Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Bezdrátové sítě a jejich zabezpečení

Bakalářská práce

Autor: Miroslav Sajvera
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Vladimír Soběslav, Ph.D.

Hradec Králové duben 2015

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 30.4.2015 Miroslav Sajvera

Poděkování:

Tímto bych chtěl poděkovat vedoucímu bakalářské práce Ing. Vladimíru Soběslavovi, Ph.D. za odborné vedení práce a udělené rady.

Anotace

Tato bakalářská práce se zabývá bezdrátovými sítěmi a problematikou jejich bezpečnosti. Nejprve je popsán standard IEEE 802.11, na kterém je založeno budování bezdrátových sítí WLAN, včetně jeho nejpoužívanějších či nejnovějších dodatků. Rovněž jsou popsány metody bezdrátového přenosu dat a přístupové metody k bezdrátovému médiu, které standard IEEE 802.11 definuje. Další kapitoly se zabývají popisem, strukturou a topologií bezdrátových sítí WLAN. Nejdůležitější a nejobsáhlejší kapitoly jsou věnovány zabezpečovacím metodám, bezpečnostním hrozbám a útokům na bezdrátové sítě. Praktická část práce je zaměřena na vybrané z možných útoků, které jsou demonstrovány za použití specializované linuxové distribuce Kali Linux.

Annotation

This Bachelor Thesis deals with wireless networks and their security. First there is mentioned standard IEEE 802.11 which is used for creating wireless local area networks WLAN also with its the most used and recent amendments. Next part of thesis defines the characteristics and methods of transmitting data and also methods of media access control which is defined by standard IEEE 802.11. Last but not least there is mentioned the structure and topology of wireless local area networks. The most important parts are dedicated to security methods, security threats and attacks on wireless networks. The practical part deals with possible attacks to wireless networks that are demonstrated by specialized distribution of Linux called Kali Linux.

Obsah

1 Úvod ... 1

2 Standard IEEE 802.11 ... 2

2.1 Fyzická vrstva PHY ... 2

2.2 Podvrstva MAC ... 4

2.3 Podstatné dodatky standardu IEEE 802.11 ... 7

3 Struktura a topologie 802.11 sítě ... 10

3.1 Struktura ... 10

3.2 Topologie ... 11

4 Zabezpečení bezdrátové sítě ... 13

4.1 Zamezení vysílání SSID ... 13

4.2 Filtrace MAC adres ... 13

4.3 Vlastnosti zabezpečovacích mechanismů ... 14

4.4 WEP ... 16

4.5 IEEE 802.1X ... 19

4.6 WPA ... 21

4.7 WPA2 ... 24

4.8 Porovnání zabezpečovacích mechanismů ... 27

5 Možné typy útoků na bezdrátové sítě ... 28

5.1 Odposlech síťové komunikace ... 28

5.2 Falšování MAC adres ... 28

5.3 Deautentizace ... 29

5.4 Slovníkové útoky ... 29

5.5 Falešná zařízení ... 29

5.6 Man-in-the-middle útoky ... 30

5.7 DoS útoky ... 31

5.8 Útoky na WEP ... 31

5.9 Útoky na WPA, WPA2 ... 35

6 Praktická část ... 39

6.1 Softwarové vybavení 39
6.2 Hardwarové vybavení 40
6.3 Příprava k útokům 41
6.4 WEP 45
6.5 WPA/WPA2 52
6.6 Shrnutí provedených útoků 55
7 Závěr 56
8 Seznam použité literatury 58

1 Úvod

V dnešní době jsou bezdrátové sítě jednou z nejrychleji se rozvíjejících síťových technologií a významnou součástí datových sítí obecně. Jedná se o počítačové sítě, které jsou tvořeny uzly, mezi nimiž probíhá bezdrátová komunikace. Oproti sítím kabelovým přenos dat probíhá nejčastěji pomocí elektromagnetických vln nebo pomocí světelného záření. Vzdálenost mezi účastníky bezdrátové komunikace se pohybuje v řádech od několika metrů až po kilometry. Přenosové rychlosti dnešních bezdrátových sítí jsou navíc již téměř srovnatelné s rychlostmi sítí kabelových, které jsou značně vysoké.

Bezdrátové sítě se těší oblibě díky poměrně jednoduché instalaci, flexibilitě při připojování stanic a následné správě. Své uplatnění najdou především v oblastech, kde by zavedení kabelů bylo příliš nákladné, případně z technických důvodů hůře realizovatelné. Další jejich výhodou je větší pohodlnost způsobená mobilitou v síti, jelikož se uživatel může volně pohybovat v dosahu bezdrátové sítě, zatímco je připojen.

Nevýhodou radiových bezdrátových sítí je náchylnost na rušení způsobené zařízeními pracujících na stejných kmitočtech. U infračervených a optických bezdrátových sítí je problémem přímá viditelnost, jelikož v cestě komunikace nesmějí být žádné překážky. Dalším problémem jsou vlivy počasí, které se mohou neblahým způsobem projevit na vlastnostech bezdrátových spojů či samotné komunikaci. Tu ovlivňuje i vzdálenost mezi jednotlivými stanicemi.

Nejožehavějším problémem se však jeví zabezpečení a ochrana přenášených dat. Jelikož jsou data volně přenášena prostorem, je možné je snadno odposlechnout či jinak zneužít, a to i bez nutné fyzické přítomnosti útočníka v síti.

Cílem bakalářské práce je prozkoumat a nastínit problematiku bezdrátových sítí WLAN se zaměřením na otázku týkající se jejich bezpečnosti. Tomu odpovídá i struktura bakalářské práce, která je rozdělena na dvě části. První, ryze teoretická část se skládá z několika dílčích kapitol. Ty se zpočátku zabývají popisem a vývojem standardu IEEE 802.11, na kterém je budování WLAN založeno. Dále je popsána struktura bezdrátových sítí a topologie, kterých mohou nabývat. Poslední a nejdůležitější kapitoly teoretické části jsou zaměřeny na bezpečnost. Jsou zde rozebrány jak zabezpečovací protokoly WEP, WPA, WPA2, tak i další bezpečnostní, respektive autentizační mechanismy. Rovněž jsou zmíněny slabiny zabezpečovacích metod a možné bezpečnostní hrozby či útoky na bezdrátové sítě WLAN a jejich zabezpečení. Druhá část bakalářské práce je praktická a zabývá se ověřením bezpečnostních mechanismů. V rámci testování ve specializované linuxové distribuci Kali Linux byly provedeny vybrané z možných útoků, kterých je možno využít buď k neautorizovanému přístupu do sítě či k odchycení a zneužití přenášených dat.

2 Standard IEEE 802.11

Standard IEEE 802.11 je průmyslový standard pro bezdrátové sítě WLAN, jehož počátky se datují k roku 1997. Byl vyvinut institucí IEEE (The Institute of Electrical and Electronics Engineers), což je nezisková organizace, která se velkou mírou podílí na celosvětovém rozvoji technologií, a to v oblastech jako je elektronika, výpočetní technika, informatika a elektrotechnika. [1] Na oficiálních stránkách této instituce se můžeme dozvědět, že sdružuje více než 430 000 odborníků a 117 000 studentů ve více než 160 zemích světa. Tito odborníci se podílejí na vývoji standardů, kterých je momentálně téměř 1700. IEEE vydává rovněž řadu knih a odborných periodik, které tvoří velké procento světové produkce odborné literatury v informatice a elektrotechnice. Důkazem může být obsah digitální knihovny, která čítá více než 3,5 milionu dokumentů. [2]

Standard IEEE 802.11 definuje z referenčního modelu ISO/OSI dvě nejspodnější vrstvy, přičemž ostatní ponechává nedotčené, aby se nemusely vytvářet upravené verze protokolů. První definovanou vrstvou je vrstva fyzická, označovaná jako PHY (Physical Layer), která řeší způsob přenosu dat. Druhou definovanou vrstvou je spojová vrstva, respektive její podvrstva MAC (Media Access Control), která se stará o řízení přístupu k bezdrátovému médiu na základě určitých pravidel. [3]

Spojová vrstva	LLC					
	IEEE 802.11 MAC					
Fyzická vrstva	IEEE 802.11 IR	IEEE 802.11 DSSS	IEEE 802.11 FHSS	IEEE 802.11a OFDM	IEEE 802.11b HR-DSSS	IEEE 802.11g OFDM

Obrázek 1: Pokrytí vrstev dle IEEE 802.11, převzato z [4]

2.1 Fyzická vrstva PHY

Fyzická vrstva je nejspodnější vrstvou ISO/OSI modelu. Jejím úkolem je starat se o vysílání a příjem dat v bezdrátovém prostředí. [3] Standard 802.11 definuje na fyzické vrstvě řadu přenosových mechanismů, z nichž převládají FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum), OFDM (Orthogonaly Frequency Division Multiplex) a MIMO (Multiple-Input Multiple-Output). Původní standard, na rozdíl od jeho nástupců, umožňoval i přenos pomocí infračervených vln. Tento způsob přenosu se však díky malému dosahu a nízké přenosové rychlosti moc nerozšířil. [4]

2.1.1 FHSS

FHSS je jedna z prvních metod bezdrátového přenosu dat využívající rozprostřeného spektra. Techniky rozprostřeného spektra se používají k dosažení větší odolnosti vůči rušícím vlivům. [6] FHSS využívá rozprostřené spektrum pomocí frekvenčních proskoků. Ve své podstatě jde o velmi jednoduchou techniku. Vysílač skáče v náhodném pořadí z jednoho frekvenčního pásma na druhé, přičemž na každém vysílá krátký datový proud. Posloupnost frekvencí, na kterých se vysílá, zná pouze oprávněný příjemce. Každé pásmo má frekvenční šířku 83,5 MHz a je rozděleno na 79 nebo 75 kanálů. Každý kanál má šířku 1 MHz a zbytek šířky pásma slouží jako ochrana proti interferencím přilehlých pásem. Po těchto kanálech radiový signál přeskakuje v náhodném pořadí a každých 30 sekund vystřídá minimálně 75 kanálů. Vysílání trvá maximálně 400 milisekund. U standardu IEEE 802.11 je to dokonce pouhých 20 milisekund [5]. Z toho vyplývá, že se rušení minimalizuje na velmi krátkou dobu. [3]

2.1.2 DSSS

DSSS je metoda přímo rozprostřeného spektra. Ve standardu IEEE 802.11 využívá dohromady 14 kanálů, které mají frekvenční šířku 22 MHz. Rozdíl mezi jednotlivými frekvencemi je 5 MHz. Přilehlé kanály, vyjma tří (1., 6. a 11. kanál), se překrývají. Komunikace pak probíhá pouze na jednom zvoleném kanále. K přenosu dat technika DSSS využívá uměle zavedené redundance. To znamená, že je před přenosem každý bit převeden na určitou sekvenci bitů a až tato sekvence je skutečně přenášena. IEEE 802.11 k takovému nahrazení jednotlivých bitů používá 11bitovou sekvenci označovanou jako tzv. „čip“. [5] Pro úspěšný přenos dat je zapotřebí, aby obě komunikující strany tento mechanismus znaly. Zavedení redundance vede k rozprostření signálu do větší části spektra, což umožňuje větší odolnosti vůči rušení a zvýšení spolehlivosti přenosu. Pokud je příslušná sekvence bitů volena pseudonáhodně, jeví se navíc signál ostatním uživatelům jako náhodný šum. [6] Technika je schopna odolat odposlechu, ale pouze pokud útočník nezná „čipový kód“. Bohužel tyto parametry jsou součástí standardu IEEE 802.11 a jsou tak veřejně známé. Útočník tedy může snadno zachytit přenášenou komunikaci. Z toho důvodu se na podvrstvě MAC používá šifrování dat. [5]

2.1.3 OFDM

OFDM je technikou ortogonálního frekvenčního multiplexu. Dalo by se říct, že nejde úplně o techniku rozprostřeného spektra (nosný signál nemění frekvenční polohu), ale i tato metoda slouží k rozprostření přenosu do větší části spektra s cílem dosáhnout nejvyšší možné přenosové rychlosti. Principem této metody je, že část frekvenčního spektra rozdě-

luje na subkanály. Skrze tyto subkanály se přenáší nosné signály, na které jsou namodulována data konkrétní podoby. Vznikají tak nezávislé přenosové kanály, které umožňují využít maximálních přenosových schopností daného média. [6] Přenosová rychlost může teoreticky nabývat až 54 Mb/s [3]. Díky tomu, že subkanály pracují paralelně, je navíc zaručena vyšší odolnost proti rušení.

2.1.4 MIMO

Síťová specialistka Pužmanová ve svém článku uvádí, že principem technologie MIMO je vysílání několika signálů různými cestami pomocí více antén u vysílače a přijímače. Vždy vysílají a přijímají všechny antény. Vysílače vysílají informace pomocí jednotlivých antén. Jelikož se signály šíří různými cestami, odrážejí se od překážek, a tím se dosahuje větší propustnosti. Signály se pak přijímají na straně přijímače od více antén, kde se následně zkombinují za pomoci náležitých algoritmů. Ty specifikují zpracování signálu a detekují cestu, kterou signál přišel. Na základě těchto faktů se signály rekonstruují a dochází k eliminaci rušení. [7]

Technologie MIMO byla vyvinuta především z důvodu lepšího využití přidělené šířky pásma. Jelikož je omezená, je potřeba využívat ji co nejefektivněji. Díky použití více antén lze dosáhnout vyšší přenosové rychlosti při zachování standardní šířky pásma 20 MHz a navíc snížit vliv různorodosti prostoru na přijímaný signál. To vede ke zvýšení kvality spojení. [8] V dnešní době se technologie MIMO nevyužívá pouze ve WLAN, ale je také zapracována ve standardu IEEE 802.16, který se věnuje metropolitním sítím WMAN a své uplatnění nalezne i v mobilních sítích vyšších generací. [10]

2.2 Podvrstva MAC

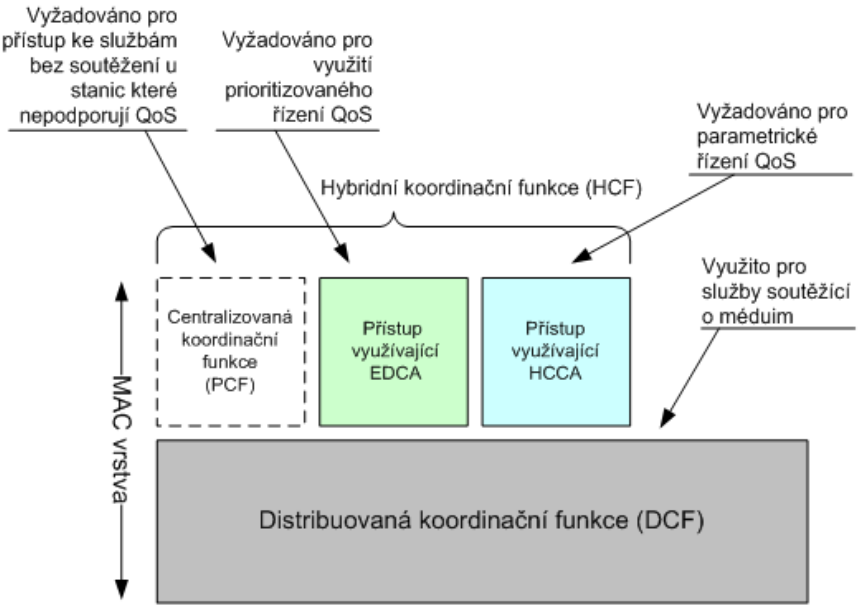
Podvrstva MAC je spodní podvrstvou spojové vrstvy, což je druhá nejnižší vrstva modelu ISO/OSI. Tato podvrstva se nachází mezi horní spojovou podvrstvou a vrstvou fyzickou. Je důležitá pro práci bezdrátových sítí WLAN, jelikož definuje pravidla pro přístup k bezdrátovému médiu. [3] Mezi její základní vlastnosti patří kladné potvrzování, fragmentace paketů, RTS/CTS metoda, cyklický kontrolní součet, autentizace, asociace a další. Pro vysílání, přenos a příjem rámců využívá služeb fyzické vrstvy. [9]

2.2.1 Přístupové metody

Pro správný chod bezdrátových sítí je zapotřebí, aby standard definoval určitá pravidla, na jejichž základě se řídí přístup stanic k přenosovému médiu, a to takovým způsobem, aby pokud možno nedocházelo ke vzniku kolizí. [3]

Původní standard IEEE 802.11 definuje pro přístup ke sdílenému médiu dvě funkce - DCF (Distributed Coordination Function) a PCF (Port Coordination Function). Ani jed-

na z těchto funkcí nerozlišuje typ provozu, takže bez rozšíření nepodporují QoS (Quality of Service), neboli kvalitu služeb. [10] Ta představuje schopnost sítě podporovat aplikace bez omezení výkonu nebo funkčnosti. Kvalita služeb tedy jednotlivým paketům zajišťuje příslušné zacházení na základě jejich priority, nebo kategorie. Pozdější dodatky standardu IEEE 802.11 již přinášejí podporu QoS a rozšiřují tak stávající metody přístupu, přičemž povinné DCF je rozšířeno na EDCF (Enhanced DCF) a volitelné PCF pak na HCF (Hybrid Coordination Function). [11]



Obrázek 2: Přístupové metody, převzato z [12]

2.2.1.1 DCF

DCF je základní metoda, kterou musí povinně podporovat všechny stanice. K řízení přístupu používá mechanismus CSMA/CA (Carrier Sence Multiple Access with Collision Avoidance), což je mechanismus využívající vícenásobného přístupu s detekcí nosné a předcházením kolizí. [12] Principem DCF je, že stanice po určitý časový úsek tzv. DIFS (DCF Interframe Space) naslouchá na přenosovém médiu. Pokud je po uplynutí této doby médium volné, zahájí vysílání. V opačném případě nadále naslouchá na médiu. Ve chvíli, kdy se médium uvolní, stanice vyčká náhodně zvolenou dobu zvýšenou o DIFS a po uplynutí tohoto časového intervalu se opět pokusí o vysílání. Situace, kdy dojde ke kolizi současným vysíláním dvou stanic, je vyřešena potvrzováním přijetí dat, tudíž se příslušná stanice okamžitě dozví o chybném přenosu. V případě, že vysílající stanice neobdrží v definovaném časovém úseku potvrzení, vyhodnotí situaci jako kolizi. [10]

Pro poskytování služeb QoS je metoda DCF nevýhodná, protože neexistuje možnost nastavení priority přenosů a navíc při větším počtu stanic narůstá pravděpodobnost kolizí. V důsledku jejich řešení pak klesá přenosová šířka pásma. [11]

2.2.1.2 PCF

PCF je dle standardu IEEE 802.11 dodatečná volitelná metoda. Využívá se v infrastrukturních sítích, kde centrální správu zajišťuje přístupový bod. V tomto případě má za úkol přidělovat registrovaným žadatelům přenosové médium, přičemž přidělování probíhá na základě priority nebo cyklické obsluhy. Přenos dat je synchronizován pomocí intervalů, kterým se říká *super rámce*. Tyto intervaly jsou rozděleny na dva menší, jimiž jsou CFP (Contention Free Period) a CP (Contention Period). V případě CFP stanice nesoupeří o přístup k médiu, neboť je určován přístupovým bodem. U druhého intervalu CP se využívá pro přístup k médiu metoda DCF. [9]

Metoda PCF je vhodná pro aplikace v reálném čase (například přenášení videa) a umožňuje lépe využít QoS. Jejím omezením je ovšem to, že nedefinuje třídy provozu. [11]

2.2.1.3 EDCF

EDCF je rozšířením metody DCF, která představuje prioritní mechanismus alokace šířky pásma podle definovaných tříd provozu. Každá ze stanic v síti může mít až čtyři tyto třídy na podporu osmi úrovní priority. Na základě priority pak lze rozlišovat možnost zatížení přenosového kanálu podle typu použití, přičemž na každou třídu se mapuje příslušná úroveň priority. Nejvyšší prioritu mají aplikace, které jsou velmi náchylné na zpoždění (například hlasové služby). [9]

Ve chvíli, kdy je médium volné, může jakákoliv ze stanic zahájit vysílání. Tomu ovšem předchází čekací doba AIFS (Arbitration Interframe Space), daná třídou provozu. AIFS se snižuje s rostoucí prioritou provozu. Z toho vyplývá, že stanice s vyšší prioritou provozu, čeká kratší dobu a je jí umožněn volnější přístup k médiu. Jinak řečeno její provoz je upřednostněn před provozy stanic s prioritou nižší. V momentě, kdy má více stanic stejnou prioritu, musí stanice čekat náhodný časový úsek přičtený k AIFS, aby nedocházelo ke kolizím. Po uplynutí této doby může daná stanice zahájit přenos připravených dat.

Metoda EDCF poskytuje velmi vysokou pravděpodobnost přidělení vyšších hodnot šířky pásma pro třídy provozu s vyšší prioritou a vyznačuje se jednoduchostí implementace. Z těchto důvodů je metodou často využívanou. [11]

2.2.1.4 HCF

Metoda HCF funguje velmi podobně jako centralizovaná metoda PCF s tím rozdílem, že jsou definované třídy a fronty provozu. Během intervalu CFP ovládá přístup k médiu takzvaný *hybridní koordinátor*, jímž je nejčastěji přístupový bod. Tento má na starost inicializaci intervalu CFP, kdykoliv je potřeba okamžitě odeslat nebo přijmout data. [10] Během doby úseku CP je využívána metoda EDCF, přičemž kdykoliv během této doby může koor-

dinátor nad přenosovým médiem převzít kontrolu. Stanice mají za úkol specifikovat své požadavky na přidělení média, které koordinátor buď schválí, nebo zamítne, pokud je nemůže zaručit. V kladném případě informuje stanici zasláním příslušného rámce, který ji opravňuje přistoupit k přenosovému médiu a zahájit tak přenos dat. Na základě informací, které stanice poskytují o délkách jejich front požadavků, může koordinátor určité stanice upřednostnit před ostatními.

