VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ÚTOKY NA STANDARD 802.11

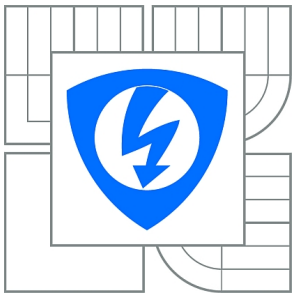
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE VOJTĚCH BURIAN
AUTHOR

BRNO 2014

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

ÚTOKY NA STANDARD 802.11

ATTACKS ON STANDARD 802.11

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

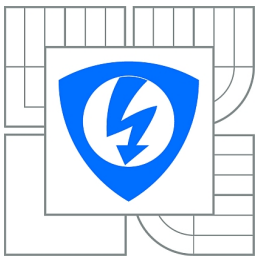
AUTOR PRÁCE — VOJTĚCH BURIAN

AUTHOR

VEDOUCÍ PRÁCE — Ing. BOHUMIL NOVOTNÝ

SUPERVISOR

BRNO 2014



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Vojtěch Burian	***ID:***	145978
Ročník:	3	***Akademický rok:***	2013/2014

NÁZEV TÉMATU:

Útoky na standard 802.11

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se se standardem zabezpečení bezdrátových sítí 802.11. Analyzujte teoretické chyby ve standardu 802.11 a popište moderní zabezpečení v současnosti. Simulujte postupně útoky na zabezpečovací mechanismy WEP, WPA a WPA2 a útoky popište. Navrhněte možnosti předcházení jednotlivým typům útoků.

DOPORUČENÁ LITERATURA:

[1] WONG, S.: The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards. SANS Institute, 2003.

[2] ODVÁRKA, P: Technologie pro zlepšení bezpečnosti datových sítí – základní charakteristika IEEE 802.1x. Svět sítí, 2004.

Termín zadání:	10.2.2014	***Termín odevzdání:***	4.6.2014

Vedoucí práce: Ing. Bohumil Novotný
Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Práce se věnuje problematice standardu 802.11, zabezpečení bezdrátových sítí, a to jak z historického hlediska, tak ze současnosti. První část je věnována problematice zabezpečených sítí WEP. Následně je navázáno na zabezpečení sítí avšak z novějšího hlediska a to zabezpečení sítí pomocí WPA a WPA2. Bude nastíněněno základní fungování a přehled standardu 802.11, uvedení známých útoků na tyto zabezpečení a poukázání na známé chyby. Mnoho starších zařízení disponují pouze zabezpečením WEP. Proto je navrhnuto lepší systémové zabezpečení tohoto protokolu WEP. Jsou uvedeny modernější metody zabezpečení WPA a WPA2. Druhá část práce je zaměřena na simulaci útoku na zabezpečení sítí. Tato část rozebírá problematiku ve spojitost s prolamováním zabezpečení WEP, WPA a WPA2.

KLÍČOVÁ SLOVA

WEP, WPA, WPA2, IEEE 802.11, Wi-Fi, bezpečnost, bezdrátové sítě, wlan, PTW, Chopchop útok, FMS, KoreK, Fragmentační útok, TKIP, CCMP, Beck-Tews útok, vylepšený útok na TKIP, Michael reset Attack, Ohigashi-Morii útok, Útok na WPA/WPA2 — PSK, Hole196, WPA migrační útok, WPS.

ABSTRACT

Thesis is concerned about standard 802.11 especially wireless network security in historical and in current way. First part is focused on WEP secured wireless network problematics. Consequently, in different point of view we are focused on network security which was developed recently, for example WPA and WPA2 security. It will be marked the basic functioning and brief overview of standard 802.11, introduction to the known attacks on wireless network security and also indicate the main mistakes. Many older devices have only WEP security. Therefore, in this thesis is designed better and more coherent system of security of the WEP protocol. As well modern methods of security WPA and WPA2 are included. Second part is focused on the simulation of attack on security networks. In this part the problematic with beaking security WEP, WPA and WPA2 is discussed.

KEYWORDS

WEP, WPA, WPA2, IEEE 802.11, Wi-Fi, security, wireless network, wlan, PTW, Chopchop attack, FMS, KoreK, Fragmentation attack, TKIP, CCMP, Beck-Tews attack, An Improved Attack on TKIP, Michael reset Attack, Ohigashi-Morii attack, Attack on WPA/WPA2 – PSK, Hole196, WPA Migration Mode, WPS.

BURIAN, Vojtěch *Útoky na standard 802.11*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2014. 78 s. Vedoucí práce byl Ing. Bohumil Novotný.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Útoky na standard 802.11“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Mé poděkování patří Ing. Bohumilu Novotnému, vedoucímu mé bakalářské práce, za jeho čas, trpělivost a rady. Také bych rád poděkoval přátelům, především Lucii Sáře Jurčové a také rodině za jejich podporu.

Brno ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Tato práce pojednává o komplexní problematice standardu 802.11 a analyzuje jeho chyby. V práci je nastíněn základní přehled standardu 802.11 a také jeho fungování.

Kvůli velkému rozvoji bezdrátových sítí v posledních letech se pozornost začala obracet zejména na jejich důsledné zabezpečení. V práci jsou popsány hlavní metody zabezpečení sítí a to s ohledem na jejich používání jak v minulosti, tak také v současnosti. Dále jsou zde uvedeny útoky na zabezpečení, a také je poukázáno na známé chyby. Vzhledem k tomu, že v začátcích se bezpečnost bezdrátových sítí zajišťovala prostřednictvím zabezpečení WEP, jsou v práci uvedeny také důležité vlastnosti tohoto zabezpečení. V souvislosti se zabezpečením sítí je rozvedena také teorie antén a kryptografie. V rámci různých druhů zabezpečení sítí jsou zde nastíněny možnosti, jak zlepšit a zefektivnit obranu proti známým útokům a to jak všeobecných, tak přímých útoků na zařízení zabezpečených nejenom prostřednictvím WEP.

Aplikovaná část práce je věnována zejména simulování útoků na zabezpečení WEP, WPA a WPA2.

1 ÚVOD DO PROBLEMATIKY

V posledních letech došlo k výraznému a poměrně rychlému rozvoji bezdrátových sítí (Wlan). Tyto sítě mají spoustu výhod pro uživatele, ale také nevýhod a to zejména v oblasti zabezpečení a odposlechu.

Díky čím dál většímu užívání Internetu se zvyšuje také potřeba rozvoje a zlepšování bezdrátových zařízení. I v této oblasti, tedy v oblasti bezdrátových sítí a zařízení, dochází k poměrně rychlému vývoji. Technologie se mění a uzpůsobují zejména potřebám jejich uživatelů. Například podniky potřebují snížit náklady na provoz a pro své zaměstnance se snaží zajistit větší komfort, a tedy poskytují svým zaměstnancům vyšší mobilitu. Bezdrátová technologie se nevyužívá jen v malých vestavěných systémech, ale často se používá také v dalších zařízeních, jako jsou například notebooky či tablety aj. Bezdrátové zařízení jsou výborným prostředkem jak za poměrně nízkou cenu dosáhnout vyšší rychlosti připojení k Internetu, a také jak zefektivnit využití všech zařízení obsahujících právě bezdrátovou technologii. Tuto technologii dnes ve vyspělých zemích používá téměř každý a téměř všude. Navíc dnešní jednoduché domácí zařízení má dosah několik desítek metrů, a proto se útočník nemusí nacházet v bezprostřední blízkosti zařízení. Je tedy třeba dbát na patřičné komplexní zabezpečení.

Bezdrátové sítě nejsou využívány jen firmami či velkými korporacemi, protože jsou již cenově dostupné na trhu, využívají je také čím dál více i běžní uživatelé jako jsou například domácnosti. S rozšířením bezdrátových sítí se rozšiřují také možnosti či způsoby útoků na sítě.

Proto se zabezpečení bezdrátové sítě stala důležitou oblastí ve výzkumu a vývoji. Stejně jako při používání kabelových rozvodů, zabezpečení bezdrátové sítě se zaměřuje především na ochranu osobních informací a zamezení neoprávněnému přístupu do systémů. Nicméně výzkum a vývoj v této oblasti směřuje zejména k tomu, aby se mohla tato bezpečnostní opatření implementovat i do zařízení s nízkým výpočetním výkonem a malou kapacitou pamětí.

Tato bezdrátová komunikační zařízení pracují podle standardu IEEE 802.11 nebo taky někdy označováno jako Wi-Fi. Norma se vztahuje zejména na bezdrátové lokální sítě.

2 HISTORIE

Kolem roku 1985 již bylo možné využít tzv. odpadní pásmo, což znamená možnost využívat také určité frekvence bez nutnosti vyžádat si icenci. Jedná se zejména o pásma s frekvencí 900 MHz, 2,4 GHz a 5,8 GHz. Tyto frekvence se využívaly i dříve a to například v mikrovlnných troubách, ale až od roku 1985 se mohly využívat také pro účely telekomunikace.

Vzhledem k prvním zkušenostem s bezlicenčními pásmy bylo potřeba zajistit jistou kompatibilitu mezi produkty ostatních výrobců v rámci bezdrátové komunikace. V roce 1990 byl ohlášen vznik nové pracovní skupiny a standardu 802.11 komisí IEEE. Tento standard je zaměřený na telekomunikaci v bezlicenčních pásmech a byl stavěn na standardu pro ethernet 802.3. [10]

3 BEZDRÁTOVÉ SÍTĚ

Wlan nebo také Wi-Fi sítě označují bezdrátovou komunikaci v počítačových sítích. Díky realizaci šíření informací pomocí étheru, se stala tato technologie velmi oblíbenou a často používanou v dnešní době. Nezisková organizace IEEE vydává právě pro tuto komunikaci několik standardů, které u bezdrátových technologiích nesou název 802.11, samozřejmě postupem času se stále vyvíjejí novější standardy. Přenos je realizovaný pomocí rádiových signálů v různých kmitočtových úrovních. Tyto úrovně můžeme ještě rozdělit na dvě hlavní části, ve kterých právě probíha rozdělení kmitočtů. Toto rozdělění má všeobecný nazev a dělí se na 2,4 Ghz a 5 Ghz. Wi-Fi sítě využívají na přenos dat bezlicenční pásmo. [30]

4 IEEE 802.11

S rozvojem bezdrátových sítí a zařízení začaly také vznikat různé a nové druhy problémů v bezdrátových systémech. Na tyto problémy bylo nutné reagovat, a proto vznikla norma 802.11. Tento standard byl publikován až v roce 1997, neboť vývoj tohoto standardu než dospěl do takové fáze, že se mohl začít užívat v praxi, byl dlouhý. Norma se stala žádanou a rozšířenou díky své vysoké rychlosti přenosu dat a také díky tomu, že umožňovala rychlé šifrování.

802.11 s sebou přináší potřebu definovat si určitá pravidla. Jedním z nich je definice o provozu tzv. bezdrátového ethernetu na fyzické vrstvě MAC, jde o princip přístupu ke společnému médiu. Bylo zvoleno stanovisko pro předcházení nebo vyhýbání se kolizím CSMA/CA , které pracují na principu výměny kontrolních zpráv (Request to Send a Clear to Send), čímž došlo k odlišení od detekce a opravování kolizí signálů (CSMA/CD), což jsou metody známé z ethernetu. [10, 18, 34]

Kromě IEEE se ještě na standardizaci podílí Wi-Fi Alliance. Wi-Fi Alliance je nezisková mezinárodní asociace vytvořená roku 1999 a zabývá se zejména certifikacemi bezdrátových LAN produktů ve smyslu vzájemné kooperace založené na IEEE 802.11 specifikaci. Cílem členů Wi-Fi Alliance je rozšířit uživatelovy zkušenosti a to díky tomu, že jednotlivé produkty s sebou budou vzájemně spolupracovat. [36]

4.1 Přehled vývoje standardu 802.11

- **802.11a** – Využívá bezlicenčního pásma v 5 GHz a jeho propustost je až 54 Mb/s.
- **802.11b** – Byl uveden v roce 1999 s využitím pásma 2,4 GHz.
- **802.11g** – V roce 2003 byl uveden standard g, který rozšiřuje využití standardu 802.11b a navyšuje propustost na max. 54 Mb/s.
- **802.11i** – V roce 2004 bylo schváleno vydání standardu 802.11i, který se zabývá zlepšení autentizace a šifrování dat ze standardu 802.11.
- **802.11n** – Vylepšení pro vyšší datovou propustnost. Tento standard byl uveden v roce 2009.

4.1.1 802.11a

802.11a využívá bezlicenčního pásma v 5 GHz a modulaci OFDM. Jeho propustnost je až 54 Mb/s. Byl vytvořen ve stejném roce jako 802.11b a to v roce 1999. Vzhledem k tomu, že jeho praktické uplatnění ještě stále nebylo dostačující, byl tento standard podnětem pro vznik nového standardu g.

4.1.2 802.11b

Tento standard využívá pásma 2,4 GHz s použitím přístupové metody k mediu CSMA/CA. Jedná se o doplněk ke standardu 802.11, který navyšuje přenosovou rychlost až na 11 Mb. Ze standardu 802.11 převzal modulaci signálu DSSS, což je metoda přímého rozprostření.

4.1.3 802.11g

V roce 2003 byla vydána nová specifikace pod označením 802.11g, který zlepšuje propustnost na fyzické vrstvě až na 54 Mb/s. Využívá modulace OFDM, na kterém je založen i standard 802.11a. Standard se považuje za nádstavbu nad standard 802.11b a tím sdílí i jeho nedostatky. Standard pracuje v bezlicenčním pásmu 2,4 GHz.

4.1.4 802.11i

Tento standard byl vydán v roce 2004 institutem IEEE. Standard se zabývá zlepšením autentizace a šifrování dat ze standardu 802.11. Tento standard nese taktéž označení RSN, který používá autentizaci 802.1x.

4.1.5 802.11n

Standard, který byl uveden v roce 2009. Vylepšuje datovou propustnost pomocí techniky MIMO a využívá šířku pásma 40 MHz. S tímto vylepšením je možné dosáhnout přenosové rychlosti až 600 Mb/s. Standard může pracovat jak pro pásmo 2,4 GHz tak i pro 5 GHz.

5 ANTÉNY

Anténa je zařízení, které je schopno přijímat nebo vysílat elektromagnetické vlny z/do éteru (vzduchu). Zařízení má jednoduchou konstrukci. Jeho funkčnost však znatelně ovlivňují podmínky, ve kterých je zařízení nainstalováno.

Antény můžeme rozdělit na vysílací a přijímací, ale i vysílací anténa má schopnost přijímat a naopak. Při volbě antény je třeba brát v úvahu, kde bude umístěna, jak velké bude rušení v okolí a co vše ji hrozí. Antény dělíme na dva základní druhy a to na všesměrové a směrové. [4, 16, 35]

5.1 Všesměrové antény

Jak již název napovídá, tyto antény vysílají signál do všech směrů. Nejčastěji jsou tyto antény vyrobeny jako plošný spoj, který se nachází uvnitř plastového krytu.

5.2 Směrové antény

Existují dva druhy a to parabolické, které mohou mít zisk i 30 dBi a vyzařovací úhel menší než 10 stupňů, nebo YAGI, což jsou antény, které vypadají jako dlouhé tubusy. Uvnitř se nachází mnoho sfázované půlvlnové dipóly, které navzájem rezonují. Jistou výhodou těchto antén je jejich cena.

5.3 Důležité parametry u antén:

- Kmitočtové pásmo
- Polarizace
- Zisk
- Impedance

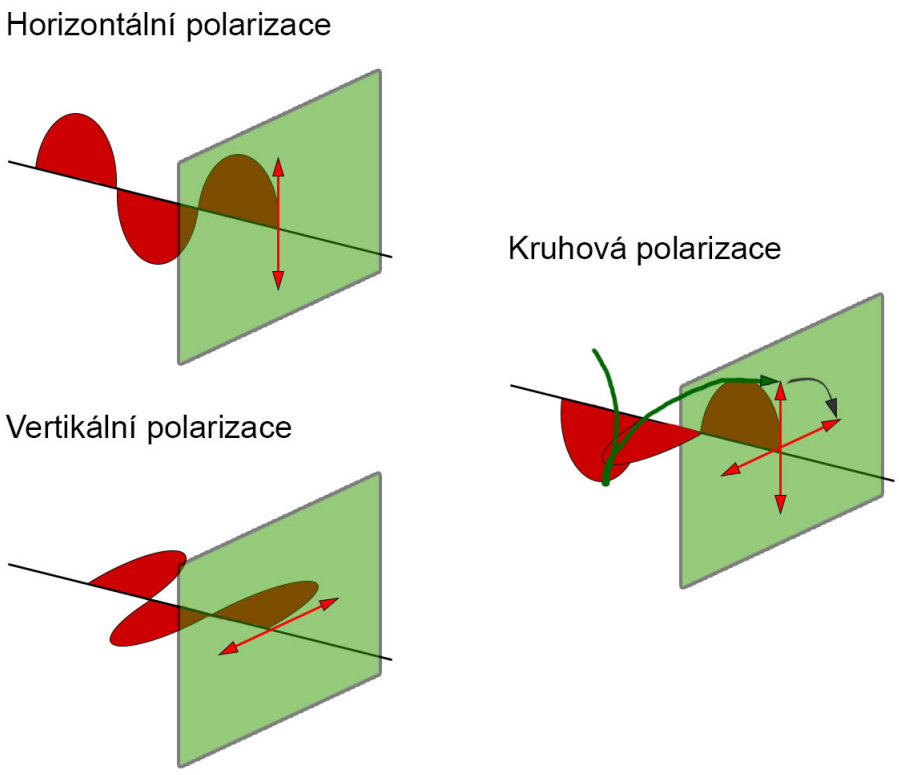
Kmitočtové pásmo znamená určitý rozsah, který je dán v kmitočtech. V tomto rozsahu pracuje anténa nejlépe.

5.3.1 Polarizace

Polarizaci dělíme na dva druhy podle polarizace elektromagnetického vlnění, na lineární a kruhovou. Lineární polarizace se dělí dále na vertikální a horizontální, kde se elektromagnetické vlnění šíří podle polarizace antény.

Pokud je signál vertikálně polarizován, vlny se budou šířit vertikálně (viz obr. 5.1). U horizontálního šíření je o 90° pootočen k vertikálnímu signálu. Avšak pro nejlepší provoz musí být obě stanice stejně polarizované. Pokud vysíláme vertikálně polarizovaný signál, nejlepší příjem bude mít vertikálně polarizovaná anténa. Jestliže vysíláme horizontálně polarizovaný signál na vertikálně umístěnou anténu, může dojít k velkým ztrátám zisku nebo k znesnadnění až k znemožnění přenosu.

Kruhovou polarizaci můžeme mít pravotočivou a levotočivou. Kruhová polarizace přenáší obě roviny, fázově otočené o 90°. [4, 35]



Obr. 5.1: Polarizace

5.3.2 Zisk

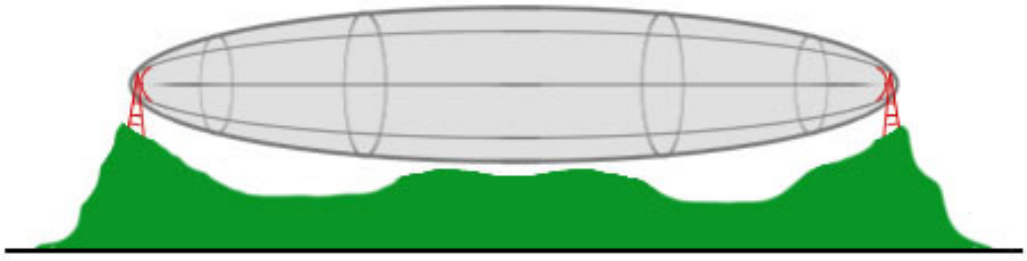
Zisk vyjadřuje výkon nebo intenzitu elektromagnetického pole. Větší zisk má vždy ta anténa, která dokáže vyzářit co nejvíce energie do určitého směru. Některé antény jsou udávány odlišnými jednotkami dBd a dBi. Jednotka dBi značí jaký má výkon vztažen k výkonu izotropního zářiče. Izotropní zářič je vysílač všesměrového vlnění. Naopak jednotka dBd (neboli také dB) udává výkon ve vztahu k půlvlnovému dipólu.

5.3.3 Impedance

Impedance je důležitý parametr antén. Impedance je fyzikální veličina, která se využívá především ve spojitosti se správným použitím kabeláže a to z toho důvodu, aby nedocházelo k odrazům signálů.

5.4 Fresnelova zóna

Jedná se o imaginární prostor, který je mezi vysílačem a přijímačem. Tento prostor má tvar elipsoidu, ve kterém by se neměly nacházet žádné objekty (viz obr. 5.2). neboť už při volných 60% průměru zóny dochází k podstatnému snížení úrovně signálu. [40]



Obr. 5.2: Fresnelova zóna

6 KRYPTOGRAFIE

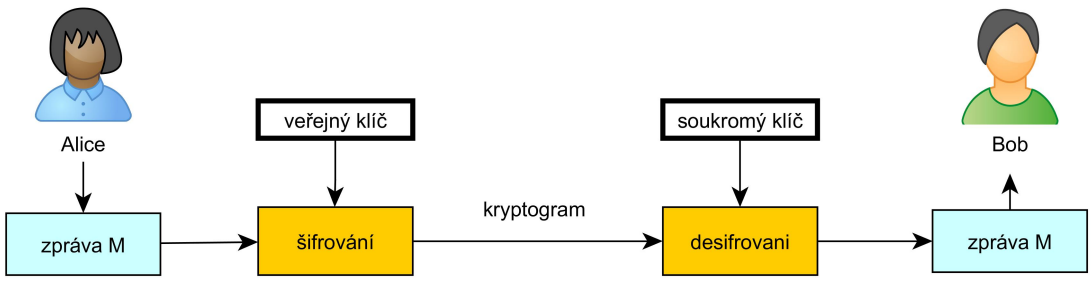
Kryptografie neboli také šifrovaní je nedílnou součásti dnešního světa. Každý se jednou dostal do situace, kdy potřeboval poslat jak přes Internet, přes síťové rozhraní, nebo po telefonu data tak, aby je nikdo neodhalil. Proto je potřeba šifrování. Například také firma potřebuje posílat tajná nebo citlivá data po otevřené síti. Nevýhoda takovéto sítě je, že data může kdokoliv odposlechnout. Šifrování je založeno na matematických pravidlech. Jedná se o základní prostředek dnešní elektronické bezpečnosti. Základní rozdělení možných prostředků k zašifrování je celá řada. Mezi nejznámější patří asymetrické, symetrické šifrování a hašovací funkce. [13, 26]

6.1 Asymetrické šifrování

Problém distribuce klíčů řeší asymetrická kryptografie. Klíče se dělí na dva základní. Jeden je znám pod pojmem veřejný klíč a druhý pod soukromým klíčem. Každý z těchto klíčů zastává určitou úlohu.

