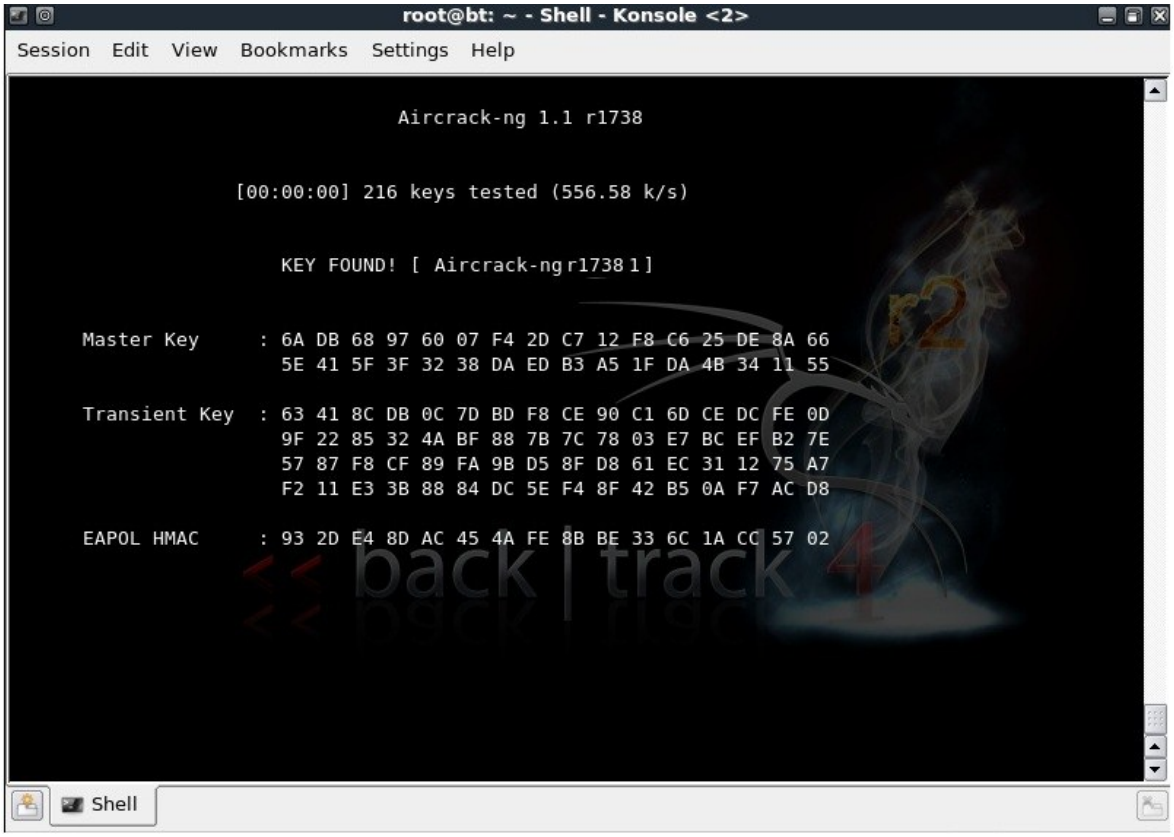
Příkazem

aircrack-ng hackMysak-01.cap -w ./slovník



Obr. 9.5 - Neúspěšný slovníkový útok

Tady vidíme, co se stane, když heslo není v námi zadaném slovníku. Jedině, co mohu poradit, tak pokračovat dalšími slovníky a vyčkávat.



Obr. 9.6 - Úspěšný slovníkový útok

Hledané heslo bylo ve slovníku a tím pádem jsme získali přístup do dané sítě. Teď už jen stačí se připojit pomocí získaného hesla a surfovat po internetu.

Pro úspěch je zapotřebí, aby v dané síti bylo hodně uživatelů a tato síť měla slabé heslo. Jinak nemáme šanci se do této sítě dostat.