Metoda HCF je nejpokročilejší a plnohodnotná koordinační metoda, která nabízí propracovanější podporu QoS. [9]

2.3 Podstatné dodatky standardu IEEE 802.11

Jelikož od roku 1997 uplynula dlouhá doba a během tohoto času se začaly objevovat určité nedostatky, původní standard 802.11 zaznamenal mnoho změn, které jsou uvedeny v takzvaných dodatcích. Dodatků k původnímu standardu IEEE 802.11 je celá řada. Tyto dodatky řeší zejména zvýšení maximální přenosové rychlosti, zavádí nové techniky modulace signálu, vylepšují zabezpečení, nebo upravují či rozšiřují předchozí specifikace. Nejznámější, nejpoužívanější a nejnovější z nich jsou uvedeny v následující tabulce i s jejich parametry pro srovnání s původním standardem IEEE 802.11. Ten využíval bezlicenční frekvenční pásmo 2,4 GHz, modulační techniky FHSS a DSSS a poskytoval přenosovou rychlost 1 a 2 Mbit/s. [13]

Standard	Rok vydání	Pásmo [GHz]	Max. rychlost [Mbit/s]	Fyzická vrstva
IEEE 802.11	1997	2,4	2	FHSS, DSSS
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	DSSS, OFDM
IEEE 802.11n	2009	2,4 nebo 5	600	OFDM, MIMO
IEEE 802.11ac	2013	5	1300	MU-MIMO

Tabulka 1: Podstatné dodatky k IEEE 802.11

2.3.1 IEEE 802.11b

K prvnímu vylepšení původního standardu IEEE 802.11 došlo v roce 1999 a to v podobě dodatku IEEE 802.11b, který stejně jako jeho předchůdce pracuje ve frekvenčním pásmu 2,4 GHz, ale nabízí další dvě rychlosti přenosu dat (5,5 a 11 Mbit/s). Pro dosažení vyšších rychlostí využívá k přenosu na fyzické vrstvě nový způsob kódování (*tzv. klíčové kódování*) v rámci techniky modulace signálu DSSS. Maximální rychlost 11 Mbit/s je ovšem teoretická, ve skutečnosti se pohybuje kolem 6 Mbit/s v závislosti na zarušení prostředí či vzdálenosti od přístupového bodu. [13]

2.3.2 IEEE 802.11a

V roce 1999 byl rovněž schválen dodatek IEEE 802.11a, který pracuje v odlišném frekvenčním pásmu 5 GHz. Důvodem přechodu na jiné frekvenční pásmo bylo veliké zarušení v pásmu 2,4 GHz, neboť ho využívá mnoho jiných bezdrátových technologií. Frekvenční pásmo 5 GHz je daleko méně vytížené a poskytuje více nepřekrývajících se kanálů, na rozdíl od pásma 2,4 GHz, kde jsou nepřekrývající se kanály pouze tři. Je to způsobeno většími rozestupy mezi jednotlivými kanály. Rovněž pracuje s výrazně vyšší přenosovou rychlostí (teoreticky až 54 Mbit/s) pro jejíž dosažení jako první využívá na fyzické vrstvě modulační techniku OFDM, která poskytuje větší datovou propustnost a větší odolnost vůči rušení. Mezi nevýhody můžeme zařadit nekompatibilitu zařízení s předešlými standardy díky rozdílnému frekvenčnímu pásmu a menší přenosovou šířku pásma způsobenou kratší vlnovou délkou signálů. [13]

2.3.3 IEEE 802.11g

Standard IEEE 802.11g, schválený v roce 2003, rozšiřuje IEEE 802.11b. Pracuje ve stejném frekvenčním pásmu 2,4 GHz. IEEE 802.11g na úrovni fyzické vrstvy využívá modulaci OFDM a nabízí tak vyšší přenosovou rychlost teoreticky až 54 Mbit/s. Navíc je možné využít i DSSS, což vede ke zpětné kompatibilitě u zařízení, která podporují jeden z těchto standardů. To znamená, že se k přístupovému bodu, který podporuje standard IEEE 802.11g mohou připojit i starší stanice podporující pouze standard IEEE 802.11b a naopak. Pokud se tak ovšem stane, dojde ke snížení rychlosti z 54 na 11 Mbit/s. [14]

2.3.4 IEEE 802.11i

Roku 2004 byla schválena specifikace IEEE 802.11i, která nedefinuje přenosovou rychlost ani frekvenční pásmo, ale zaměřuje se na bezpečnost. Tato specifikace, rovněž známa jako WPA2, má za úkol poskytnout bezpečnost při autentizaci uživatele či přístupového bodu, zajistit integritu a bezpečnost přenosu dat pomocí vylepšených šifrovacích protokolů TKIP a CCMP. Jedná se prozatím o nejlepší možné zabezpečení bezdrátových sítí. [14]

2.3.5 IEEE 802.11n

Standard IEEE 802.11n byl vyvíjen už od roku 2004, ale k jeho schválení došlo až v roce 2009. Důvodem vzniku bylo zvýšení propustnosti sítě ve srovnání s předchozími standardy IEEE 802.11a/g. Tento standard dokáže pracovat v obou bezlicenčních frekvenčních pásmech (2,4 a 5 GHz), přičemž pro dosažení maximální propustnosti se doporučuje využít pásma 5 GHz. Důležité je, že kromě technologií předchozích standardů využívá na fyzické vrstvě technologii MIMO, která se vyznačuje použitím více antén a odolností vůči rušení. Maximální teoretická rychlost je až 600 Mbit/s. [14]

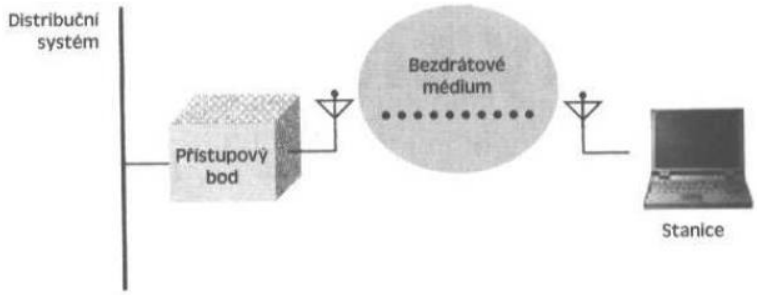
2.3.6 IEEE 802.11ac

IEEE 802.11ac je standard schválený roku 2013. Je též označován jako Wi-Fi páté generace či gigabitová Wi-Fi síť. Standard IEEE 802.11ac komunikuje výhradně ve frekvenčním pásmu 5 GHz. Je však zaručena zpětná kompatibilita s předchozími standardy, takže čip schopný 802.11ac může komunikovat i na 2,4 GHz, ale jen v případě starších standardů. Na rozdíl od 5GHz pásma u standardu IEEE 802.11n, který nejběžněji používal šířku kanálu 20 MHz, používá IEEE 802.11ac nejběžněji šířku kanálu 80 MHz. [15] První specifikace 802.11ac využívaly technologii MIMO převzatou ze staršího standardu 802.11n, která umožňuje přenos dat na jednu stanici více svazky. Další vývoj zavádí tzv. MU-MIMO, s jehož pomocí přístupový bod dokáže vysílat několika stanicím naráz, a to nejčastěji třemi svazky. V jednom svazku lze dosáhnout rychlosti až 433 Mbit/s (při třech svazcích tedy 1300 Mbit/s dohromady). [16]

3 Struktura a topologie 802.11 sítě

3.1 Struktura

Podle Zandla [3] se každá bezdrátová síť založená na standardu IEEE 802.11 skládá ze čtyř hlavních fyzických prvků, jimiž jsou distribuční systém, přístupový bod, bezdrátové přenosové médium a stanice. Vzájemná součinnost všech těchto nezbytných prvků je znázorněna na následujícím obrázku.



Obrázek 3: Struktura 802.11 sítě, převzato z [3]

3.1.1 Distribuční systém

Distribuční systém je logický prvek, směrující tok dat na klientskou stanici podle toho, kde v síti se nachází. Jelikož v síti může být umístěno více přístupových bodů, které tak tvoří rozsáhlejší síť, mají za úkol spolu komunikovat a předávat si informace o pohybu stanic v síti, aby nedocházelo ke ztrátě spojení. Důležité je, že standard 802.11 nespecifikuje technologii distribučního systému, tudíž jím může být jakákoliv forma síťového spojení používaná pro přenos dat mezi přístupovými body. V drtivé většině případů se však jedná o metalický Ethernet. [3]

3.1.2 Přístupový bod

Přístupový bod je nejdůležitější součástí bezdrátové sítě, jelikož přemosťuje spojení mezi bezdrátovou a kabelovou sítí. Kromě této funkce nabízí i mnoho dalších funkcí, jež jsou definovány standardem 802.11 nebo přidané výrobcem. Jedná se o směrování, práci s porty, ale také o zabezpečení bezdrátové sítě, neboť každý, kdo se připojí k přístupovému bodu, musí projít procesem autentizace, na základě které přístupový bod zjistí, zda má klient oprávnění připojit se k dané síti. Tou nejdůležitější funkcí ovšem zůstává ono přemostění mezi kabelovou a bezdrátovou částí sítě. [3]

3.1.3 Bezdrátové přenosové médium

Přenosové médium slouží pro přenos dat a informací v síti. V kabelových sítích se data přenáší pomocí kabelu, kdežto u bezdrátových sítí jsou přenosovým médiem radiové frek-

vence. Standard 802.11 definuje dvě frekvence, a to 2,4 a 5 GHz. Skrze tyto frekvence kolují data a informace mezi stanicemi a přístupovými body. [3]

3.1.4 Stanice

Bezdrátové sítě se budují hlavně z důvodu přenosu dat mezi jednotlivými stanicemi. Za stanici můžeme považovat jakékoliv zařízení podporující bezdrátovou technologii. Většina z těchto zařízení je mobilní, ale není to nutnou podmínkou. Jak již bylo řečeno v úvodu, může nastat situace, kdy je vybudování kabelové sítě technicky hůře realizovatelné, nebo velmi nákladné. Z toho důvodu je lepší volbou vybudování bezdrátové alternativy, i když bude propojovat mezi sebou pouze stanice, které jsou prakticky nepřenosné. [3]

3.2 Topologie

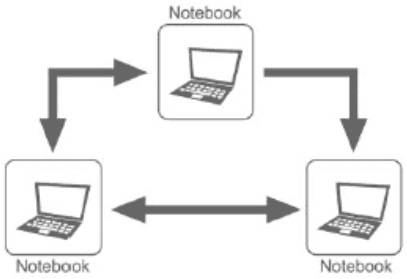
Topologií sítě se rozumí skutečné a logické zapojení různých prvků do počítačové sítě. [17] U bezdrátových sítí je stavebním kamenem základní soubor služeb BSS (Basic Service Set), což je skupina komunikujících stanic. Komunikace mezi stanicemi probíhá v území vymezeném průnikem těchto stanic a nazývá se BSA (Basic Service Area). Každé dvě stanice z BSS spolu mohou komunikovat, pokud se nacházejí v BSA. Pomocí BSS jsme schopni vytvořit síť menších rozměrů. Vytvoření rozsáhlejších sítí, které se rozpínají na větším prostoru, docílíme propojením více BSS skrze páteřní síť do ESS (Extended Service Set), což je označení pro rozšířený soubor služeb. Výsledkem je síť složená z více přístupových bodů či základnových stanic. Stanice náležící do ESS spolu mohou komunikovat, i když náleží do různých BSS. Rovněž se mohou mezi jednotlivými BSS pohybovat. Takto vytvořenou rozsáhlejší síť můžeme s přenosným počítačem procházet beze změn konfigurace. [3]

V praxi se používají dvě základní topologie a to ad-hoc a infrastrukturní sítě. Výběr topologie sítě záleží na jejím funkčním účelu. Bez ohledu na topologii, bezdrátovou síť identifikujeme pomocí SSID (Service Set Identifier), což je označení dané sítě. U infrastrukturních sítí je SSID nastaveno na přístupovém bodu, u Ad-hoc sítí pak na základnové stanici. Přístupový bod nebo základnová stanice následně SSID vysílá v pravidelných intervalech prostřednictvím řídícího rámce. Na základě toho pak můžeme vidět seznam v daný okamžik dostupných bezdrátových sítí, ke kterým je možné se připojit. [13]

3.2.1 Ad-hoc sítě

Jedná se o nezávislé sítě, jelikož stanice spolu komunikují přímo, jsou si rovny a nepotřebují k tomu žádného prostředníka (přístupový bod). První připojená stanice se stává základnovou stanicí a přebírá některé funkce, které jinak nabízí přístupový bod. Mezi tyto funkce patří periodické vysílání SSID a řízení veškeré komunikace v síti. V momentě, kdy dojde k výpadku základnové stanice, ujímá se této řídící role další, náhodně zvolená stani-

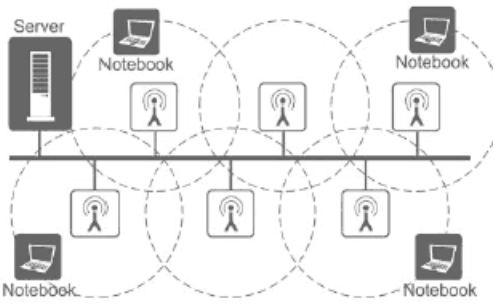
ce. [13] Podmínkou navázání komunikace mezi stanicemi je vzájemná radiová dosažitelnost. Z toho vyplývá, že tato topologie se používá pro menší sítě čítající několik zařízení vzdálených pár metrů od sebe a především na menší časový úsek (výměna dat, hraní her). Pro rozsáhlejší sítě, nebo sítě s více zařízeními, jsou nevhodné. Další nevýhodou je, že vyžadují nakonfigurování nastavení sítě, a proto je v dnešní době daleko jednodušší data přenést například pomocí USB flash disku, nebo se připojit přes přístupový bod (viz následující podkapitola). [3]



Obrázek 4: Topologie sítě Ad-hoc, převzato z [3]

3.2.2 Infrastrukturní sítě

Druhým a častěji používaným typem topologie jsou infrastrukturní sítě, které mají přesně definovanou strukturu. Oproti Ad-hoc sítím mají řadu výhod, mezi které můžeme zařadit například centrální správu či jednodušší nastavení. Obsahují minimálně jeden přístupový bod, který obstarává veškerou komunikaci, a samozřejmě bezdrátové stanice, které přístupový bod využívají pro přístup k běžné kabelové síti. Jeden přístupový bod společně s jednou či více stanicemi tvoří dohromady BSS. Dva a více přístupových bodů zapojené do stejné kabelové sítě pak tvoří ESS. V obou případech platí, že se pro připojení k síti musí stanice nacházet v dosahu některého z přístupových bodů. Přístupový bod může komunikovat i s více než jednou stanicí, avšak jedna stanice může být připojena pouze na jeden přístupový bod. Pro komunikaci mezi stanicemi se využívá přístupového bodu jako prostředníka. Přenášená data putují tedy nadvakrát, nejprve z vysílající stanice na přístupový bod a v druhém kroku z přístupového bodu na cílovou stanici. [3]



Obrázek 5: Topologie Infrastrukturní sítě, převzato z [3]

4 Zabezpečení bezdrátové sítě

Bezdrátové sítě mají oproti kabelovým sítím jednu velkou nevýhodu, a to z bezpečnostního hlediska. V případě kabelových sítí je totiž pro odposlech komunikace protékající sítí zapotřebí, aby měl potenciální útočník fyzický přístup ke kabelovým rozvodům, čemuž se snadno dá zabránit uzamčením příslušných zařízení. U sítí bezdrátových je situace jiná, jelikož se signál šíří volně prostorem, přičemž není technicky možné přesně vymezit prostor, ve kterém lze signál zachytit. Možným útočníkům tedy pouze stačí být v dosahu přístupového bodu. Dosah sítě lze omezit snížením výstupního výkonu přístupového bodu, nicméně problém bezpečnosti to nevyřeší, pouze se zkrátí vzdálenost, ve které se útočník bude muset nacházet. Ovšem použije-li směrovou anténu s dostatečným výkonem, může být vzdálen i několik kilometrů. [5] Dalším bezpečnostním problémem je, že v prostoru vymezeném bezdrátovou sítí může každá stanice zachytit veškerou komunikaci mezi ostatními stanicemi v síti. Výše zmíněná bezpečnostní rizika vedla k zavedení bezpečnostních opatření, která brání útočníkům proniknout do sítě a odposlechnout tak citlivá uživatelská či firemní data. [13]

4.1 Zamezení vysílání SSID

Zamezení vysílání SSID identifikátoru je jednoduchým a často používaným zabezpečením, kdy je přístupovému bodu změnou konfigurace zamezeno vysílat SSID identifikátor, čímž dochází ke skrytí dané sítě. Pakliže uživatel nezná SSID sítě, nemůže se asociovat s přístupovým bodem a je mu tak přístup do sítě znemožněn. K prolomení tohoto velmi jednoduchého zabezpečení ovšem stačí vyčkat na připojení některé ze stanic do sítě a odposlechnout komunikaci při asociaci této stanice, jejíž analýzou lze SSID snadno zjistit. Tento identifikátor se totiž vysílá v nezašifrované podobě. Dokonce ani nemusíme na tuto situaci čekat. Můžeme k odpojení některou ze stanic donutit a při její reasociaci SSID odposlechnout. Na základě zjištěných informací se pak lze připojit do sítě. [5]

4.2 Filtrace MAC adres

MAC adresa, též označovaná jako fyzická adresa, je celosvětově jedinečný identifikátor síťových zařízení skládající se ze 48 bitů, nejčastěji zapsaných pomocí šestice hexadecimálních čísel, která jsou od sebe oddělena pomlčkou. [18] Na základě toho, že žádná dvojice zařízení nemůže mít shodnou fyzickou adresu, můžeme tohoto faktu využít k řízení síťového provozu. Jedná se svým způsobem o velmi triviální variantu zabezpečení bezdrátové sítě. Princip spočívá v omezení provozu v síti na uživatele, kteří mají přípustnou MAC adresu odpovídající povolenému seznamu MAC adres. Tento seznam je uchováván na přístupovém bodu. Pokud by se pokusila do sítě připojit stanice s MAC adresou, která není

obsažena v seznamu, přístup k síti je jí odepřen. V opačném případě dojde k asociaci s přístupovým bodem. [3]

4.3 Vlastnosti zabezpečovacích mechanismů

4.3.1 Autentizace

Autentizace je základní prvek ochrany sítí, který se využívá k řízení přístupu oprávněných uživatelů do dané sítě. Předtím, než je uživateli umožněna komunikace a výměna dat v síti, musí dojít k jeho jednoznačné identifikaci. [5] K této identifikaci dochází na základě uživatelem poskytnutých údajů (nejčastěji dvojice jméno a heslo). Ověřením správnosti těchto údajů lze v kladném případě potvrdit totožnost příslušného uživatele. Další varianty identifikace jsou jednorázová hesla, identifikace pomocí hmotných předmětů (přístupová karta, klíč) a identifikace na základě biometrických údajů (hlas, otisky prstů či sítnice). [18]

Autentizaci můžeme z pohledu směru, ve kterém probíhá, rozdělit na jednosměrnou a obousměrnou. V případě jednosměrné autentizace dochází k autentizaci pouze jedné strany vůči druhé straně. U obousměrné autentizace se obě strany autentizují vzájemně, přičemž každá ze stran sdílí určitou tajnou informaci. Tato informace je samozřejmě pro každou dvojici komunikujících stran odlišná. Stále častěji se rovněž využívá autentizace pomocí důvěryhodné třetí strany. Ta může ověřovat totožnost uživatelů nebo poskytovat údaje potřebné k jejich autentizaci. [5]

4.3.2 Integrita dat

Jednou z dalších vlastností bezpečné komunikace je ochrana přenášených dat, neboli zajištění integrity dat a to před neautorizovanou modifikací během přenosu. Modifikací dat se myslí jejich záměrné nebo náhodné pozměnění či poškození. Integrita dat je tedy udržena tehdy, když je zajištěno, že data jsou úplná, se zaručeným obsahem a jsou provedena opatření proti jejich neautorizované změně. Udržení integrity dat dává příjemci jistotu, že během přenosu data nebyla nikým zmodifikována či poškozena. [5]

4.3.3 Šifrování

Šifrování dat se využívá k utajení a zabezpečení přenášených dat, mnohdy citlivého charakteru, a to před jejich neautorizovaným únikem. [18] Pod pojmem utajení se rozumí přenos dat takovým způsobem, kdy neautorizovaný posluchač v případě odposlechu nerozumí významu přenášených dat. Šifrování dat je tedy proces, kdy jsou nezabezpečená data převedena pomocí šifrovacího algoritmu a klíče na data zašifrovaná a tím pádem čitelná pouze pro držitele dešifrovacího klíče. [5]

Šifrování dat můžeme principiálně rozdělit na dva přístupy, jimiž jsou symetrické a asymetrické šifrování.