Výhodou asymetrického šifrování je faktorizace. Faktorizace neboli prvočíselný rozklad je výpočetně velmi složitý matematický problém. Asymetrické šifrování je založeno právě na složitém prvočíselném rozkladu. Je totiž početně nemožné v krátkém časovém intervalu přijít na prvočísla, která se zde využívají. Nevýhodou asymetrického šifrování je fakt, že se zvyšujícím se výpočetním výkonem je potřeba delšího klíče. V dnešní době je doporučeno používat klíče o délce 2048 bitů.

Uživatel si vygeneruje pár klíčů. Veřejný klíč se objeví v síti. Odesílatel zprávy si zjistí jeho veřejný klíč a pomocí něj zašifruje zprávu, kterou chce poslat. Zašifrovaná data jsou odeslána příjemci, neboť jen on je může dešifrovat, protože vlastní soukromý klíč k dešifrování (viz obr. 6.1). Hlavní výhodou asymetrických šifer je, že není problém s distribucí klíčů. Nejznámějším algoritmem v oblasti asymetrických šifer je tzv. algoritmus RSA.



Obr. 6.1: Asymetrická šifra

6.2 Symetrické šifrování

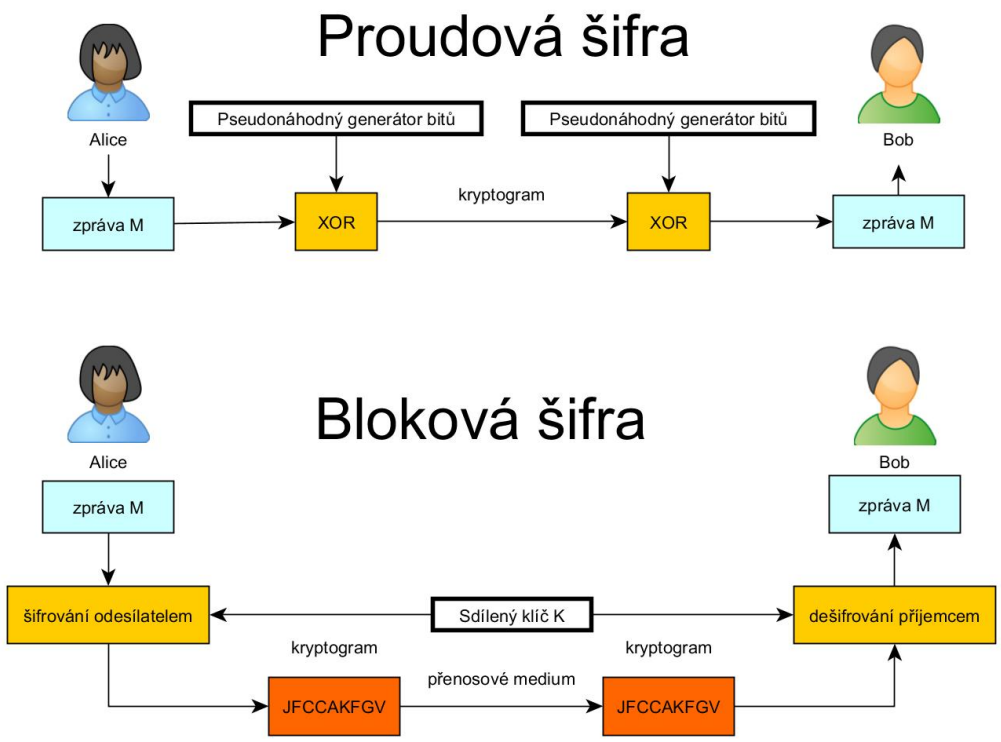
Symetrické šifry používají stejný klíč při šifrování i dešifrování. Základní komplikací je distribuce klíče. Významnou výhodou symetrického šifrování je, že se nejčastěji používá pro šifrování velkých objemů dat, neboť jsou velmi rychlé a jednoduché. Existují dva druhy symetrického šifrování a to proudová a bloková šifra.

6.2.1 Proudová šifra

Symetrická šifra proudová je rychlejší a jednoduší než bloková šifra. Narozdíl od blokových šifer (viz obr. 6.2) mají i vnitřní stav. Od tohoto stavu se dále odvíjí způsob generování šifrovacího klíče. Důležité je, aby se tento klíč neopakoval. Příkladem této šifry je RC4.

6.2.2 Bloková šifra

U blokových šifer se zpráva dělí na bloky o konstantních délkách, které jsou šifrovány tajným klíčem (viz obr. 6.2). Nevýhodou je, že pokud na vstup přijdou dva stejné bloky, budou zašifrovány identicky. Proto je zde využité zřetězování zpráv. Příkladem této šifry je AES.



Obr. 6.2: Symetrické šifry

7 WEP

Protokol WEP byl výchozím šifrovacím protokolem, jenž byl poprvé uveden v roce 1999 ve standardu IEEE 802.11. Byl navržen tak, aby poskytoval zabezpečení pro bezdrátové sítě. Byl vyvinut skupinou dobrovolníků. Účelem bylo nabídnout zabezpečení bezdrátových sítí. WEP se používal k zabezpečení bezdrátové komunikace od odposlouchávání, prevenci neautorizovaných přístupů k bezdrátové síti až k prevenci zásahu do přenášené zprávy. WEP používá symetrické šifrování, kdy se používá stejný algoritmus při dešifrování i při šifrování. Vážné bezpečnostní nedostatky, které byly objeveny v protokolu, vycházejí z nesprávných kryptografických systémů. Útoky na WEP se objevily již v roce 2001, tedy dva roky po spuštění tohoto protokolu. [10, 17]

WEP používá proudovou šifru RC4, která je kombinována s 40–bitovým nebo 104–bitovým WEP klíčem s 24–bitovým náhodným číslem.

7.1 Šifrování

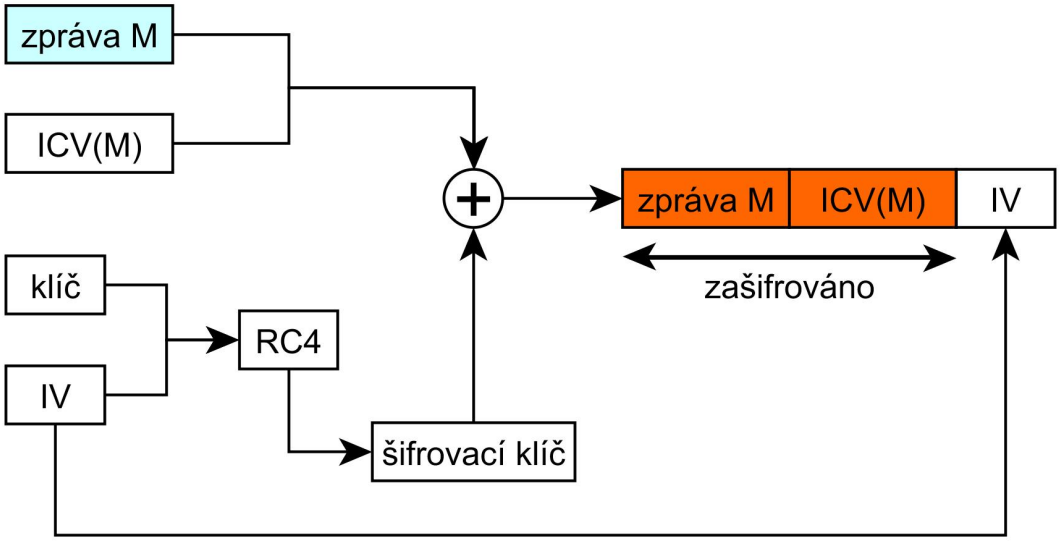
Než je zpráva zašifrována, je k ní přidáno několik kontrolních bajtů nazývaných ICV. Vygeneruje se inicializační vektor spojený s tajným klíčem, který je zašifrován pomocí RC4 algoritmu. Výstupem z algoritmu RC4 je šifrovací klíč. Do funkce XOR vstupuje zpráva M s přidanou ICV hodnotou a šifrovacím klíčem (viz obr. 7.1). Výstupem je zašifrovaná zpráva (viz rovnice. 7.1), ke které se nakonec dodá IV, MAC hlavička a CRC hodnota. Takto je paket odeslán příjemci. [10, 14, 25]

Příjemce dekóduje paket pomocí uloženého WEP klíče a přiloženého IV. Šifrovanou zprávu lze vyjádřit pomocí níže uvedeného vzorce [25]

$$\mathrm{C} = [M||ICV(M)] + [RC4(K||IV)]. \tag{7.1}$$

C – zašifrovaná zpráva, M – zpráva, ICV – kontrolní součet, K – klíč, IV – inicializační vektor, + – XOR, || – zřetězení

Šifrovací protokol WEP bohužel nebyl před zveřejněním pořádně otestován, proto v algoritmu zůstaly vážné nedostatky zejména v oblasti zabezpečení. Přestože použití WEP šifrování může odradit některé útočníky, zkušenější uživatel nemusí mít problém při prolamování tohoto zabezpečení. V dnešní době se WEP považuje z bezpečnostního hlediska za vyřazený. I přesto se ještě stále velmi často využívá, především je používán obyčejnými uživateli bezdrátových sítí. [10, 14, 25]



Obr. 7.1: Šifrování WEP

7.2 RC4

RC4 neboli také ARCFOUR je symetrická proudová šifra. Byla navržena již v roce 1987 Ronem Rivestem, ale nebyla zveřejněna a to z důvodu patentu. V roce 1994 byla odhalena pomocí zpětného inženýrství. Je využita u protokolu WEP, kdy vstupem do tohoto algoritmu u WEP tvoří IV zřetězený s klíčem. Výstup z tohoto algoritmu je šifrovaný klíč. Aby se dalo předejít stejným výstupním metodám a šifra zůstala dynamická, jedinou možností bylo změnit IV, jehož funkce je popsána výše. Tato šifra je složena ze dvou částí. [13, 23]

První část algoritmu se jmenuje KSA 7.1 [13, 23], který provádí inicializaci. Pole S se na začátku inicializuje a poté se jednotlivé prvky mezi sebou popřehází. Pole S má 256 bytů a N má právě hodnotu 256.

Druhou část tvoří PRGA algoritmus. 7.2 [13, 23], který upravuje vnitřní stav. V každém kroku se vytvoří 1 bajt šifrovacího klíče a provede se smyčka, která mění stav v poli S.

```
for i = 0 to N-1
S[i] = i
end for
j = 0
for i = 0 to N-1
j = (j + S[i] + K[i mod l]) mod N
swap(S[i], S[j])
endfor
```

Popis 7.1: KSA - algoritmus.

```
i = 0
j = 0
while
i = (i + 1) mod N
j = (j + S[i]) mod N
Swap(S[i], S[j])
Output z = S[(S[i] + S[j]) mod N]
endwhile
```

Popis 7.2: PRGA - algoritmus.

7.3 IV

Jeho úkolem je zajistit to, aby se ze dvou stejných vstupních řetězců nevytvořily dva totožné zašifrované řetězce, zároveň však zaručuje také to, že se neopakují stejné hodnoty pseudonáhodně generovaného šifrovacího klíče. Kdyby šifrovací klíč vznikal z konstantního tajného klíče, měl by totožnou hodnotu pro každý paket a za takových podmínek by nebylo potřeba získávat tajný klíč, ale stačil by pouze šifrovací klíč. IV by měl sloužit k udržení lepší úrovně zabezpečení, být zvětšen pro každý paket tak aby se pakety šifrovaly pokaždé jinými klíči. Hlavním nedostatkem je, že se IV přenáší v nezabezpečené formě a nezvětšuje se, čímž poskytuje případnému útočníkovi výhodu. Dalším nedostatkem je, že lze dopočítat WEP klíč a to proto, že jsou známé 3 bajty klíče a navíc také IV má jen 2^{24} možností což znamená, že existuje poměrně velká pravděpodobnost k duplicitě stejného IV. [23, 25, 32]

7.4 CRC, ICV (Integrita zprávy)

Týká se neautorizovaného dešifrování a špatné integrity dat. Tím, že známe klíč, můžeme automaticky měnit obsah zpráv a to bez toho, aby na to někdo přišel.

Algoritmus CRC se používá při kontrole integrity a slouží k detekci chyb při digitálním přenosu. CRC tedy poskytuje ochranu proti náhodným chybám, bohužel

však zprávy neuchrání před úmyslným falšováním, neboť útočník může zprávu změnit a CRC opět přepočítat.

Díky tomu vznikla ochrana zpráv pomocí ICV, která má podobný princip fungování jako CRC, ale hodnota ICV se spočítá ještě před šifrovacím procesem a následně je spolu se zprávou zašifrována, a tímto může být zajištěna správná integrita dat. Bohužel tento předpoklad je mylný, protože ICV metoda je metodou lineární, což znamená, že změníme-li určitý bit zprávy, můžeme předurčovat, které bity budou v ICV změněny. A protože WEP šifrování používá operaci XOR, změněné bity se projeví i ve výsledné šifře. [23, 25, 32]

7.5 Správa klíčů

Jestliže je jednou klíč prozrazen, musí se jeho obsah změnit. Tato změna probíhá v zařízeních v síti. Zabezpečení správy klíčů řeší převážně v podnikové sféře, kde se klade velký důraz na utajení přenášených informací. Nemá metodu pro aktualizaci klíčů. Tuto problematiku řeší převážně velké podniky, které mají více budov, může se nacházet v jedné budově i přes 30 AP. [14]

7.6 Autentizace

Jedná se o proces ověření pravosti komunikačních stran. WEP poskytuje pouze jednocestné ověření k autentizaci. Přístupový bod totiž neautentizuje síťovou kartu. Výsledkem je, že pro útočníka bude možné přesměrovat data do přístupového bodu přes alternativní cestu, krádež identity, třeba jím vytvořenou. Nejprve přijde ze strany mobilního zařízení žádosti o autentizaci, následně pošle AP zpětně zprávu v podobě náhodného 128-bitového čísla. Mobilní zařízení zašifruje výzvu a pošle ji AP, který učiní dešifrování a porovnání s původní odeslanou zprávou. Teprve pak je mobilní zařízení přijato nebo odmítnuto. [14, 23]

7.7 Autorizace

V tomto případě slouží řízení přístupu především k udílení práva ke komunikaci se sítí. Mobilní zařízení sice může být úspěšně autentizováno, ale v zájmu provozovatele sítě to nemusí znamenat, že má zařízení právo komunikovat v síti. IEEE 802.11 standard nemá žádnou definici pro metody řízení přístupů. Kromě kontroly MAC adres, která vychází ze standardu a spočívá v zachycení existence všech MAC adres. Vzhledem k triviálnosti falšování MAC adres je metoda nedostačující. [10, 23]

7.8 Historie prolomení WEPu

V roce 2001 byla zveřejněna publikace od Scott Fluhrer, Itsik Mantin a Adi Shamir, kde popisují dvě slabiny v šifrovacím algoritmu RC4. Jednalo se o útok na IV a invariaci. O rok později David Hulton přišel na to, jak optimalizovat FMS útok. V roce 2004 přišel nový útok s názvem KoreK, který využívá optimalizovaného FMS útoku a invertního induktivního útoku Arbaugh.

FMS typ útoku na WEP je uskutečněn pomocí analyzování síťového provozu, kdy při větším vytížení sítě bylo zapotřebí celkem hodně času k zpracování dat a obnovování klíčů. Tato metoda byla zdlouhavá, proto David Hulton přišel na to, jak celý útok vylepšit. Zapojil nejenom první bajt výstupu RC4 jako u metody FMS, ale také zbytek bajtů. Kvůli takovému vylepšení už není zapotřebí velké množství dat, které jsou k analýzám nutné. Pro srovnání, například u základního FMS útoku byla potřeba zachytit přibližně milion paketů.

Arbaugh indukční útok lze chápat jako inverzní verze k útoku KoreK. Arbaugh prokázal, že ICV lze použít k rozšíření šifrovacího klíče. Na Arbaugh indukčním útoku a KoreK útoku se vyvinul Chopchop útok. KoreK útok bere v potaz stav a chování u KSA a PRGA (viz 7.2). [14, 25]

7.9 Historické řešení problému

- **Zesílení klíče** – V roce 1998 vynalezl Lucent 128-bitový WEP k rozšíření WEP klíče ze 40 bitů na 104 bitů k posílení bezpečnosti. Toto řešení pomohlo při útoku hrubou silou. Ale tento přístup byl zbytečný, protože přetrvávaly předchozí bezpečnostní problémy. [14, 25]
- **Odstranění „slabých“ IV** – Odstranění některých IV, které napomáhaly rychlejšímu prolomení a odhalení tak tajného klíče. [10, 25]
- **Dynamický WEP** – Hlavní myšlenkou dynamického WEPu bylo automaticky generovat krátkodobé dynamicky vysílané WEP klíče v nastaveném intervalu. Dynamické WEP klíče sloužily jako prevence proti útočníkům, kteří se snažili odposlouchávat komunikaci. [10, 14, 25]

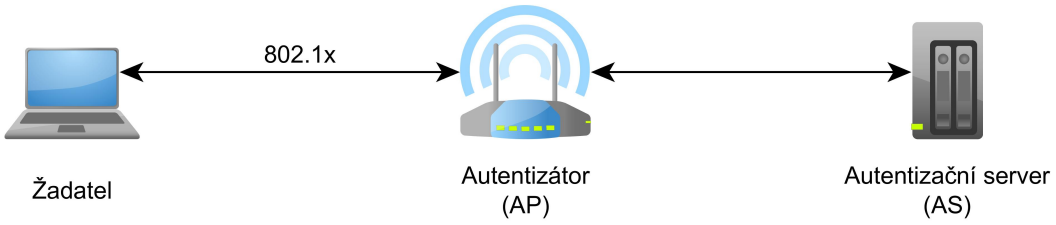
8 IEEE 802.1X

IEEE 802.1x (Port Based Network Access Control) jedná se o bezpečnostní standard schválený v roce 2001 organizací IEEE zaměřený na poskytnutí autentizačních možností. Využívá se v LAN tak i u Wlan slouží jako doplněk k použitému zabezpečení sítě – WEP, WPA a WPA2. Nejčastěji se používá právě v sítích zabezpečených WPA anebo WPA2. Při použití ve Wlan je řadění přístupu k síti řešené na úrovni logických portů AP, kde každá klientská stanice komunikuje právě s jedním AP. Cílem 802.1x je blokace komunikace v síti neoprávněným uživatelům. [23, 24, 25]

Klient i stanice se mezi sebou autentizují. Při této autentizaci jsou generované dynamické klíče pro danou relaci a stanici. Tyto klíče mají omezenou životnost.

Cíl 802.1x je tvořen právě pomocí autentizačního protokolu EAP, na kterém je tento standard založen. Proces autentizace pomocí IEEE 802-1 probíhá na třech různých prvcích (viz obr. 8.1), které jsou potřebné pro vzájemnou autentizaci:

- **Žadatel** – klient, který se chce připojit k dané síti.
- **Autentizátor (AP)** – zařízení, které povoluje nebo blokuje provoz. Většinou se jedná o přístupový bod.
- **Autentizační server (AS)** – entita, která ověřuje přihlašovací data. Obsahuje autentizační informace. AS určuje jaký typ protokolu bude použit pro autentizaci. Většinou se jedná o server RADIUS.



Obr. 8.1: Autentizace 802.1x - základní entity

8.1 Autentizace v IEEE 802.1X

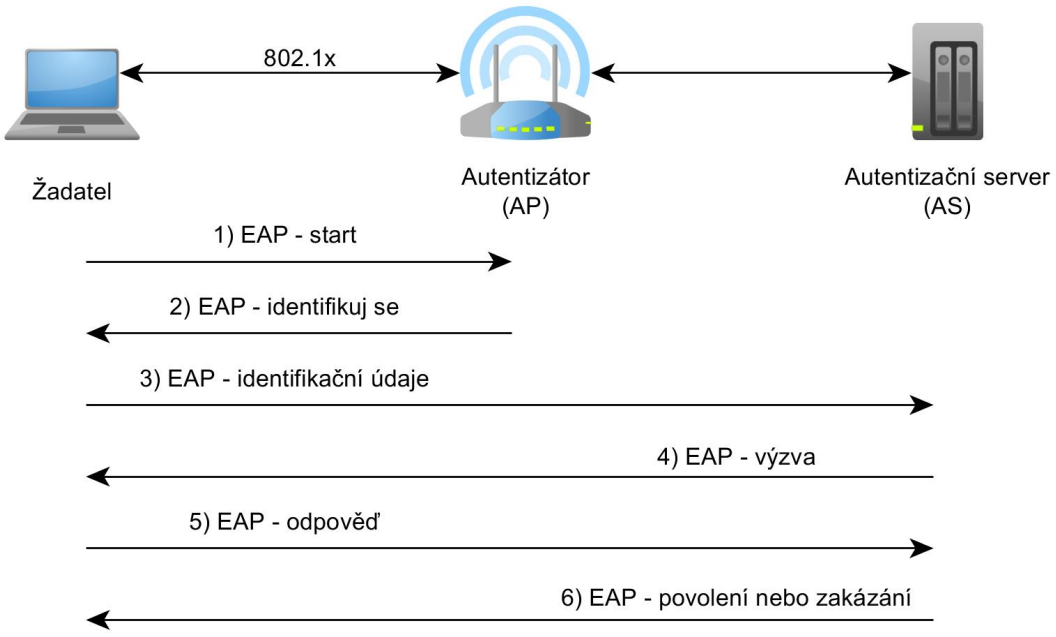
Pr získání přístupu do sítě potřebuje dohodu mezi zařízeními o zásadách, které budou používat. První fázi zahajuje žadatel. Probíhající komunikace je řízená AP, neboli autentizátorem, který blokuje veškerou komunikaci klienta. Aby klient získal přístup do sítě musí se nejdříve autentizovat. Veškerá komunikace v normě 802.1x používá protokol EAP (viz obr. 8.2). Pomocí EAP je zajištěna podpora více autentizačních protokolů. [19, 25, 30]

Autentizátor využívá dvou virtuálních portů:

- **Řízený port** – Po úspěšné autentizaci klienta dochází k odblokování veškerého provozu.
- **Neřízený port** – Blokuje veškerou komunikaci kromě EAP na autentizaci s AS.