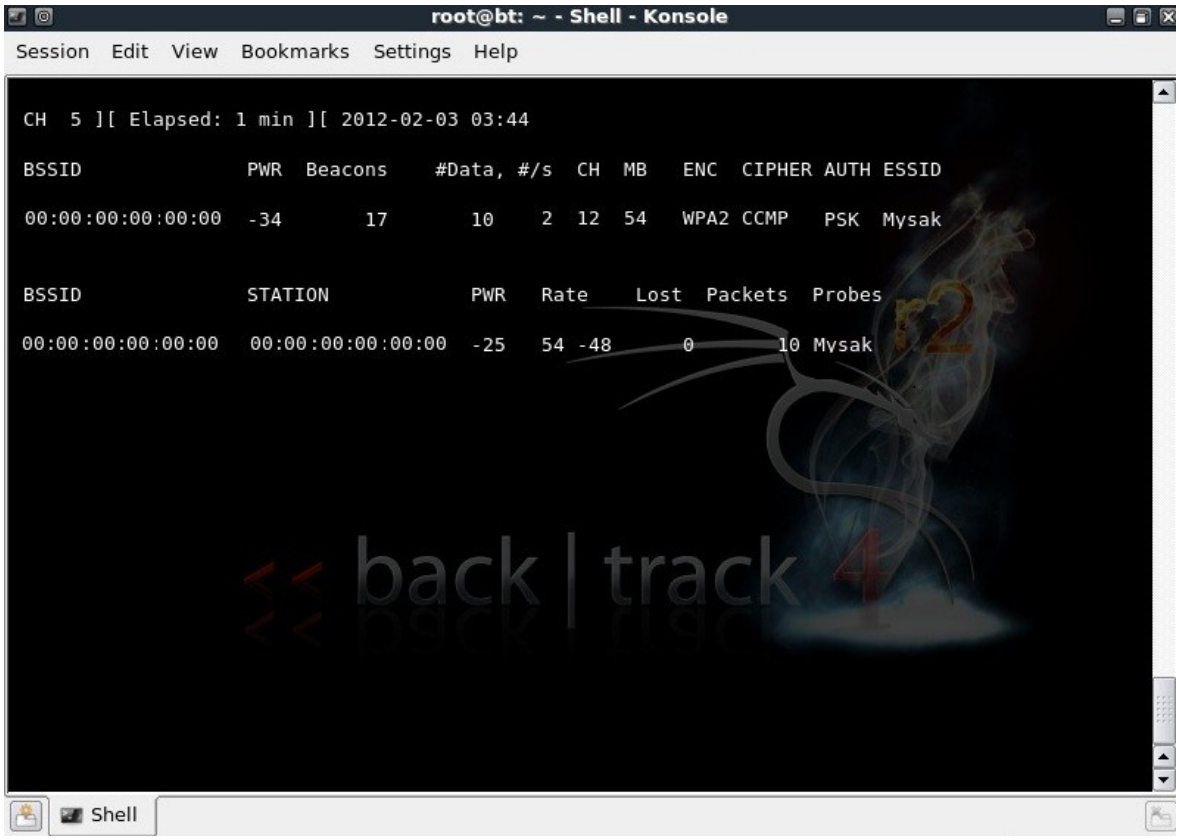
10 Ukázka prolomení protokolu WPA2

Nejdříve si zjistíme název naší externí antény. Více informací nalezneme na [18][19].

airmon-ng

V mém případě je to wlan0. Poté můžeme příkazem níže shlédnout všechny dostupné sítě okolo nás a vybrat si síť se zabezpečením WPA2.