4.3.3.1 Symetrické šifrování

Symetrické šifrování je prvním z přístupů utajení dat. Principem tohoto typu šifrování je, že obě komunikující strany používají stejný soukromý klíč a to jak pro šifrování, tak i dešifrování přenášených dat. Jinými slovy, soukromý klíč je využíván symetricky. [18] Největším problémem symetrického šifrování je však distribuce soukromého klíče všem, kteří jej potřebují. Při přenosu klíče sítí je tedy nezbytně nutné zajistit jeho bezpečnost. Z tohoto důvodu je potřeba klíč často měnit. Mimo ochrany dat při přenosu lze symetrické šifrování využít i pro autentizaci. [5]

Mezi symetrické šifrovací algoritmy, které jsou většinou velmi rychlé a veřejně popsané, můžeme zařadit například DES (Data Encryption Standard), 3DES (Triple DES) a AES (Advanced Encryption Standard). Síla těchto blokových šifer se vyjadřuje délkou použitého klíče, přičemž za bezpečné klíče se považují ty, jež mají 128 a více bitů. [18]

- **DES, 3DES** - Šifrovací algoritmus DES byl původně navržený pro banky. Využívá bloky o délce 64 bitů, přičemž pro šifrování je využito 56bitového klíče (každý osmý bit je totiž parita). Při rostoucí výkonnosti počítačové techniky a malé délce klíče došlo k tomu, že byl DES v roce 1997 prolomen pomocí útoku hrubou silou. Algoritmus DES byl tedy vylepšen na algoritmus 3DES. Jak název napovídá, principem je trojité použití DES, což zaručuje větší odolnost vůči prolomení. Nevýhodou je však menší rychlost.
- **AES** – V roce 2001 došlo k nahrazení algoritmu DES algoritmem AES, který používá klíče o délce 128, 192 či 256 bitů. To zaručuje mnohem větší počet všech možných kombinací, které by bylo nutné při útoku hrubou silou projít. Momentálně je prolomení AES považováno za nemožné. [19]

4.3.3.2 Asymetrické šifrování

Dalším přístupem ochrany a utajení dat je asymetrické šifrování, které spočívá ve využití dvojice doplňujících se klíčů (veřejný a soukromý klíč), přičemž každá z komunikujících stran vlastní jeden z nich. Pro zašifrování dat se používá veřejný klíč, který může použít kdokoliv, zatímco dešifrování lze provést pouze pomocí soukromého klíče. Každá dvojice stanic může bezpečně komunikovat bez předchozího předávání klíčů díky dvojímu šifrování (veřejným a soukromým klíčem). [18] Velká výhoda tohoto typu šifrování je jednoduchá správa klíčů, jelikož pro distribuci veřejného klíče není nutná zabezpečená komunikace a soukromý klíč se skrze síť nepřenáší (je uchováván v systému). Případně se pro kaž-

dou novou relaci generuje nový pár klíčů. Pokud dojde ke změně soukromého klíče, vygeneruje se i nový veřejný klíč, který je inzerován namísto původního. [5]

Mezi asymetrické šifrovací algoritmy, které jsou pomalejší než symetrické, můžeme zařadit například algoritmy Diffie-Hellman či RSA. Používají klíče o velikosti i několika kilobitů.

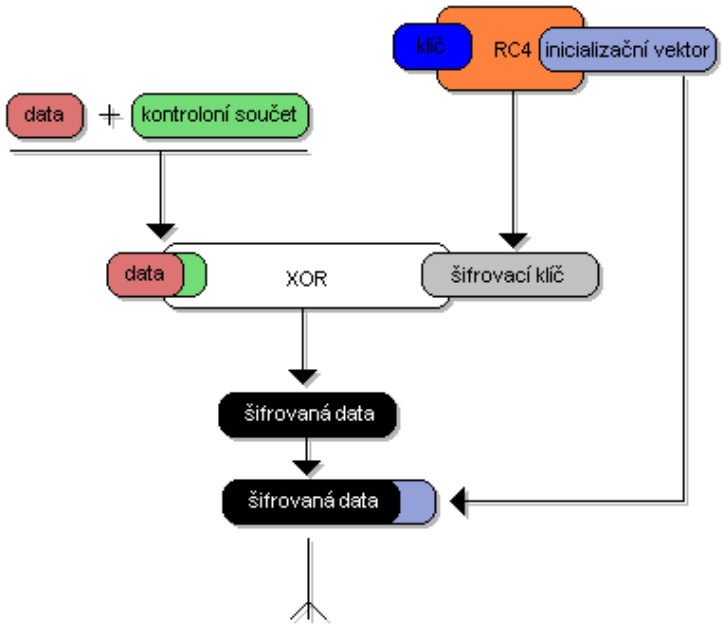
- **Diffie-Hellman** – Jeden z prvních algoritmů pro asymetrické šifrování, publikovaný roku 1976. Používá se pro distribuci klíčů a ty následně pro šifrování dat.
- **RSA** – Algoritmus RSA byl vyvinut v roce 1997, přičemž zkratka RSA představuje počáteční písmena jmen jeho autorů. Jedná se o nejznámější asymetrickou šifru tvořící základ většiny asymetricky šifrujících systémů a navíc se dá využít i pro autentizaci či v elektronické poště. Spolehlivost tohoto algoritmu závisí na délce použitého klíče, přičemž se doporučuje použít klíče o délce alespoň 2048 bitů. [18]

4.3.3.3 Kombinované šifrování

Ani jeden z předešlých přístupů šifrování dat není dokonalý. V případě symetrického šifrování se vyžaduje použití identického klíče a asymetrické šifrování je díky své výpočetní náročnosti pomalé. Tyto nedostatky se řeší kombinovaným použitím obou zmíněných metod. Princip spočívá v tom, že data se zašifrují symetrickou šifrou. Klíč pro symetrickou šifru je zašifrován asymetricky, přiložen k datům a bezpečně přepraven. Asymetricky se pak šifrují nebo dešifrují pouze data malé velikosti. [18]

4.4 WEP

Dnes již zastaralý bezpečnostní protokol WEP (Wired Equialent Privacy) byl prvním způsobem zabezpečení bezdrátových sítí přítomným již v původním standardu IEEE 802.11. Používání tohoto typu zabezpečení bylo volitelné a standardem nebylo vyžadováno, ale pouze doporučováno. Cílem WEP bylo zamezit možnému odposlechu a poskytnout zabezpečení bezdrátové sítě na stejné úrovni odpovídající sítím kabelovým. [3] Skutečnost byla ovšem poněkud jiná a tato očekávání se nenaplnila, jelikož návrh a provedení čítá mnoho nedostatků. Mezi tyto nedostatky můžeme zařadit například nevhodné provedení šifrovacího algoritmu, částečnou předvídatelnost obsahu zašifrovaných dat a chybějící distribuci klíčů. Díky těmto nedostatkům se zabezpečení WEP stalo snadno prolomitelné a jako zabezpečení dnešních bezdrátových sítí je považováno za nevyhovující. [20] Nutno však podotknout, že ochrana bezdrátové sítě pomocí WEP je stále lepší variantou, než nepoužít zabezpečení žádné a ponechat tak síť naprosto nezabezpečenou.



Obrázek 6: WEP, převzato z: http://wiki.airdump.cz/Hacking_WiFi_sítí

4.4.1 Šifrování

Pro šifrování dat se u protokolu WEP využívá symetrická proudová šifra RC4 (Rivest Cipher 4) a to zejména díky jednoduchosti její hardwarové implementace přímo do síťového adaptéru. Jelikož se jedná o symetrickou šifru, používá stejný šifrovací klíč pro šifrování i dešifrování dat (viz kapitola 4.3.3.1). Síla šifry RC4 je dána délkou použitého šifrovacího klíče a četností jeho obměny. Tento šifrovací klíč může nabývat hodnot 64, 128, 152 či 256 bitů (podle výrobce zařízení), přičemž se skládá ze dvou částí. První z nich je tajný klíč a druhou inicializační vektor IV, který se mění a má konstantní délku 24 bitů. Na tajný klíč tedy připadá 40, 104, 128 nebo 232 bitů. [23] Šifrovací klíč je výstupem pseudonáhodného generátoru, na jehož vstup se přivede tajný klíč společně s inicializačním vektorem, přičemž velikost šifrovacího klíče je přímo úměrná velikosti šifrované zprávy. Takto vzniklý šifrovací klíč se poté sečte na bitové úrovni s vlastní přenášenou zprávou pomocí funkce XOR, čímž vzniká zašifrovaný text. Tento se společně s vektorem IV odešle. Na straně příjemce pak dešifrování probíhá opačným postupem a tedy tak, že se použije inicializační vektor obsažený v přijatém rámci společně se sdíleným tajným klíčem jako vstup pseudonáhodného generátoru, čímž dostaneme šifrovací klíč, kterým byla zpráva zašifrována. Následně provedeme součet zjištěného klíče se zašifrovaným textem pomocí operace XOR a dostaneme původní zprávu. [3]

Nejdůležitější předpoklad pro použití proudové šifry RC4, je jedinečnost každého šifrovacího klíče, avšak problém tkví v tom, že inicializační vektor má délku 24 bitů a může tedy nabývat maximálně 2^{24} (zhruba 16,7 milionu) hodnot. Z toho vyplývá, že neopakovatelnost šifrovacího klíče, je při běžném síťovém provozu zaručena jen po určitou dobu

a poté dojde k jejich opakování. V důsledku tohoto opakování pak sítí začnou kolovat rámce, které byly zašifrovány pomocí stejného klíče. To pochopitelně vede k možným útokům a následnému prolomení použitého klíče, jelikož část šifry je již známa (IV je přenášen nezašifrovaně). [5] Standard IEEE 802.11 nedefinuje způsob, jakým mají být tajné klíče přidělovány či distribuovány a ponechává to tak čistě v režii výrobců. Dokonce ani nedefinuje, jak často má za účelem zvýšení bezpečnosti docházet k obměně tajných klíčů. Na mnoha zařízeních lze navíc změnu provést pouze manuálně, což může být v případě rozsáhlých sítí velmi obtížné. [3]

4.4.2 Autentizace

Protokol WEP podporuje dva možné způsoby provedení autentizace. Prvním z nich je autentizace otevřená (Open-system) a druhým autentizace sdíleným klíčem (Shared-key). V obou případech se jedná o jednosměrnou autentizaci, což znamená, že si stanice o autentizaci do sítě musí zažádat, zatímco přístupový bod se vůči stanici autentizovat nemusí. [5]

4.4.2.1 Open-system autentizace

V případě otevřené autentizace se jedná o tzv. *dvoucestnou výměnu údajů* mezi stanicí a přístupovým bodem. Každá stanice, která se chce připojit do sítě, musí znát SSID identifikátor dané sítě. Nejdříve stanice pošle přístupovému bodu požadavek na autentizaci v podobě vyplněného SSID identifikátoru a pokud je vyplněno správné SSID, je každá tato stanice autentizována a připojena do sítě. Nedochází tedy k žádnému ověřování totožnosti zadáváním přístupového hesla atp. Pro zamezení přístupů nežádoucích stanic se doporučuje vypnout vysílání SSID, jelikož stanice která nezná SSID se do sítě připojit nemůže. Nicméně zjistit SSID takto skryté sítě není až takový problém (viz kapitola 4.1). [3]

4.4.2.2 Shared-key autentizace

Autentizace sdíleným klíčem je propracovanější metodou, než výše zmíněná otevřená autentizace. I zde se jedná o výměnu údajů mezi stanicí a přístupovým bodem. [3] V tomto případě jde však o výměnu čtyřcestnou a za použití sdíleného WEP klíče. Stanice přistupující do sítě musí tento sdílený klíč znát, přičemž znalost klíče ověřuje přístupový bod. Proces zahajuje stanice zasláním požadavku na autentizaci přístupovému bodu. Ten vygeneruje náhodný text a zašle jej stanici jako výzvu. Stanice přijatý náhodný text zašifruje pomocí sdíleného WEP klíče proudovou šifrou RC4 a odešle zpět přístupovému bodu jako odpověď na výzvu. Přístupový bod dešifruje odpověď a v případě shodnosti původně odeslaného a dešifrovaného náhodného textu dochází k autentizaci stanice.

Byť se zdá, že tento způsob autentizace je lepší a propracovanější, než autentizace otevřená, z bezpečnostního hlediska tomu tak není. Důvodem je, že potenciální útočník

může zachytit jak nezašifrovanou výzvu, tak i šifrovanou odpověď. Pokud se tak stane, následnou kryptoanalýzou lze rozluštit sdílený WEP klíč. [5]

4.4.3 Integrita dat

Pro zajištění integrity přenášených dat se využívá kontrolního součtu, což je režijní informace přidaná k vlastním datům sloužící k ověření, zda jsou přenášená data úplná a nedošlo tedy k jejich poškození. [18] Princip spočívá v tom, že se na straně odesílatele vypočte kontrolní součet nad přenášenými daty. K tomuto výpočtu se v případě protokolu WEP používá lineární metoda CRC-32 (Cyclic Redundant Check). Hodnota výpočtu, označovaná ICV (Integrity Check Value), se společně s vlastními daty a fyzickou adresou příjemce a odesílatele vloží do rámce. Poté dojde k zašifrování celého rámce a jeho přenosu. Na straně příjemce se nejprve rámec dešifruje, a nad jeho datovou částí se opět metodou CRC vypočítá hodnota ICV. Následně se obě hodnoty ICV porovnají. Pokud se shodují, přenos proběhl v pořádku a data nebyla poškozena. V opačném případě to znamená, že během přenosu došlo k chybě nebo špatnému výpočtu kontrolního součtu a rámec se zahodí.

Metoda CRC-32 pro výpočet kontrolního součtu je spíše vhodná pro předcházení náhodně vzniklých chyb během přenosu. Díky své lineární povaze totiž snadno podlehne útokům, kdy dojde k záměrné změně dat společně s podvržením nově vypočtené hodnoty ICV a to aniž by příjemce tuto změnu zjistil. [5]

4.5 IEEE 802.1X

Standard IEEE 802.1X je obecný bezpečnostní rámec, který se používá pro řízení přístupu jak v kabelových sítích, pro které byl původně určen, tak i v bezdrátových sítích, kde se řízení přístupu stalo daleko větším problémem. Tento bezpečnostní rámec zahrnuje autentizaci uživatelů, šifrování dat a distribuci klíčů. [3] 802.1X je implementován na druhé vrstvě modelu ISO/OSI a zamezí tedy komunikaci využívající vyšších vrstev, pokud selže autentizace na vrstvě MAC. Ověřování se v případě bezdrátových sítí realizuje na úrovni logických portů přístupového bodu, přičemž 802.1X blokuje komunikaci do té doby, než je uskutečněna úspěšná autentizace příslušným klientem. [13] Celý mechanismus řízení přístupu využívá tři funkční entity:

- **Suplikant** - program na klientovi, který se pokouší připojit do sítě.
- **Autentizátor** - aktivní prvek na síťové straně, se kterým komunikuje suplikant. Jeho cílem je ověřit klienta. V případě bezdrátových sítí jde o přístupový bod.
- **Autentizační server** - zařízení rozhodující o autentizaci suplikantů na základě autentizačních informací, které poskytuje autentizátoru. Nejčastěji se jedná o Kerberos nebo RADIUS. [20]

Autentizační mechanismus 802.1X je založen na standardizovaném protokolu EAP (Extensible Authentication Protokol), což je rozšiřitelný autentizační mechanismus umožňující implementovat různé druhy autentizace (EAP-MD5, EAP-TLS, EAP-TTLS, PEAP a další). Protokol EAP zprostředkovává výměnu autentizačních zpráv mezi suplikantem (klientská stanice) a autentizátorem (přístupový bod), které autentizátor dále předává autentizačnímu serveru. Jedná se o mechanismus přenosu EAP paketů zapouzdřených do 802.1X rámců prostřednictvím spojové vrstvy LAN. Díky tomu se 802.1X označuje též jako EAPOL (Extensible Authentication Protocol Over LANs). [21]

Ověřování klienta provádí v bezdrátové síti přístupový bod, který zastává roli autentizátora. Port, na kterém je klient připojen, se do momentu úspěšné autentizace klienta nachází v blokovaném stavu a jediný způsob komunikace mezi klientem a přístupovým bodem je prostřednictvím autentizačních rámců. Proces ověřování probíhá následovně - Ve chvíli, kdy je klientská stanice v dosahu přístupového bodu, odešle počáteční zprávu na přístupový bod. Přístupový bod v roli autentizátora odpoví dotazem na identitu klienta zprávou EAP-Request/Identity (obsahuje například označení sítě, ke které se chce klient připojit) zabalenou do 802.1X rámce. Suplikant na klientovi dotaz vyhodnotí a odpoví zprávou EAP-Response/Identity, která obsahuje identifikační údaje uživatele. Autentizátor z přijatého 802.1X rámce zprávu vybalí, zapouzdří ji do paketu protokolu RADIUS a odešle autentizačnímu serveru (RADIUS server) pro ověření. Na základě údajů uvedených klientem autentizační server odpoví zprávou obsahující povolení nebo zákaz přístupu do sítě pro příslušného klienta (RADIUS ACCESS_ACCEPT/DENY). Tato zpráva obsahuje informaci EAP SUCCESS/FAILURE, kterou autentizátor vyhodnotí a přepošle klientovi. V kladném případě (EAP SUCCESS) je příslušný port přes který probíhala autentizační komunikace odblokován a danému uživateli je díky úspěšné autentizaci umožněn přístup do sítě. V opačném případě zůstává port blokovaný a přístup je zamítnut. [3]

Pro každou autentizovanou klientskou stanici výše zmíněným způsobem používá standard 802.1X k šifrování datové komunikace dynamické klíče. Ty jsou známy pouze dané stanici a mají omezenou životnost (dokud se stanice neodhlásí nebo neodpojí). [3] Pro ukončení komunikace v síti, klient vyšle autentizátoru zprávu EAPOL-LOGOFF, na jejímž základě autentizátor převede příslušný port opět do blokovaného stavu. Do tohoto stavu se port převede i v případě, kdy je klient odpojen nebo vyprší časový úsek, během kterého se měl klient opětovně autentizovat.

Mezi výhody mechanismu 802.1X patří možnost zablokovat přístup k síti neautorizovaným osobám a použití dynamických klíčů, které poskytují větší míru bezpečí proti případným průnikům do sítě. Nutno však podotknout, že hlubší problematiku bezpečnosti tento mechanismus neřeší, tudíž není neprolomitelný a je potřeba používat i další bezpeč-

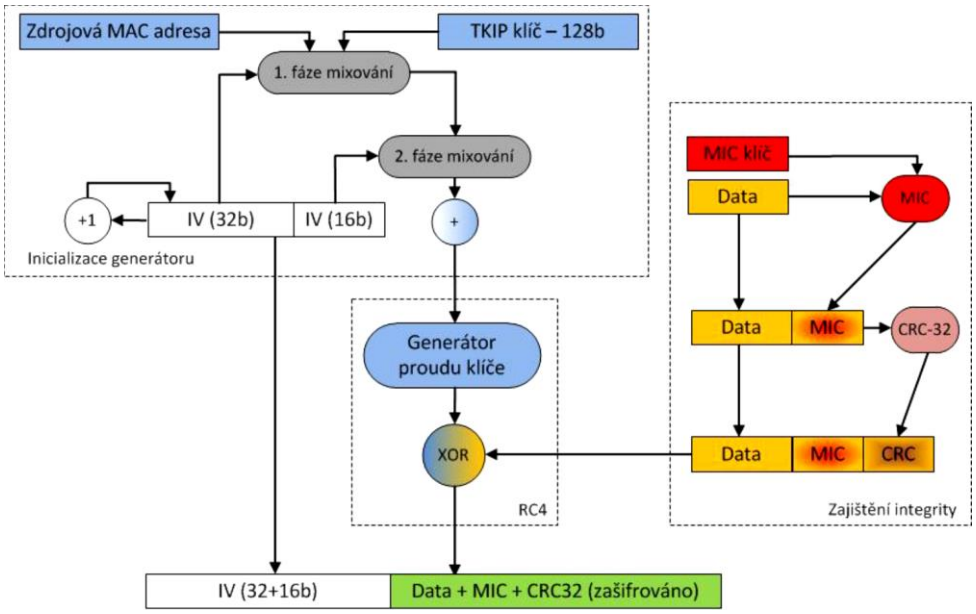
nostní mechanismy. Nevýhodou je i nemožnost komunikace se stanicemi, které jsou připojeny na neautorizovaný port. Je tak znemožněna jejich vzdálená správa. [22]

4.6 WPA

Jelikož v roce 2001 došlo k prolomení zabezpečení bezdrátových sítí WEP, bylo zapotřebí tento problém vyřešit. Organizace IEEE přišla s tím, že vytvoří nový bezpečnostní standard IEEE 802.11i, ale jeho vývoj byl značně pomalý. Z důvodu oddalování ratifikace standardu IEEE 802.11i a velkého úpadku prodeje bezdrátových zařízení se tedy sdružení Wi-Fi Alliance rozhodlo v roce 2003 publikovat vybrané a již hotové části budoucího standardu. Byl vydán popis zabezpečení bezdrátových sítí, který vycházel ze třetího pracovního návrhu IEEE 802.11i, nazvaný WPA (Wi-Fi Protected Access). [20] Bezpečnostní protokol WPA představoval jakýsi mezistupeň mezi původním, z hlediska bezpečnosti nevyhovujícím protokolem WEP a zcela nově vyvíjeným komplexním standardem IEEE 802.11i. Úkolem WPA bylo eliminovat bezpečnostní slabiny WEP (slabá autentizace, management klíčů, šifrování statickým klíčem) při zachování zpětné hardwarové kompatibility s již existujícími zařízeními, u kterých bylo pouze potřeba provést aktualizaci firmwaru. [23] WPA mělo sloužit jako dočasné řešení pro zabezpečení bezdrátových sítí do doby, než bude dokončen vývoj standardu IEEE 802.11i [5], ovšem i v dnešní době poskytuje celkem dobrou míru zabezpečení.