Komunikační autentizace k přístupu do sítě je složena ze tří zařízení a 2 částí komunikace. První část komunikace se řeší mezi AP a žadatelem a druhá část mezi AP a AS. Samozřejmě veškerá komunikace mezi žadatelem a AS probíhá skrz AP.

- **1** – Žadatel se hlásí o přístup do sítě, tím autentizátor zašle žadateli paket s žádostí o identifikaci. Žadateli je mezitím povolena pouze komunikace EAP.
- **2** – Neřízený port blokuje všechnu komunikaci kromě EAP na autentizaci s AS.
- **3** – AP přepošle identifikační údaje AS.
- **4** – AS odpoví výzvou k žadateli o ověření například heslem.
- **5** – Žadatel odpoví patřičnými údaji, které zasílá zpět na AS.
- **6** – AS ověří tyto údaje a na základě těchto informací zašle svůj výsledek (úspěšný/neuspěšný) AP. V případě povolení vstupu do sítě se otevře AP daný port pro žadatele na komunikaci v síti.



Obr. 8.2: Autentizace 802.1x/EAP

8.1.1 EAP

EAP je protokol, který podporuje více autentizačních protokolů. V sítích jak bezdrátových tak i drátových našel EAP uplatnění, neboť byl prvně využit v protokolu PPP a zabezpečuje kvalitní autentizační proces mezi žadatelem a AS. EAP povoluje využití více autentizačních protokolů bez toho, aby byly přednastaveny. [19, 24, 30]

- **EAP-MD5** – U tohoto autentizačního protokolu je použito jako přihlašovací údaj jméno a heslo. Přenášené zprávy jsou chraněné hašovací funkcí. Bohužel již delší dobu hašovací funkce MD5 je považována za prolomenou. Heslo je velice náchylné na útoky hrubou silou. Nedochází zde k vzájemné autentizace mezi klientem a AP, ale pouze k ověření klienta. Což podporuje použití útoku MITM. Dále nepodporuje dynamické generování šifrovacích klíčů.
- **EAP-TLS** – Metoda nejvíce rozšířená v bezdrátových sítích. Pomocí TLS je zajištěná vzájemná autentizace komunikujících stran, na základě digitálních certifikátů, které jsou založené na veřejném klíčí PKI. Tato metoda přináší silné zabezpečení. Komunikace mezi zařízeními je prostřednictvím TLS tunelu, což zamezuje odposlouchávání případně MITM. Nevýhodou této metody je, že obě strany musí podporovat PKI certifikáty, což může dělat větší problém při rozsáhlejších sítích.
- **EAP-TTLS** – Jedná se o rozšířenou verzi TLS, která poskytuje silné šifrování. Jedná se o jednoduší řešení, kdy se certifikát používá jen pro autentizaci AS vůči klientvi. Komunikace zde také probíhá v šifrovaném tunelu a klient zde používá přihlašovací údaje jako je jméno a heslo.
- **EAP-PEAP** – PEAP je druhou nejrozšířenější metodou pro autentizaci díky Microsoftu. V mnoha ohledech je PEAP velice podobný vzájemné autentizaci TTLS. Autentizace AS a klienta pomocí digitálních certifikátů probíha pomocí šifrovaného tunelu a použití další metody EAP.
- **Cisco LEAP** – Společnost CISCO vytvořila jednoduší model vzájemné autentizace klienta a AS, který stojí na ověření identity pomocí přihlašovacích údajů. Jedná se o firemní řešení, mezi ostatními výrobci se tento mechanismus příliš neujal.

8.2 Správa klíčů v IEEE 802.11i

Na rozdíl od WEPu, kde se šifrovalo více méně hned pomocí tajného klíče, přichází standard 802.11i se složitějším způsobem šifrování a generování klíčů. Rozdíl mezi WPA a WPA2 nastává při generování klíčů, a tím je výpočet PTK a GTK, u kterých jsou použité rozdílné délky klíčů. Existují dva druhy klíčů, které se dělí podle způsobu použití a jejich časového intervalu k životu. [19, 30]

- **Pairwise-key – Unicast**
- **Group-key – Multicast/Broadcast**

8.2.1 Pairwise-key

U WPA a WPA2 jsou možné dva režimy autentizace a to buďto pomocí PSK, anebo 802.1x/EAP. Každý z těchto dvou možností jinak definuje jak budou generovány klíče. Pokud není použit AS, potom PMK=PSK, pokud-li však je použit AS je PMK odvozen z MSK. Odvození z MSK ovšem záleží na použitém autentizačním EAP protokolu. Mezi AP a klientem je definovaný další klíč a to PTK, který je specifický pro aktuální spojení, což definuje, že při použití více stejných PMK budou i přesto PTK rozdílné. Samostatný klíč PMK nikdy není použit jako proces šifrování nebo ke kontrole dat. Avšak je z něho generován PTK (viz obr. 8.3). [19, 30]

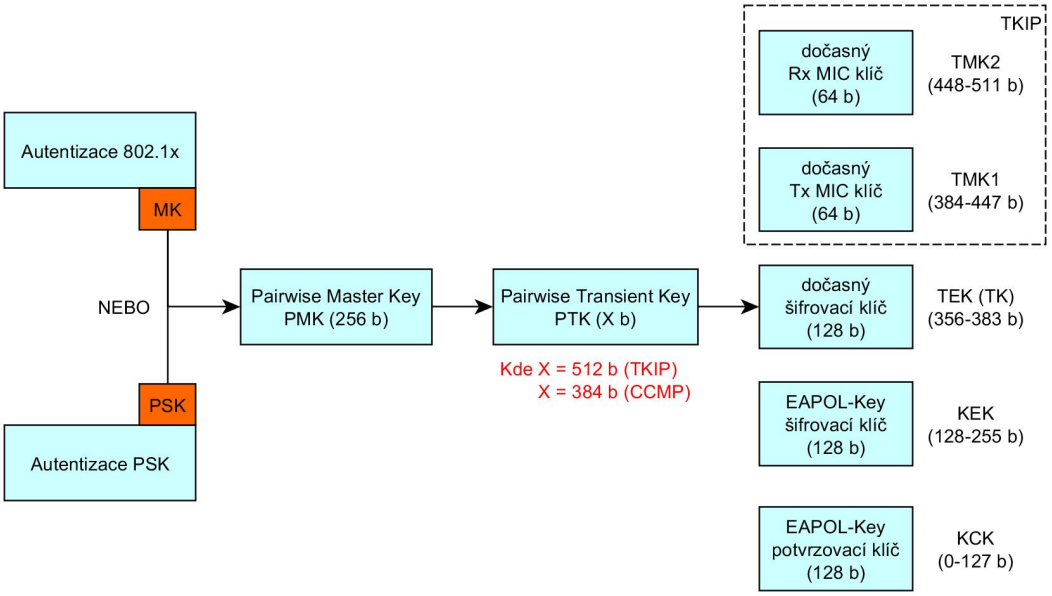
- **KCK** – klíč pro autentizaci zprávy (MIC) během 4- Way Handshake a Group Key Handshake
- **KEK** – klíč pro zabezpečení důvěrnosti dat během 4-Way Handshake a Group Key Handshake
- **TK** – klíč pro šifrování dat (použitý při TKIP anebo CCMP)
- **TMK** – klíč určený k autentizaci dat (MICHAEL v TKIP). Klíč je použitý na každé straně komunikace

8.2.2 Group-key

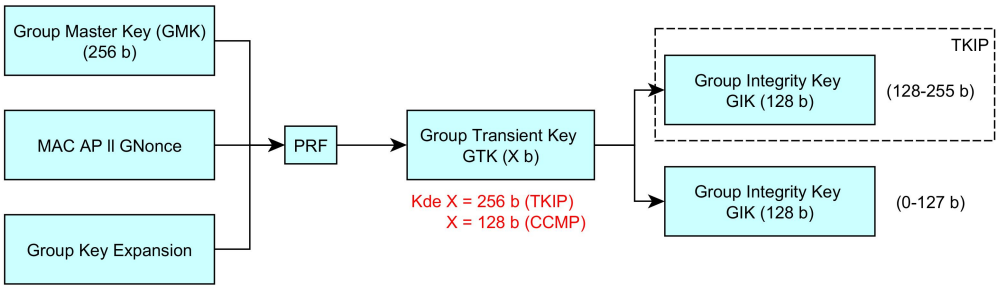
Způsob, který byl uvedený u Unicastu, by se zde dal aplikovat, ale s jistou problematikou (musela by se zpráva šifrovat tolikrát, kolik je aktuálních klientů). Proto je využito pro tuto problematiku odlišného generování klíče v případě Unicastu. Vždy při změně topologie v síti (připojení/odpojení klienta) dochází ke generování ze strany AP nového GTK z GMK, což označuje náhodné číslo generované AP. Následně je každé GTK doručeno každému klientovi v sítí. GTK délka závisí na použitém šifrovacím protokolu. Pro WPA a WPA2 jsou právě tyto délky rozdílné. U WPA (s použitím TKIP) je to 256 b. U WPA2 (CCMP) je zde použito právě 128 b.

GTK je možné rozdělit na dva dočasné klíče (viz obr. 8.4). [19, 30]

- **GEK** – klíč pro šifrování dat v TKIP a CCMP
- **GIK** – klíč pro datovou autentizaci (pouze u algoritmu Michael u TKIP)



Obr. 8.3: Hiearchie párového klíče, Unicast



Obr. 8.4: Hiearchie skupinového klíče, Multicast

8.2.3 PRF

Funkce PRF ve složení se vstupem HMAC-SHA1 generuje klíče v rozmezí 128 b až 512 b. Algoritmus funkce PRF se zvyšuje každým krokem v určitém opakování. Každým krokem je zvětšena délka bitů, dokud není dosáhnuto požadované délky výstupu. Pomocí funkce PRF jsou generovány: TK, KEK, KCK a GTK. Kvůli různým požadovaným délkám výstupu je nutné tyto klíče dělit v závisloti na použití. [19, 30]

- TK pro TKIP (256 b)
- TK pro CCMP (128 b)
- KCK a KEK (128 b)

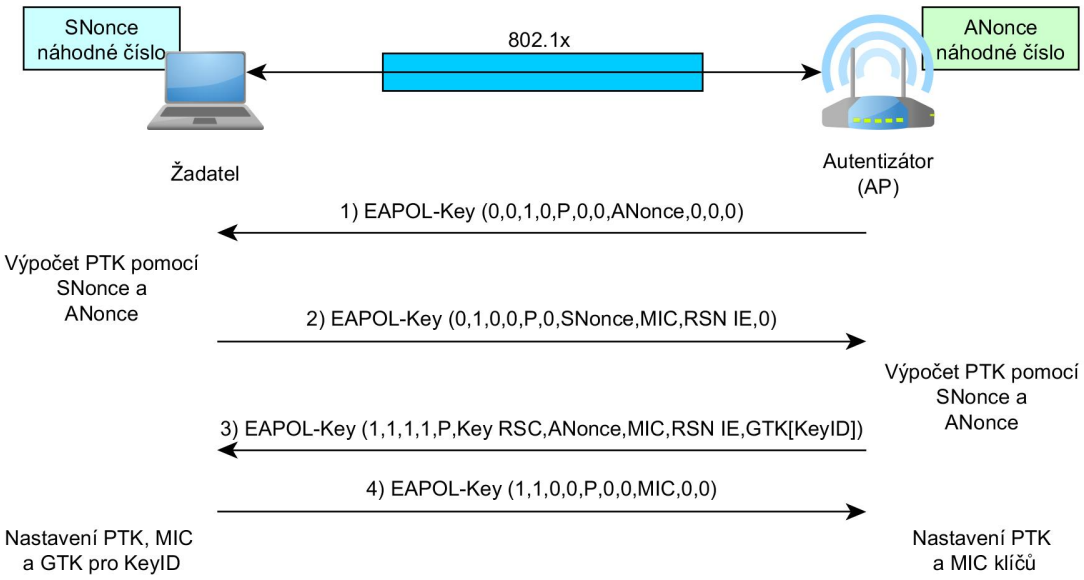
8.3 4-Way Handshake

Protokol, který zajišťuje výměnu dočasných klíčů. Tyto klíče jsou použity k šifrování dat nebo k důvěrnosti spojení a dat. Protokol využívající 802.1x EAPOL-Key [19, 25, 30]

- **S** – zda je dokončená výměna klíčů
- **M** – určuje přítomnost MIC (kromě první zprávy)
- **A** – určuje, zda je vyžadována odpověď
- **I** – výzva k instalování klíče
- **K** – určuje typ klíče (P/G = Pairwise/Group)
- **S/ANonce** – náhodné generované čísla
- **MIC** – kontrolní součet
- **KeyRSC** – klíč RSC
- **RSN IE** – dodatečné informace k výměně klíčů
- **GTK** – zapouzdření GTK
- **N** – index GTK

8.3.1 4-Way Handshake (Unicast)

AP vygeneruje ANonce číslo a pošle jej klientovi v nezašifrované podobě. Po přijetí si klient vygeneruje (SNonce) náhodné číslo a pomocí přijatého čísla a svého vygenerovaného čísla vytvoří PTK a odvodí dočasné klíče. Klient pošle zprávu obsahující číslo SNonce a MIC, vypočítaný z této zprávy, s užitím klíče KCK a posílá jí AP. Po přijetí druhé zprávy na straně AP, AP využije číslo Snounce obsažené ve zprávě a tím pádem je schopný dopočítat PTK spolu s dočasnými klíči. AP zašle zprávu číslo 3 klientovi, tato zpráva obsahuje GTK, které je zašifrováno pomocí KEK a obsahuje MIC, které bylo vytvořeno na základě KCK ze zprávy. Po přijetí této zprávy klient ověří MIC. Po ověření klient zasílá potvrzení o úspěšné výměně a instalaci těchto klíčů. Po obdržení této zprávy na straně AP, si AP opět ověří MIC a poté si taktéž dokončí instalaci klíčů. Celý průběh je zobrazen na obrázku 8.5. [19, 25, 30]

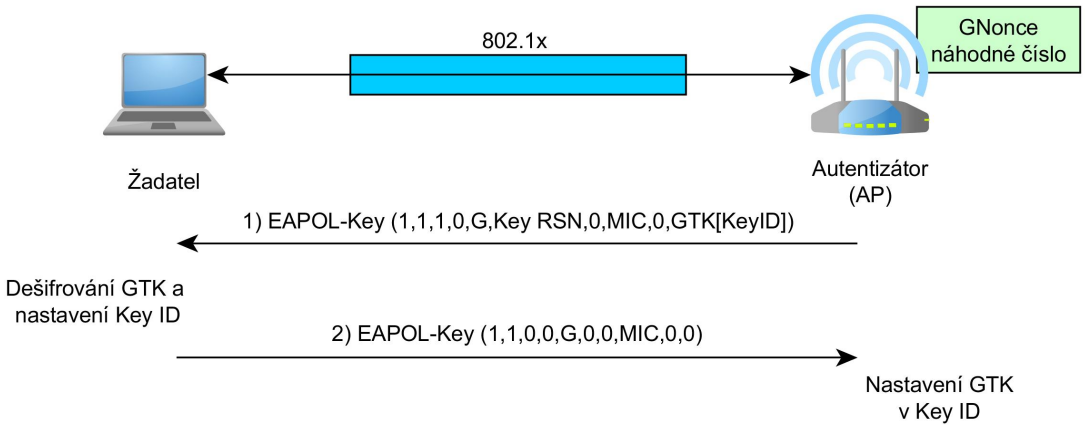


Obr. 8.5: 4-Way Handshake (Unicast)

8.3.2 Group Key Handshake (Multicast/Broadcast)

Při použití Group Key Handshake dochází pouze k výměně dvou EAPOL-key zpráv (viz obr. 8.6). Nutná je komunikace s každým klientem ze strany AP. AP vygeneruje GTK na základě GMK a pomocí funkce PRF vygeneruje náhodné číslo GNonce. GTK je následně zašifrováno pomocí dočasného klíče KEK a posláno každému klientovi v síti. Na straně klientů se ověří MIC a při úspěšném ověření je možno vypočítat GTK a uloží si jej pro budoucí komunikaci. Klienti pošlou AP potvrzovací zprávu, která obsahuje GTK a MIC této zprávy. AP ověří MIC a nakonfiguruje nový GTK.

MIC se počítá a ověřuje pomocí klíče KCK. Pokud nastane změna v topologii sítě a to taková, že se kterýkoli klient odpojí, tak AP vygeneruje nový GMK a Group Key Handshake začíná od znova. [19, 25, 30]



Obr. 8.6: Group Key Handshake (Multicast/Broadcast)

9 WPA

WPA neboli Wi-Fi Protected access ve své době měl nahradit WEP. Na vývoji standardu WPA se podílelo již mnoho lidí před první použitím. Standard WPA již v roce 2002 byl prvně implementován v bezpečnostním protokolu 802.1x pro bezdrátovou distribuci bezpečnostních klíčů. WPA je vytvořen tak, aby jej šlo využít na zařízeních, které ve své době podporovali WEP. Většině těchto zařízení pomohlo vyřešit problém s kompatibilitou nového zabezpečení upgrade vnitřního software.

WPA je jakýmsi prostředním krokem mezi WEP a novým funkčním zabezpečením WPA2. Bylo to dočasné řešení bezpečnosti u WEP a to do doby, než bude schválen standard 802.11i, který byl již v té době ve vývoji, ale dokončen byl až v období, kdy se bezdrátové sítě rychleji a více vyvíjely.

Díky tomu, že WPA je nadstavbou WEP, přebírá tím i některé z jeho nevýhod. WPA používá stále staré šifrování pomocí algoritmu RC4, tím pádem zdědil i jeho nedostatky. Používá již nový protokol TKIP. Tento protokol řeší nedostatky protokolu WEP tím, že zavádí silnější šifrování dat. Také je zde použit nový algoritmus pro výpočet integrity dat, který se jmenuje Michael. Je v něm implementována oboustranná autentizace. Obousměrná autentizace je řešená buďto pomocí 802.1x (EAP) nebo PSK (viz 8). [10, 17]

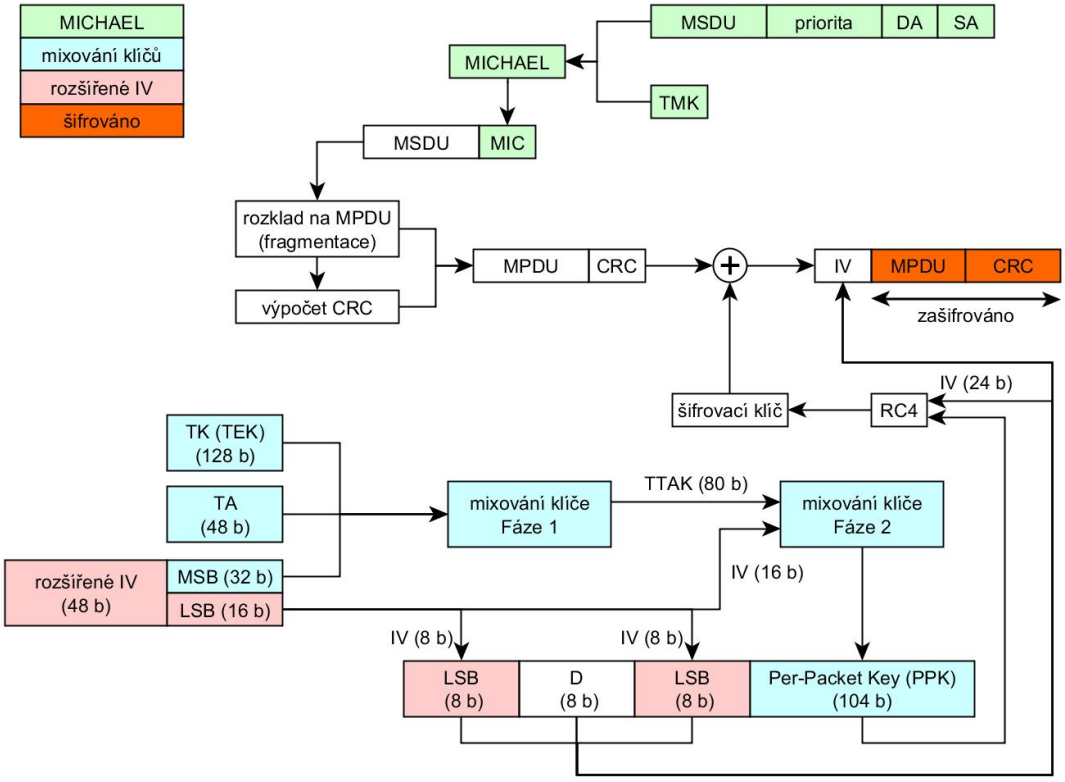
9.1 TKIP

TKIP vydaný jako nový standard pro vylepšení bezpečnosti. Standard pod názvem WPA byl vydán společností Wi-Fi Alliance. TKIP rozšiřuje WEP bez nutnosti měnit HW, stačí pouze update FW. Díky tomuto vylepšení bylo možné na starších zařízeních zvýšit bezpečnost bez nutnosti změny HW. TKIP dědí po svém předchůdci WEPu způsob šifrovaní a to pomocí RC4 a kontrolní součet ICV. Dále je u TKIP vylepšená funkce míchání IV a dočasného klíče. Místo CRC32 je zde využit MIC algoritmus na kontrolu integrity jménem Michael. Kontrolní hodnota se nachází tentokrát v každém paketě. Proti opakovaným útokům je zde zavedeno počítadlo TSC, které dovolí paketům přijít v určitém pořadí, jak odešly od odeslané stanice. [15, 19, 30]

9.1.1 Šifrování

TKIP protokol je nádstavba WEPu. TKIP využívá dvě úrovně kontroly integrity dat MIC a CRC oba kontrolní součty jsou přidané na konec paketu a to nejdříve MIC a po fragmentaci i CRC. Rozšířené IV se používá v přidané funkci mixování klíčů, a taktéž je použito i klasické IV přidáním před odesláním. Výstup mixování klíčů je

PPK, který je spojený s IV, PPK a IV tvoří vstup do RC4, kde výstup je šifrován, výstup z RC4 je nakonec spojen s daty MPDU a CRC do závěrečných šifrovacích dat. K těmto datům se pak přidá IV a data se odešlou (viz obr. 9.1). [15, 27]



Obr. 9.1: Šifrování TKIP

9.1.2 MIC

Kvůli bezpečnostním kriteriím u CRC32 byl využit u TKIP MIC mechanismus, který představuje hašovací funkci Michael. Algoritmus Michael používá pouze bitové posuny a XOR. Kvůli tomuto důvodu není moc výpočetně náročný. Kvůli svému nedostatečnému bezpečí byl aplikován mechanismus na protiopatření, ten je aktivován v případě, že během 60 sekund jsou na přijaté straně detekovány dva špatné kontrolní součty MIC. Pokud tato problematika nastane AP přeruší veškerou komunikaci a odstraní všechny dočasné klíče PTK po dobu 60 sekund. Během této doby se ustanoví nové klíče PTK a po uplynutí 60 sekund je povolena komunikace.