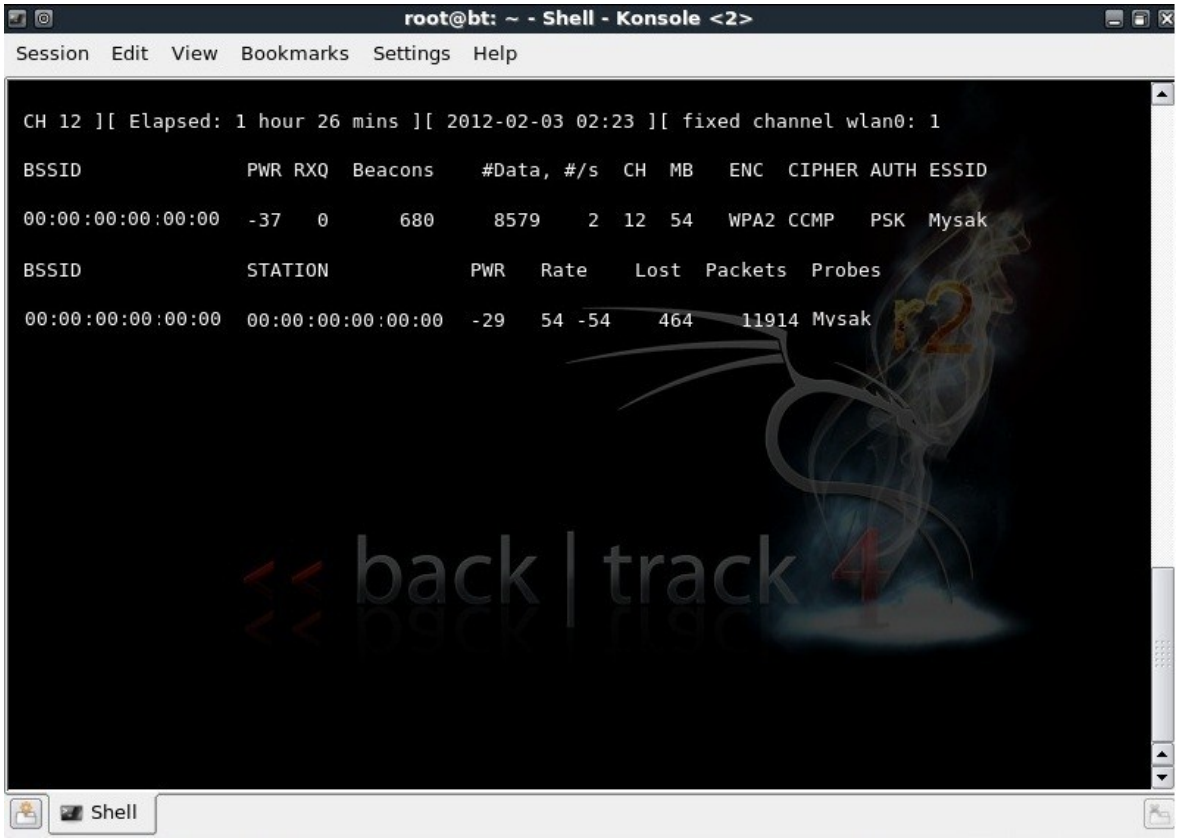
airodump-ng wlan0



Obr. 10.1 – Odposlech

Zjistili jsme si, na jakém kanálu námi vybraný cíl komunikuje (viz Obr. 8.1 - Odposlouchávání přenášených) a následně tímto příkazem ho začneme odposlouchávat a zapisovat si do souboru.