Základní vlastnosti WPA:

- Autentizace - pomocí PSK (Pre-Shared Key) nebo 802.1X a protokolu EAP
- Šifrování dat - použit protokol TKIP (Temporal Key Integrity Protocol)
- Integrita dat - zajištěna pomocí algoritmu MIC (Message Integrity Code)



Obrázek 7: WPA, převzato z: http://wiki.airdump.cz/Wi-Fi_Protected_Access

4.6.1 Šifrování

Standard WPA vyžaduje šifrování dat pomocí protokolu TKIP, který nahrazuje šifrování WEP novým silnějším šifrovacím algoritmem. K provádění šifrovacích operací využívá možnosti existujících bezdrátových zařízení. [23] Z toho důvodu je opět použita proudová šifra RC4, avšak s 128bitovým klíčem a inicializačním vektorem rozšířeným na 48 bitů. Hlavní vylepšení oproti WEP spočívá v tom, že data se nešifrují statickým klíčem. Protokol TKIP zavádí dynamické generování dočasných TKIP klíčů, které se mění každých 10 000 paketů. Výměna se provádí tak, že nový klíč je zašifrován tím starým a odeslán jako zpráva. TKIP rovněž poskytuje důkladnější způsob inicializace RC4 šifry a zavádí sekvenční počítadlo paketů, díky kterému se hodnota IV postupně zvyšuje. Očíslovaný paket, který je přijat mimo tuto posloupnost, je zahozen (obrana proti útokům typu replay). [5]

Hodnota IV se v případě TKIP dělí na dvě části, z nichž první o délce 16 bitů se pro klasické IV doplní do 24 bitů. Druhá část o délce 32 bitů zaznamenává pořadové číslo paketu a využívá se ke kombinování klíčů pro jednotlivé pakety. Celý proces inicializace generátoru se skládá ze dvou fází (viz obrázek č. 8). V první fázi se promíchá 32bitová část IV, MAC adresa zařízení a dočasný TKIP klíč relace. V druhé fázi se výsledek první fáze promíchá s dočasným TKIP klíčem relace a 16bitovou částí IV. Výstup druhé fáze má délku 128 bitů a je využit pro inicializaci šifry RC4, kdy následné šifrování probíhá stejně jako v případě WEP. [5]

4.6.2 Autentizace

WPA umožňuje dvě různé metody autentizace, jejichž způsob provedení se rozlišuje na základě prostředí, ve kterém je autentizace prováděna. Při návrhu WPA byl tedy brán ohled na možnost využití jak ve firemním, tak i domácím prostředí.

4.6.2.1 WPA - Enterprise

Režim Enterprise je vhodný především pro rozsáhlé bezdrátové sítě sdružující velké množství uživatelů, které vyžadují maximální zabezpečení (typicky velké firmy). [24] Pro distribuci klíčů a zejména pak pro autentizaci se předpokládá použití standardu 802.1X, který využívá několika desítek možných metod autentizace v rámci EAP a ověřování totožnosti uživatele pomocí centralizovaného autentizačního serveru (RADIUS). Autentizace je prováděna na základě přihlašovacích údajů (každý uživatel má jiné), smart karty, certifikátu nebo pomocí jiných forem zabezpečení. Proces autentizace viz kapitola 4.5. Díky bezpečnému ověření uživatele a autentizačního serveru zabraňuje útokům typu man-in-the-middle (viz kapitola 5.6). [20]

4.6.2.2 WPA - PSK

Režim autentizace PSK je vhodný pro menší podnikové či domácí sítě, kde se nevyplatí provozovat autentizaci pomocí standardu 802.1X. Z tohoto důvodu je občas přezdíván jako *osobní režim*. [24] Autentizace uživatele probíhá na úrovni přístupového bodu pomocí předsdíleného klíče, který je zadán manuálně jak na straně přístupového bodu, tak na straně uživatele. Hodnota tohoto klíče se skládá z 64 hexadecimálních čísel (určených ze zadaného hesla o délce 8 až 63 tisknutelných znaků) a využívá se jako výchozí hodnota pro protokol TKIP, který z této hodnoty následně generuje šifrovací klíče. Pro přístup do sítě je nutné klíč znát. Na základě jeho znalosti přístupový bod rozhoduje o autentizaci daného uživatele. Bezpečnostním rizikem tohoto přístupu je použití slabého hesla, které nemusí odolat slovníkovým útokům či útokům hrubou silou. [20]

4.6.3 Integrita dat

Pro zajištění integrity přenášených dat je v případě standardu WPA využit protokol MIC, jehož základem je metoda pro výpočet kontrolního součtu označovaná jako Michael. Jedná se o rychlý algoritmus, který není náročný na výpočetní výkon, jelikož obsahuje pouze výpočetní operace posunu a sčítání. To z toho důvodu, aby mohl být použit na již existující 802.11 hardware bez snížení výkonu. [20]

Osmibytový kontrolní součet MIC je vypočten z datové části rámce, zdrojové a cílové adresy MAC a 64bitového MIC klíče odvozeného z klíče každého paketu. Vypočtená hodnota MIC je umístěna mezi datovou část rámce IEEE 802.11 a čtyřbajtovou hodnotu ICV, která je výsledkem metody CRC-32. Pole kontrolního součtu MIC je šifrováno společně s hodnotou ICV a daty rámce.

Pro zajištění integrity před záměrnou modifikací, vícenásobným použitím zpráv, či falešným zprávám používá algoritmus Michael ochranný mechanismus. Jestliže jsou během definovaného časového sledu přijaty dva rámce, u kterých nesouhlasí hodnota MIC, dojde k odpojení klienta, jelikož se předpokládá, že je vystaven útoku. Jako protiopatření vymaže své klíče a po dobu jedné minuty čeká, než se znovu připojí a dojedná si nové TKIP klíče. [5]

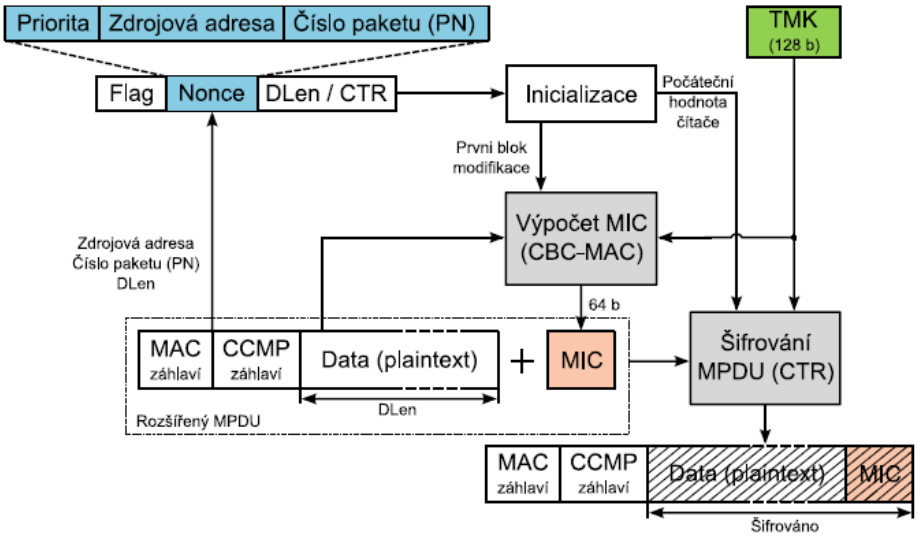
4.7 WPA2

V roce 2004 byl konečně dokončen vývoj komplexního bezpečnostního standardu IEEE 802.11i, jehož cílem bylo eliminovat nedostatky prolomitelného zabezpečení WEP a zajistit tak celkovou informační bezpečnost bezdrátových sítí založených na standardu IEEE 802.11. [5] Jelikož WPA vycházelo pouze ze třetího návrhu IEEE 802.11i, bývá tento již komplexní standard komerčně označován jako WPA2. Bezpečnostní komplexnost si však vyžádala daň v podobě vyšší výpočetní náročnosti nově implementovaných bezpečnostních mechanismů, které jsou zabudovány přímo v síťovém hardwaru. Z tohoto důvodu WPA2 nelze používat na starších, výpočetně slabších zařízeních, jelikož nepostačí pouhá aktualizace firmwaru jako v případě přechodu z WEP na WPA. Při návrhu však byl brán ohled na skutečnost, že stále existuje značné množství bezdrátových zařízení, která nedokáží vyhovět nárokům WPA2 a vznikly tak dvě možné alternativy nasazení 802.11i. Pro zařízení s plnou podporou je využita architektura bezdrátových sítí s označením RSN (Robust Security Network), která je sice složitější, ale za to nabízí bezpečná a škálovatelná řešení bezdrátové komunikace (autentizace 802.1X, silná distribuce klíčů, nové mechanismy pro zajištění integrity a utajení přenášených dat). Pro starší zařízení byla v 802.11i definována architektura TSN (Transition Security Network) umožňující koexistenci WEP systémů společně s RSN systémy. [20]

Distribuce klíčů a metody autentizace zůstaly obdobné jako v případě WPA. Pro sítě malých rozměrů (domácí či menší podnikové sítě) se využívá režim WPA2-Personal s předsdíleným klíčem PSK, zatímco pro rozsáhlejší firemní sítě je vhodný režim WPA2-Enterprise, který využívá standard IEEE 802.1X za pomoci centralizovaného autentizačního serveru. Jedním z nových bezpečnostních prvků oproti WPA je předběžná autentizace, která je sice volitelná, avšak její použití usnadňuje funkčnost sítí podporujících kvalitu služeb QoS, jelikož umožňuje bezpečný přechod (roaming) mezi jednotlivými přístupovými body (v rámci ESS) s minimálním zpožděním.

Podstatná změna spočívá ve způsobu šifrování a zajištění integrity dat. WPA využívá k šifrování proudovou šifru RC4 společně s protokolem TKIP. Ten je v případě WPA2 už jen volitelný a je zde zachován z důvodu zpětné slučitelnosti. WPA2 zavádí nový šifrovací protokol CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), který poskytuje silnější šifrování pomocí symetrické blokové šifry AES (Advanced Encryption Standard) založené na algoritmu Rijndael. [25] Protokol CCMP se navíc stará i o zajištění a kontrolu integrity dat. Pro tyto účely je využito dvou režimů činnosti šifry AES. Prvním z nich je takzvaný režim počítadla CTR (Counter Mode) používaný k šifrování dat a druhým pak režim CBC-MAC (Cipher Block Chaining Message Authentica-

tion Code) používaný k zajištění autentičnosti a integrity dat, přičemž oba tyto režimy protokol CCMP využívá společně pod souhrnným označením CCM (CTR with CBC-MAC). [28]



Obrázek 8: WPA2, převzato z [23]

Šifra AES pracuje s bloky dat pevné délky, která je standardem 802.11i stanovena na 128 bitů, stejně jako velikost použitého dočasného klíče. V případě, že jsou šifrovaná data delší, dochází k jejich rozdělení na 128bitové bloky, které se zpracovávají jednotlivě. V opačném případě je nutné data kratší délky doplnit na požadovanou délku 128 bitů pomocí takzvané vycpávky (nulové bity), která je přidávána v rámci výpočtu MIC, ale do přenosu se nezahrnuje. [26]

K rozdělení původní zprávy na bloky dat o pevné délce dochází v režimu CTR, který pro svou činnost využívá počítadlo. Toto počítadlo je inicializováno na počáteční náhodnou hodnotu, která se pro každý zpracovávaný blok zprávy zvyšuje o určitou velikost (většinou o 1). Hodnota počítadla se zašifruje šifrou AES, čímž dochází k vygenerování 128bitového dočasného klíče, jehož hodnota se sečte na bitové úrovni pomocí funkce XOR společně s daným 128bitovým blokem dat původní zprávy. Výsledkem je zašifrovaný text. [28] Svým způsobem se bloková šifra AES vlastně používá jako proudová. Tím dochází ke kombinaci bezpečnosti blokové šifry společně s jednoduchým užitím šifry proudové. [27]

Výše zmíněným způsobem je zajištěno utajení dat, ale ne jejich integrita. Ta je zajištěna pomocí autentizačního kódu zprávy MAC (Message Authentication Code) v rámci režimu CBC-MAC, který poskytuje možnost kontroly přenášených dat jak před úmyslnou modifikací útočníkem, tak i tou neúmyslnou, způsobenou vlivem rušení při přenosu. [28] Pro výpočet hodnoty MAC (respektive MIC) je využit algoritmus založený na blokových šifrách, který obsahuje operaci pro jejich řetězení. Jedná se o CBC (Cipher Block Chaining) algoritmus, jehož principem je, že se odpovídající blok otevřeného textu před zašifrováním bitově sečte pomocí funkce XOR společně se zašifrovaným textem bloku předcházejícího.

Výsledek operace XOR se následně zašifruje pomocí AES a slouží jako vstup funkce XOR pro další šifrovaný blok. Takto se pokračuje až do konce šifrované zprávy. Nutno však dodat jak probíhá zpracování prvního bloku dat, kterému žádný blok nepředchází. První blok je modifikován inicializační hodnotou a funkcí XOR, přičemž výsledek této operace je zašifrován pomocí AES a použit pro druhý blok. Z výše uvedeného vyplývá vzájemná závislost mezi jednotlivými bloky. Pro dešifrování určitého bloku je tedy potřeba dešifrovat všechny bloky, které tomuto předcházejí. [29]

Protokol CCMP rozšiřuje původní velikost rámce o 16 bytů (8 bytů CCMP hlavička a 8 bajtů kontrola integrity MIC). CCMP hlavička mimo jiné obsahuje důležitý prvek v podobě 48bitového čísla paketu PN (Packet Number), které je využito jako sekvenční čítač a poskytuje tak ochranu proti útokům typu replay. Tento čítač totiž čísluje jednotlivé pakety, přičemž ten, který je přijat mimo posloupnost, je zahozen. Svým způsobem se číslo paketu PN dá přirovnat k dříve zmíněné hodnotě inicializačního vektoru IV v protokolu TKIP. Hlavička CCMP je umístěna mezi MAC hlavičkou a datovou částí rámce a nešifruje se. Šifruje se pouze datová část rámce (pomocí CTR), jelikož fyzické adresy komunikujících stanic a další pole obsažené v hlavičce musejí být odesílány v nezašifrované podobě. Nicméně, i když hlavička rámce není šifrována, příjemce potřebuje záruku, že data nebyla po cestě změněna. Tuto záruku poskytne 64bitová hodnota MIC určená pomocí CBC-MAC. Použitím protokolu CCMP je tedy současně zajištěno utajení, autenticita, kontrola integrity dat a číslování paketů. [28]

Zabezpečení pomocí WPA2 využívající protokol CCMP a šifru AES je v dnešní době nejlepším možným typem zabezpečení bezdrátových sítí. Toto zabezpečení je považováno za zcela bezpečné, jelikož doposud nebylo prolomeno.

4.8 Porovnání zabezpečovacích mechanismů

Náplní celé páté kapitoly bylo seznámení s dostupnými typy zabezpečovacích mechanismů bezdrátových sítí WLAN. Vhodnost jejich nasazení v příslušném prostředí shrnuje následující tabulka.

	WEP	**WPA (PSK)**	**WPA (plná)**	**WPA2 (PSK)**	**WPA2 (plná)**
Autentizace	Nulová	PSK	802.1x (EAP-TLS, PEAP)	PSK	802.1x (EAP-TLS, PEAP)
Šifrování	WEP (RC4)	TKIP (RC4)	TKIP (RC4)	CCMP (AES)	CCMP (AES)
Podnikové sítě	nevhodné	nevhodné	vhodné	nevhodné	velmi vhodné
Domácí a malé sítě	nevhodné	vhodné	nevhodné	velmi vhodné	nevhodné

Tabulka 2: Porovnání zabezpečení dle vhodnosti použití

Z uvedené tabulky vyplývá, že ne vždy je nutné pro kvalitní zabezpečení bezdrátové sítě použít WPA2. Pro domácí sítě či menší podniky bohatě postačí i WPA, jelikož pro tyto sítě WPA2 neznamená výrazný posun, respektive nutnost.

5 Možné typy útoků na bezdrátové sítě

Stejně jako se vyvíjejí metody zabezpečení, vyvíjejí se i způsoby, jak tato zabezpečení obejít, nebo prolomit a zneužívat tak data, která sítí putují. Principiálně můžeme útoky na bezdrátové sítě rozdělit na pasivní a aktivní. V případě pasivních útoků útočník pouze odposlouchává síťovou komunikaci, kterou následně analyzuje, přičemž v drtivé většině případů je tento typ útoku nezjistitelný. Aktivní útoky se naopak vyznačují tím, že útočník přímo ovlivňuje průběh síťové komunikace a to vysíláním svých vlastních či odchycených a zmodifikovaných paketů.

5.1 Odposlech síťové komunikace

Odposlech a identifikace síťové komunikace je velice běžný útok v prostředí bezdrátových sítí. Tento typ pasivního útoku využívá toho, že se útočník může nacházet kdekoliv v prostoru, který je vymezen dosahem dané bezdrátové sítě. [30] Při špatném zabezpečení sítě umožňuje útočníkovi odposlouchávat komunikaci v síti a získat tak nejen informace o uživatelích (citlivá data, přístupová hesla), ale i představu o činnosti a infrastruktuře odposlouchávané sítě. Tyto znalosti pak může dále využít například pro realizaci některého z aktivních útoků. [5] Samotný odposlech komunikace se provádí přepnutím bezdrátového síťového adaptéru útočícího stroje do tzv. monitorovacího režimu, ovšem pokud to daná síťová karta podporuje. V normálním režimu jsou zpracovány pouze rámce, které jsou určeny pro hostitelský stroj. To znamená ty, ve kterých je uvedena cílová MAC adresa hostitelského adaptéru. V monitorovacím režimu lze zachytávat všechny rámce, které síťová karta zaslechne a to bez nutnosti asociace a znalosti SSID. Stačí pouze zadat kanál, přes který probíhá komunikace v síti.

Jelikož se jedná o pasivní typ útoku, nelze ho běžně detekovat pomocí aktivních prvků sítě. Existují však hardwarové sondy, které to dokáží a to na základě reakce adaptéru na rámce typu žádost a odpověď. [31]

5.2 Falšování MAC adres

Velmi jednoduchý typ aktivního útoku, kdy jedinou bezpečnostní překážkou je zabezpečení pomocí filtrace MAC adres. V případě, že je filtrace MAC adres použita současně například se zabezpečením WEP, je nutné nejprve dekódovat WEP. [3] Jak již bylo řečeno v kapitole 4.2, princip filtrace MAC adres spočívá v omezení přístupu do sítě pouze na uživatele, jejichž MAC adresa je obsažena v seznamu povolených MAC adres. K překonání tohoto velmi jednoduchého způsobu zabezpečení však útočníkovi stačí odposlechnout jen určitou část síťové komunikace mezi aktivní uživatelskou stanicí a přístupovým bodem. Následnou analýzou pak lze snadno zjistit příslušnou MAC adresu odpovídající povolené-

mu seznamu, neboť se zdrojová i cílová MAC adresa obsažená v rámci posílá v nezašifrované podobě. Odposlechnutou adresu MAC pak útočník pouhou softwarovou změnou (například pomocí programu SMAC nebo MAC MakeUp), či úpravou registrů operačního systému nastaví na síťové kartě a vydává za svou. Od této chvíle je útočník schopen připojit se k síti a využívat tak naplno síťové prostředky. Pochopitelně za podmínky, že stanice, jejíž MAC adresu útočník odposlechl, nebude vysílat. [23] To znamená, že buď vyčká, než se stanice sama odpojí, nebo ji k tomu donutí (viz následující podkapitola).

5.3 Deautentizace

Tento útok lze použít k zachycení čtyřfázového handshake WPA, vynucení odmítnutí služby DoS (Denial of Service, více viz kapitola 5.7), nebo zjištění skrytého SSID, pokud je zamezeno jeho vysílání na přístupovém bodu. Účelem útoku je donutit některého z klientů k opětovné autentizaci, což ve spojení se slabou autentizací pro řízení rámců (užívanou k autentizaci, asociaci apod.) útočníkovi umožňuje spoofovat (falšovat) MAC adresy. Deautentizace bezdrátového klienta se provádí prostřednictvím spoofingu BSSID pomocí deautentizačních paketů, které se odesílají z BSSID na klienta. Též lze provést i hromadnou deautentizaci, která spočívá v nepřetržitém spoofingu BSSID pomocí opakovaného zasílání deautentizačních paketů na vysílací adresu. Hromadná deautentizace však není vždy spolehlivá. [20]

5.4 Slovníkové útoky

Slovníkové útoky jsou založeny na využití slovníků pro útoky na uživatelská jména a hesla. Útočník posílá výzvu na odezvu zaheslovaného protokolu, přičemž se snaží pomocí databáze běžně využívaných uživatelských jmen a hesel o prolomení šifry. Ve chvíli, kdy se mu podaří zjistit správnou kombinaci těchto údajů, získává plný přístup do bezdrátové sítě. Základ slovníkového útoku pochopitelně spočívá ve využití dostatečně kvalitního slovníku. Útočník může použít některý z již vytvořených slovníků, které lze snadno získat z Internetu nebo si vytvořit svůj vlastní za pomoci speciálních programů k tomu určených.