MIC u TKIP je počítán z každého MSDU na rozdíl od CCMP, kde je počítán z každého MPDU. Rozdíl mezi MSDU a MPDU je, že MSDU představuje data před fragmentací a MPDU jsou data až po fragmentaci. MSDU se tzv. rozdělí na několik MPDU.

Na vstupu do hašovací funkce Michael jsou (MSDU) nešifrovaná data, priorita, MAC adresy jak příjemce tak odesílatele a dočasný klíč. Výstupem z této funkce je 64-bitový kontrolní součet MIC. Tento kontrolní součet je dále připojen k přenášeným datům. [15, 27, 30]

9.1.3 IV

U TKIP je využita nová metoda obrany a to sekvenční kontrola (TSC). TSC se inkrementuje s každým paketem. Na přijímači je TSC kontrolována a v případě neshody je paket automaticky zahozen. Díky TSC mechanismu eliminujeme možnost příjmu jiného paketu než s očekávánou hodnotou. U TKIP je použit prodloužený IV, který disponuje délkou 48 b. Tato délka je ještě dělena na dvě poloviny na 16 b a 32 b, neboť TKIP využívá RC4. [15, 19, 30]

9.1.4 Mixování

Pro každý nový paket je zajištěn nový klíč pomocí mixování klíčů. Mixování klíčů probíhá ve dvou krocích, kvůli výpočetní náročnosti, neboť většina těchto implementací běžela na starých zařízeních podporující WEP. Do vstupu při první fázi mixování přichází šifrovací klíč (TK), delší část prodlouženého IV (32 b MSB) a MAC adresa vysílače (TA). Jednoduchost první fáze spočívá v tom, že není zapotřebí počítat výstup (TTAK) stále dokola, ale stačí jej vypočítat v případě změny MSB. Výstup z první fáze je i vstupem do druhé fáze mixování, kde je TTAK přetransformovaný na PPK, který je počítán pro každý paket zvlášť. [15, 19, 30]

10 WPA2

WPA2 je řešen úplně jinak. Je založen na úplně nové architektuře podporující nejnovější bezpečnostní opatření. U WPA2 plně uplatňuje standard 802.11i, který vyšel v roce 2004 a vylepšuje všechny autentizační a šifrovací bezpečnosti. V roce 2006 byl WPA plně nahrazen WPA2. Hlavní změnou oproti WPA je, že využívá symetrickou šifru Advanced Encryption Standard. Někdy se WPA2 označuje jako RSN. Má taktéž nový protokol CCMP pro správu klíčů. Jelikož WPA2 je velice podobný v obousměrné autentizaci ke svému předchůdci WPA, využívá tím pádem také dvou režimů pro autentizaci. Jedná se o autentizaci buďto pomocí PSK nebo 802.1x/EAP (viz 8). V dnešní době patří WPA2 mezi to nejlepší, co může veřejnost dostat. [10, 17]

10.1 CCMP

CCMP je právě tvořen CCM (viz obr. 10.1). K šifrování využívá klíče TEK z PTK. Jehož délka je 128 b. Záhlaví paketu v komunikaci standardu 802.11 musí být přenášeny v nezašifrovaném stavu. Z toho vyplívá že režim CTR bude využit pouze pro datovou část přenášeného paketu. Aby si mohl příjemce ověřit integritu právě nešifrované části (záhlaví) před modifikací, k tomu slouží právě CBC-MAC. CCMP a TKIP jsou si vlastně velice podobné v určitých věcech. Největší rozdíly jsou v nejnižších vrstvách. CCMP totiž šifruje data na úrovni MPDU, ty vzniknou po fragmentaci z MSDU. MPDU u CCMP je zvětšeno o 16 b. CCMP je založené na CCM s AES šifrovacím algoritmem. [15, 19]

Autentizace a správa klíčů mezi zařízeními je velice podobná jako u WPA.

10.1.1 AES

AES je bloková symetrická šifra, která podporuje možnost změny délky klíče 128, 192 a 256 b. Ve standardu 802.11i je definovaná délka klíče i bloku dat na pevnou délku a to na 128 b. Algoritmus AES pomocí matematických a logických operací vytváří šifrovaný blok dat. Aby se mohli vytvářet bloky pevné délky, což v bezdrátových sítích je problém, musí být aplikovány operační režimy blokových šifer. V rámci protkolu CCMP jsou důležité pouze dva a to CTR, který zajišťuje utajení dat a CBC-MAC, který je použit k autentizaci a integritě dat. Společně tyto dva režimy jsou více známy pod označením CCM. [19, 20, 22]

10.1.2 CTR

Činností režimu CTR je rozdělení zprávy do bloků pevné délky. Pro každý blok zprávy je čítač (PN, které je použito jako ochrana před útoky využívající opakované

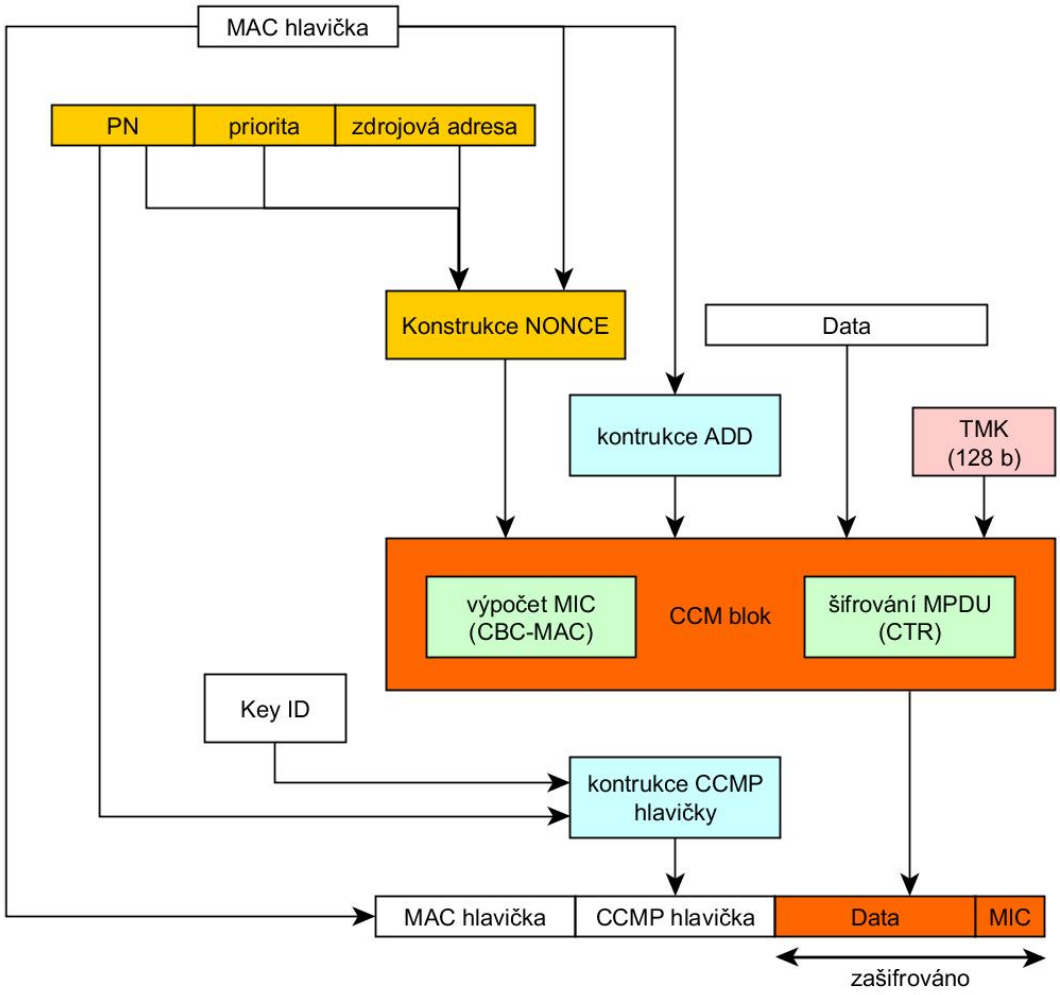
zasílaní zpráv) inicializován na počáteční hodnotu Nonce, což představuje náhodné číslo, které lze použít jen jednou, a každý další blok se inkrementuje o 1. Nesmí se stát, že by čítač označil dvě zprávy stejnou hodnotou, což zajišťuje výše zmíněná inkrementace. Každý blok představuje vstup do operace XOR s použitým číslem Nonce. Výsledkem je šifrovaný blok dat. [19, 20, 22]

10.1.3 CBC-MAC

Režim CBC-MAC funguje pro vytváření MIC, zajišťuje možnost kontroly přijatých dat. U režimu CBC se první blok modifikuje pomocí náhodné inicializace ve funkci XOR. Výstup z funkce XOR je dále šifrován pomocí šifrovacího algoritmu AES, který zašifruje první blok. Další blok je zašifrován pomocí předchozího zašifrovaného bloku, místo inicializační hodnoty, proces takto pokračuje ze všemi následujícími bloky. Tímto systémem docílíme závislosti šifrovacího bloku. To znamená, že změna obsahu bloku vyvolá změnu výstupu. [19, 20, 22]

10.1.4 CCM

CCM stojí na režimech CTR a CBC-MAC a přídává pár jednoduchých úprav pro RSN. Tento režim umožňuje volbou dvou parametrů M a L. M vyznačuje indikovanou velikost MIC. M může nabývat hodnot 4, 6, 8, 10, 12, 14 a 16 B, kdy u režimu CCM v protokolu CCMP je využit M=8. L, což je druhý parametr, je infikovaná maximální velikost zprávy. L může nabývat hodnot v rozsahu od 2 až 8 B. Při využití v režimu CCM v protkolu CCMP odpovídá hodnota L=2. Tato hodnota plně postačuje maximální možné délce MPDU. [19, 20, 22]



Obr. 10.1: Šifrování CCMP

11 WPS

Kvůli většímu počtu uživatelů se základními znalostmi problematiky bezdrátových sítí, kteří si chtěli vytvořit zabezpečenou domácí síť (SOHO), byl vytvořen nový standard. Tento standard byl představen veřejnosti roku 2007. Jedná se o standard, který poskytuje jednoduché nastavení bezdrátových sítí. Cílem WPS je usnadnit uživatelům konfiguraci domácích bezdrátových zařízení. WPS provádí automaticky synchronizaci mezi dvěma bezdrátovými zařízeními.

WPS provádí automatické nastavování zabezpečení. WPS automatický nastaví šifrování pomocí protokolů TKIP nebo CCMP, dále metodu autentizace a konfiguraci SSID. [11, 33, 38]

Mezi AP a zařízením existují čtyři způsoby konfigurace:

- **PIN** – PIN je až osmi ciferné číslo, které bývá uvedeno na štítku, který se nachází na spodní straně zařízení, popř. lze jej změnit nebo vygenerovat. PIN je zadáván na straně nově připojovaného zařízení.
- **PBC** – PBC metoda neboli také pomocí konfiguračního tlačítka, jedná se o metodu, kdy uživatel zmáčkne tlačítko na AP i na novém zařízení, které chce připojit v určitém časovém intervalu.
- **NFC** – nastavení zařízení na velmi krátkou vzdálenost
- **UFD** – pro přenos požadovaného nastavení je využito USB disku.

11.1 Problematika WPS

Vienböck v roce 2011 zveřejnil studii, kde popsal, jak je poměrně lehkým způsobem možné prolomit zabezpečení WPS a díky tomu i odhalit tajný klíč WPA-PSK. Dále odhalil dvě hlavní slabiny v tomto standardu. Na úspěšnou autentizaci je potřeba znát pouze PIN, který se skládá jen z číslic, tím pádem je WPS více zranitelné na útok metodou hrubou silou.

PIN je rozdělen na dvě části, kdy každá část se chová jako nezávislá. Útočník tak útočí na rozdělený 8ciferný PIN kód. První část obsahuje 4 číslice a druhá část pouze 3 číslice, protože poslední 8 číslice je kontrolním součtem. Tím, že je autentizace rozdělena na dvě části, je jednoduší pro útočníka získat rychleji informace, zda jeho kombinace jsou správné. Výrázným nedostatkem WPS je především u starších zařízení, že nelze deaktivovat WPS, protože výrobce neimplementoval žádnou blokovací ochranu.

Vienböck pomocí specializovaného programu Wpscrack, který využívá metody hrubé síly, potřebuje maximálně 4 hodiny k prolomení WPS hesla. V dnešní době existují zveřejněné pouze dva programy specializované na tuto problematiku, nalezneme je pod názvy Wpscrack a Reaver. [19, 33, 38]

11.2 Obrana

Existuje několik druhů zařízení:

- Nemají implementované WPS.
- Některé zařízení (starší) mají implementováno WPS a neumožňují jehovypnutí.
- Určitá část zařízení poskytují vypnutí WPS, ale i přesto stále je tato metoda dostupná. Router se tváří jako, že jej má vypnutý.
- Některé zařízení umožňují vypnutí WPS a přitom dávájí na výběr z dalších autentizačních metod.
- Některé zařízení podporují vypnutí WPS ze stále funkčním PBC.

Výrobci v nových bezdrátových zařízení začali již implementovat lepší ochranu. Jedná se o možnost deaktivace WPS popřípadě výraznějšího exponenciálního nárůstu časového intervalu při zkoušení PINu právě metodou hrubou silou. Někteří přišli k drastičtější metodě, a to pokud neuhodnete PIN do určitého počtu pokusů, je WPS automaticky deaktivováno. [19, 38]

12 POPIS APLIKOVANÝCH ÚTOKŮ

12.1 Útoky na WEP

Tyto útoky můžeme rozdělit na několik druhů od pasivního poslouchání na síti, až k aktivnímu zapojení do prolomení této sítě. Útoky dále dělíme podle toho, na jaké známé chyby se zaměřuje. Útoky na WEP se dělí do dvou hlavních kategorií. První kategorie se specializuje na útok na protokol WEP (Chopchop, Fragmentační a Indukční Arbaugh útok). Druhou skupinou jsou útoky využivající slabin algoritmu RC4, proto je nazýváme útoky na RC4 (FMS, KoreK, PTW).

12.1.1 Chopchop útok

Tento útok nám dokáže dešifrovat WEP data bez znalostí klíče. Tento útok funguje i proti dynamickému WEPu. Chopchop útok je vlastně inverzní induktivní Arbaugh útok.

Možnost útoku spočívá v linearitě RC4 a CRC. Poslední bajt datové části odebereme, přepočítáme ICV. Paket vyšleme do sítě. Pokud dostaneme odezvu (AP na něj odpoví) znamená to, že jsme postupovali správně. A pokračujeme interativně. Některé druhy paketu nelze dešifrovat celé, protože po dosáhnutí malé délky přestanou dávat smysl a nedostaneme žádnou odezvu. Aby celý proces běžel rychleji, nebude se čekat na odezvu každého paketu, ale očíslujeme si pakety pomocí cílové MAC adresy.

Snahou je zamezit opakovanému výskytu množství paketů se stejným IV, vůči tomuto útoku jsou AP více náchylné na zahazovaní paketů kratších než 60 bajtů, nebo použití RSN. [7, 9, 32]

12.1.2 Fragmentační útok

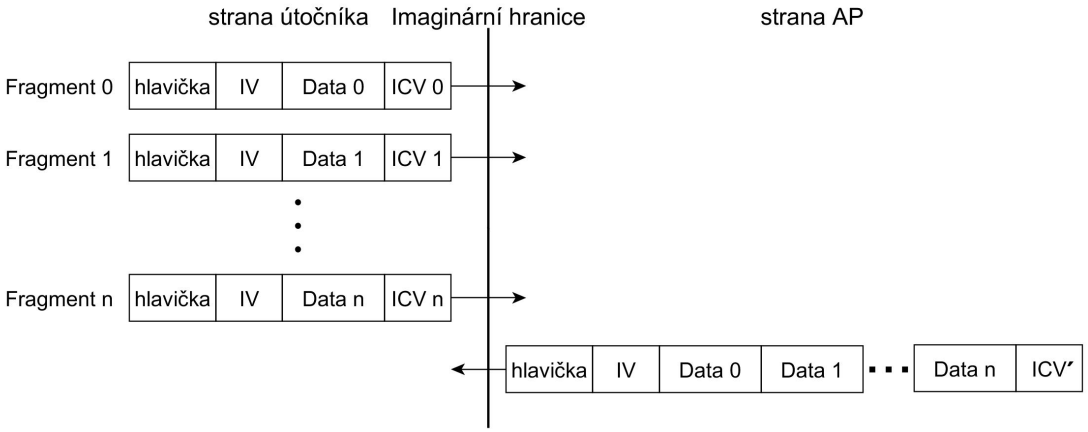
V roce 2005 Adrea Bittau představil tento útok. Zde je zapotřebí jeden vhodně zachycený paket. Výhoda je v rychlosti tohoto útoku, díky němuž lze získat dlouhé šifrovací klíče.

Útok spočívá na fragmentaci a následné defragmentaci paketů (viz obr. 12.1). Fragmenty se zpracovávají až u AP, kde je AP zpracuje tím, že je spojí tzv. defragmentuje je. Takto defragmentované pakety pak přeposílá dál. AP pozná o jaké fragmenty se jedná, neboť tyto fragmenty mají stejný IV. Tento přeposlaný paket odposlechneme.

Z každého paketu je útočník schopný získat 8 bajtů šifrovacího klíče. Je možné zaslání až 16 fragmentů zašifrovaných pomocí stejného sdíleného klíče. Útočník může poslat 64 bajtů dat v 8 bajtových fragmentacích bez znalosti šifrovacího klíče.

Těchto 64 bajtů může útočník využít na to, aby před zachycený paket X přidal hlavičku IP protokolu a odešle ho přístupovému bodu. AP potom paket dešifruje a v otevřené podobě pošle na IP adresu v hlavičce. Jestliže útočník vybere IP adresu jím kontrolovanou, dostane dešifrovaný obsah paketu X. Pomocí jeho obsahu může navíc zjistit, jakým sdíleným klíčem byl zašifrován. [1, 9]

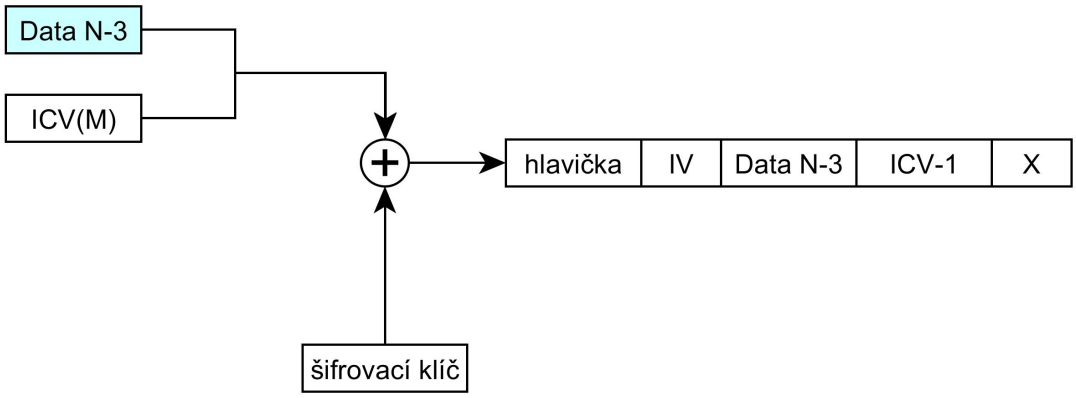
Fragmentace se dají využít i na zrychlení předchozích útoků na protokol WEP.



Obr. 12.1: Fragmentační útok

12.1.3 Indukční útok Arbaugh

Pomocí zachytávání paketů jako jsou ARP, DHCP, které jsou běžnou komunikací na síti, je možné získat N bajtů PRGA pro dané IV. Takto lze vytvořit paket, který bude mít data délky N-3, pro které vypočítáme ICV a připojíme z něho jen 3 bajty. Připojíme ještě další bajt, který označíme jako X. Takovýto paket (viz obr. 12.2) vyšleme do sítě. Pokud dostaneme odezvu na takovýto paket znamená to, že hodnota X je správná. N+1 bajt RC4 vypočítáme jako X XOR 4. Bajt ICV. Pro získání 1 bajtu je 256 možností. Získali jsme správných N+1 bajtů RC4 a indukčním způsobem můžeme pokračovat až do požadované délky. [1, 9]



Obr. 12.2: Indukční útok Arbaugh

12.1.4 FMS

Jedná se o útok na slabiny algoritmu RC4, kdy FMS útok používá slabiny v části zvané KSA. Používá takového IV, který dovoluje útočníkovi získat první bajt ze šifrovacího klíče z algoritmu KSA. Po odchycení dostatečného množství dvojic stejného IV je možné odhadnout WEP klíč. Časově může tento útok zabrat i několik dní k posbírání dostatečného množství dvojic IV. Vše záleží na hustotě provozu v dané síti. [7, 9, 32]

12.1.5 KoreK

V roce 2004 publikoval KoreK způsob prolomení RC4. A to tím, že se zaměřil na přesné hodnoty IV v souvislosti s tím, jak ovlivňují KSA. KoreK využívá optimalizovaného FMS útoku a invertního induktivního útoku Arbaugh. [7, 32]

12.1.6 PTW

V roce 2007 byla zveřejněná práce od Erik Tews, Andrei Pyshkin a Ralf Phipipp Weinmann, která rozšiřuje Kleinův útok na WEP. Jedná se o útok na RC4, který byl publikovaný již v roce 2005. Ta říká, že existuje větší vzájemný vztah mezi výstupem a vstupem do algoritmu RC4. PTW zachytává pakety, z nichž získává IV. Tato má výhodu, že nepotřebuje tolik stejných párů IV, aby bylo možné dopočítat klíč. Používá metodu pravděpodobnosti k zjištění klíče. Zde se čas zkrátil na několik minut. [7, 32]

12.2 Útoky na TKIP

12.2.1 Beck–Tews útok

V roce listopadu roku 2008 byl vydán dokument, ve kterém byl zveřejněn útok na TKIP. Nejedná se o útok, který dokáže zjistit heslo sítě jako takové, ale využívá slabosti sítě šifrované právě pomocí TKIP. Útočník dostane šifrovací klíč a MIC hodnotu. Útok požaduje povolení QoS. Protokol QoS se snaží zajistit kvalitu přenášených služeb. QoS umožňuje použití několika kanálů (8), kdy každý kanál má své počítadlo TSC. Pro většinu provozu je použit kanál 0. Daná TSC hodnota se vždy inkrementuje pokud daným kanálem projde paket. Proto je možné aplikování modifikace zachyceného paketu z kanálu s vyšším TSC na kanál s nižším TSC.