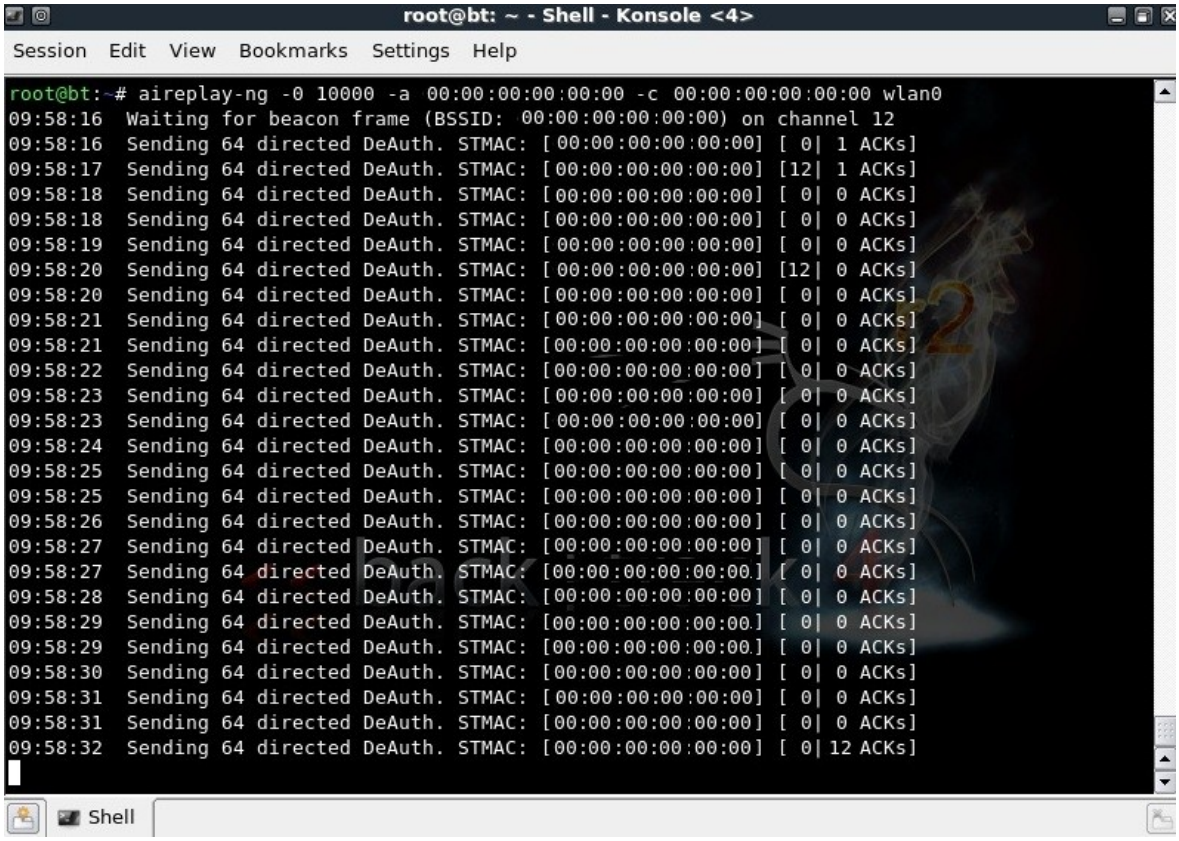
airodump-ng --bssid 00:00:00:00:00:00 –w hackMysak –c 12 wlan0



Obr. 10.2 - Ukládání do souboru

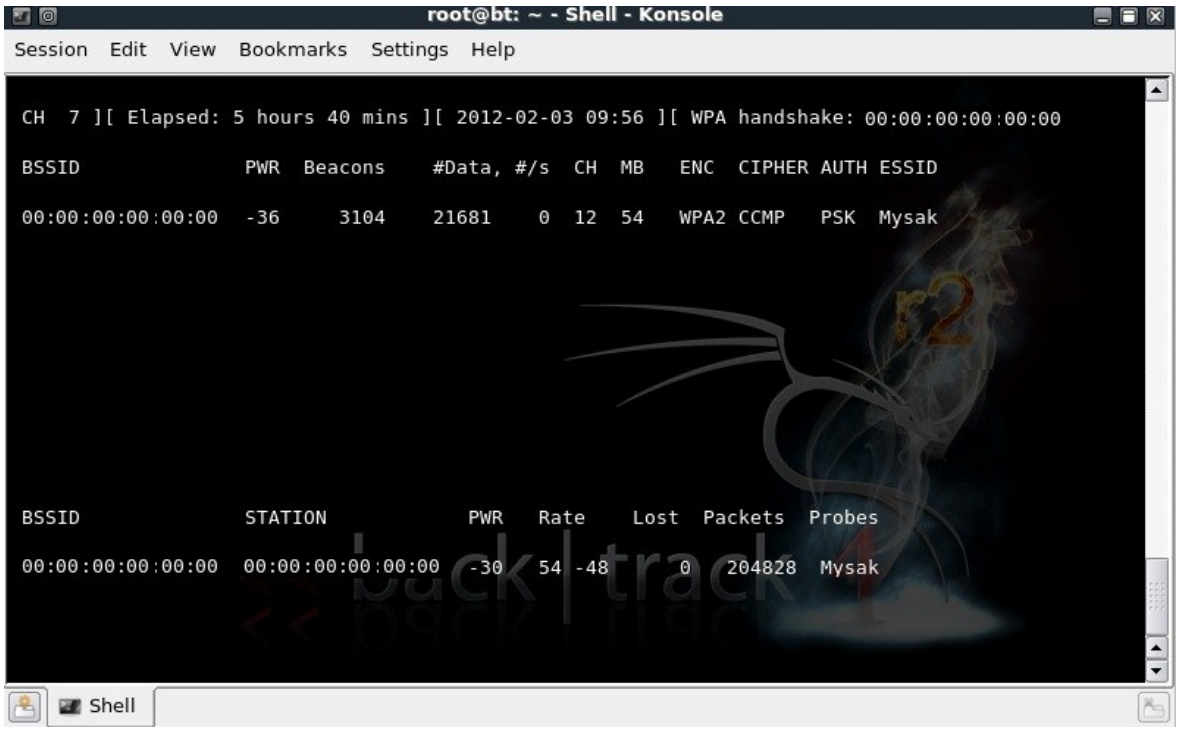
Použita deautentizace a to za pomoci příkazu, který se nachází níže.