Obranou proti těmto útokům je volba vhodných přihlašovacích údajů, respektive takových, která nejsou obsahem slovníků. Použitá hesla by se navíc měla skládat minimálně z osmi alfanumerických znaků. Další možnou ochranou je využití autentizačních mechanismů, například 802.1x. [3]

5.5 Falešná zařízení

V bezdrátových sítích jsou velmi nebezpečná neautorizovaná falešná zařízení, jimiž mohou být jak přístupové body, tak i počítače nacházející se v dané síti. Z počítače lze falešný pří-

stupový bod vytvořit konfigurací jeho síťové karty a to pomocí softwarových programů, či ovladačů (například HostAP). Útok pak spočívá v zamaskování autorizovaného přístupového bodu tím falešným. To znamená, že útočník musí na svém falešném přístupovém bodu nastavit stejné SSID a číslo kanálu odpovídající autorizovanému přístupovému bodu. Dále je potřeba k falešnému zařízení připojit anténu s dostatečně vysokým ziskem, respektive takovým, aby falešný přístupový bod vykazoval lepší úroveň signálu než ten autorizovaný. Tím útočník docílí toho, že se autorizace klienta uskuteční skrze jeho přístupový bod, jelikož klientská síťová karta upřednostní přístupový bod s lepší úrovní signálu. Po připojení klienta k falešnému přístupovému bodu může útočník zachytávat data nezabezpečeného klienta, které mají mnohdy citlivý charakter (např. přístupová hesla). [5]

5.6 Man-in-the-middle útoky

Útoky typu Man-in-the-middle, tedy „muž uprostřed“, útočníci používají pro únosy relací a pro vkládání svého vlastního provozu do sítě. Samotné útoky se provádí velmi podobně jako v kabelových sítích, až na rozdíl, že v bezdrátových sítích se útočník může nacházet ve značné vzdálenosti. [5] Pro MITM útoky je charakteristické, že útočník vstoupí mezi dvě komunikující strany, přeruší mezi nimi veškerý provoz a přesměruje datový tok tak, aby jej mohl odposlouchávat. Toto mu navíc dává možnost komunikujícím stranám škodit například použitím nebezpečného softwaru. V případě bezdrátových sítí se útočník typicky postaví mezi klientskou stanici a autorizovaný přístupový bod (fyzicky to tak samozřejmě být nemusí). Pomocí odposlechu útočník zachytává a identifikuje zprávy přenášené mezi klientem a přístupovým bodem během asociačního procesu, čímž o nich získá základní informace (IP a MAC adresy obou zařízení, SSID přístupového bodu, asociační ID klienta). Na základě zjištěných informací je pak schopen vytvořit falešný přístupový bod, přičemž je nutné donutit klienta, aby se k tomuto bodu asocioval. Jednou z možností je nalákat ho na lepší úroveň signálu anebo se pokusit autorizovaný přístupový bod vyřadit z provozu pomocí DoS útoku (viz kapitola 5.7). V okamžiku, kdy je toho dosaženo, tak veškerá data, která útočník přijme na falešný přístupový bod, zaznamenává či modifikuje a dále přeposílá na autorizovaný přístupový bod, takže jak skutečný přístupový bod, tak i klient se domnívají, že spolu komunikují přímo. Ve skutečnosti však jejich komunikaci zachytává a zprostředkovává „muž uprostřed“ a dostává se tak ke všem datům včetně hesel apod. [3]

Obrana proti MITM útokům spočívá v použití vhodných autentizačních metod, elektronického podpisu, šifrování komunikačního kanálu či monitorování přístupových bodů. [3, 5]

5.7 DoS útoky

Cílem většiny již zmíněných útoků je získat informace, které útočník využije k průniku do bezdrátové sítě. V případě DoS se však jedná o aktivní útoky, které vedou k odepření, či zamítnutí služby (Denial of Service) a tím pádem k vyřazení určitého zařízení či dokonce celé sítě z provozu. Nejčastěji se tak děje vyčerpáním nebo zahlcením některého ze síťových zdrojů a to generováním nesmyslného provozu prostřednictvím velkého množství dotazů, které cílové zařízení nestíhá zpracovávat. [3, 32] V případě bezdrátových sítí je útok směrován na přístupový bod, který se snaží nadměrné množství dotazů vyhodnotit. Po určitém čase však náporu požadavků podlehne (naplní se buffer) a dojde k jeho zahlcení či zahlcení přenosového pásma. To v konečném důsledku způsobí, že se zpomalí nebo dokonce zcela znemožní připojení ostatních klientů. DoS útoky často předcházejí útokům MITM (viz kapitola 5.6), kdy mají za cíl odpojit klienta od autorizovaného přístupového bodu a umožnit tak přepojení na přístupový bod falešný. [3]

Obranu proti DoS útokům se v dnešní době snaží zajistit drtivá většina výrobců, kteří do zařízení implementují obranné mechanismy, jejichž cílem je při detekci DoS útoku zablokovat IP adresu klienta, ze které přicházejí nesmyslné dotazy. [33] Další účinnou možností je filtrace podle MAC adres, či předřazení firewallu s dobrou analýzou paketů (v případě, že jsou útoky vedeny z Internetu). [3]

5.8 Útoky na WEP

Jak již bylo popsáno v kapitole věnované protokolu WEP, k šifrování se používá proudová šifra RC4 a k zajištění integrity přenášených dat hodnota ICV vypočtená pomocí metody CRC-32, která je rovněž šifrována. K inicializaci RC4 algoritmu slouží spojení soukromého klíče a inicializačního vektoru IV.

Útoky na WEP vycházejí z následujících nedostatků:

- Použití statického klíče (mění se pouze inicializační vektor IV)
- Opakování inicializačního vektoru (cyklus poskytuje pouze 2^{24} možností)
- Použití stejného algoritmu pro autentizaci i šifrování
- Linearita CRC-32 a operace XOR
- Šifrování ICV společně s daty

5.8.1 Útok hrubou silou

Jednou z variant, jak zjistit šifrovací klíč je útok hrubou silou (Brute-force attack), který spočívá v postupném zkoušení všech možných kombinací šifrovacího klíče. V případě tohoto útoku stačí zachytit pouze jeden jediný zašifrovaný rámec a následně použít obrovskou výpočetní sílu pro nalezení správné kombinace. V praxi se však využívají zachycené

rámce dva - jeden pro zjištění hesla a druhý pro jeho ověření. Útok hrubou silou lze v přijatelném čase provádět pouze na 64bitovou variantu WEP, jelikož se v případě té 128bitové jedná o poměrně časově náročnou činnost. Z tohoto důvodu se často realizuje v kombinaci s útokem slovníkovým.

Obrana spočívá v časté obměně klíče či v omezení počtu pokusů o autentizaci. [34]

5.8.2 Injekce rámců

Injekce rámců je aktivní technika útoku, při které dochází k softwarové úpravě celého rámce nebo jeho části (hlavička, datová část). Účelem injekce může být například únos spojení mezi klientem a přístupovým bodem a ovládnutí či přesměrování spojení. [35] Hlavní využití však spočívá ve zvýšení provozu v bezdrátové síti, což vede ke zkrácení doby nutné pro zachycení dostatečného počtu inicializačních vektorů potřebných k rozluštění WEP klíče (cílový adresát na dotazy odpovídá vygenerováním nových rámců s novými IV). Inicializační vektory lze samozřejmě získat i pasivním odposlechem, ovšem za dobu závislou na provozním vytížení dané bezdrátové sítě, která se mnohdy počítá na hodiny, či dny. V případě využití injekce rámců je získání dostatečného množství inicializačních vektorů otázkou pouhých vteřin či minut. Tuto techniku však nepodporují všechny bezdrátové adaptéry, navíc bývá samotná funkce na bezdrátové kartě vypnuta a je ji tedy potřeba zapnout.

Ochrana proti injekci rámců není standardem IEEE 802.11 definována. Některá zařízení jí však dokáží částečně zabránit tím, že si IV přijatých rámců ukládají do vyrovnávací paměti a ignorují všechny rámce se stejným IV v případě, že jejich počet přesáhne určitou hranici. [34]

5.8.3 Fragmentační útok

Útok využívá toho, že standard IEEE 802.11 podporuje fragmentaci rámců. Vlastností fragmentace je schopnost větší rámce rozdělit na dílčí fragmenty, které pak lze odeslat samostatně. V případě standardu 802.11 je možno rozdělit každý rámec až na 16 fragmentů. Pokud se útočníkovi podaří zjistit proud klíče délky n, může odeslat libovolná data o délce $n - 4$ byty (odečtena ICV). Jestliže chce odeslat data větší délky, může data rozdělit do oněch 16 fragmentů (každý o délce $n - 4$ byty). Každý z fragmentů je klíčem šifrován samostatně a dále označen hodnotou o jaký fragment rámce se jedná. Poté co přístupový bod přijme všechny fragmenty, složí z nich původní rámec, který zašifruje novým proudem klíčem a odešle jako jediný fragment. Na základě znalosti původních dat a zachyceného přeposlaného fragmentu je pak útočník schopen dopočítat nový proud klíče o délce $16 * (n - 4) + 4 = 16 * n - 60$ bytů, přičemž pro získání celého 1500bytového proudu

klíče stačí odeslat 34 fragmentů. Pokud chce útočník získat hodnoty proudu klíče pro jednotlivé inicializační vektory, stačí odeslat data zašifrovaná zjištěným 1500bytovým proudem klíče a zachytávat přeposlané rámce od přístupového bodu, který pokaždé použije nový inicializační vektor. Na základě toho je pak útočník schopen vytvořit kompletní slovník inicializačních vektorů.

Způsob jakým se proti útoku bránit spočívá v použití přístupového bodu, který nepřijímá krátké rámce. Další možností je zabránit opakování IV zahazováním rámců se stejnou hodnotou IV. [36]

5.8.4 FMS útok

FMS (Fluhrer-Mantin-Shamir) útok využívá slabiny šifrovacího RC4 algoritmu. Způsob, jakým jsou generovány jedinečné šifrovací klíče pro jednotlivé rámce, z něj činí v případě protokolu WEP velikou hrozbu. [34] Skutečnost, že WEP pouze zřetězí tajný klíč s IV pro inicializaci generátoru RC4, a to, že samotné IV se odesílá příjemci v nezašifrované podobě, činí šifru RC4 velmi náchylnou na útok FMS. Pouhé zřetězení tajného klíče s 24bitovým IV vede k vytváření řady slabých RC4 klíčů a jedinečné šifrovací klíče pro každý rámec způsobují, že je pravděpodobnost použití slabého klíče velmi vysoká. Přibližně 9 tisíc z 16,7 milionů možných IV (resp. šifrovacích klíčů) lze považovat za slabé. V případě, že se útočníkovi podaří získat dostatečný počet slabých IV, může šifrovací WEP klíč odhalit s minimálním úsilím pomocí pravděpodobnostního algoritmu. K více než 50% úspěšnosti odhalení klíče stačí přibližně 60 slabých IV. Pokud jich bude 100 a více, úspěšnost odhalení je téměř 100%. Nutnou podmínkou pro provedení útoku, je však znalost alespoň několika počátečních bytů šifrovaných dat. To ale nepředstavuje veliký problém, neboť všechny IP i ARP pakety začínají hexadecimální hodnotou 0xAA a lze ji tak jednoduše splnit. [20]

Jako obrana vůči útoku FMS byla vytvořena technologie nazvaná WEP+, která zajišťuje vynechávání slabých IV. Tuto technologii však musí podporovat všechna zařízení v síti, jinak je útok FMS opět možné použít. [34]

5.8.5 Indukční útok Arbaugh

Tento útok umožňuje libovolně prodloužit známý RC4 proud klíče délky n. Autor útoku Arbaugh byl prvním, kdo prokázal, že hodnotu ICV lze použít k rozšíření RC4 proudu pomocí zašifrovaného rámce byte po bytu. Postup útoku se skládá ze dvou kroků a to ze získání inicializační hodnoty proudu klíče a indukčního kroku. [20] N bytů RC4 proudu pro dané IV lze získat z krátkých rámců s předpokládaným obsahem (např. DHCP či ARP komunikace) nebo pomocí Shared-Key autentizace. Útočník potom v rámci indukčního kroku může sestrojit rámec s daty délky $n - 3$ bytů, pro které vypočítá ICV, přičemž k rámci při-

pojí pouze první 3 byty. K zašifrovaným datům přidá hlavičku, hodnotu IV a tzv. byte Y a rámec odešle. Pokud přístupový bod tento rámec přepošle, respektive útočník na něj dostane odpověď, znamená to, že hodnota bytu Y je správná (v opačném případě zkusí jinou hodnotu, kterých může být maximálně $2^8 = 256$). Hodnotu bytu $n + 1$ RC4 proudu pak získá provedením operace XOR mezi bytem Y a posledním a tedy čtvrtým bytem ICV. V tuto chvíli má útočník k dispozici $n + 1$ správných bytů RC4 proudu, přičemž indukčním způsobem pokračuje až do požadované délky.

Obrana vůči indukčnímu útoku je obdobná jako proti injekci rámců. Je tedy nutné zabránit opakování IV a falšování rámců prostřednictvím zahazování často se opakujících rámců se stejnou hodnotou IV. [34]

5.8.6 Chopchop útok

Chopchop útok, na rozdíl od předchozích útoků, nevyužívá nedostatků RC4 algoritmu, ale soustředí se na protokol WEP jako takový. Je tedy založen na chybách samotného protokolu, na chybějící obraně proti útokům opakováním a nedostatcích algoritmu CRC-32. K jeho provedení není ani potřeba velké množství zachycených dat. Chopchop útok, v případě úspěchu, dovoluje útočníkovi dešifrovat libovolný zachycený rámec aktivním iterativním způsobem. Lze tak získat jeho obsah (nebo jeho část), a to bez znalosti šifrovacího klíče. Z toho vyplývá, že sám o sobě nevrací šifrovací klíč. Pro daný otevřený text P WEP připojí ICV a XORuje ho s RC4 šifrou. Výsledná šifrovaná zpráva se dá zapsat jako:

$$M = \big(P + ICV(P)\big)\ XOR\ RC4$$

Útočník po zachycení šifrované zprávy potřebuje změnit otevřený text P na text P‘ a vyslat modifikovanou zprávu zpět do sítě. Vztah mezi P a P‘ se dá vyjádřit následovně:

$$P' = P\ XOR\ Mod$$

kde Mod je specifický vzor bitů (bit maska). Potom platí:

$$P' + ICV(P') = \big(P + ICV(P)\big)XOR\ (Mod + ICV(Mod))$$

Pro celou útočníkem vytvořenou šifrovanou zprávu platí:

$$M' = \big(P' + ICV(P')\big)\ XOR\ RC4 = \big(P + ICV(P)\big)\ XOR\ RC4\ XOR\ \big(Mod + ICV(Mod)\big) =$$

$$M\ XOR\ \big(Mod + ICV(Mod)\big)$$ [39]

To znamená, že útočník dokáže libovolně změnit šifrovaný rámec a zároveň ponechat ICV validní. Chopchop útok využívá i další slabinu ICV. Když se zkrátí šifrovaná zpráva o poslední byte, jeho ICV nebude validní. To se napraví XORováním s určitou hodnotou. Velkým bezpečnostním nedostatkem je, že tato hodnota závisí přesně na odtrhnutém bytu. Proto se odhadem vybere jeden z 256 bytů a XORuje se se zprávou. Ke zjištění správnosti odhadu se odešle takto změněná zpráva přístupovému bodu. Pokud byl odhad správný, přístu-

pový bod odešle zprávu nazpět do sítě, v opačném případě se vyzkouší další z možných bytů. Opakováním tohoto postupu se získá otevřený text zprávy, nebo alespoň jeho část.

Obrana spočívá v zamezení vysílání velkého množství rámců se stejnou hodnotou IV. Další možností je využít přístupové body, které zahazují rámce kratší než 60 bytů. [38]

5.9 Útoky na WPA, WPA2

Napříč tomu, že WPA i WPA2 poskytují vysokou úroveň bezpečnosti pro sítě WLAN, obsahují i tyto bezpečnostní protokoly několik nedostatků, které mohou představovat potenciální rizika pro zneužití útočníky. V případě WPA jde hlavně o dědictví, které si s sebou nese díky kompatibilitě s WEP, tudíž některé útoky, případně jejich obměny, realizovatelné na WEP je možno aplikovat i na WPA. WPA2 si v tomto ohledu vede mnohem lépe, neobsahuje téměř žádnou spojitost s WEP a je postaveno na nové bázi. Avšak i v případě tohoto zabezpečení se dají najít některé slabiny, které mohou představovat bezpečnostní rizika.

5.9.1 PSK cracking

Tento útok funguje proti sítím typu WPA/WPA2 využívající k autentizaci předsdílený klíč PSK a není ho tedy možné aplikovat na zabezpečení WPA/WPA2 využívající k autentizaci 802.1x a protokol EAP. K prolomení PSK není možno zachytávat IV jako v případě WEP, jelikož se klíč mění dynamicky. V tomto případě se využívá útok hrubou silou, potažmo slovníkový útok, přičemž je potřebné získat čtyřcestný handshake mezi přístupovým bodem a klientem. Handshake se používá k získání dočasného klíče, který slouží k ochraně provozu v síti. Jeho slabinou je, že přenáší náhodně generovaná čísla ANonce a SNonce v nezašifrované podobě. K získání handshaku stačí počkat na připojení některého z klientů k přístupovému bodu nebo jednoduše některého z již připojených klientů de-autentizovat. Po získání handshaku není potřeba získávat další rámce ani odposlouchávat či měnit komunikaci v síti, jelikož v tomto momentě útočník zná čtyři hodnoty z pěti (ANonce, SNonce a MAC adresu přístupového bodu a klienta), které se nacházejí na vstupu algoritmu PRF. Postupným dosazováním klíče (vybraného ze slovníku nebo vygenerovaného hrubou silou) za hodnotu PMK a následným opakováním algoritmu PRF se útočník snaží získat stejný výsledek, který zachytil v handshaku. Při těchto útocích velkou mírou závisí na složitosti klíče a na výkonnosti stroje, na kterém útok probíhá. Procesor o taktu 2,6 GHz otestuje přibližně 250 klíčů za sekundu, čtyřjádrový procesor zvládne tisíc až dva tisíce klíčů za sekundu. Využitím grafické karty je možné toto číslo zvýšit až na 20 tisíc, což dělá z poměrně bezpečného hesla zranitelné.

Obrana vůči útokům na PSK spočívá ve vhodné volbě hesla, které by mělo být co možná nejdelší, poskládané z náhodně vybraných znaků (včetně těch speciálních) a nemělo by být slovníkové. [37, 38]

5.9.2 Beck-Tews útok na TKIP

Jedná se o útok na protokol TKIP, který je rozšířením Chopchop útoku na WEP. Beck-Tews útok nevrací hlavní klíč, útočník získá proud klíče a MIC hodnotu pro daný rámec, čehož může využít k injekci rámců v síti. Aby bylo možné útok provést, musí síť splňovat určité vlastnosti. První z nich je podpora QoS, která se snaží zajistit kvalitu přenosu vyhrazením více kanálů, přičemž každý z nich má svoje počítadlo TSC. Využitím faktu, že se TSC hodnota pouze inkrementuje a v jednotlivých kanálech není provoz stejný, je možné zachytit paket z kanálu s vyšším TSC, injektovat ho a poslat do kanálu s TSC nižším. Ve většině případů je největší provoz na kanále s číslem nula a všechny ostatní kanály tedy mají nižší provoz a tedy i nižší hodnotu TSC, čímž se tato síť stává zranitelná vůči modifikovanému Chopchop útoku. Další důležitou vlastností pro Beck-Tews útok je Key Renewal Interval (interval výměny klíče). Když TKIP zjistí neshodu v MIC a zároveň je hodnota ICV správná, vyhodnotí tento stav jako pokus o útok na síť. Pokud do minuty nastane stejná situace, přístupový bod vymaže všechny dočasné klíče a přeruší veškerou komunikaci na jednu minutu. Po jedné minutě je každý klient přinucený se znovu autentizovat a vytvořit nové dočasné klíče. Útok tedy musí proběhnout dříve, než vyprší doba pro výměnu klíče.

První částí útoku je de-autentizace klienta, čímž je donucen znovu se připojit k přístupovému bodu a vyprodukovat handshake pro vytvoření nových klíčů. Kvůli konfiguraci a obnovení komunikace jsou posílány i další kontrolní pakety (ARP, DHCP). Díky charakteristické malé velikosti a dobré předvídatelnosti obsahu útočník odchytává ARP pakety posílané z přístupového bodu. Jakmile se podaří ARP získat, je možné začít s modifikovaným Chopchop útokem. Rozdíl oproti původnímu Chophop útoku je hlavně ve snaze zabránit vypnutí provozu TKIP sítě (způsobené MIC obranou). Další změnou je vydávání se za přístupový bod, namísto za klienta. Klient je v TKIP síti jediný, kdo posílá zprávu o selhání MIC (nesprávnost MIC, správnost ICV). Tuto zprávu zachytí útočník a díky ní zjistí korektnost svého odhadu. Po uplynutí 60 sekund může pokračovat v tipování dalšího bytu, přičemž takto pokračuje až do zjištění všech bytů. Po provedení Chopchop útoku se vytvoří ICV hodnota z odhadovaného ARP paketu a porovná se s hodnotou již dešifrovanou. Pokud hodnoty souhlasí, ARP paket je dešifrovaný, útočník získal otevřený text a MIC. Poté může jednoduchým reverzním postupem použít algoritmus Michael k získání MIC klíče. Po úspěšně provedeném útoku, útočník může získat další proud klíče za 4 až

5 minut, protože potřebuje pouze dešifrovat čtyři byty ICV. IP adresa je získána odhadem, MIC hodnota se vypočítá použitím MIC klíče a ověří se správné ICV. [37, 38]

Obrana před tímto útokem spočívá ve zkrácení doby, po které dochází k překlíčování (např. 120 sekund) nebo v použití dlouhého tajného klíče (20 a více znaků).