Pro útok je potřeba Key Renewal Interval (čas nutný na výměnu klíče), jedná se o interval platnosti klíče PTK. Pokud TKIP zjistí nesrovnalost mezi MIC a ICV hodnotami, kdy ICV je správné, ale MIC je špatně, je vyhlášen pokus o útok. Kvůli své vnitřní bezpečnosti na straně AP přeruší veškerou komunikaci na dobu jedné minuty. Po uběhnutí jedné minuty AP vygeneruje novou sadu dočasných klíčů a každý klient se musí znova autentizovat. Útočník avšak musí této možné situaci předcházet, ale paradoxně dostává útočník tímto potvrzení, že postupuje správně.

Nejdříve útočník provede deautentizaci klienta, klient se musí znova přihlásit pomocí 4-Way Handshake, poté útočník odchytne pakety 4-Way Handshake a následně ARP a DHCP pakety. Po odposlechu ARP paketu provede upravený Chopchop útok k obnovení ICV a MIC paketu.

Útočník musí obejít MIC opatření, proto byla vyvinuta upravéná verze Chopchop útoku, která pracuje následově. Útok probíhá při odesílání dat z AP ke klientovi. Odstraní se poslední bajt přenášeného paketu tak, jak funguje obyčejný Chochop útok. Poslední bajt datové části odebereme a odhadneme ICV zkráceného paketu, Pokud dostaneme správné ICV, ale špatné MIC, to způsobí, že klient pošle MIC zprávu o selhání. Pokud útočník získá tuto zprávu, ví ,že byl jeho odhad správný. Po obdržení této zprávy musí útočník počkat 60 sekund, aby předešel opatření MIC. Následně pokračuje interaktivně.

Až útočník provede výše zmíněný upravený Chopchop útok, čeká na něj již poslední část packetu a tím se stává zjistění IP adresy, která se získává odhadem. Nejčastěji jsou použité IP adresy pro lokální sítě. Po zjištění IP adresy nakonec obrátí algoritmus Michael a získá MIC klíč. Když už útočník zná šifrovací klíč a MIC klíč, je útočník schopný dešifrovat všechny zprávy probíhající v síti. [15, 27, 30]

12.2.2 Ohigashi-Morii útok

Jedná se o vylepšenou verzi Beck–Tews útoku s použitím MITM. Tento útok odstraňuje nutnou podmínku podpory QoS ze strany AP. Během použití MITM útoku klient zaznamenává výpadek komunikace s AP. [28, 30]

Existují tři druhy režimu útoku:

- **Repeater mode** – jedná se o obyčejné přeposílání nezměněných SSID Beacon zpráv. Tento mód je použit jako pauza mezi dvěma použitými MIC recovery mode
- **MIC recovery mode** – režim, který má získat MIC a kontrolní součet pomocí Chopchop útoku. Pravděpodobná doba trvání 12 až 15 minut
- **Message falsification mode** – jedná se o falšování šifrovaných zpráv pomocí získaného MIC klíče. Pomocí této metody je možné prolomení TKIP do 4 minut, pokud je cílem ARP paket

12.2.3 Michael Reset Attack

V roce 2010 Beck zjistil, jak provést útok založený na nedostatcích v algoritmu Michael v TKIP protokolu. Beck objevil, že pokud vnitřní stav Michael algoritmu dosáhne určité hodnoty, tak umožní útočníkovi resetovat vnitřní stav MIC. MIC klíč je délky 64 b, který je rozdělen na polovičku a vznikají dvě stejné části o délce 32 b. Tyto dvě části tvoří vnitřní stav, který slouží k vytváření následujících 32 b slov. Pokud vnitřní stav algoritmu Michael dosáhne bodu, kdy dvě interní slova dostanou stejné hodnoty jako na začátku, tak dostane zprávu, na které právě proběhl on algoritmus, by neměl mít vliv na hodnotu MIC dané zprávy (MIC by měl být stejný jako na začátku). Pro vytvoření hodnot magických slov je nutné, aby pro útočníka, který připojí na začátek libovolného paketu se známou hodnotou MIC, byly vytvořeny hodnoty vnitřních slov tak, aby byly rovné vnitřním stavům. Útočník na výpočet těchto dvou magických slov použije inverzní Michael algoritmus a hodnoty vnitřních stavů. Během tohoto procesu je zjištění druhého vnitřního slova, že je zapotřebí druhé magické slovo, které je ve funkci XOR s prvním vnitřním slovem. Útočník již zná druhé vnitřní slovo. Útočník pokračuje hrubou silou, kde hádá první magické slovo, které je ropvno hodnotě druhému vnitřnímu slovu. Po uhodnotí této hodnoty, je možné pomocí Michael algoritmu dopočítat i druhé vnitřní slovo a pomocí inverzního Michael algoritmu zjištění hodnoty tohoto vnitřního slova. Pomocí této hodnoty ve spojení s funkcí XOR a druhým magickým slovem, útočník získává i druhé magické slovo. Pomocí těchto dvou známých magických slov je útočník schopný resetovat vnitřní slova Michael algoritmu. [6, 27]

12.2.4 Vylepšený útok na TKIP

Jedná se o útok využívající ACK DHCP pakety. Na rozdíl od obyčejného útoku Beck–Tews, který využívá pouze k dešifrování ARP pakety a odchytává je v komunikaci od AP ke klientu, které jsou delší a jsou taktéž jednoznačné svou jasnou délkou v síti. V roce 2009 byla zveřejněná práce, kde je právě tento útok popsán. Autory jsou Halvorsen a Haugen. Tento útok umožňuje útočníkovi provést sofistikovanější útok, a tím i získat delší šifrovací klíč. [15]

12.2.5 Hole 196

Jedná se o slabinu v zabezpečení WPA/WPA2 jak řešení domácího použití (PSK), tak i pro podnikovou sféru WPA/WPA2 Enterprise, kde tato slabina je mnohem větším rizikem než při použití PSK. V roce 2010 přišel Sohail Ahmad, když objevil na posledním řádku (196) ve standardech 802.11 „díru“. Nejedná se o útok, který dokáže obnovit tajný klíč. Útočník musí být autentizovaným uživatelem sítě. Jedná se o útok, který je znám jako MITM. Útočník nejprve odposlechne Multicast, který je vysílán celou sítí, aby získal GTK klíč. Po odchycení GTK klíče útočník vytvoří falešné AP. Potom rozpošle ostatním klientům, že si mají aktualizovat ARP tabulky. Takto budou všichni klienti přeposílat všechnu jejich komunikaci (na MAC adresu útočníka) přes útočníka. Tímto způsobem získá útočník dešifrované pakety pravým přístupovým bodem, který zašifruje pakety jeho klíčem (PTK). [30, 37]

12.2.6 WPA migration mode

V červenci roku 2010 byl představen tento útok. Nejedná se o útok na zabezpečení TKIP jako takový, ale na implementaci WPA migračního módu na CISCO zařízeních. Pomocí WPA migračního módu na zařízeních rodiny CISCO je možné připojení klienta jak skrz WEP, tak i TKIP zabezpečení ke stejnému SSID. A zde nastává problém. Jakožto WEP je využit na nejnižší vrstvě ochrany, tak i zde vznikají největší rizika. AP si vede vnitřní informace o klientech a jimi používaného šifrování. Aby mohl útočník využít této slabiny, musí nejprve zjistit zda dané zařízení disponuje tímto módem a jestli jej má zapnuté. Všechny potřebné informace však jdou zjistit z beacon paketu, kde jsou uvedené záznamy o použitých šifrách, které jsou použity na šifrování Multicastu a Unicastu. Pokud zanalyzujeme tento paket a zjistíme, že u Multicastu je použit WEP a u Unicastu TKIP, tak potom dané AP disponuje touto implementací.

Jeden ze dvou možných útoků cílených na tento mód je použití útoku na zabezpečení WEP, jestliže daný uživatel používá právě WEP. Rozdíl u tohoto toku spočívá v tom, že útok probíhá proti klientovi.

Jestliže není připojený žádný klient, který by využíval právě šifrování pomocí WEPu, musí se útočník autentizovat vůči AP a čekat než AP vyprodukuje ARP paket, který následně zachytí a modifikuje jej a takto modifikovaný ARP paket pošle zpět AP. Pomocí tohoto ARP požadavku AP vygeneruje pakety šifrované pomocí WEP, které útočník zachytí. Útok pokračuje do té doby, kdy útočník získá dostatečné množství zachycených paketů, pomocí nichž dokáže získat WEP klíč. [1, 27]

12.3 Útok na WPA/WPA2 – PSK

Útok spočívá v tom, že útočník musí uhodnout heslo (PSK) sítě. Celý útok potom spočívá na složitosti použitého hesla. Pokud se bude jednat o slabé heslo, bude vysoká pravděpodobnost, že bude toto heslo obsaženo ve slovníku. Cílem celého tohoto útoku je odchycení paketů 4-Way Handshake. Slabinou v řešení 4-Way Handshake je, že obě náhodně generované čísla jsou přenášené v otevřené podobě. Útočník zachytí právě tuto komunikaci a dále hádá. Útočník ovšem může čekat na odchycení této komunikace nebo může zahájit deautentizaci klienta vůči AP. Následně útočník porovnává jeho vypočítaný MIC s MIC odchycené zprávy, dokud nebudou tyto dvě hodnoty stejné. Pokud jsou tyto dvě hodnoty stejné, útočník našel požadované heslo (PTK). Při odhalení PTK je velice jednoduché dopočítat zbylé hodnoty KCK, KEK a MIC.

Útok avšak záleží na výpočetním výkonu útočníka, kterým disponuje, dále zda je heslo obsaženo v jeho slovníku. Pokud by útočníkův slovník nedisponoval hádaným heslem. Je možnost využití útoku hrubou silou (brute–force). [1, 27, 30]

13 PŘEHLED RŮZNÝCH ÚTOKŮ

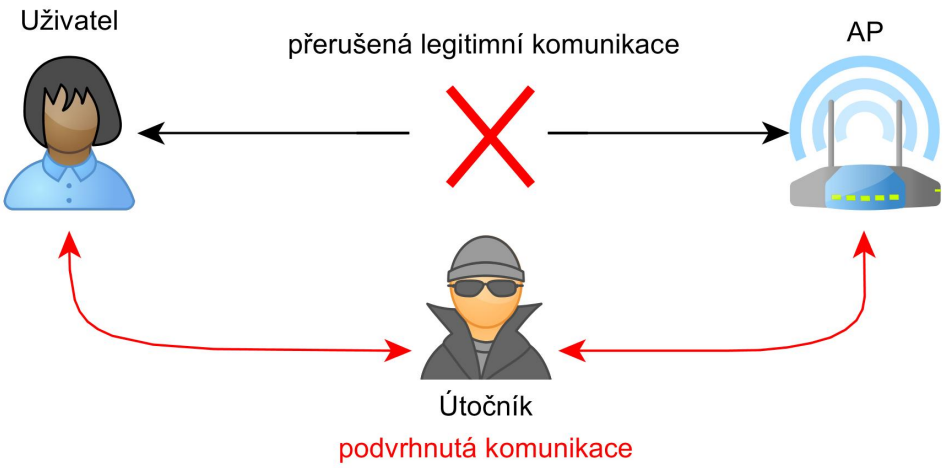
V dnešní době je kladen velký důraz na bezpečnost bezdrátových sítí. Abychom se mohli spolehlivě bránit, musíme znát, jaké jsou možné metody útoků.

Mezi nultou skupinu patří fyzický útok, kdy útočníkem se může stát kdokoliv.

Prvním definovanou skupinou je tzv. sniffing neboli sběr dat. Tímto způsobem většina útoků začíná. Útočník se snaží vždy získat co nejvíce informací, které může záhy použít na další útoky.

Další druh útoku funguje na principu, který se zakládá na krádeži identity a spočívá v tom, že útočník se tváří jako autorizovaná osoba. Nejčastějším případem je krádež MAC adresy. Nebezpečí tohoto útoku spočívá v tom, že je útočník těžce dohledatelný.

MITM označuje útočníka uprostřed, který se snaží odposlouchávat medium aktivně. Tím, že na sebe vezme podobu (viz obr. 13.1) uživatele pro AP a pro uživatele se tváří jako AP, všechna komunikace prochází tímto „středem“. Tento útok je sice mírně náročnější, ale zato efektivnější.



Obr. 13.1: MITM

Slovníkový útok, jedná se o útok, který funguje na principu uhodnout heslo pomocí předem připravených seznamů. Tato metoda je efektivnější, než metoda hrubou silou (brute–force). Neboť u metody hrubou silou se snažíme dostat klíč generováním systematické množiny všech možných klíčů, aniž bychom dešifrovali provoz.

Útok jménem DDoS je mírně odlišný od ostatních. Jedná se o útok, kdy se útočník snaží o zablokování sítě vlivem nadměrného provozu.

Všechny tyto zmíněné útoky se dají kombinovat. [1, 9, 10, 23, 39]

14 MOŽNOSTI ZLEPŠENÍ OCHRANY

Samozřejmě záleží pokaždé na umístění sítě, zda se jedná o poklidné městečko, kde naleznete 4 Wi-Fi sítě v rozsahu nebo se jedná o rušné město nebo podnikovou sféru, kde budou jistě nastaveny jiné priority v zabezpečení. Pokud chceme a dovoluje nám to naše zařízení, je možné použít lepší šifrování v podobě WPA nebo ještě novějšího WPA2. Pokud pracujeme z domu, určitě budeme potřebovat řádné zabezpečení. Protože starší zařízení nedisponují lepším zabezpečením, zaměříme se především na to, jak zlepšit bezpečnost u Wi-Fi s protokolem WEP. Některá nastavení popsaná níže můžeme brát a aplikovat všeobecně u bezdrátových sítí a nejen u WEP.

Jako jedna z prvních věcí je nastavení hesla, které by mělo být dosti dlouhé a složité. Heslo by mělo být složeno z malých a velkých písmen abecedy v kombinaci s číslicemi. Jedná se o dobrou ochranu před slovníkovými útoky, kdy může obyčejný soused zkoušet, zda se mu nepovede prolomit vaši síť.

Za další výhodu můžeme považovat, že WEP jako takový disponuje několika úrovněmi šifrování. Proto nejlepší je nastavení co nejlepšího šifrování. Pokud použijeme nejlepší šifrování, které nám nabízí naše zařízení, musí útočník nasbírat více dat než při slabším šifrování. Můžeme místo všesměrové antény použít směrovou anténu, kterou budeme směřovat jen do určité oblasti, kterou potřebujeme pokrýt. Další možností je vypnutí vysílání SSID sítě. To znamená, že naše síť bude tzv. „neviditelná“. Tímto můžeme nebezpečí útoku omezit, nikoli však eliminovat, protože síť jen přestala vysílat svůj název. Další možnou obranou je nastavení na zařízení, a to filtrování a přihlašování pomocí MAC adresy. Jedná se o tabulku, která se nachází v našem zařízení, kde podle této tabulky s MAC adresy filtruje připojené zařízení. Následně jim je přístup povolen, či zakázán. Poslední specifikovanou, i když dosti složitější obranou, je přechod ke službě, která využívá virtuální privátní síť známou jako VPN. Tato síť zajišťuje bezpečné šifrování. [14, 23, 31]

15 APLIKOVANÁ ČÁST

Aplikovaná část je zaměřena na simulování útoků na šifrovací protokoly WEP a TKIP a jejich důkladné popsání. Dále je ukázán a popsán útok hrubou silou a útok pomocí slovníkového útoku. Pro útoky bylo zapotřebí mít dostatečný hardware i software pro provedení. Pro tuto příležitost byl vybrán notebook, kvůli mobilitě, na který byl nainstalován potřebný software. Dále byla využita externí Wi-Fi karta se směrovou anténou. Bylo využito zařízení, na kterém byl směřován útok. Nejlepší volbou byl router, který je využíván v domácnosti.

15.1 Použitá zařízení

- Notebook MSI CX 640
- Externí Wi-Fi karta alfa AWUS036H
- Směrová anténa Yagi 16 vBi 2,4 GHz NF
- Router TP-LINK TL WE841ND

15.1.1 Externí Wi-Fi karta Alfa AWUS036H

Alfa AWUS036H -1- WiFi Wlan 1000 mW b/g 2,4 GHz s aircrack packet injection je speciální vysoce citlivá a výkonná Wi-Fi karta pro bezdrátové sítě s čipem Realtek RTL8187L. Bylo vybráno toto zařízení, neboť je podporováno jak u MS Windows operačních systémech, tak i u Backtrack Linuxu. Kartu můžeme vidět na obrázku 15.1 funkčního zapojení. Tato Wi-Fi karta disponuje až 10x silnějším výkonem, než je povoleno v České Republice a ostatních státech v rámci EU. V ČR je nutné nastavit vysílací výkon na max. 100 mV, pokud chceme tuto kartu využívat v souladu se zákonem. Pro experimentální účel byla karta nastavena na plný výkon. [2]

15.1.2 Směrová anténa Yagi 16 vBi 2,4 GHz NF

Směrová anténa Yagi 16 dBi s horizontální a vertikální polarizací je vhodná jak do venkovních podmínek, tak také do vnitřního použití. Anténa je uvnitř plastového obalu, který ji chrání. Pracuje na frekvenci 2,4 – 2,5 GHz. Její vyzařovací úhel je zhruba mezi 25 až 30°. Anténa je zobrazena na obrázku (viz obr. 15.1) funkčního zapojení. [3]

Obr. 15.1: Funkční zapojení

15.1.3 Router TP-LINK TL-WE841ND

Jedná se o router podporující standardy 802.11 b/g/n. Jeho nejrychlejší teoretická rychlost může být až 300 MB/s. Přenosová rychlost je automaticky přizpusobována přenosovým podmínkám. Má v sobě zabudovaný stavový SPI firewall. Což znamená, že je schopen rozlišovat různé stavy paketů v rámci jednotlivých relací. Router disponuje dvěma všesměrovými anténami o síle každé z nich 5 dBi Jeho celkový výstupní výkon je 20 dBm. [8]

15.2 Použitý software

- BackTrack 5r3
- VirtualBox 4.2.18 r88780

15.2.1 BackTrack

BackTrack Linux, dále jen BT, jak již název napovídá, je speciální distribucí Linuxu zaměřující se na bezpečnosti a to na všech úrovních, od nováčka až po odborníka. Distribuce BackTrack vznikla sloučením dvou konkurenčních dřívějšími verzemi živých distribucí Linuxu zvané Whoppix a IWHAX.

Jedná se o největší sbírku nástrojů využívající celou řadu různých programů na otestování úrovní zabezpečení zařízení, sítě atd. Najdete v něm nástroje používané bezpečnostními odborníky, ale také obyčejnými uživateli. Dnes je využíván bezpečnostní komunitou po celém světě.

Výhoda BT je, že se nemusel instalovat, pokud nechcete. Tím pádem po něm nezůstávají žádné zbytky na počítacích, kde byl používán. Jedním z důvodů proč

byl BackTrack tak populární, byla jeho anonymita.

V současné době je BT 5r3 zastaralý a nemá již podporu. Ale je možné najít jeho nástupce KALI Linux od stejných vývojářu. Avšak pro simulování a testování dané problematiky této bakalářské práce bohatě postačí BT. [5, 21]

15.3 Provedení útoku

Byly simulovány a popsány útoky pomocí BT nainstalovaného v počítači. Prvně bylo prováděno nastavení Wi-Fi karty pro útoky a dále je popsán útok po útoku jak probíhaly, popsány vč. zadaných příkazů do terminálu.

- **Útok na WEP** – U útoku na zabezpečení WEP byl použit PTW útok s aplikovanými ARP pakety, PTW je útok, který pasivně odposlouchává dané medium. Vychází ze zachycených ARP paketů, avšak rychlost prolomení záleží na hustotě provozu v dané síti.
- **Útok na TKIP** – Při tomto útoku byl použit Beck–Tews útok, který využívá vylepšeného Chochop útoku. Útok je ze začátku závislý na dostatečně hustém provozu.
- **Útok na WPA/WPA2 – PSK** – budou ukázany dvě metody (slovníkový útok, brute–force) prolamování a popsány
- **Útok na WPS** – jedná se o útok hrubou silou

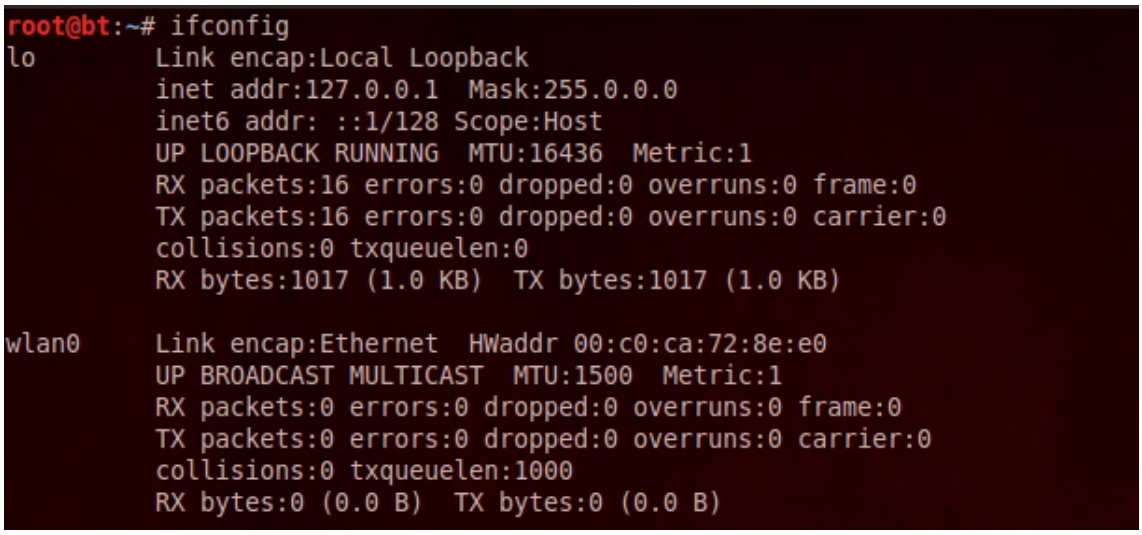
15.4 Základní nastavení

Po přihlášení se do BT je nejdůležitější zapnout a nastavit Wi-Fi kartu do monitorovacího módu. Je to stav, který nám umožňuje sledovat veškerý provoz kolem nás. Wi-Fi karta nic nevysílá, jen pouze odposlouchává veškerou komunikaci. Některé karty dokonce podporují vytvoření a následné vysílání libovolného rámce. Některé útoky přímo tyto karty potřebují.