aireplay-ng -0 10000 -a 00:00:00:00:00:00 -c 00:00:00:00:00:00 wlan0



Obr. 10.3 – Deautentizace

Teno příkaz jak u WPA, tak i tady mi nefungoval. Nedokázal donutit odpojit uživatele. Musel jsem čekat, dokud se nějaký uživatel nepřipojí. Jestli jsme získali handshake, zjistíme sledováním viz Obr. 10.4 - Získaný handshake. Bude zobrazen v pravém horním rohu.

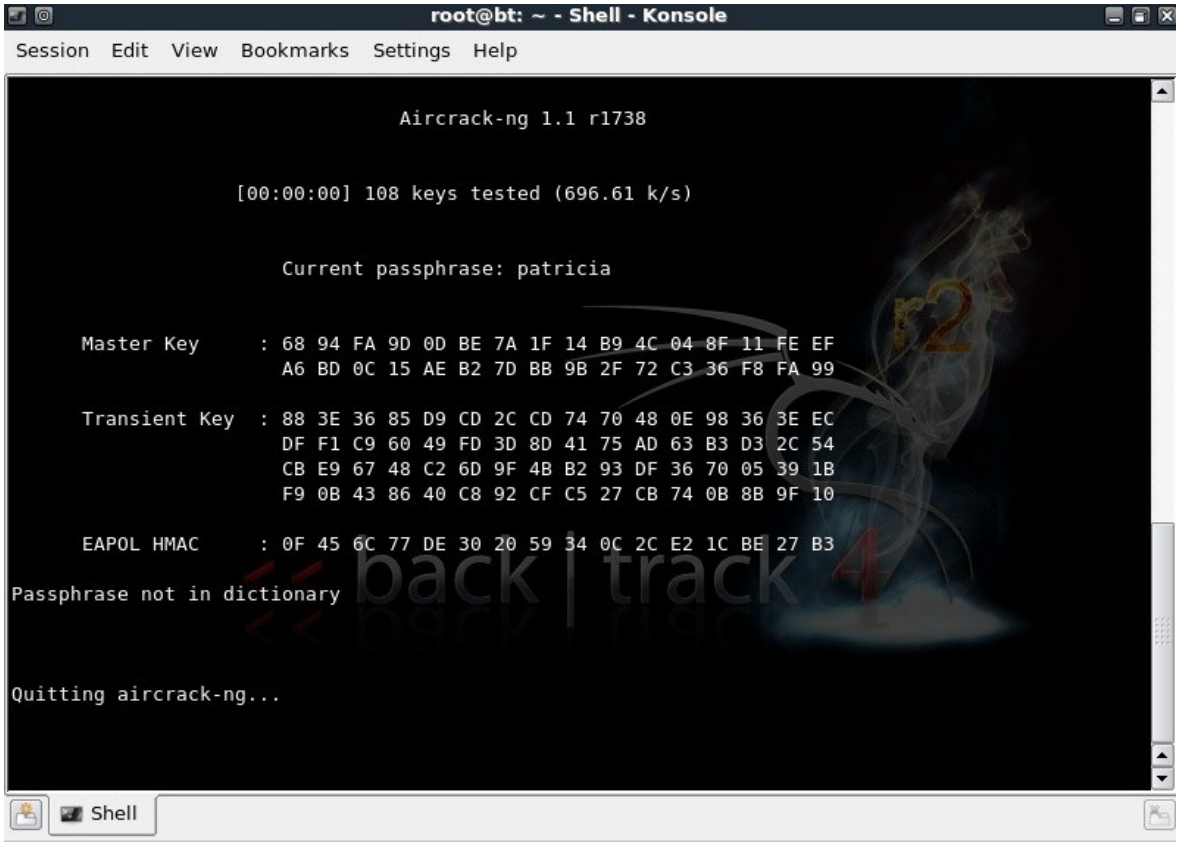