5.9.3 Ohigashi-Morii útok

Tento útok představuje vylepšení Beck-Tews útoku na WPA. Beck-Tews útok potřeboval k provedení QoS, což limitovalo útok pouze na cíle, které tuto vlastnost podporují. Ohigashi-Morii útok rozšířil pole působnosti na všechny implementace WPA protokolu. Dalším vylepšením je snížení času na vykonání útoku. Beck-Tews útok obešel TSC počítadlo využitím dalších kanálů vytvořených QoS. Ohigashi-Morii útok aplikuje Beck-Tews útok v kombinaci s MITM útokem. MITM útok přerušuje komunikaci mezi klientem a přístupovým bodem a po modifikaci paketu ho posílá správnému příjemci. Při tomto útoku je možné získat šifrovaný paket, který má TSC hodnotu větší než hodnotu TSC počítadla u příjemce, což je způsobené tím, že paket nedorazil k příjemci. Díky těmto podmínkám je možné aplikovat Chopchop útok na MITM útok. Ohigashi-Morii útok má tři režimy vytvořené pro redukování ztráty komunikace, střídající se podle povahy provozu v síti.

- **Repeater mode** – útočník se chová jako opakovač, všechny pakety obsahující SSID přeposílá nezměněné. Používá se jako pauza mezi dvěma použitými MIC recovery mode.
- **MIC recovery mode** – má za úkol získat MIC klíč a kontrolní hodnotu pomocí Chopchop útoku. Čas potřebný k vykonání je zhruba 12 až 15 minut.
- **Message falsification mode** – používá se k falšování šifrované zprávy pomocí získaného MIC klíče (vykonává se tedy až po jeho získání). Pokud je cílem ARP paket, čas na vykonání je přibližně 4 minuty. [37, 40]

5.9.4 Slabina „Hole 196“

„Hole 196“ je slabina bezpečnostních protokolů WPA/WPA2, která byla zdokumentována na posledním řádku 196. strany revize standardu IEEE 802.11 z roku 2007. Tato slabina je zneužitelná pouze autentizovanými uživateli, jinak řečeno umožňuje útoky pouze zevnitř sítě (útočník má již přístup k síti). Je možné ji zneužít jak v případě WPA/WPA2 - Personal, tak i WPA/WPA2 - Enterprise. Na zabezpečení typu Personal však ztrácí význam, neboť útočník má přístup ke všem datům v síti i bez využití této slabiny. Větší riziko tedy představuje pro sítě využívající zabezpečení typu Enterprise, které se spoléhají na řídící protokoly 802.1x a řízení přístupu na základě portů.

Princip zneužití slabiny je následující - Klíč GTK je vysílán pomocí broadcast, či multicast do celé sítě, který pak klienti používají pro dešifrování komunikace. GTK však může být zneužit útočníkem, který jako autorizovaný klient obdrží GTK od přístupového bodu. Po obdržení klíče útočník vytvoří falešný přístupový bod a začne broadcastovat falešné pakety ostatním klientům v síti (šifrované klíčem GTK), přičemž MAC adresa falešného přístupového bodu je totožná s tou legitimního. Útočník se tváří jako MITM a s použitím ARP injekce je schopný měnit ARP tabulky ostatních klientů. Všichni takto zasažení klienti přeposílají pakety zašifrované pomocí svých osobních klíčů pravému přístupovému bodu, který pakety dešifruje a následně zašifruje pomocí PTK falešného přístupového bodu a přepošle mu je. Tímto způsobem útočník může získat přístup ke všem informacím ostatních klientů v síti (přihlašovací údaje, emaily apod.). [41]

6 Praktická část

Praktická část bakalářské práce se zabývá ověřením a analýzou bezpečnosti bezdrátových sítí WLAN. Pro ověření bezpečnosti budou demonstrovány útoky na bezdrátovou síť zabezpečenou různými zabezpečovacími mechanismy. Ostatně jak jinak ověřit bezpečnost bezdrátové sítě, než na ni doopravdy zaútočit.

Útoky lze aplikovat na jakoukoliv reálnou bezdrátovou síť. Z praktických, etických a právních důvodů však byly útoky provedeny na vlastní domácí síť a nedošlo tak k protiprávnímu a nezákonnému jednání.

6.1 Softwarové vybavení

V dřívější době bylo softwarové vybavení pro analýzu bezpečnosti bezdrátových sítí dostupné pouze pro operační systémy Linux. V té dnešní se již vyskytují nástroje i pro platformu Windows. Podpora aplikací potřebných k analýze a provedení útoků ve Windows je však na daleko nižší úrovni a navíc je drtivá většina z nástrojů převzata právě z Linuxu. Ve výsledku je tedy pouze na uživateli, jaký operační systém si pro testování zvolí. Stále však platí, že je k těmto pokusům daleko přívětivější OS Linux. Je to zejména kvůli dostupnosti knihoven pro zachytávání a ukládání síťové komunikace, jednoduché vzájemné interakci programů (skriptování) a možnosti nízkoúrovňového přístupu hardwaru. Pro realizaci útoků je v prostředí OS Linux možné použít jakoukoliv standardně vydávanou distribuci (Ubuntu, Fedora, Centos, Debian apod.) s nutností doinstalovat potřebné penetrační balíčky, ovladače a jednotlivé utility. Mnohem lepší variantou je však využít speciální distribuce přímo určené pro penetraci a analýzu bezpečnosti, které již všechny potřebné balíčky a ovladače mají předinstalované. Mezi tyto distribuce můžeme zařadit GnackTrack, WifiSlax, věhlasný BackTrack, či jeho následovatelku Kali Linux, která byla využita pro účely této bakalářské práce.

Kali Linux je distribuce vycházející z Debianu primárně navržená k penetračním testům počítačových sítí. Překypuje všemožnými skripty a nástroji, jak čistě textovými, tak s grafickým rozhraním, kterými lze útočit prakticky na cokoliv. Jsou jimi nejen různé lamače hesel, ale také nástroje pro analýzu a mapování sítí, síťový spoofing a mnoho dalších. Nutno však dodat, že její autoři ji nevyvíjeli proto, aby škodila, ale především proto, aby měli správci sítí a bezpečnostní specialisté po ruce silný nástroj pro skutečné testy, zdali je jejich síť dostatečně bezpečná proti útokům hackerů. Kali Linux je zcela zdarma a nejnovější verzi lze stáhnout na stránkách vývojářů Offensive Security. Systém lze na jakýkoliv počítač buď nainstalovat (i ve virtualizovaném prostředí), nebo v případě LIVE distribuce spustit přímo z DVD, vytvořeného vypálením .iso obrazu, či USB Flashdisku, pro jehož vytvoření poslouží například multiplatformní utilita Unetbootin.

6.1.1 Nástroje pro útoky

Jak již bylo popsáno výše, distribuce Kali Linux obsahuje nespočet penetračních balíčků a utilit. Tím nejpodstatnějším z nich je balíček *aircrack-ng*, na kterém je postaveno celé naše testování bezpečnosti bezdrátové sítě. Jedná se o souhrn několika nástrojů určených pro bezpečnostní audit bezdrátových sítí obsahující nejnovější implementace útoků na slabiny zabezpečovacích mechanismů WEP a WPA/WPA2-PSK. V podstatě jde o skener bezdrátových sítí, WEP cracker, injektor, generátor paketů a packet sniffer. Důležité nástroje a jejich funkce v rámci balíčku *aircrack-ng* jsou následující:

- airbase-ng Zahrnuje techniky pro útoky na klienty.
- aircrack-ng Prolomení WEP a WPA/WPA2-PSK klíčů.
- airdecap-ng Dešifrování zachycených souborů se známým klíčem.
- aireplay-ng Umožňuje generovat provoz v síti pomocí injekce paketů, deautentizaci či falešnou autentizaci.
- airmon-ng Přepnutí bezdrátového adaptéru do monitorovacího režimu.
- airodump-ng Zachytává a ukládá provoz do PCAP nebo IVS souborů a zobrazuje informace o sítích a k nim připojených klientech.
- airserv-ng Umožňuje přístup k síťovému adaptéru z ostatních počítačů.
- packetforge-ng Vytváří různé typy šifrovaných paketů k provedení injekce.
- easside-ng Nástroj ke komunikaci s přístupovým bodem bez WEP klíče.
- tkiptun-ng Umožňuje provést útok na WPA-TKIP.

Další užitečná utilita je *macchanger*, která slouží ke změně MAC adresy síťového zařízení.

6.2 Hardwarové vybavení

Pro ověřování bezpečnosti bezdrátových sítí v podobě penetračních testů je kromě softwarového vybavení důležité použít i příslušné hardwarové vybavení. Základem je bezdrátový síťový adaptér umožňující monitorovací režim pro odposlech síťové komunikace a injekci paketů, která je důležitá pro zkrácení doby potřebné k provedení útoku. V nejlepším případě s přímou podporou v Kali Linux. V opačném případě je nutné použít buď nejnovější dostupný ovladač dané síťové karty, nebo použít úplně jiný bezdrátový adaptér v libovolném provedení (USB, PCMCIA, PCI). Dále je více než vhodné použít i další zařízení jako jsou například externí směrové antény pro dosažení lepšího signálu. V případě tohoto testování však byla využita zařízení na základě dostupných prostředků, která jsou popsána níže.

6.2.1 Přístupový bod

Jako bezdrátový přístupový bod byl použit domácí směrovač **TP-LINK TL-WR741ND**. Jedná se o směrovač kompatibilní se standardy 802.11b/g/n. Jeho maximální teoretická přenosová rychlost může být až 150 Mbit/s, přičemž je přizpůsobována přenosovým podmínkám. Disponuje jednou odnímatelnou všesměrovou anténou o síle 5dBi a celkový výstupní výkon činí 20 dBm. Podporuje zabezpečení WEP (64, 128 a 152 bitů), WPA-PSK/WPA2-PSK, WPA/WPA2 a dále umožňuje zamezit vysílání SSID či filtraci IP/MAC adres.

- MAC adresa: F8:D1:11:87:6D:06

6.2.2 Klientské stanice

Jako klientské stanice připojující se do bezdrátové sítě byly zvoleny dvě zařízení. Prvním z nich je notebook **Lenovo G580** s dvoujádrovým procesorem Intel Pentium 2020M o taktu 2,4 GHz, operační paměti 4 GB a podporující standardy 802.11b/g/n. Druhé klientské zařízení je mobilní telefon **Sony Xperia Tipo** s taktovací frekvencí procesoru 0,8 GHz a rovněž podporující standardy 802.11b/g/n.

- MAC adresa notebooku: 80:56:F2:E8:A8:C9
- MAC adresa telefonu: 30:39:26:8E:72:B9

6.2.3 Útočící stroj

Pro tuto příležitost se zařízením, ze kterého byly vedeny útoky na bezdrátovou síť, stal kvůli mobilitě notebook **Lenovo V570** s dvoujádrovým procesorem Intel Core i3-2310M o taktovací frekvenci 2,1 GHz, operační pamětí o velikosti 4 GB a disponující výše zmíněnou distribucí Kali Linux. Pro realizaci samotných útoků posloužil integrovaný síťový adaptér osazený chipsetem společnosti Broadcom podporující standardy 802.11b/g/n. Tento bezdrátový adaptér umožňuje všechny režimy činnosti včetně potřebného monitorovacího režimu a rovněž podporuje i injekci paketů.

- MAC adresa: C0:F8:DA:1C:58:5E

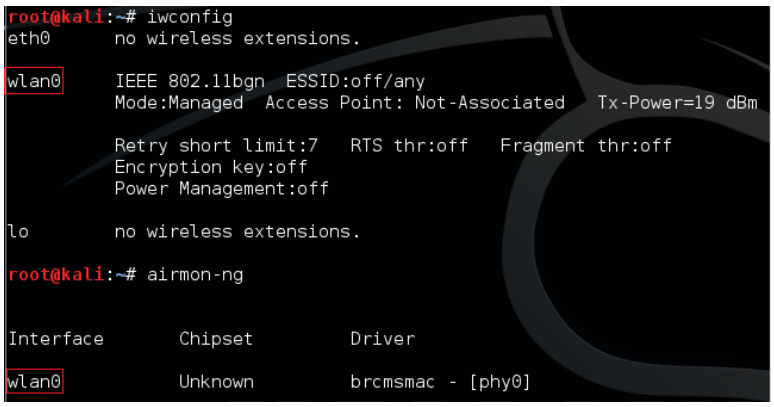
6.3 Příprava k útokům

6.3.1 Monitorovací režim

Po startu LIVE distribuce Kali Linux je nejprve nutné nakonfigurovat daný hardware. Pro provedení všech útoků je potřeba přepnout bezdrátový adaptér útočícího stroje do moni-

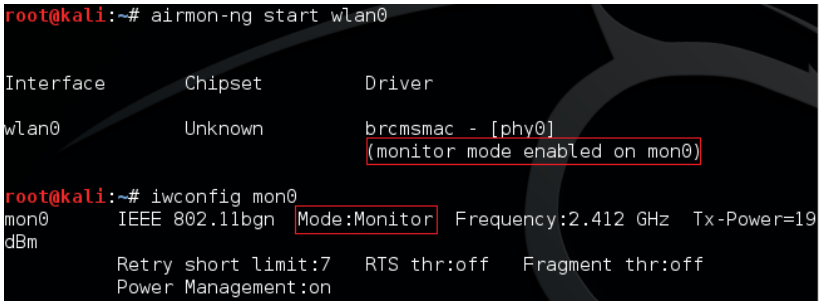
torovacího režimu, který umožňuje odposlouchávat veškerý síťový provoz. K identifikaci příslušného adaptéru otevřeme terminálové okno a zadáme jeden z dvojice příkazů:

iwconfig | *airmon-ng*



Obrázek 9: Identifikace bezdrátového adaptéru

V obou případech vidíme, že se adaptér hlásí pod označením *wlan0.* Toto označení však může být u každého adaptéru jiné. Do monitorovacího režimu lze následně bezdrátový adaptér přepnout dvěma způsoby. Prvním způsobem je zadat příkaz *airmon-ng start wlan0,* přičemž dojde k vytvoření nového virtuálního rozhraní s názvem *mon0*, na kterém bude dostupný monitorovací režim (viz obrázek č. 10). Pochopitelně je nutné následně pracovat s tímto virtuálním rozhraním.



Obrázek 10: Monitorovací režim na virtuálním rozhraní

Druhým způsobem je nastavit monitorovací režim přímo na fyzickém rozhraní *wlan0*. Provádí se skrze příkaz *iwconfig wlan0 mode monitor*, přičemž je dobré bezdrátový adaptér nejprve vypnout příkazem *ifconfig wlan0 down* a po přepnutí režimu následně zapnout pomocí příkazu *ifconfig wlan0 up*. Situaci opět shrnuje níže uvedený obrázek č. 11.

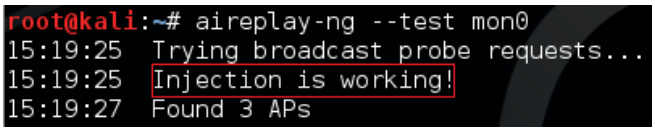
Obrázek 11: Monitorovací režim na fyzickém rozhraní

6.3.2 Test injekce paketů

Jak již bylo zmiňováno, je velmi vhodné pokud bezdrátový adaptér umožňuje funkci injekce paketů, neboť s jejím využitím jsme schopni aktivně zvýšit provoz v síti a tím mnohonásobně urychlit například prolomení WEP klíče. Injekce paketů má mnoho různých podob, které se s příchodem nové techniky stále vylepšují. Kontrolu funkčnosti provedeme pomocí nástroje *aireplay-ng* příkazem:

aireplay-ng --test mon0

Místo přepínače příkazu *--test* lze rovněž použít přepínač *-9*, který značí totéž, pouze ve zkrácené podobě.

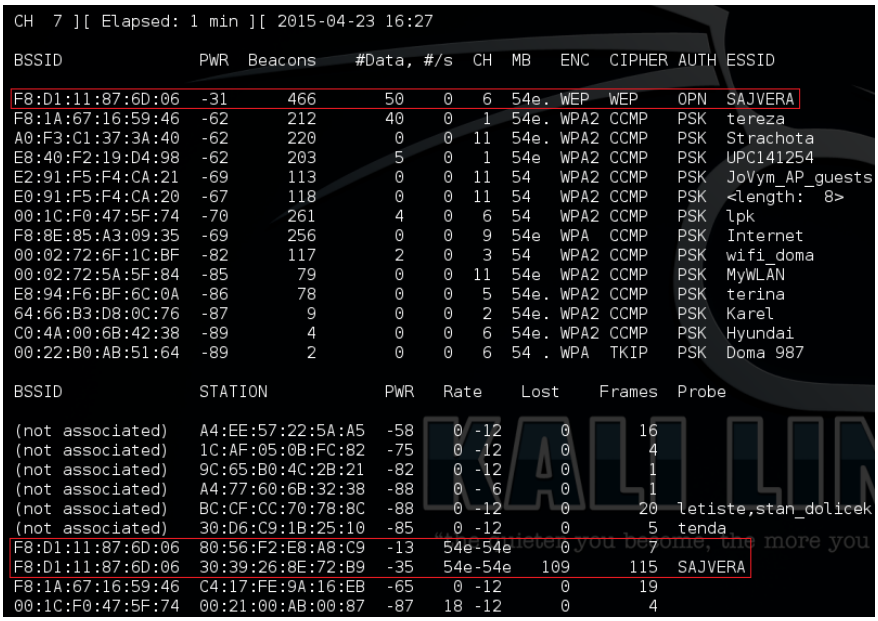


Obrázek 12: Test injekce paketů

Z uvedeného obrázku je na základě vypsané hlášky „Injection is working!“ patrné, že injekce paketů je funkční a můžeme ji tedy využít k prováděným útokům.

6.3.3 Skenování okolí

Dalším přípravným krokem je prozkoumání okolních dostupných sítí a zjištění informací potřebných k provedení útoku na vybraný cíl. K tomu využijeme nástroj airodump-ng, přičemž skenování okolí spustíme příkazem: *airodump-ng mon0.*



Obrázek 13: Monitorování dostupných sítí a klientů

Po provedení příkazu uvidíme výpis obsahující spoustu zajímavých a námi potřebných informací (viz obrázek č. 13). Nejvíce nás zajímají sloupce BSSID (MAC adresa přístupové-

ho bodu), CH (kanál, na kterém probíhá komunikace), ENC (typ zabezpečení) a ESSID (název bezdrátové sítě). Dalším výstupem je například počet vyslaných řídících rámců Beacon, přenosová rychlost a použitý typ šifrování. Ve spodní části výpisu se pod sloupcem STATION nacházejí klientské stanice, respektive jejich MAC adresy. V případě, že jsou tato zařízení připojena do nějaké sítě, je ve výpisu uvedena i MAC adresa příslušného přístupového bodu, se kterým jsou asociována. To vidí případný útočník velmi rád, jelikož ví, že na síti probíhá komunikace a tudíž sběr dat nebude trvat tak dlouho.

Po určení cíle a zjištění všech potřebných informací proces skenování vypneme pomocí klávesové zkratky *ctrl+c*. V rámci této práce bude vždy cílem bezdrátová síť s parametry:

- ESSID: SAJVERA
- BSSID: F8:D1:11:87:6D:06
- CH: 6

6.3.4 Změna MAC adresy

Posledním přípravným krokem je změna MAC adresy útočícího bezdrátového adaptéru. Změna MAC adresy je potřebná k zachování anonymity a špatné zpětné dohledatelnosti útočníka. Pomocí nástroje *macchanger* můžeme s příslušným přepínačem buď náhodně vygenerovat, nebo dosadit námi libovolně zvolenou MAC adresu. Nejlepším řešením je však zneužít MAC adresu klienta sítě, na kterou útočíme. Vyhneme se tak problémům s filtrací MAC adres, která na přístupovém bodu může být nastavena. V předešlém kroku jsme zjistili, že jsou k síti s SSID SAJVERA připojeny dvě klientské stanice. První z nich má MAC adresu 80:56:F2:E8:A8:C9 a druhá 30:39:26:8E:72:B9. Můžeme tedy použít jakoukoli z nich, přičemž změny docílíme následujícím příkazem:

macchanger –m 30:39:26:8E:72:B9 mon0

```
root@kali:~# ifconfig mon0 down
root@kali:~# macchanger -m 30:39:26:8E:72:B9 mon0
Permanent MAC: c0:f8:da:1c:58:5e (Hon Hai Precision Ind. Co.,ltd.)
Current   MAC: c0:f8:da:1c:58:5e (Hon Hai Precision Ind. Co.,ltd.)
New       MAC: 30:39:26:8e:72:b9 (unknown)
root@kali:~# ifconfig mon0 up
```

Obrázek 14: Duplikace MAC adresy

Přepínač *–m* slouží k nastavení konkrétní fyzické MAC adresy. Dále je možné použít přepínač *–a* nebo přepínač *–r* pro vygenerování adresy náhodné. Ve všech případech je však potřeba bezdrátový adaptér nejprve vypnout, následně změnit MAC adresu a poté opět zapnout (viz obrázek č. 14).

Po provedení přípravných kroků, kdy jsme bezdrátový adaptér nastavili do monitorovacího režimu, otestovali injekci paketů a proskenovali své okolí, máme vybraný cíl a zjištěné všechny potřebné informace pro provedení útoků na bezdrátovou síť.

6.4 WEP

Útoků směrovaných na protokol WEP je díky jeho špatné implementaci celá řada. V rámci této práce budou však demonstrovány pouze dva (útok generováním ARP paketů a injekce paketů pomocí Chopchop útoku). Důvod výběru spočíval ve využití injekce a tedy rychlejšího získání WEP klíče. Dalším kritériem výběru byl rozdíl mezi oběma útoky. Při injekci ARP paketů bylo nutné, aby k přístupovému bodu byla připojena alespoň jedna klientská stanice, zatímco u Chopchop útoku tato nutnost odpadá.