Pro všechny nástore uvedené v kapitole aplikované části, použité v BT. Existuje mnoho způsobů nastavení a možností. Většinu těchto nastavení je možné zjistit pomocí názvu daného nástroje a napsání příkazu --help za tento nástroj.

Nejprve je nutné zjištění a zprovoznění dané síťové karty, v tomto případě se jedná o USB Wi-Fi kartu. Následujícím příkazem (viz obr. 15.2) zjistíme, zda je tato karta připojena a jakou má MAC adresu. [1]

```
ifconfig
```

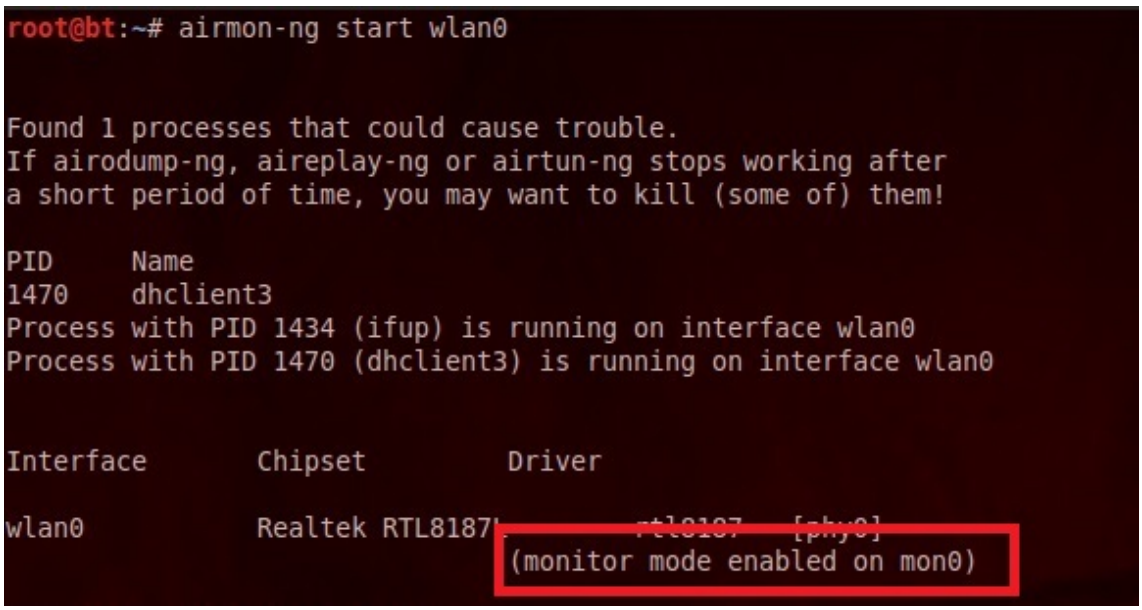


Obr. 15.2: Ifconfig

Do monitorovacího stavu je karta přepnuta pomocí následujícího příkazu:

```
airmon-ng start wlan0
```

,kde wlan0 je název bezdrátové karty, samozřejmě se může jmenovat i jinak, záleží na okolnostech na obrázku 15.2 je již zobrazená MAC adresa Wi-Fi karty. V našem případě se jedná o rozhraní wlan0. Toto nastavení nám přepne kartu do monitorovacího stavu. Jako je zobrazeno na obr. 15.3.

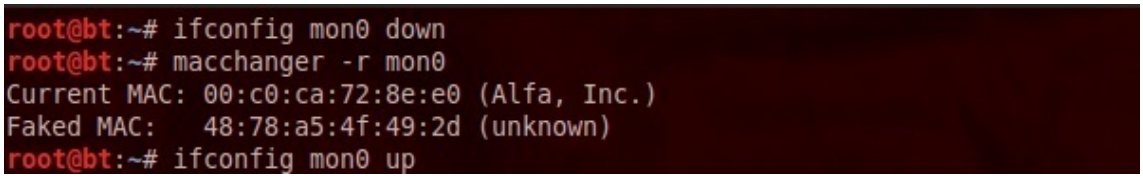


Obr. 15.3: Monitorovací režim

Kvůli špatné zpětné dohledatelnosti podvrhnuté MAC adresy využijeme této situace a změníme MAC adresu naší externí karty pomocí násedující kombinace. Jako je zobrazeno na obr. 15.4.

```
ifconfig mon0 down
macchanger -r mon0
ifconfig mon0 up
```

Výše zmíněné příkazy shodí rozhraní mon0, následně je aplikována náhodná MAC adresa na právě toto rozhraní a pak je zpětně spuštěno s dispozici náhodně vygenerované MAC adresy.

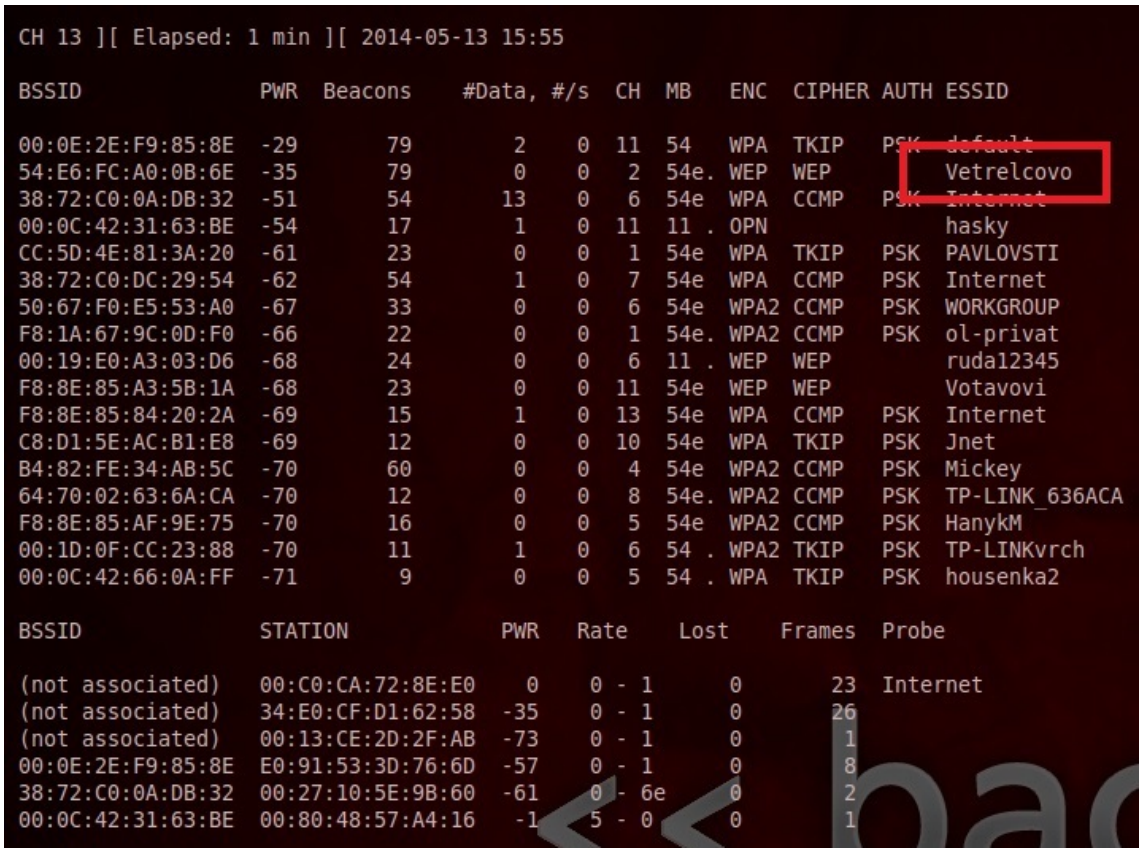


Obr. 15.4: Macchanger

Od této chvíle budeme používat mon0 rozhrání. Zapnutí antény do monitorovacího stavu můžeme využít k proskenování okolí. My se zaměříme na nalezení naší sítě. Sítě jménem Vetrelcovo (viz obr. 15.5). V našem případě pomocí příkazu:

```
airodump-ng mon0
```

Tabulka se mění v závislosti na skenovaném prostřední. V uvedeném obrázku (viz obr. 15.5) nalezneme tabulku se sloupci, které nám poskytují spoustu zajímavých údajů. Nás nejvíce budou zajímat sloupce BSSID – MAC adresa, CH – kanál, ENC – šifrování, ESSID – název. Ve spodní části výpisu se nalézají zařízení (jejich MAC adresa), které momentálně komunikují s jednotlivými AP. Výhodou tohoto příkazu je, že nám zobrazí i tzv. „skryté“ sítě, jak je možné vidět na obr. 15.5, že nevysílají své SSID. Po vyhledání a určení cíle je nezbytné vypnout proces skenování. Neboť skenování využívá a všech kanálů a při budoucím útoku na určité zařízení budeme používat pouze jeden kanál.



Obr. 15.5: Skenování okolí

15.5 Útok na WEP

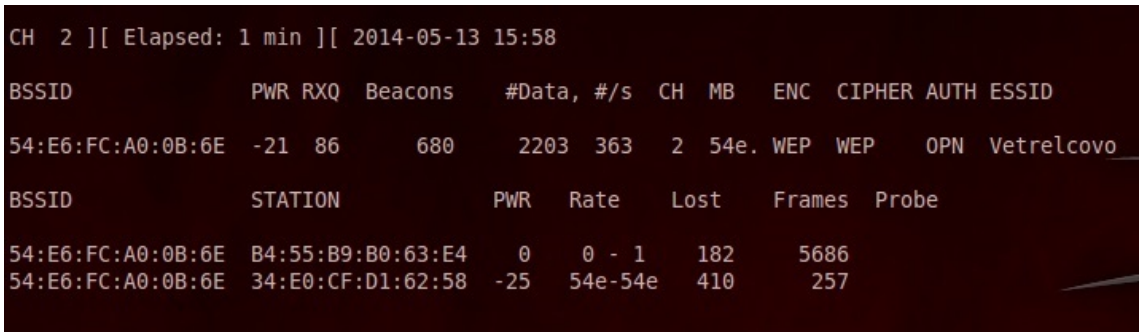
Kartu jsme nastavili podle základního nastavení (viz kapitola 15.4) a také jsme proskenovali své okolí, kde jsme nalezli právě naše zařízení vysílající SSID (Vetrelcovo). Při nalezení sítě se zabezpečením WEP, využijeme tyto příkazy, které jsou níže rozepsány a použity v jednotlivých sekcích této kapitoly. [5, 41]

- **airodump–ng** –bssid (MAC adresa vysílače) –c (kanál) –w (název souboru) (rozhraní)
- **aireplay–ng** –(číslo útoku 0-9) (časový interval) –a (MAC adresa vysílače) –h (MAC adresa, kterou chceme použít) (rozhraní)
- **aireplay–ng** –(číslo útoku 0-9) –b (MAC adresa vysílače) (interface)
- **aircrack–ng** –a (číslo 1,2) –b (MAC adresa vysílače) (název souboru).cap

Předchozí část byla věnována přípravě na útok a nalezení cíle. A pomocí právě předchozí části jsme zjistili MAC adresu cílového zařízení, MAC adresu klienta a další informace. V nově otevřeném okně terminálu zadáme příkaz:

```
airodump-ng --bssid 54:E6:FC:A0:0B:6E -c 2 -w wephack mon0
```

Airodump-ng je nástroj, který sbírá data do souboru (viz obr. 15.6). Tím, že určíme jeden kanál, nemusí karta zbytečně přepínat mezi všemi kanály a zrychlujeme tak čas ke sběru dat. Důležitým aspektem je zadání cílové MAC adresy. Pod výpisem sběru dat (viz obr. 15.6) se nalézají zařízení (jejich MAC adresa), které momentálně komunikují s AP včetně naší externí antény. Tento proces sběru dat nevypínáme, necháme jej běžet celou dobu. Jedná se o spoluproces při prolamování.

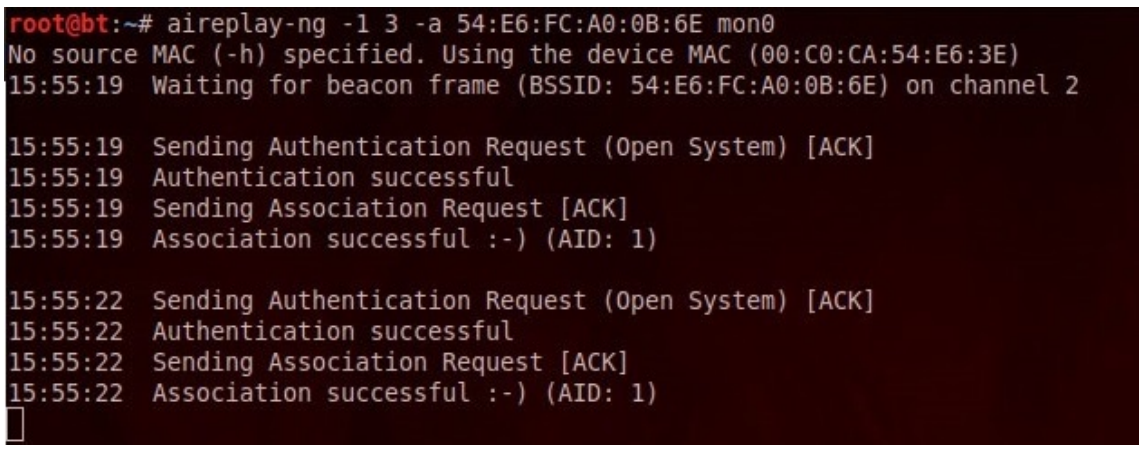


Obr. 15.6: Sběr dat, WEP

Máme momentálně dvě možnosti a to, že můžeme teď čekat, i celý den, než nasbírá dostatečný počet dat pomocí běžného provozu v síti, což je zdlouhavá metoda, anebo tomu trochu pomůžeme. Pro tento účel je použito následujících metod. Použijeme tedy dalších nástrojů k urychlení sběru a to tím, že budeme aplikovat ARP pakety.

Otevřeme další nový terminál, již potřetí. Pro vytváření falešné autentizace, pomocí příkazu aireplay-ng (viz obr. 15.7):

```
aireplay-ng -1 3 -a 54:E6:FC:A0:0B:6E mon0
```

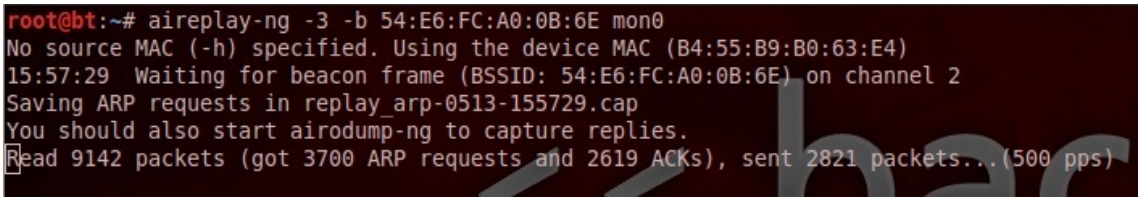


Obr. 15.7: Uspěšná falešná autentizace

Což znamená, že jde o útok, útok na MAC adresu zařízení, vytváření falešné autentizace po 3 sekundách. S použitím rozhraní mon0. Tento příkaz necháváme v pozadí taktéž běžet.

V následujícím kroku znova otevřeme další nový terminál a začneme tvořit a aplikovat ARP pakety, pomocí příkazu (viz obr. 15.8):

```
aireplay-ng -3 -b 54:E6:FC:A0:0B:6E mon0
```



Obr. 15.8: Aplikace ARP paketů

Jde o útok, který tvoří a aplikuje ARP pakety. B značí cílovou stanici a příkaz h označuje MAC adresu klienta s použitím rozhraní mon0. Pomocí tohoto útoku se nám urychluje sběr dat.

Na získávání rychlosti počtu datových paketů má vliv mnoho věcí, například jak silný signál máme a podobně. Se zvětšující vzdáleností se zhoršuje zisk a signál. Signál můžou zhoršovat i věci kolem nás jako je zeď a další. Také záleží na tom, kolik máme rušení kolem sebe (jiné sítě na stejném i jiném kanálu).

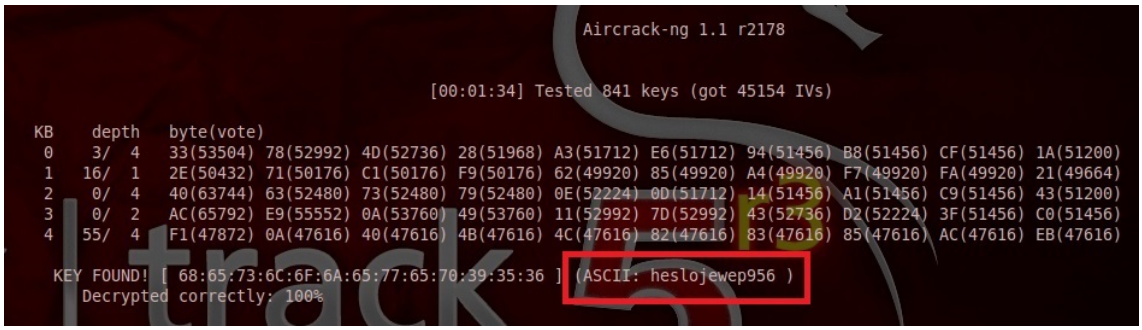
Ze zachycených dat je možné prolomení WEP klíče. K prolomení pomocí PTW útoku (pouze pro prolomení 40 a 104 bitového WEPu) použijeme analýzu nasbíraných dat a to pomocí nově otevřeného terminálového okna a s následujícím příkazem (viz obr. 15.9):

```
aircrack-ng -a 1 -b 54:E6:FC:A0:0B:6E wephack-12.cap
```

–a označuje útočící mód (1,2) nebo-li také (WEP, WPA), zadáváme stejné jméno (wephack), které jsme nastavili pro zápis při sběru dat.

Záleží na tom, kolik dat bylo odchyceno, čím větší počet, tím dřív jej zjistíme. K většině dnešních WEP sítí je předpoklad 20 – 50 tisíc dat (IV) k zjištění hesla. Po každých 5000 dat nám sám vypíše, že je jich stále málo, nebo že už jej nalezl. V našem případě bylo potřeba pouze 30 tisíc IV. Po každých 5 tisících zkouší, zda je možné dopočítání klíče.

Zde se útok povedl a dokonce nám ukázal, jaké je heslo (viz obr. 15.9), které zadal uživatel. Úspěšný útok s nalezením klíče lze provést do 5 minut.



Obr. 15.9: Úspěšný útok, Aircrack–ng

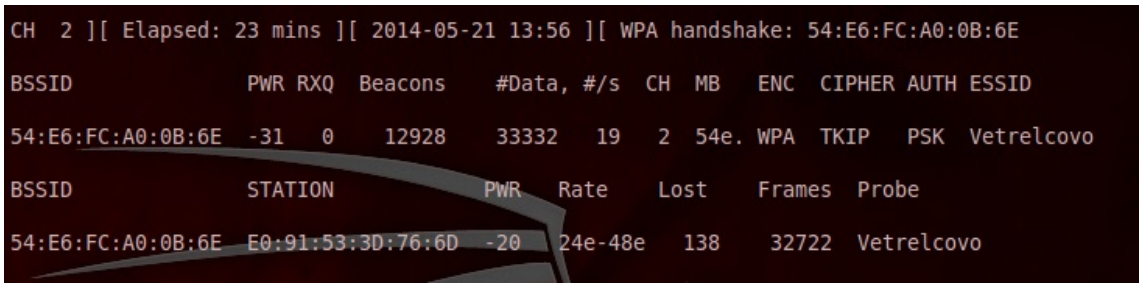
15.6 Útok na TKIP

Podle základního nastavení (viz 15.4) již opět máme nastavenou kartu i proskenované okoli, kde jsme nalezli právě námi hledané zařízení se zabezpečením WPA/TKIP. Využijeme tyto příkazy, které jsou níže rozepsány a použity v jednotlivých sekcích této kapitoly. [1]

- **airodump–ng** –bssid (MAC adresa vysílače) –c (kanál) –w (název souboru) (rozhraní)
- **tkiptun–ng** –(číslo útoku 0-9) –a (MAC adresa vysílače) –h (MAC adresa, kterou chceme použít nejlépe aktivního klienta) (interface)
- **aireplay–ng** –(číslo útoku 0-9) (počet aplikování) –a (MAC adresa vysílače) –h (MAC adresa, kterou chceme použít) (rozhraní)

Opět je potřeba zajistit sběr dat pomocí airodump-ng (viz obr. 15.10). S nástrojem airodump-ng již jsme obeznámeni, a proto nebude znova rozepsána jeho funkce.

```
airodump-ng --bssid 54:E6:FC:A0:0B:6E -c 2 -w tkip mon0
```



Obr. 15.10: Sběr dat, TKIP

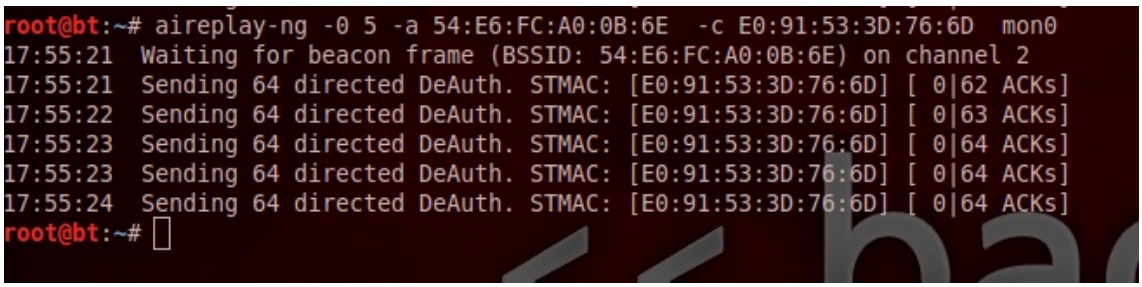
I tento proces sběru dat nevypínáme, necháme jej běžet paralelně celou dobu.