Obr. 10.4 - Získaný handshake

A teď už jen spustit nástroj aircrack a doufat, že heslo bude ve slovníku. Více informací nalezneme na [16].

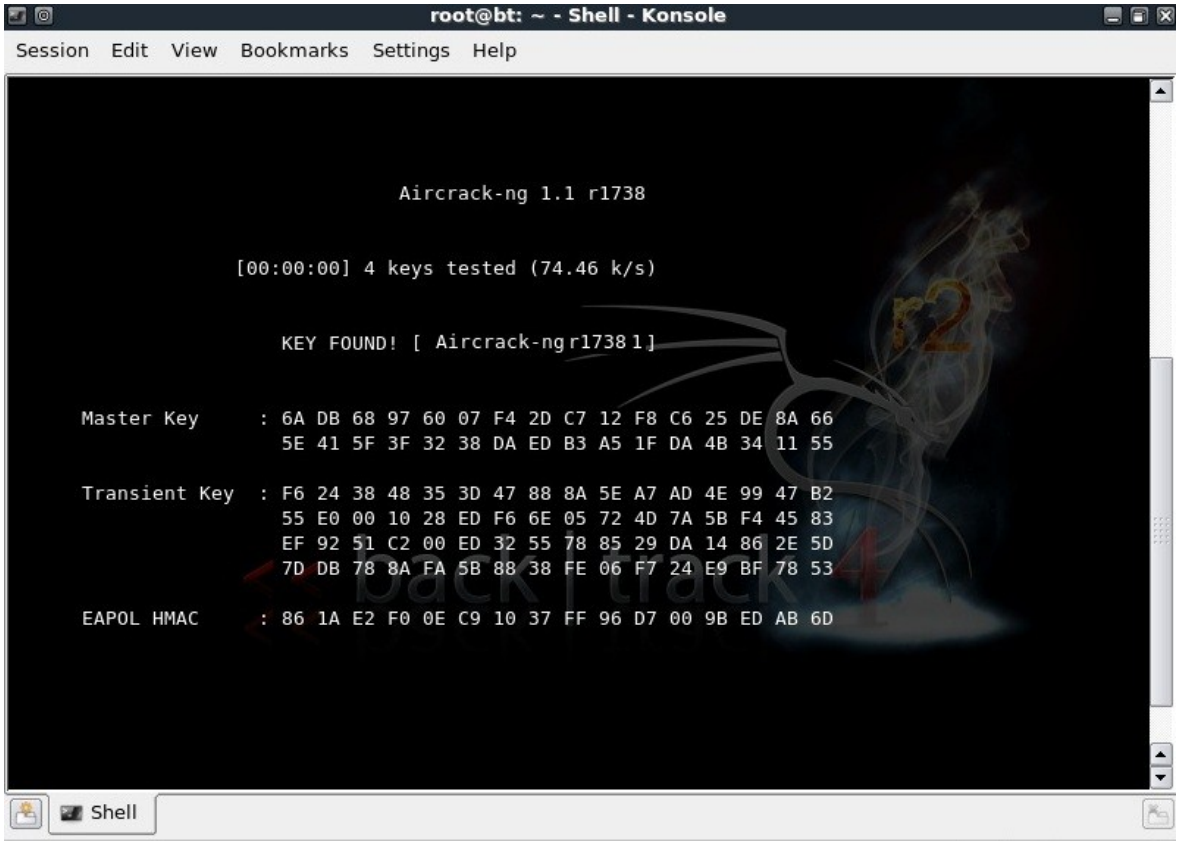
Příkazem

aircrack-ng hackMysak-01.cap -w ./slovník



Obr. 10.5 - Neúspěšný slovníkový útok

Tady vidíme, co se stane, když heslo není v námi zadaném slovníku. Jedině, co mohu poradit, tak pokračovat dalšími slovníky a vyčkávat.