6.4.1 Injekce ARP paketů

Útok generováním ARP paketů se řadí mezi skupinu aktivních útoků. Jak již bylo zmíněno výše, pro jeho uskutečnění je bezpodmínečně nutná asociace alespoň jedné stanice na přístupový bod. Celý útok pak spočívá v opakovaném odesílání ARP paketů z útočícího adaptéru na přístupový bod (injekce ARP paketů). Abychom byli schopni ARP paket injektovat, je nejprve nutné alespoň jeden takový paket zachytit ze směru od přístupového bodu ke klientské stanici. Poté, co ho získáme, můžeme jej odesílat stále dokola. Přístupový bod je nucen pokaždé paket přijmout, dešifrovat a následně přeposlat dále. Odesílá se však již s novou hodnotou inicializačního vektoru. Generováním velkého množství těchto paketů jsme pak schopni odhalit tajný šifrovací klíč.

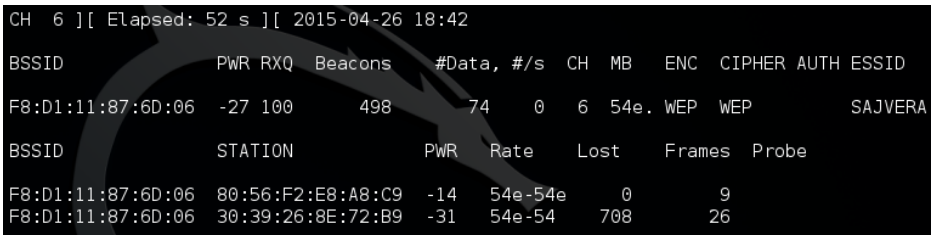
6.4.1.1 Realizace

Ze všeho nejdříve spustíme nástroj *airodump-ng* s příslušnými parametry, které jsme získali pomocí skenování okolí. *Airodump-ng* slouží ke shromáždění a uložení potřebných dat do souboru, který na konci použijeme k odhalení klíče. Příkaz je následující:

airodump-ng -c 6 --bssid F8:D1:11:87:6D:06 --ivs -w wepcrack mon0

Význam parametrů příkazu:

- -c – zvolený kanál pro zachytávání
- --bssid – MAC adresa přístupového bodu
- --ivs – nástroj zaznamenává pouze inicializační vektory
- -w – určuje soubor pro zápis dat
- mon0 – rozhraní útočícího adaptéru



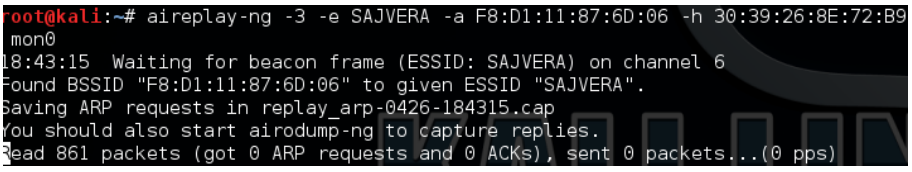
Obrázek 15: Monitorování cíle při ARP injekci

Následně v novém terminálovém okně zahájíme útok:

aireplay-ng –3 –e SAJVERA –a F8:D1:11:87:6D:06 –h 30:39:26:8E:72:B9 –x 600 mon0

Význam parametrů příkazu:

- -3 – označení pro ARP replay útok
- -e – název sítě (ESSID)
- -a – MAC adresa přístupového bodu
- -h – MAC adresa útočícího adaptéru
- -x – počet injektovaných ARP paketů za sekundu
- mon0 – rozhraní útočícího adaptéru



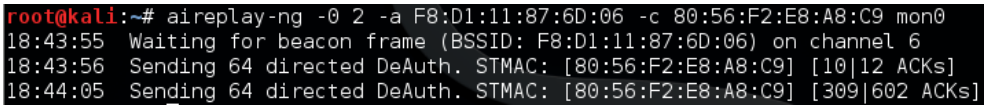
Obrázek 16: Zahájení ARP injekce

V tuto chvíli je potřeba zachytit paket směřující od přístupového bodu ke klientské stanici, přičemž existují dvě možnosti, jak toho docílit. Buď budeme čekat do doby, než se připojí nějaká legitimní stanice nebo některou z již připojených stanic deautentizujeme. Abychom nemuseli čekat, zvolíme postup pomocí deautentizace, kterou provedeme následovně:

aireplay-ng –0 3 –a F8:D1:11:87:6D:06 –c 80:56:F2:E8:A8:C9 mon0

Význam parametrů příkazu:

- -0 číslo – označení pro deautentizační útok s počtem deautentizačních rámců
- -a – MAC adresa přístupového bodu
- -c – MAC adresa deautentizované stanice
- mon0 – rozhraní útočícího adaptéru



Obrázek 17: Deautentizace klienta

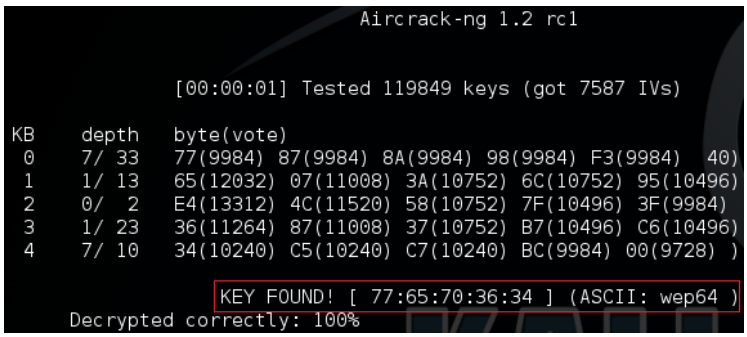
Po provedení deautentizace a odchycení potřebného paketu uvidíme velký nárůst injektovaných ARP paketů. Nyní postačí pouze vyčkat pár desítek vteřin pro odchycení dostatečně velkého množství dat.

Obrázek 18: Intenzivní komunikace mezi přístupovým bodem a útočníkem

Po nasbírání dostatečného počtu inicializačních vektorů je posledním krokem rozluštění klíče nástrojem *aircrack-ng*, který dešifruje získané pakety ze souboru *wepcrack-01.ivs* pomocí následujícího příkazu:

aircrack-ng wepcrack-01.ivs

Na výstupu nástroje *aircrack-ng* lze vidět, že díky odchyceným 7 587 IV se podařilo klíč rozluštit za jednu vteřinu s 100% přesností, přičemž bylo otestováno 119 849 klíčů.



Obrázek 19: Odhalení WEP klíče

6.4.1.2 Zhodnocení

Realizace útoku se skládá pouze z několika málo příkazů a zdárného výsledku bylo dosaženo zhruba po pěti minutách práce, včetně napsání uvedených příkazů. Demonstrovaný postup byl proveden na 64bitovou variantu WEP. Pro srovnání byla stejným způsobem otestována i 128bitová varianta. Při odchycení přibližně stejného množství paketů a použití shodného hesla, jako v případě 64bitové varianty, trvalo rozluštění klíče 207 vteřin. Z této zřetelně vyšší časové náročnosti zisku klíče vyplývá, že je pro rozluštění 128bitového klíče v řádu několika vteřin nutné odchytit větší množství paketů.

6.4.2 Injekce pomocí Chopchop útoku

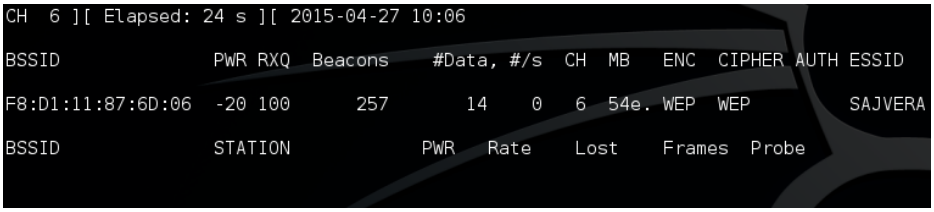
Chopchop útok, který se rovněž řadí mezi skupinu aktivních útoků, byl rozebrán již v kapitole 5.8.6. Pro připomenutí, tímto útokem jsme schopni dešifrovat jakýkoliv rámec bez znalosti šifrovacího klíče. Ovšem ne všechny přístupové body je možné tímto typem útoku napadnout.

Princip testování spočívá v odchycení alespoň jednoho vhodného datového rámce. Na základě jeho analýzy jsme pak schopni vytvořit rámce vlastní a následně je injektovat do sítě za účelem zisku tajného klíče. Samotný Chopchop útok lze, na rozdíl od předešlého útoku, provést na přístupový bod, na kterém není připojena žádná stanice. Ovšem za předpokladu, že přístupový bod bude nějaká data vysílat ven (ze síťového LAN segmentu), například ARP požadavek.

6.4.2.1 Realizace

Stejně jako u předchozího útoku nejdříve spustíme nástroj *airodump-ng* s údaji, které jsme získali pomocí skenování okolí. Význam parametrů příkazu je naprosto stejný, pouze budeme data shromažďovat do souboru se jménem *chopc*, který na konci použijeme k odhalení klíče. Příkaz je tedy následující:

airodump-ng -c 6 --bssid F8:D1:11:87:6D:06 --ivs -w chopc mon0



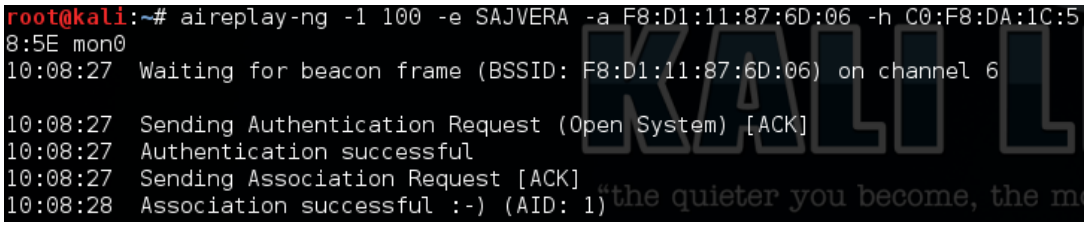
Obrázek 20: Monitorování cíle při Chopchop

Z uvedeného obrázku je patrné, že k přístupovému bodu nejsou připojeny žádné stanice. Z toho důvodu je nutné provést falešnou autentizaci útočícího adaptéru na přístupový bod. Tu provedeme pomocí nástroje *aireplay-ng* následovně:

aireplay-ng -1 100 -e SAJVERA -a F8:D1:11:87:6D:06 -h C0:F8:DA:1C:58:5E mon0

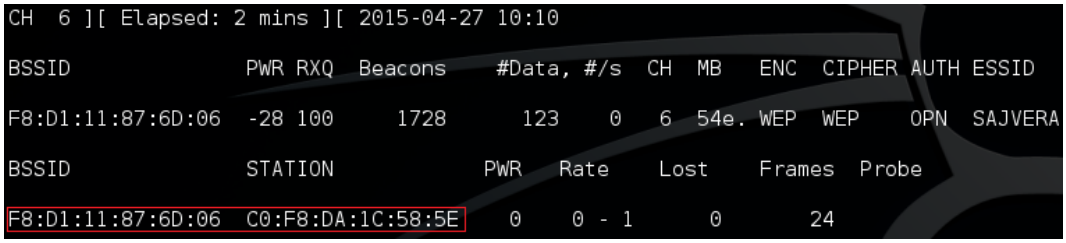
Význam parametrů příkazu:

- -1 číslo – falešná autentizace a reasociační čas v sekundách
- -e – název sítě
- -a – MAC adresa přístupového bodu
- -h – MAC adresa útočícího adaptéru
- mon0 – rozhraní útočícího adaptéru



Obrázek 21: Falešná autentizace

Z výpisu nástroje vidíme, že autentizace a asociace s přístupovým bodem proběhla v pořádku. Tuto skutečnost můžeme ověřit nástrojem *airodump-ng*, který sleduje a zaznamenává síťový provoz.



Obrázek 22: Ověření falešné autentizace

Útočící bezdrátová karta je autentizována na přístupový bod. Můžeme tedy zahájit Chopchop útok tímto příkazem:

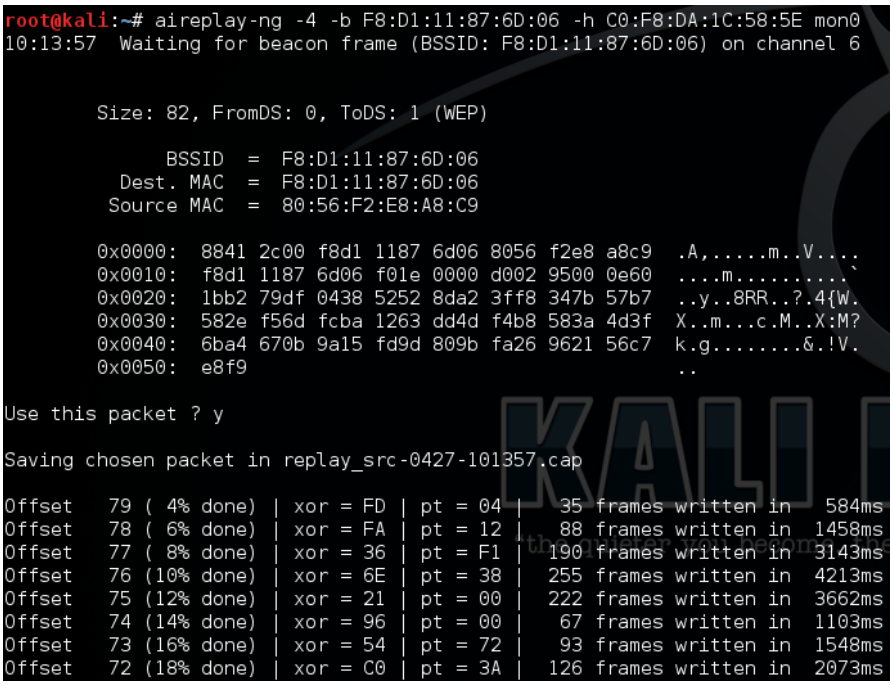
aireplay-ng -4 -b F8:D1:11:87:6D:06 -h C0:F8:DA:1C:58:5E mon0

Význam parametrů příkazu:

- -4 – Chopchop útok
- -b – MAC adresa přístupového bodu
- -h – MAC adresa útočící karty
- mon0 – rozhraní útočící karty

Je bezpodmínečně nutné, aby MAC adresa specifikovaná parametrem –h byla totožná s MAC adresou, která byla použita při falešné autentizaci. V opačném případě útok nebude úspěšný.

Po provedení příkazu program čeká na vhodný rámec. Ve chvíli, kdy rámec zachytí, požaduje jeho potvrzení stiskem klávesy Y. Při výběru daného rámce se řídíme podle MAC adresy přístupového bodu a rovněž podle cílové MAC adresy. Po potvrzení rámce se provede Chopchop útok, který ho hádáním dešifruje byte po bytu. Celou situaci znázorňuje obrázek č. 23.



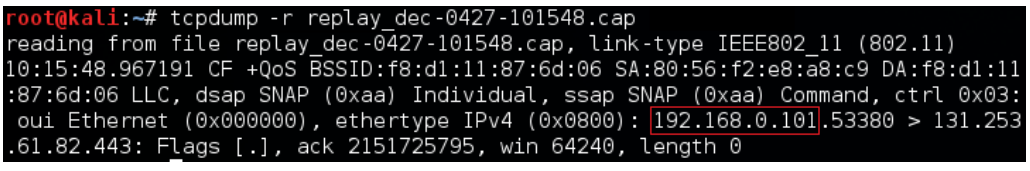
Obrázek 23: Potvrzení odchyceného rámce a provedení Chopchop útoku

Po uhádnutí všech bytů zachyceného rámce získáme dva výsledné soubory. První soubor má příponu .cap a obsahuje otevřený text rámce. Druhý soubor s příponou .xor obsahuje tajnou šifrovací sekvenci.

Obrázek 24: Získané soubory po úspěšném Chopchop útoku

Oba získané soubory po úspěšném Chopchop útoku nyní použijeme k vytvoření falešného ARP paketu, který budeme injektovat do sítě za účelem zisku klíče. Jelikož většina přístupových bodů nerozlišuje použitou cílovou a zdrojovou IP adresu, je možné použít adresu broadcastu (255.255.255.255), nebo si IP adresu jednoduše vymyslet. My však použijeme nástroj *tcpdump* a zjistíme alespoň IP adresu přístupového bodu analýzou souboru s příponou .cap:

tcpdump -r replay_dec-0427-101548.cap



Obrázek 25: Výstup nástroje tcpdump

Zjistili jsme, že přístupový bod má IP adresu 192.168.0.101. S touto znalostí a souborem s příponou .xor jsme schopni vytvořit potřebný paket pomocí nástroje *packetforge-ng*. K tomu slouží následující příkaz:

packetforge-ng -0 -h C0:F8:DA:1C:58:5E -a F8:D1:11:87:6D:06 -l 192.168.0.102 -k 192.168.0.101 -y replay_dec-0427-101548.xor -w arp.cap

Význam parametrů příkazu:

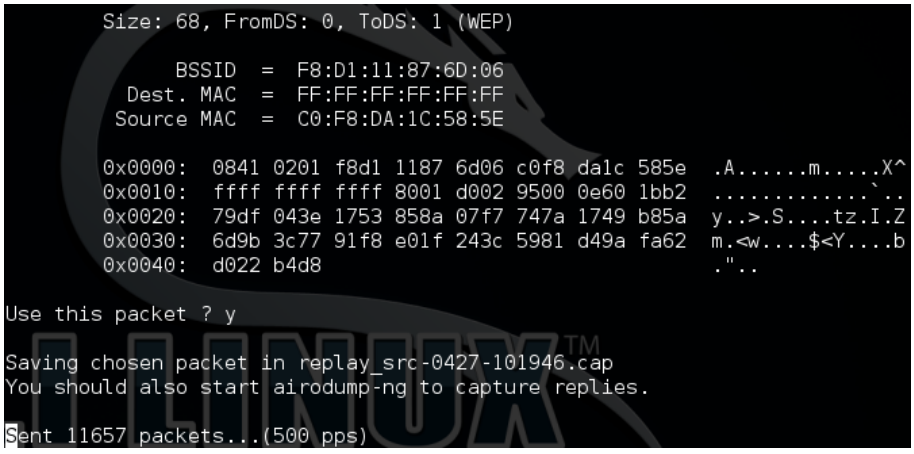
- -0 – značí vytvoření ARP paketu
- -h – zdrojová MAC adresa (útočící karty)
- -a – MAC adresa přístupového bodu
- -l – zdrojová IP adresa (smyšlená)
- -k – cílová IP adresa (přístupového bodu)
- -y – soubor s šifrovací sekvencí
- -w – soubor, do kterého bude vytvořený paket uložen

Po úspěšném vytvoření ARP paketu zahájíme jeho injekci do sítě nástrojem *aireplay-ng* s následujícími parametry:

aireplay-ng -2 -r arp.cap mon0

Význam parametrů příkazu:

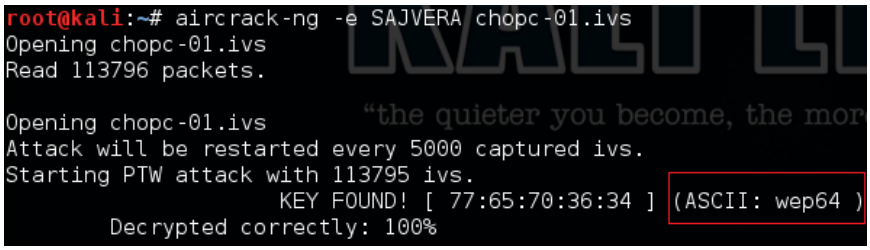
- -2 – značí injekci libovolného paketu
- -r – soubor s injektovaným paketem
- mon0 – rozhraní útočící karty



Obrázek 26: Injekce podvrženého ARP paketu

Pro započetí injekce potvrdíme vybraný paket. Následně můžeme vidět obrovský nárůst hodnot, a to jak v tomto terminálu, tak i v terminálu, kde běží *airodump-ng*, který je zaznamenává do souboru.

Nakonec spustíme *aircrack-ng* a z odchycených 113 795 IV rozluštíme tajný klíč, viz obrázek č. 27.



Obrázek 27: Výsledek injekce pomocí Chopchop útoku

6.4.2.2 Zhodnocení

Realizace tohoto útoku byla o něco složitější, než předešlá varianta útoku. K zisku tajného WEP klíče bylo tedy nutné provést více kroků. Nicméně i tento útok lze úspěšně vykonat v řádu pouhých minut.

6.5 WPA/WPA2

Mezi útoky, které lze provést na bezdrátové sítě zabezpečené pomocí WPA/WPA2 můžeme zařadit Beck-Tews útok na TKIP, či jeho modifikovanou podobu Ohigashi-Morii útok. Tyto útoky však nevracejí klíč a z toho důvodu si ukážeme prolomení PSK klíče pomocí slovníkového útoku, který byl dlouhou dobu jediným způsobem, jak na zabezpečení WPA, respektive WPA2 zaútočit. Obě metody zabezpečení jsou totiž silně závislé na zvoleném hesle.