Využitím nástorje tkiptun-ng nezískáme tajný klíč sítě, ale šifrovací klíč a MIC hodnotu. Tkiptun-ng nástroj funguje na výše zmíněném (viz 12.2.1) útoku jménem Beck–Tews, což je upravená verze Chopchop útoku, kdy nejprve v prní řadě potřebuje získat 4-Way Handshake pro výpočet dočasného klíče a pro zpětnou kontrolu toho docílí pomocí zasílání deautentizačních zpráv. Po získání této hodnoty začne odchytávat ARP pakety ze strany AP a uloží si je, aby s nimi mohl nadále pracovat. Totéž provede s odchycenými ARP pakety ze strany klienta. Po těchto krocích začíná samotný vylepšený Chochop útok. Celý proces fungování nástorje tkiptun-ng je ukázán na obrázku 15.12.

```
tkiptun-ng -a 54:E6:FC:A0:0B:6E -h E0:91:53:3D:76:6D mon0
```

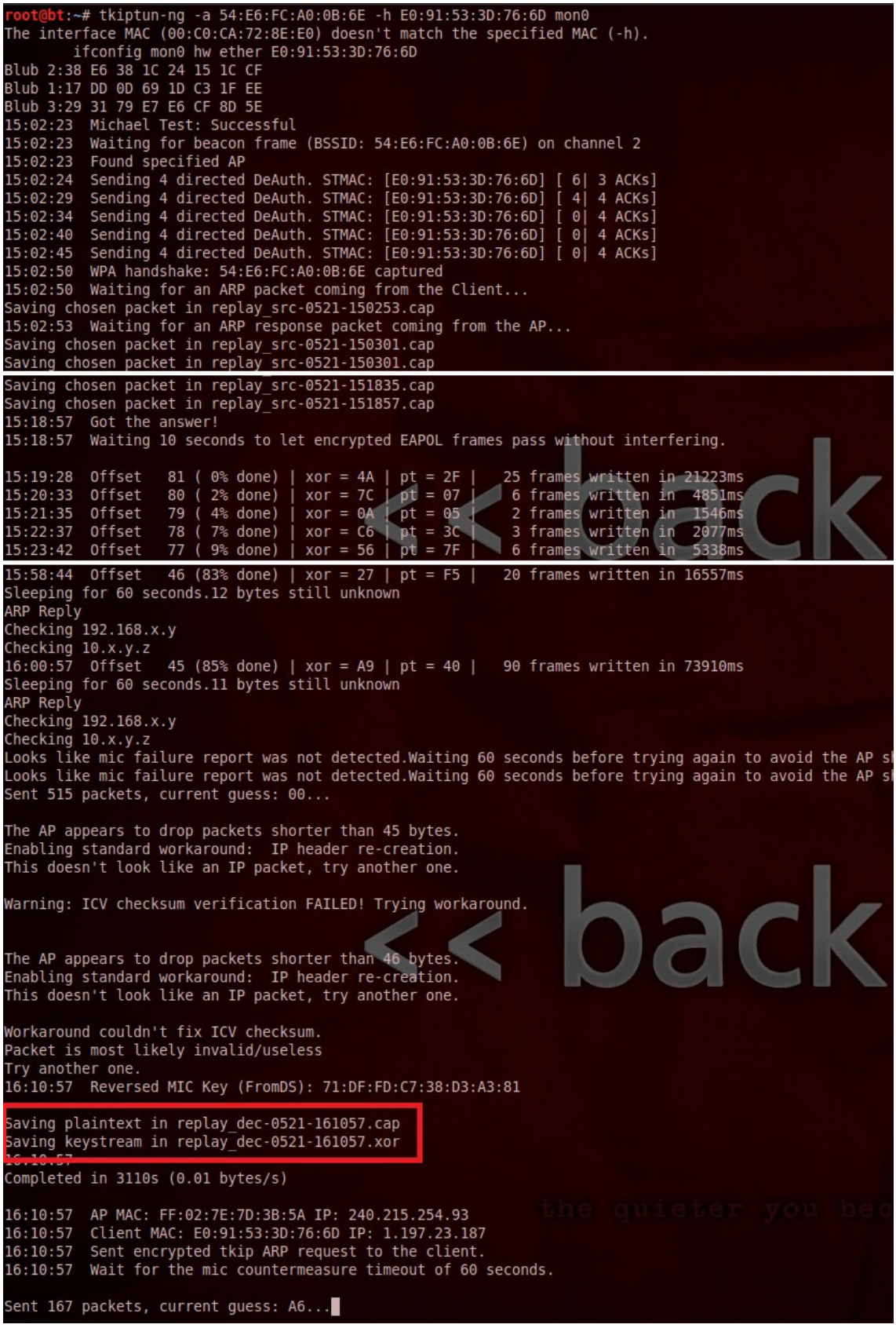
Abychom zachytili v co nejkratším čase určité ARP pakety, využijeme proto aireplay pro deautentizaci klienta (viz obr. 15.11). Avšak s tímto útokem musíme být velice opatrní neboť může nastat situace, že se klient přepojí automaticky na jiné AP, když je zrovna odhlašován námi, ke kterému má přistup. Tento nástroj použijeme pouze při procesu tkiptun při chytání ARP paketů. Kdybychom jej použili v pozdější fázi tak si přerušíme celý útok.

```
aireplay-ng -0 5 -a 54:E6:FC:A0:0B:6E -c E0:91:53:3D:76:6D
mon0
```



Obr. 15.11: Deautentizace klienta

Celý tento útok spočívá na co nejrychlejším odcyhcení určitých ARP paketů. Neustálém připojení klienta, dostatečné komunikaci na síti a zapnutém QoS. Celý útok trval 1 hodinu a 9 minut. Útok na protokol TKIP je složitější narozdíl od útoku na WEP, ale stále zde existují slabiny.



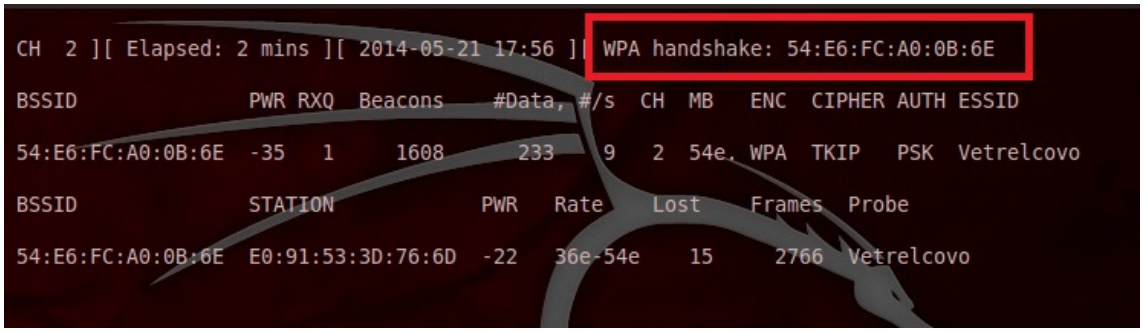
Obr. 15.12: Tkiptun-ng

15.7 Útok na WPA/WPA2 – PSK

Tak jako v předchozích útocích využíváme bodu (viz 15.4) základního nastavení. Opět znova nalezneme požadovanou síť. Pomocí níže uvedených příkazů pokračujeme. V tomto případě testujeme dvě metody prolamování a to metodou slovníku a brute–force neboli hrubou silou. [1, 12, 29]

- **airodump–ng** –bssid (MAC adresa vysílače) –c (kanál) –w (název souboru) (rozhraní)
- **aireplay–ng** –(číslo útoku 0-9) (počet aplikování) –a (MAC adresa vysílače) –h (MAC adresa, kterou chceme použít) (rozhraní)
- **aircrack–ng** –w (umístění slovníku) (název souboru)
- **pyrit** –r (název souboru) -b (MAC adresa vysílače) -i (použití slovníku) (definice útoku)
- **crunch** (nejnižší možné ciferné číslo) (maximální ciferné číslo) (použité znaky)

Opět využijeme předchozího základního nastavení (viz 15.4) a spustíme sběr dat (viz obr. 15.13).



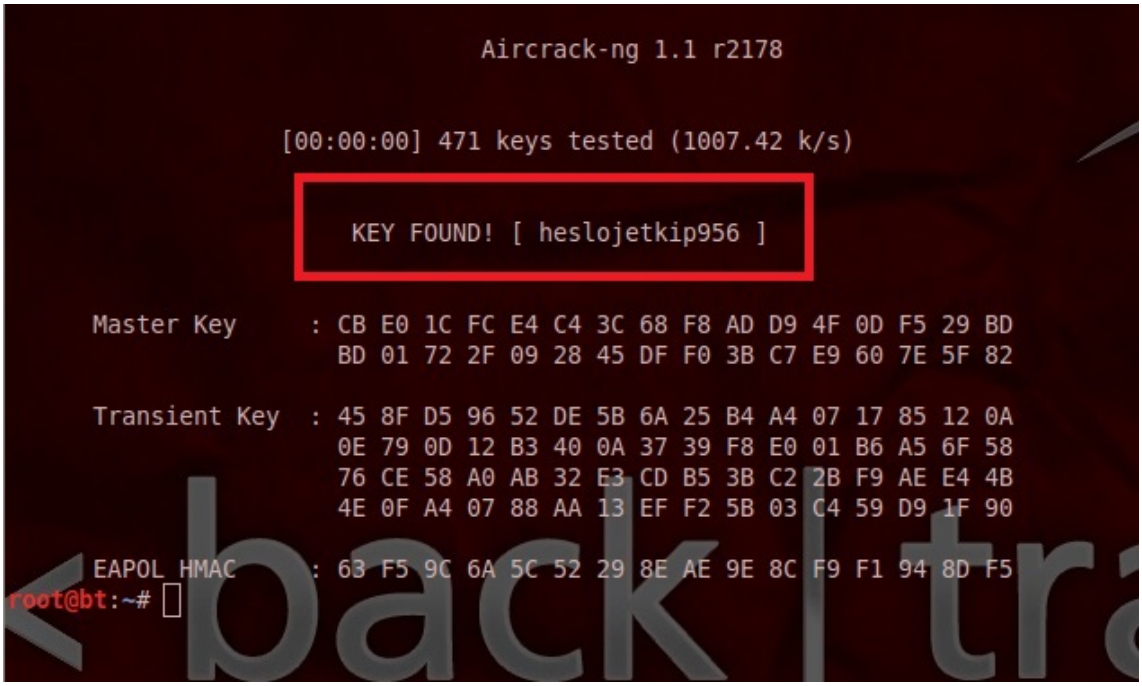
Obr. 15.13: Sběr dat, PSK

V tomto případě potřebujeme ještě odchytit 4-Way Handshake. To provedeme pomocí deautentizace klienta (viz obr. 15.11). Po odchycení této komunikace je zobrazen Handshake (viz obr. 15.13). A je možné všechnu komunikaci s okolím uzavřít. Teď již budeme pouze počítat. Samozřejmě existují různe techniky prolamování hrubou silou např. pomocí cloudu (za peníze si zakoupíte výpočetní výkon), využití různých programů atd.

První metoda, která byla použita v této práci za použití nástorje aircrack–ng využívá pouze procesoru počítače. Kdy podle zadaného souboru hledá shodné slovo s heslem, porovnávání dvou hodnot (viz obr. 15.14). Vše záleží na velikosti a obsáhlosti slovníku a složitosti tajného hesla. Čím je heslo komplikovanější, potom je

tím menší šance, že by slovník heslo obsahovalo. Pro naše experimentální účely byl vytvořen slovník (VBslovnik.txt), který dané heslo obsahoval.

```
aircrack-ng -w '/root/Deskop/VBslovnik.txt' slovnik-01.cap
```

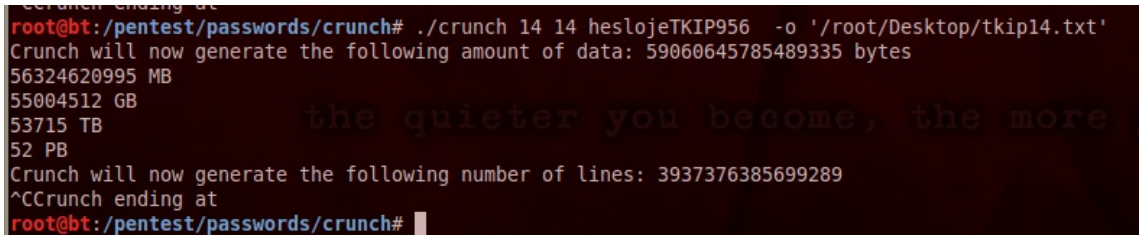


Obr. 15.14: Nalezení hesla ve slovníku, Aircrack–ng

Je vidno, že procesoru prozkoumání 471 testovancýh slov ve slovníku nezabralo ani vteřinu. Samozřejmě existuje na Internetu spoustu vytvořených slovníků. Jeden z nejznámějších je asi darkc0de. Každý slovník je jinak obsáhlý a složitý. Slovník se dá i vytvořil, dokonce BT obsahuje pár programu, jako je Crunch, který je použit níže pro tvorbu slovníků.

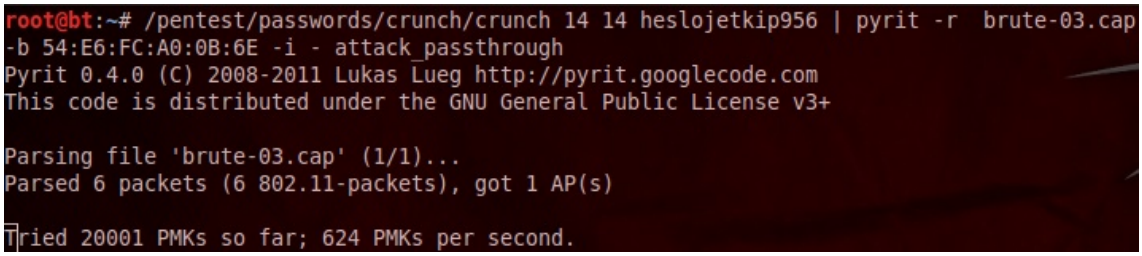
Druhá metoda je zaměřena na útok hrubou silou neboli brute–force. Je využito nástorje Crunch, který vygeneruje určitý slovník, jenž obsahuje různé kombinace ze zadaných hodnot (znaků). Jedná se o výpočetně náročnější proces nežli při slovníkovém útoku, proto byla zapojena do výpočtu i grafická karta pomocí nástroje Pyrit. Aby bylo možné si udělat představu, kolik místa může zabírat slovník se 14 pozicemi v kombinací pouze pár znaků (viz obr. 15.15).

```
crunch 14 14 PITKhesloje956 | pyrit -r brute-03.cap
-b 54:E6:FC:A0:0B:6E -i - attack_passthrough
```



Obr. 15.15: Vytovření slovníku, Crunch

Při útoku hrubou silou byly využity dva nástroje. Crunch, který vytváří určitý slovník a zároveň je možné použít nástroj Pyrit, který využívá výkonu grafické karty ke zrychlení celého procesu. Pomocí nástrojů Crunch a Pyrit (viz obr. 15.16), vytvoříme slovník o určité délce s určitými znaky. Pyrit potřebuje taktéž určité příkazy ke správnému fungování. Příkazem (-r) určíme vytvořený soubor sběrem dat, se kterým má pracovat. Příkazem (-i) určujeme, zda má využít slovník, v tomto případě není definovaný žádný a (-b) BSSID. Posledním příkazem říkáme, že má objevit heslo.



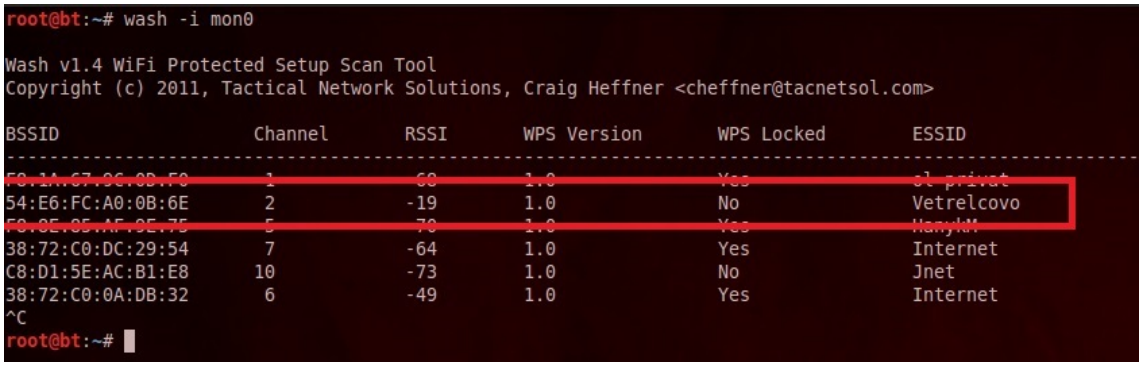
Obr. 15.16: brute–force s GPU, Crunch a Pyrit

Z časových důvodů byla nastíněna problematika hrubou silou, kvůli malému vypočetnímu výkonu nebylo heslo nalezeno. Této varianty útoku se používá v těch nejhorších situacích nebo pro experimentální účely.

15.8 Útok na WPS

Podle základního nastavení(viz 15.4) již opět máme nastavenou kartu. Za použití níže uvedených příkazu provedeme útok na WPS, ale tentokrát proskenujeme okolí pomocí nástroje Wash (viz obr. 15.17), který skenuje okolí ohledně WPS a zobrazí nám potřebné informace. [1, 11, 42]

- **wash** –i (rozhraní)
- **reaver** –i (rozhraní) –b (MAC adresa vysílače) –c (kanál) –f –S –L –d (časový interval) –t (časový interval) –x (časový interval) –l (časový interval) –vv

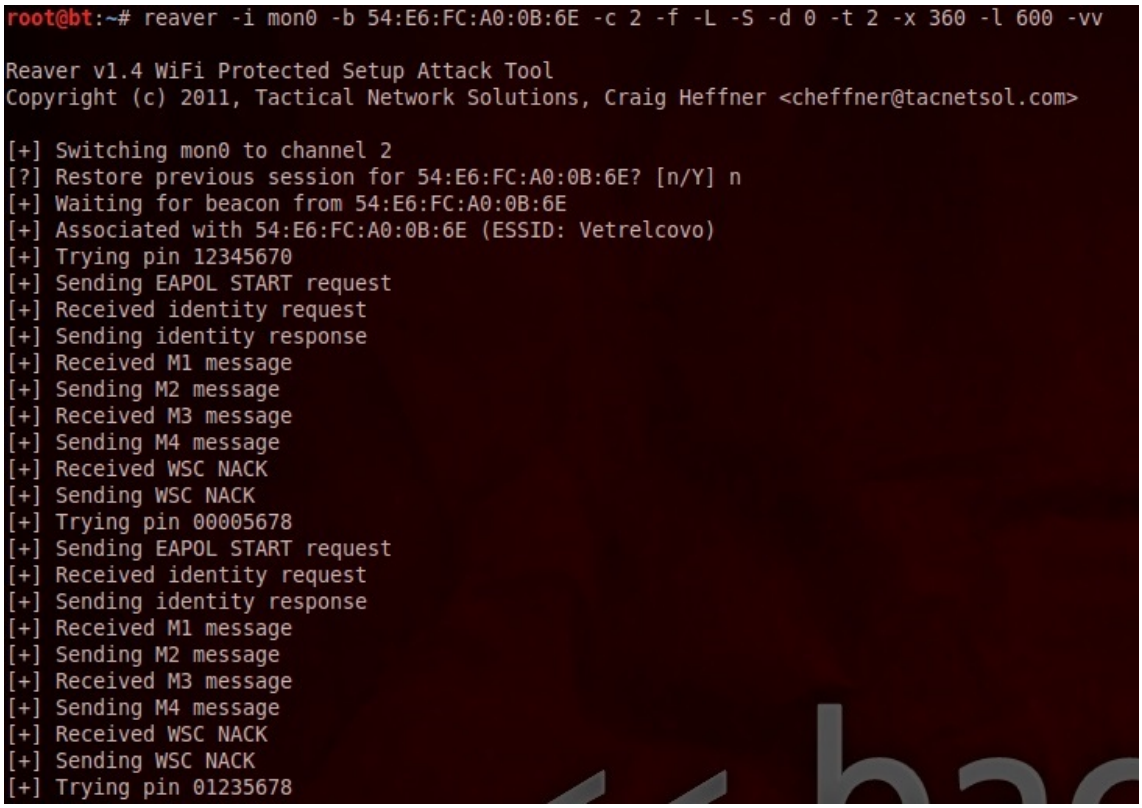


Obr. 15.17: Skenování okolí pomocí nástroje Wash

Tabulka použítá při nástroji Wash má mírné změny naproti na rozdíl od nástroje airodump–ng, neboť již není zapotřebí tolika informací. Důležitými sloupci jsou pro nás BSSID – MAC adresa, Channel – kanál, WPS Locked – zda má zařízení vypnuté WPS, ovšem určité zařízení se mohou pouze tvářit, že mají vypnuté WPS. Tuto ochranu lze jednoduše obejít pomocí jediného příkazu, jak bude popsáno.

Po nalezení dané sítě můžeme přistoupit k úotku. K útoku využijeme nástroje Reaver, který je specializovaný na tuto problematiku. Pomocí následujícího příkazu (viz obr. 15.18) zahájíme útok.