Obr. 10.6 - Úspěšný slovníkový útok

Hledané heslo bylo ve slovníku a tím pádem jsme získali přístup do dané sítě. Teď už jen stačí se připojit pomocí získaného hesla a surfovat po internetu.

Pro úspěch je zapotřebí jako u WPA hodně uživatelů na síti a slabé heslo. Handshake se dá získat poměrně snadno, ale rozluštit silné heslo je v reálném čase nemožné.

11 Závěr

Závěr budu věnovat shrnutí poznatků bakalářské práce. Praktickou demonstrací se mi povedlo poukázat na nedostatky některých protokolů, jelikož se mi podařilo rozluštění přístupových hesel do ukázkových sítí. Vše je v bakalářské práci zdokumentováno a doprovázeno pomocí obrázků obrazovek.

Co se týče bezpečnostního protokolu WEP, byl shledán jako nejméně bezpečný. Hlavním důvodem bylo, že zjištění jakéhokoli hesla je velice snadné. Ale důležitým faktorem pro úspěšné zdolání tohoto protokolu je zachycení trafiku na dané síti, do které se snažíme dostat. Trafikem mám na mysli – velký proud dat a minimálně jeden uživatel, ale čím více, tím méně času nám bude trvat rozluštění. V praktické části jsem se snažil do sítě s tímto zabezpečením dostat, což bylo úspěšné. Ukládal jsem inicializační vektory a za jejich pomoci získal heslo a mohl se volně pohybovat v získané síti.

Dále jsem použil slovníkový útok na protokol WPA-PSK.

Demonstroval jsem útok na svou síť a ukázal úspěšný a neúspěšný útok. Vše je v praktické části popsáno pomocí print screanů obrazovek pro lepší přehled. Ukládal jsem si rámce do souboru a vyčkával do doby, než se uživatel připojí nebo odpojí a následně připojí zpět. Pro získání handshaku můžeme čekat jednu minutu nebo dokonce i celý den. Po získání handshaku ještě není zdaleka vyhráno, protože teď nastává čas použití nástroje aircrack a slovníku. Pro úspěšné prolomení je nutné, aby administrátor nastavil slabé heslo, které je obsaženo v daném slovníku, který jsme si sami vytvořili nebo stáhli z databází dostupných na internetu. Pokud administrátor nastavil silné heslo a bude ho například jednou za měsíc měnit, tak se útočník nemůže dostat do této sítě.

Doporučení z bakalářské práce je zřejmé, že šifrování pomocí WEP a WPA není zcela bezpečné a proto lze doporučit nasazení WPA2, které nebylo prolomeno v kombinaci s dalšími bezpečnostními prvky jako je filtrování MAC adresy atd.

12 Literatura

1. Bezdrátové sítě. *Wikipedia, otevřená encyklopedie.* [Online] 7. 2 2012. [Citace: 23. 1 2012.] http://cs.wikipedia.org/wiki/Bezdr%C3%A1tov%C3%A1_s%C3%AD%C5%A5.

2. Extensible Authentication Protocol. *Wikipedia, otevřená encyklopedie.* [Online] 8. 1 2012. [Citace: 24. 1 2012.] http://cs.wikipedia.org/wiki/Extensible_Authentication_Protocol.

3. IEEE 802.11. *Wikipedia, otevřená encyklopedie.* [Online] 12. 2 2012. [Citace: 12. 12 2011.] http://cs.wikipedia.org/wiki/IEEE_802.11.

4. OvisLink AirLive všesměrová anténa 2,4GHz, 10dBi RSMA interiérová (WAI-101). *Wifi Aspa.* [Online] 16. 3 2012. [Citace: 16. 3 2012.] http://wifi.aspa.cz/ovislink-airlive-vsesmerova-antena-2-4ghz-10dbi-rsma-interierova-wai-101-z83408/.

5. Zisk smerovost WiFi anten. *Občanské sdružení PVfree Wiki.* [Online] 4. 12 2007. [Citace: 29. 11 2011.] http://wiki.pvfree.net/index.php/Zisk_smerovost_WiFi_anten.

6. BackTrack. *Wikipedie, otevřená encyklopedie.* [Online] 9. 3 2012. [Citace: 30. 1 2012.] http://cs.wikipedia.org/wiki/BackTrack.

7. **Panther.** Decibel. *Radiolokátory.* [Online] 10. 5 2009. [Citace: 23. 2 2012.] http://www.radiolokatory.cz/teorie/decibel.html.

8. **Hráček, Jiří.** IEEE 802.11n - Zrychlete a rozšiřte svou bezdrátovou síť. *INTELEK - komponenty datových a telekomunikačních sítí.* [Online] 3. 2 2009. [Citace: 23. 2 2012.] http://www.intelek.cz/art_doc-5C56A0147621A13AC12575510053AE3E.html.

9. Princip a prvky bezdrátových sítí. *Bezdrátové připojení k internetu.* [Online] 16. 3 2012. [Citace: 10. 3 2012.] http://www.bezdratovepripojeni.cz/cs/cz/clanky/princip-a-prvky-bezdratovych-siti.

10. **Čapek, Miloslav.** Sektorová anténa. *Stránka katedry elektromagnetického pole.* [Online] 17. 12 2009. [Citace: 24. 1 2012.] http://www.elmag.org/doku.php/k317:simulace_elmag_poli:sektor.

11. **Fesl, Jan.** *Principy zabezpečení bezdrátových sítí.* 2007.

12. **Lehembre, Guillaume.** *Bezpečnost Wi-Fi - WEP, WPA a WPA2.* 2006.

13. **Fikejz, Martin.** *Zabezpečení bezdrátových sítí 802.11 b, g.* 2006.

14. **Bouška, Petr.** Cisco WiFi - základní principy a protokoly. *Vítejte v mém světě.* [Online] 3. 11 2009. [Citace: 23. 12 2011.] http://www.samuraj-cz.com/clanek/cisco-wifi-zakladni-principy-a-protokoly/.

15. **Přibyl, Tomáš.** Šifrovací protokoly využívané WiFi. *Nezávislý odborný on-line magazín ICT SECURITY.* [Online] [Citace: 26. 2 2012.] http://ictsecurity.cz/odborne-clanky/sifrovaci-protokoly-vyuzivane-wifi.html.

16. **Darkaudax.** Aircrack-ng - slovníky. *Aircrack-ng.* [Online] 2. 10 2011. [Citace: 12. 12 2011.] http://www.aircrack-ng.org/doku.php?id=faq#where_can_i_find_good_wordlists.

17. Wifi crack WPA handshake. *Airdump.* [Online] [Citace: 10. 1 2012.] http://airdump.cz/wifi-crack-wpa-handshake/.

18. **safeLinux.** *How To Crack WPA [Backtrack 5 / Aircrack]* . YouTube, 2011.

19. **MegaGazzy.** *[BT5] -Cracking WPA2* . YouTube, 2011.

20. **Vašek, Martin.** *Návrh a realizace bezdrátových sítí.* Zlín : autor neznámý, 2009.

21. **Zandl, Patrick.** *Bezdrátové sítě Wifi. Praktický průvodce.* Brno : Computer Press, 2003. 80-7226-632-2.

22. **Píša, Miroslav.** *Datová Bezpečnost bezdrátové komunikace v rámci vnitřních podnikových sítí.* Zlín : autor neznámý, 2008.

23. **Báča, Martin.** *BEZDRÁTOVÁ TECHNOLOGIE WI-FI.* Brno : autor neznámý, 2007.

24. **Jelínek, Martin.** *Bezpečnost bezdrátových počítačových sítích.* Brno : autor neznámý, 2010.

25. **Rohleder David, Lorenc Václav.** *802.1X – autentizace v počítačových sítích.* 2008.