Aby celý útok proběhl nejlépe v co nejkratším čase jsou přidány v příkazu nastavení, které nemusí AP podporovat a nemusely by fungovat v určitých případech. Příkazu výšše uvedeného provede: na rozhraní mon0 provede útok nástorje Reaver na cílovou MAC adresu (-b) s fixovaným kanálem (-f) nastaveným na kanál (-c) číslo 2 a úplným vypsáním (-vv) celého průběhu útoku. Za použití (-S) zkrácených DH (Diffie-Hellman) zpráv a (-d) časového intervalu mezi zkoušenými PINy, u těchto možností může vzniknout problém na straně AP, které si stímto útokem neporadí, v tom případě se Reaver musí přizpůsobit. Reaver dokáže útočit i na tzv. zablokované WPS, samozřejmě pouze pokud se jedná o zařízení, které se jen navenek tváří,

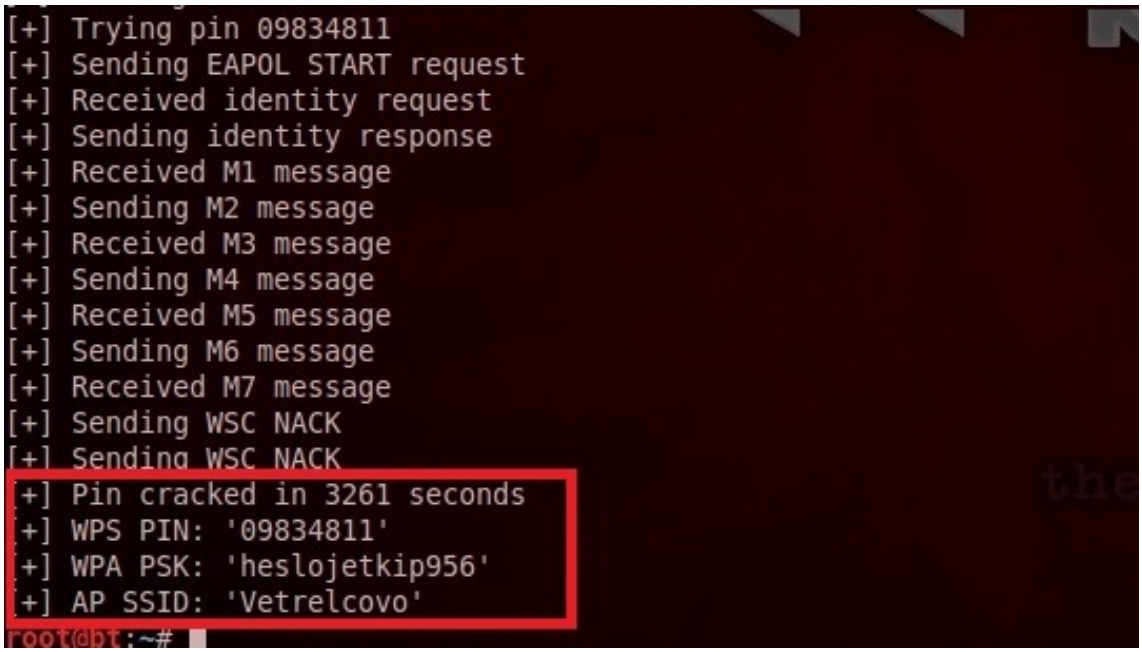


Obr. 15.18: Reaver nastavení

že jej má vypnuté. Díky přidání příkazu (-L) dokáže Reaver ignorovat toto upozornění. Přijímací časová perioda (-t) nastavena na dvě vteřiny. Další časový údaj (-x) nastavuje dobu po 10 neuspěšných pokusech čekání. (-l) nastavuje jak dlouho má Reaver počkat, když AP na určitou dobu zamkne WPS (obraný mechanismus), ale po chvíli jej opět spustí.

S nastevením nástroje Reaver se dá různě nastavovat pro přízpůsobení co nejoptimalnějšího útok. Avšak spuštění více paralelních Reaver útoku nefunguje, neboť WPS na straně AP nedisponuje tak velkým výpočetním výponem, je proto snažší využít plně možností jednoho Reaveru. Tento útok trval 55 minut při nastavení hesla uvedeného na obrázku 15.19. Pokud vezmeme v potaz, že Reaver funguje na principu vyzkoušení všech možných kombinací stím, že začína od nejnižší hodnoty, tak při nastavení hesla začínající mnohem vyším číslem (např. 9) může útok probíhat mnohem déle. Pokud si útočník nenastaví právě jiný slovník (začínající třeba právě hodnotou 9) a nezačne jej aplikovat.

Při prolomení této slabiny je nám zaslán PSK klíč (viz obr. 15.19). Délky útoku Reaver na WPS jsou průměrně kolem 10 hodin. Avšak záležína na mnoha faktorech. Mnoho poskytovatelů internetu se snaží WPS deaktivovat na svých zařízeních, což je dobrý krok kupředu. Avšak obyčejní uživatelé většinou ani neví, že nějaká



Obr. 15.19: Úspěšný útok, Reaver

takováto problematika existuje, a proto stále najdeme spoustu AP disponující nezablokovaným WPS. WPS je zjevné ulehčení úživatelům o vytvoření bezdrátové sítě v domácnosti, ale i přesto je to stále slabina, kterou se výrobci snaží nějak zmenšit. Buďto již je WPS od výroby vypnuto nebo využívají agresivnějších pravidel, jako je třeba exponenciální navyšování časového intervalu při znovu zadání PINu.

16 ZÁVĚR

Tato práce se zabývá komplexní problematikou zabezpečení bezdrátových sítí a standardu 802.11. Díky rychlému technologickému rozvoji a díky potřebám uživatelů se v posledních letech vývoj ubíral spíš směrem ke zrychlení sítí a směrem zlepšení bezpečnosti těchto sítí. Zabezpečení bezdrátových sítí dělíme na dvě různé skupiny. Jedná se o sféru podnikovou, kde je kladen důraz především na bezpečnost těchto sítí. Na rozdíl od domácností, kde se vyskytují uživatelé s minimálními nebo omezenými znalosti problematiky, a tedy pro tuto skupinu uživatelů je důležitější komfort.

Na počátku zajišťování bezpečnosti bezdrátových sítí stál WEP. Proto jsou v první části také uvedeny důležité aspekty tohoto zabezpečení. Jakožto první zabezpečovací protokol nebyl řádně před jeho vydáním otestován, proto s sebou nese také jisté chyby. Jedná se například o algoritmus RC4, u kterého byly známy jeho omezení ještě v době, kdy samotný WEP aplikován nebyl. Takovýchto chyb, existuje více. Kvůli nedostatečnému zabezpečení bezdrátových sítí přišel protokol TKIP, který je nadstavbou WEPu, využívající taktéž algoritmu RC4. Kvůli této problematice nese i jisté slabiny, které jsou v práci popsány. Dále se práce věnuje nejnovějšímu zabezpečení známé pod pojmem WPA2, u kterého se nebrala v potaz zpětná kompatibilita se zařízeními a kde bezpečnost byla stavěna na první řadu. Dále se teoretická část věnuje popsání útoku jak na zebezpečení WEP, tak i na WPA a WPA2. V aplikované části byly shromážděné nedostatky aplikovány a využity k tomu, aby došlo k prolomení zapezpečení WEP a WPA.

Z bezpečnostního hlediska by se WEP ani WPA neměly již využívat. Ovšem kvůli tomu, že tato problematika není velmi známá běžnému uživateli, WEP a WPA je stále využíván poměrně frekventovaně, a to především v domácnostech.

Dále práce pojednává o možnostech lepší obrany proti známým útokům jak všeobecným, tak přímým útokům na zařízení zabezpečených prostřednictvím nejenom WEPu. Jako za nejlepší obranu je považováno využití modernějšího šifrovacího protokolu, čímž je dnes WPA2. Protokol WPA2 se v současné době považuje za neprolomený, neboť využívá nejmodernější zabezpečovací techniky. Mnoho starších zařízení nepodporují lepší zabezpečení než WEP, a proto je navrhnuto i několik možností, jak zlepšit ochranu takovýchto sítí, například zeslabením vysílacího signálu, použitím filtrování podle MAC adres nebo použitím dlouhého a složitého hesla. To je pouze několik možností, jak zlepšit ochranu sítě.

Velká část práce se věnuje především simulovaným útokům na zabezpečení bezdrátových sítí. Tato část by se dala rozdělit na části podle typu útoku na cílené zabezpečení. Prvním otestovaným zabezpečením se stal WEP. Byl simulován útok, který využívá pasivního PTW útoku a aktivního aplikování APR paketů pomocí něhož se dá vytvořit nadměrná komunikace v síti. V dnešní době je již možné po-

mocí nadměrného provozu v síti se zabezpečením WEP zjistit heslo do 5 minut. Druhá část se věnuje útoku na zabezpečení WPA/TKIP. Je použit specializovaný nástroj jménem tkiptun–ng, který využívá vylepšeného Chochop útoku. Jedná se již o složitější útok, ke kterému je nutné mít jisté znalosti s práci v BT. Další část je věnována útoku hrubou silou a útoku pomocí slovníku. U těchto útoků je nejprve nutné získat a odcyhtit 4-Way handshake. U útoku slovníkem jsme si ověřili, že slovník musí dané heslo obsahovat, aby bylo nalezeno. Čím tedy máme delší a složitější heslo mít, tím bude menší pravděpodobnost, že v daném slovníku heslo bude obsaženo. Je simulován neuspěšný útok hrubou silou. Tato metoda je hodně výpočetně složitá, proto byla využita i GPU jako názorná ukázka metody hrubou silou. Tyto útoky jsou použity jako poslední možnost o porlomení se do sítě útočníkem. Skutečností, že výrobci implementovali do svých zařízení WPS pro pohodlí uživatelů, vznikla nová slabina. V tomto útoku je využito nástroje Reaver, který je specializovaný na tuto problematiku. Reaver využívá metody hrubou silou, kdy zkouší jednotlivé kombinace PINu.

Útočník se nebude řídit zákony při napadnutí domácí nebo podnikové sítě. Bude se snažit získat jakoukoli cestou dostatek informací k prolomení té sítě, kterou si vybere za cíl.

LITERATURA

[1] *Aircrack-ng* [online]. 2009 [cit. 2013. 12. 17] Dostupné z: <http://www.aircrack-ng.org>.

[2] Alfa AWUS036H -1- WiFi WLAN 1000mW b/g 2,4GHz aircrack Wireshark. *EuroShop Store* [online]. 2011 [cit. 2013. 12. 17] Dostupné z: <http://www.antiradary-distributor.cz/alfa-awus036h-1-wifi-wlan-1000mw-bg-24ghz-aircrack-\wireshark-p-20550.html>.

[3] Anténa Yagi směrová 16dBi 2,4GHz NF. *pcsk* [online]. [cit. 2013. 12. 17] Dostupné z: <http://www.pcsk.sk/zbozi/antena-yagi-smerova-16dbi-2-4ghz-nf/detail.aspx?p=z:142782&>.

[4] Antény. *RC - Eagle Eye* [online]. 2005 [cit. 2013. 12. 17] Dostupné z: <http://www.rc-eagleeye.cz/rc-eagleeye/5-Theory-Trocha-teorie/13-Antennas-Anteny>.

[5] *BackTrack Linux* [online]. 2011 [cit. 2013. 12. 17] Dostupné z: <http://www.backtrack-linux.org/>.

[6] BECK, Martin. *Enhanced TKIP Michael Attacks* [online]. 2010. 10 s. [cit. 2014. 05. 27] Dostupné z: <http://dl.aircrack-ng.org/wiki-files/doc/enhanced_tkip_michael.pdf>.

[7] BECK, Martin a TEWS, Erik. *Practical attacks against WEP and WPA* [online]. 2008. 12s. [cit. 2013. 12. 17] Dostupné z: <http://dl.aircrack-ng.org/breakingwepandwpa.pdf>.

[8] Bezdrátový směrovač 300 Mbit/s Wireless N TL-WR841ND. *TP-LINK* [online]. 2010 [cit. 2013. 12. 17] Dostupné z: <http://cz.tp-link.com/products/details/?model=TL-WR841ND>.

[9] Bezpečnost a Hacking WiFi (802.11) - 3. WEP. *Security-Portal* [online]. 2009 [cit. 2013. 12. 17] Dostupné z: <http://www.security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-3-wep>.

[10] BOZDĚCH, Martin. *Testování bezdrátových sítí s využitím SW Boingo* [online]. Brno, 2006. 22s. [cit. 2013. 12. 17] Dostupné z: <http://is.muni.cz/th/72877/fi_b/bakalarka.pdf>.

[11] Cracking Wifi WPA/WPA2 passwords using Reaver-WPS. *Black MORE ops* [online]. 2013 [cit. 2014. 05. 27] Dostupné z: <http://www.blackmoreops.com/2013/10/12/cracking-wifi-wpawpa2-passwords-using-reaver-wps/>.

[12] Creating wordlists with crunch v3.0 . *Adaywithtape* [online]. 2011 [cit. 2014. 05. 27] Dostupné z: <http://adaywithtape.blogspot.cz/2011/05/creating-wordlists-with-crunch-v30.html>.

[13] ČEČUNDA, Marián. *Analýza bezpečnosti prúdovej šifry RC4* [online]. Brno, 2013. 44 s. Dostupné z: <http://is.muni.cz/th/359319/fi_b/RC4-BAPR.pdf>.

[14] EMRAH, Tomur a ERTEN, Yusuf M. Application of temporal and spatial role based access control in 802.11 wireless networks. *Computers & Security* [online]. 2006, 25, 6 s. [cit. 2013. 12. 17] Dostupné z: <http://www.sciencedirect.com/science/article/pii/S0167404806000927>.

[15] HALVORSEN, Finn a HAUGEN, Olav. *Cryptanalysis of IEEE 802.11i TKIP* [online]. 2009. 156 s. [cit. 2014. 05. 27] Dostupné z: <http://download.aircrack-ng.org/wiki-files/doc/tkip_master.pdf>.

[16] *Homewifi* [online]. 2006 [cit. 2013. 12. 17] Dostupné z: <http://homewifi.wz.cz/>.

[17] HTG Explains: The Difference Between WEP, WPA, and WPA2 Wireless Encryption (and Why It Matters). *How-to geek* [online]. 2013 [cit. 2013. 12. 17] Dostupné z: <http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-\wireless-encryption-and-why-it-matters/>.

[18] IEEE Computer Society. *IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks— Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* [online]. 2012 [cit. 2013. 12. 17] Dostupné z: <http://standards.ieee.org/getieee802/download/802.11-2012.pdf>.

[19] JELÍNEK, Martin. *Bezpečnost bezdrátových počítačových sítí* [online]. Brno, 2010. 101. [cit. 2013. 05. 27] Dostupné z: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=26998>.

[20] JONNSON, Jakob. *On the Security of CTR + CBC-MAC* [online]. 2012. 18s. [cit. 2013. 05. 27] Dostupné z: <http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm-ad1.pdf>.

[21] *KALI Linux* [online]. 2014 [cit. 2014. 05. 27] Dostupné z: <http://www.kali.org/>.

[22] KLÍMA, Vlastimil. *Základy moderní kryptologie - Symetrická kryptografie III. operační mody blokových šifer a hašovací funkce* [online]. 2005. 27s. [cit. 2013. 05. 27] Dostupné z: <http://www.karlin.mff.cuni.cz/~tuma/ciphers09/Symetricka_kryptografie_III.pdf>.

[23] KOLAŘÍK, Jan. *Kryptografická ochrana bezdrátových sítí* [online]. Praha, 2007. 66 s. Dostupné z: <https://dip.felk.cvut.cz/browse/pdfcache/kolarj6_2007bach.pdf>.

[24] KWAN, Phillip. *White Paper: 802.1X Authentication & Extensible authentication Protocol (EAP)* [online]. 2003. 12s. [cit. 2013. 05. 27] Dostupné z: <http://www.brocade.com/downloads/documents/white_papers/wp-8021x-authentication-eap.pdf>.

[25] LEHEMBRE, Guillaume. Bezpečnost Wi-Fi – WEP, WPA a WPA2. *hakin9* [online]. 2006, 1/2006, 14 s. [cit. 2013. 12. 17] Dostupné z: <http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf>.

[26] LEVICKÝ, Dušan. *Kryptografia v informačnej bezpečnosti.* Košice: Elfa, 2005. 266 s. ISBN 80-808-6022-X.

[27] MALLO, Petr. *Vybrané útoky v prostředí bezdrátových sítích standardu Wi-Fi* [online]. Brno, 2011. 46s. [cit. 2013. 05. 27] Dostupné z: <http://is.muni.cz/th/207877/fi_b_a2/Bachelor_thesis_Peter_Mallo_23_05.pdf>.

[28] OHIGASHI, Toshihiro a MORII, Masakatu. *A Practical Message Falsification Attack on WPA* [online]. 2008. 12 s. [cit. 2014. 05. 27] Dostupné z: <http://dl.packetstormsecurity.net/papers/wireless/A_Practical_Message_Falsification_Attack_On_WPA.pdf>.

[29] pyrit WPA/WPA2-PSK and a world of affordable many-core platforms. *code.google.com* [online]. 2010 [cit. 2014. 05. 27] Dostupné z: <https://code.google.com/p/pyrit/wiki/Tutorial>.

[30] SKOVAJSA, Tomáš. *Bezpečnost WiFi sítí* [online]. Brno, 2012. 78s. [cit. 2013. 05. 27] Dostupné z: <http://is.muni.cz/th/208041/fi_m/tomas_skovajsa.pdf>.

[31] *Svět sítí* [online]. 2000 [cit. 2013. 12. 17] Dostupné z: <http://www.svetsiti.cz/default.asp>.

[32] TEWS, Erik. *Attacks on the WEP protocol* [online]. Darmstadt, 2007. 125 s. Dostupné z: <http://eprint.iacr.org/2007/471.pdf>.

[33] VIEHBÖCK, Stefan. *Brute forcing Wi-Fi Protected Setup* [online]. 2011. 9 s. [cit. 2014. 05. 27] Dostupné z: <http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf>.

[34] Všechno, co byste měli vědět o Wi-Fi. *Zive.cz* [online]. 2005 [cit. 2013. 12. 17] Dostupné z: <http://www.zive.cz/clanky/vsechno-co-byste-meli-vedet-o-wi-fi/omezena-pasma-a-standardy-anteny/sc-3-a-162796-ch-80485/default.aspx#articleStart>.

[35] Všeobecně o anténách. *Pira* [online]. 1999 [cit. 2013. 12. 17] Dostupné z: <http://www.pira.cz/antena.htm>.

[36] Who We Are. *Wi-Fi Alliance* [online]. 1999 [cit. 2013. 12. 17] Dostupné z: <http://www.wi-fi.org/who-we-are>.

[37] WiFi "Hole196?: major exploit or much ado about little? *ARStechnica* [online]. 2010 [cit. 2013. 05. 27] Dostupné z: <http://arstechnica.com/business/2010/07/wifi-hole196-major-exploit-or-much-ado-about-little/>.

[38] Wi-FI Protected Setup (WPS) is Insecure: Here's Why You Should Disable It. *How-to geek* [online]. 2013 [cit. 2014. 05. 27] Dostupné z: <http://www.howtogeek.com/176124/wi-fi-protected-setup-wps-is-insecure-heres-why\-you-should-disable-it/>.

[39] Wi-Fi Security: Cracking WPA With CPUs, GPUs, And The Cloud. *Toms Hardware* [online]. 2011 [cit. 2014. 05. 27] Dostupné z: <http://www.tomshardware.com/reviews/wireless-security-hack,2981.html>.

[40] *PCTuning* [online]. Wi-Fi sítě - vše co jste kdy chtěli vědět 1/2. 2008 [cit. 2013. 12. 17] Dostupné z: <http://pctuning.tyden.cz/hardware/site-a-internet/11138-wi-fi_site-vse_co_jste_kdy_chteli_vedet_12?start=3>.

[41] Wireless Hacking - WEP. *How to Crack a Wi-Fi Network's WEP Password with BackTrack* [online]. 2010 [cit. 2013. 12. 17] Dostupné z: <http://lifehacker.com/5305094/how-to-crack-a-wi-fi-networks-wep-password-with-backtrack>.

[42] WPS (Wi-Fi Protected Setup) Exploiting / Cracking (Crack any WPA-/WPA2/WEP). *Sethioz* [online]. 2013 [cit. 2014. 05. 27] Dostupné z: <http://sethioz.com/mediawiki/index.php5/WPS_%28Wi-Fi_Protected_Setup%29_Exploiting_/_Cracking_%28Crack_any_WPA/WPA2/WEP%29>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resoluton Protocol
AS	Authentication Server
BSSID	Basic Service Set IDentifier
BT	BackTrack Linux
CBC-MAC	Cipher-Block Chaining with Message Authentication Code
CCM	Counter with CBC-MAC
CCMP	Cipher Block Chaining Message Authentication Code Protocol
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTR	Counter Mode
DDoS	Distributed Denial of Service, přehlcení serveru
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protokol
EAPOL	EAP over LAN
ESSID	Extended Service Set Identifier
FMS	iniciály autorů (Fluhrer, Mantin, Shamir)
FW	Firmware
GEK	Group Encryption Key
GIK	Group Integrity Key
GPU	Graphic Processing Unit

HMAC	Keyed-Hash Message Authentication Code
HW	Hardware
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IV	Initialization Vector, inicializační vektor
KCK	Key Confirmation Key
KEK	Key Encryption Key
KoreK	pseudonym autora útoku na WEP
KSA	Key Scheduling Algorithm
LEAP	Lightweight EAP
MAC	Media Access Control
MD5	Message-Digest 5
MIC	Message Integrity Check
MIMO	Multiple-Input and Multiple-Output
MITM	Man In The Middle, člověk uprostřed
MPDU	MAC Protocol Data Unit
MSB	Most Significant Bit
MSDU	MAC Service Data Unit
MSK	Master Session Key
NFC	Near-Field Communication
OFDM	Orthogonal Frequency Division Multiplexing
PBC	Push Button Configuration
PEAP	Protected EAP
PIN	Personal Information Number
PKI	Public Key Infrastructure

PMK	Pairwase Master Key
PN	Packet Number
PPK	Per-Packet Key
PPP	Point-to-Point Protocol
PRF	Pseudo-random Function
PRGA	Ipseudo-random Generation Algorithm
PSK	Pre-Shared key
PTK	Pairwise Transient Key
PTW	iniciály autorů (Pyshkin, Tews, Weinmann)
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RC4	algoritmus generující pseudonáhodnou posloupnost bytů
RSA	iniciály autorů (Rivest, Shamir, Adlemann)
RSC	Receive Sequence Counter
RSN	Robust Security Network
SOHO	Small Office Home Office
SPI	Stateful Packet Inspection
SSID	Service Set Identifier
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TMK	Temporary MIC Key
TSC	TKIP Sequence Counter
TTAK	TKIP-mixed Transmit Address and Key
TTLS	Tunneled Transport Layer Security

UFD	USB Flash Drive
VPN	Virtual Private Network
WEP	Wired Equivalent Privace
Wi-Fi	Wireless Fidelity
Wlan	Wireless Local Area Network
WPA	Wireless Protected Access
WPA2	Wireless Protected Access 2
WPS	Wi-Fi Protected Setup