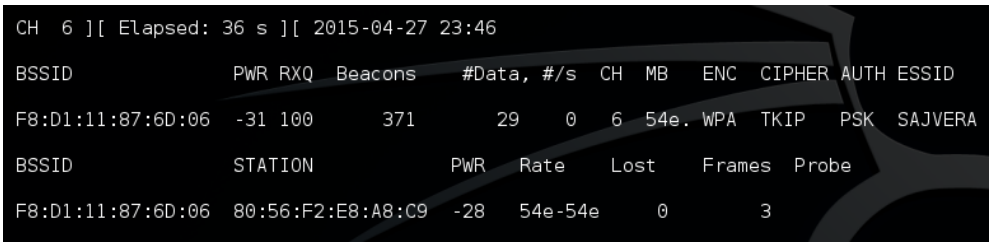
6.5.1 Útok na PSK

Pokud je na přístupovém bodu nastaven osobní režim, znamená to, že je pro autentizaci použita metoda s předsdíleným klíčem PSK. Ten se generuje na základě zadaného hesla, které musí být od 8 do 63 znaků dlouhé. Jediná možnost, jak ho prolomit, spočívá v odchycení autentizačních rámců během jejich čtyřcestné výměny mezi přístupovým bodem a klientem (čtyřcestný handshake) a následně vynaložené velké výpočetní síle v podobě slovníkového útoku (resp. útoku hrubou silou).

6.5.1.1 Realizace

Vlastní útok začíná stejně jako v předešlých případech spuštěním nástroje *airodump-ng* pro zachytávání komunikace do souboru. V případě WPA/WPA2 však nestačí zachytávat pouze inicializační vektory, ale je nutné zachytávat celé pakety. Spustíme tedy již známý příkaz, nyní však bez parametru *--ivs*:

airodump-ng -c 6 --bssid F8:D1:11:87:6D:06 -w psk mon0

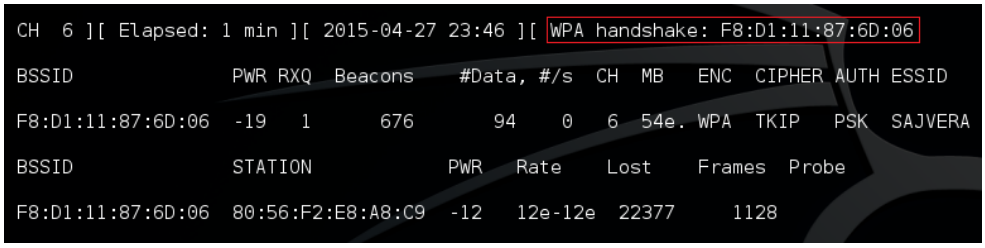


Obrázek 28: Monitorování sítě s WPA

V dalším kroku je nutné zachytit čtyřcestný handshake mezi přístupovým bodem a klientskou stanicí. Ten je možné získat jak pasivně, vyčkáním dokud se k přístupovému bodu nějaká stanice nepřihlásí, tak aktivně, provedením deautentizace již připojené stanice. Z výpisu je patrné, že je k přístupovému bodu jedna stanice připojena. Zahájíme tedy deautentizaci rovněž známým příkazem:

aireplay-ng -0 3 -a F8:D1:11:87:6D:06 -c 80:56:F2:E8:A8:C9 mon0

Po provedení deautentizace jsme získali potřebný handshake, což indikuje popisek v pravém horním rohu následujícího výpisu nástroje *airodump-ng*.



Obrázek 29: Zachycený čtyřcestný handshake

V tuto chvíli můžeme proces zachytávání komunikace ukončit, neboť k provedení slovníkového útoku již máme všechny potřebné komponenty. K dešifrování souboru je nutné nachystat si kvalitní slovník, který buď můžeme stáhnout z internetu, nebo si vygenerovat vlastní. Použitý slovník *all.lst* se skládá z více dílčích slovníků nejvíce používaných frází několika jazyků, přičemž obsahuje téměř 4 miliony slov. Pro spuštění slovníkového útoku slouží tento příkaz:

aircrack-ng -w all.lst psk-01.cap

kde pomocí parametru -w specifikujeme cestu k použitému slovníku a dále uvádíme soubor z odchyceným čtyřcestným handshakem.

Obrázek 30: Prolomení PSK klíče

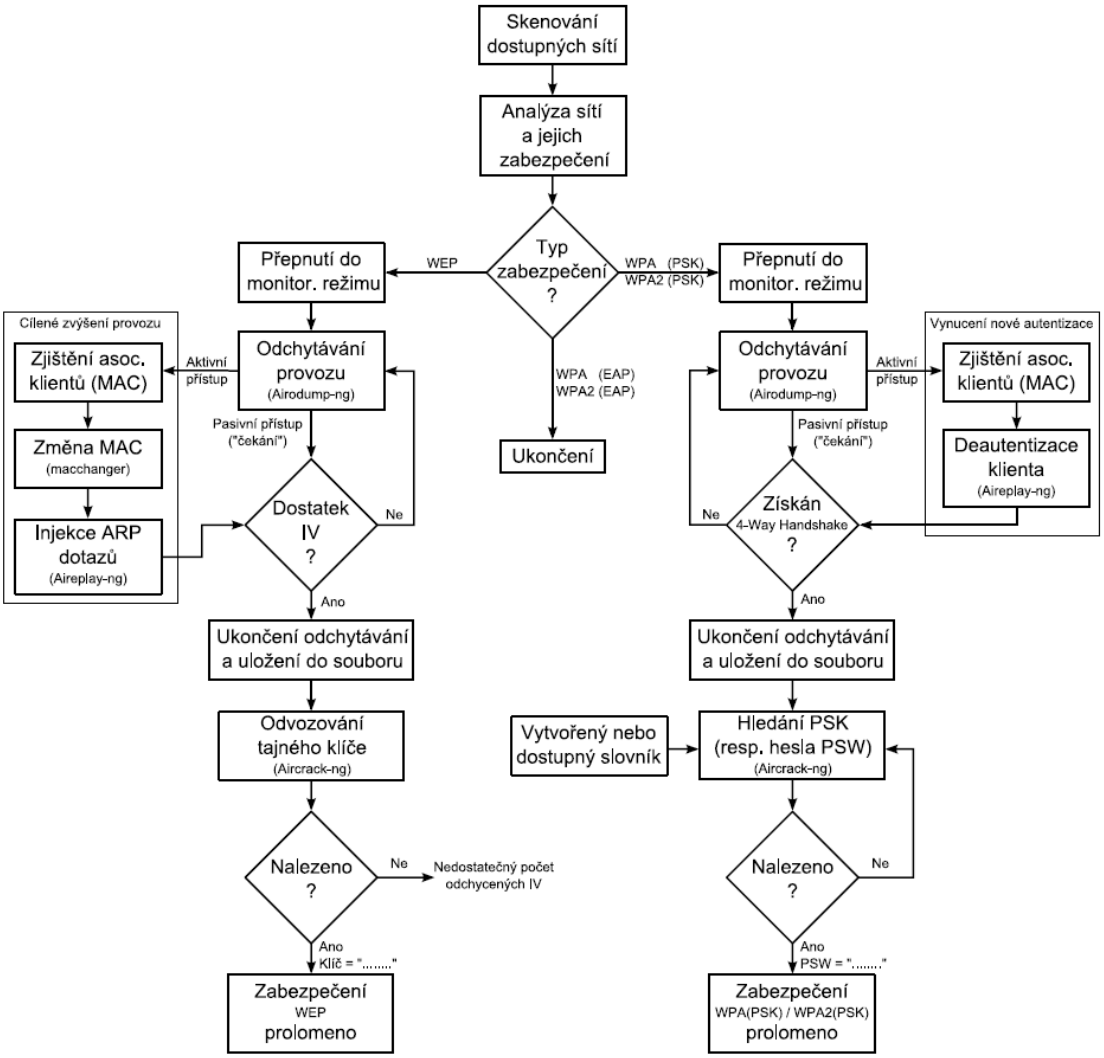
Jak můžeme vidět, celý útok proběhl po více než 13 minutách úspěšně. Otestováno bylo 886 052 klíčů s průměrnou rychlostí 955 klíčů za sekundu.

6.5.1.2 Zhodnocení

Při provedení útoku bylo využito slabiny, kterou nabízí autentizační proces mezi stanicí a přístupovým bodem. Zachycení potřebného handshaku bylo vynuceno pomocí deautentizace. Celková doba trvání útoku byla při takto simulovaných nastaveních přibližně 16 minut včetně luštění klíče. Nicméně použité heslo pro zabezpečení bezdrátové sítě bylo zvoleno tak, aby byl slovníkový útok úspěšný, a to v přiměřeném čase. Ve skutečnosti se tedy doba potřebná k provedení útoku může mnohonásobně lišit v závislosti na složitosti použitého hesla a vhodně zvoleném slovníku.

6.6 Shrnutí provedených útoků

V rámci ověřování bezpečnosti bezdrátových sítí WLAN bylo provedeno testování těchto sítí zabezpečených nejdříve pomocí dnes již nevyhovujícího, ale stále občas využívaného zabezpečení WEP a následně pomocí implementačně dokonalejšího protokolu WPA, který eliminuje bezpečnostní slabiny protokolu WEP. Průběh testování, respektive realizaci útoků na tato zabezpečení lze vyjádřit blokovým diagramem znázorněným na obrázku č. 31. Uvedený diagram zahrnuje i možnost cíleného zvýšení provozu sítě v rámci WEP, nebo vynucení opětovné autentizace již připojené stanice za účelem odchycení čtyřcestného handshake v případě WPA.



Obrázek 31: Diagram průběhu testování

7 Závěr

Bezdrátové sítě prochází neustálým technologickým vývojem. I když hlavním cílem je zvyšování jejich rychlosti, tento faktor je většinou následovaný požadavky na povolení přístupu do sítě pouze autorizovaným osobám, sdílení žádaných prostředků a služeb, či šifrování a zabezpečení přenášených dat.

Zabezpečení bezdrátových sítí je rozdílné z pohledu prostředí, ve kterém je bezdrátová síť provozována. V domácích bezdrátových sítích jde hlavně o uživatelské pohodlí, přičemž všeobecná znalost dané problematiky není na tak vysoké úrovni jako je tomu u sítí firemních. Hlavní faktory, které neblahým způsobem ovlivňují bezpečnost, jsou neznalost elementárních pojmů a charakteristik bezpečnostní problematiky, pohodlnost nebo omezené možnosti prostředků. V domácích sítích jsou bezpečnostní rizika velmi často podceňována, nebo zanedbávána. To v konečném důsledku vede k velké náchylnosti a malé odolnosti těchto sítí vůči vnějším útokům.

Ve firemních sítích je situace poněkud odlišná. Jelikož se v tomto prostředí pracuje s velmi citlivými daty, je potřeba je náležitým způsobem chránit. Z toho důvodu se zde na bezpečnost klade velký důraz. Pochopitelně záleží na prostředí každé společnosti, ale v podstatě se bezpečnost sítě v každé z nich vyvíjí dlouhodobě, mají ji na starosti odborníci a většinou bývá kvalitní. Využívají se komplexní metody zabezpečení, které společně s důkladným nastavením a prováděnými kontrolami bezpečnosti poskytují vysokou úroveň ochrany před vnějším zneužitím.

Ze zkoumání jednotlivých standardů, jejich slabin a provedené analýzy bezpečnosti vyplynuly zajímavé výsledky, znalosti a zkušenosti týkající se zabezpečení bezdrátových sítí WLAN a operačního systému Linux. Velkým překvapením bylo, že pro provedení testů není nutné využívat speciální, či nákladné hardwarové vybavení, ale postačí běžný notebook s integrovanou bezdrátovou kartou.

Na základě provedených útoků lze jasně potvrdit, že je používání protokolu WEP pro zabezpečení bezdrátové sítě nevhodné a silně nedoporučované, a to i v kombinaci s doplňujícími mechanismy jako je filtrace MAC adres, či zamezení vysílání SSID identifikátoru. Tajný klíč je možno s cíleným zvýšením provozu odhalit se 100% úspěšností v řádu pouhých minut. Protokol WEP tak nelze považovat za bezpečný. Protokol WPA a zejména pak protokol WPA2 podstatným způsobem zvýšily úroveň bezpečnosti, jelikož využívají silnější šifrovací mechanismy. Bohužel i tyto protokoly, které jsou považované za nejbezpečnější, mohou být při nesprávném nastavení náchylné k neautorizovanému průniku. Záleží na důkladném nastavení přístupového bodu, klientských stanic a případně i autentizačního serveru. Kritickým bodem je však kvalita a délka použitého hesla, které se tak může stát terčem slovníkového útoku. Z tohoto důvodu je důležité použít co nejdelší heslo

složené kombinací čísel, písmen a speciálních znaků, aby se toto riziko co nejvíce minimalizovalo.

Obecně lze doporučit použití protokolu CCMP založeného na blokové šifře AES, jelikož pro tento typ ochrany prozatím nebyl objeven způsob, jak toto zabezpečení prolomit. V případě domácích sítí je stále možné využívat protokol TKIP, avšak za podmínky použití silného hesla. Ve firemním prostředí je nejlepším možným způsobem ochrany AES CCMP s autentizací prováděnou vůči autentizačnímu serveru RADIUS. Tento způsob šifrování a autentizace je v dnešní době neprolomitelnou kombinací a v žádné společnosti by tedy neměl chybět.

Závěrem lze říci, že nejlepším řešením vůbec je přenechat vybudování a zabezpečení bezdrátové sítě na odbornících, kteří se v této problematice pohybují a vyznají, nebo sledovat vývoj bezpečnostních rizik a reagovat na ně odpovídajícími metodami zabezpečení.

8 Seznam použité literatury

[1] IEEE. In: *Http://www.fei.stuba.sk* [online]. 2008 [cit. 2015-04-14]. Dostupné z: http://www.fei.stuba.sk/docs//kniznica/ieee_cz.pdf

[2] IEEE at a Glance. IEEE. *Http://www.ieee.org* [online]. 2015 [cit. 2015-04-14]. Dostupné z: http://www.ieee.org/about/today/index.html

[3] ZANDL, Patrick. *Bezdrátové sítě WiFi: praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003, 190 s. ISBN 80-722-6632-2.

[4] KOCOUR, Zbyněk a Miroslav ŠAFRÁNEK. Fyzická vrstva Wi-Fi. *Access server* [online]. 2008, roč. 13, č. 6 [cit. 2015-04-14]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2008050006

[5] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G*. Vyd. 1. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.

[6] Jak probíhají bezdrátové přenosy v sítích WLAN. In: *Combitrading* [online]. 2009 [cit. 2015-04-14]. Dostupné z: http://www.combitrading.cz/technologie/jak-probihaji-bezdratove-prenosy-v-sitich-wlan.html

[7] PUŽMANOVÁ, Rita. WLAN může být rychlejší. In: *Lupa.cz* [online]. 2004 [cit. 2015-04-14]. Dostupné z: http://www.lupa.cz/clanky/wlan-muze-byt-rychlejsi/

[8] SIMANDL, Martin. IEEE 802.11n - Jak na rychlé Wi-Fi doma i venku: Technologie použití více antén. In: *PCTuning.cz* [online]. 2010 [cit. 2015-04-14]. Dostupné z: http://pctuning.tyden.cz/hardware/site-a-internet/16921-ieee-802-11n-jak-na-rychle-wi-fi-doma-i-venku?start=3

[9] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 2. aktualizované vydání Brno: Computer Press, 2006, 430 s. ISBN 80-251-1278-0.

[10] ZELINKA, Tomáš a Miroslav SVÍTEK. *Telekomunikační řešení pro informační systémy síťových odvětví*. 1. vyd. Praha: Grada, 2009, 218 s. ISBN 978-80-247-3232-9.

[11] PUŽMANOVÁ, Rita. Kvalita služby ve WLAN: 802.11e. In: *Lupa.cz* [online]. 2004 [cit. 2015-04-14]. Dostupné z: http://www.lupa.cz/clanky/kvalita-sluzby-ve-wlan-802-11e/

[12] KOVÁŘ, P. a V. NOVOTNÝ. Přístupové metody bezdrátových sítí. *Access server* [online]. 2008, roč. 13, č. 3 [cit. 2015-04-14]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2008100003

[13] BRISBIN, Shelly. *Wi-fi: postavte si svou vlastní wi-fi síť*. Praha: Neocortex, 2003, 248 s. ISBN 80-863-3013-3.

[14] POOLE, Ian. IEEE 802.11 Wi-Fi Standards. In: *Radio-electronics.com* [online]. 2007, 2013 [cit. 2015-04-14]. Dostupné z: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php/ieee-802-11af-white-fi-tv-space.php

[15] TRČÁLEK, Antonín a Dušan KOS. Nový standard Wi-Fi: Gigabit vzduchem. *Živě.cz* [online]. 2012, roč. 3, č. 165687 [cit. 2015-04-14]. Dostupné z: http://www.zive.cz/clanky/novy-standard-wi-fi-gigabit-vzduchem/sc-3-a-165687/default.aspx

[16] LEITNER, Miroslav. Co přináší druhá generace Wi-Fi sítí 802.11ac Wave 2. *Svět sítí* [online]. 2015, č. 922015 [cit. 2015-04-14]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Co-prinasi-druha-generace-bezdratovych-siti-80211ac-Wave-2-1-cast-922015

[17] ODVÁRKA, Petr. Základy topologie a komunikace. *Svět sítí* [online]. 2000, č. 192000 [cit. 2015-04-15]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Zaklady-topologie-a-komunikace-192000

[18] SATRAPA, Pavel. TUL. *Počítačové sítě*. Liberec, BR. Dostupné z: http://www.nti.tul.cz/~satrapa/vyuka/site/

[19] PŘIBYL, Tomáš. Stručná historie lámání šifer. *Computerworld* [online]. 2011, č. 48338 [cit. 2015-04-14]. Dostupné z: http://computerworld.cz/securityworld/historie-hackingu-strucna-historie-lamani-sifer-48338

[20] LEHEMBRE, Guillaume. *Bezpečnost Wi-Fi – WEP, WPA a WPA2* [online]. 2006 [cit. 2015-04-14]. Dostupné z: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf

[21] ODVÁRKA, Petr. Technologie pro zlepšení bezpečnosti datových sítí - standard 802.1x. *Svět sítí* [online]. 2004, č. 922004 [cit. 2015-04-15]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Technologie-pro-zlepseni-bezpecnosti-datovych-siti-standard-8021x-1-922004

[22] ROHLEDER, D. a V. LORENC. 802.1X - autentizace v počítačových sítích. *Zpravodaj ÚVT MU* [online]. 2008, XIX, č. 1, s. 2-4 [cit. 2015-04-15]. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/590.html

[23] BARKEN, Lee. *Wi-Fi: jak zabezpečit bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2004, 174 s. ISBN 80-251-0346-3.

[24] BOUŠKA, Petr. WiFi - základní principy a protokoly. *Samuraj-cz* [online]. 2009 [cit. 2015-04-17]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-wifi-zakladni-principy-a-protokoly/

[25] FITZPATRICK, Jason. The Difference Between WEP, WPA, and WPA2 Wireless Encryption (and Why It Matters). *How-To Geek* [online]. 2013 [cit. 2015-04-17]. Dostupné z: http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/

[26] DOLEŽAL, Petr. AES (Advanced Encryption Standard) šifra pro třetí tisíciletí. In: *Jikos* [online]. 2001 [cit. 2015-04-17]. Dostupné z: http://www.jikos.cz/~gumysh/docs/AES/

[27] KLÍMA, Vlastimil. *Symetrická kryptografie III: Mody činnosti blokových šifer a hašovací funkce*. 2007 [cit. 2015-04-17]. Dostupné z: http://crypto-world.info/klima/mffuk/Symetricka_kryptografie_III_2007.pdf

[28] FRANKEL, Sheila, Bernard EYDT, Les OWENS a Karen SCARFONE. NIST. *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i* [online]. 2007 [cit. 2015-04-17]. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[29] JOHNSON, Jakob. NIST. *On the Security of CTR + CBC-MAC* [online]. 2012, 18 s. [cit. 2015-04-17]. Dostupné z: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm-ad1.pdf

[30] OBR, Jiří. Sniffing: Odposlech datové komunikace. *ITBIZ* [online]. 2009 [cit. 2015-04-17]. Dostupné z: http://www.itbiz.cz/sniffing-odposlech-datove-komunikace

[31] Bráníme se odposlechu: promiskuitní režim. *Lupa.cz* [online]. 2006, č. 1 [cit. 2015-04-17]. Dostupné z: http://www.lupa.cz/clanky/branime-se-odposlechu-promiskuitni-rezim/

[32] HALLER, Martin. Denial of Service (DoS) útoky. *Lupa.cz* [online]. 2006 [cit. 2015-04-17]. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-dos-utoky-uvod/

[33] PŘIBYL, Tomáš. Zákeřný útok jménem DoS. *SystemOnLine* [online]. 2006 [cit. 2015-04-17]. Dostupné z: http://www.systemonline.cz/it-security/zakerny-utok-jmenem-dos.htm

[34] ŠUSTR, Matěj. Bezpečnost a Hacking WiFi (802.11): 3. WEP. *Security-portal* [online]. 2009, [cit. 2015-04-18]. Dostupné z: http://www.security-portal.cz/clanky/bezpečnost-hacking-wifi-80211-3-wep

[35] Packet injection. *Wiki airdump*. 2011. Dostupné z: http://wiki.airdump.cz/Packet_injection

[36] BITTAU, Andrea. The fragmentation attack in practice. In: *IEEE Symposium on Security and Privacy, IEEE Computer Society* [online]. 2005 [cit. 2015-04-17]. Dostupné z: http://download.aircrack-ng.org/wiki-files/doc/Fragmentation-Attack-in-Practice.pdf

[37] HALVORSEN, Finn Michael a Olav HAUGEN. *Cryptanalysis of IEEE 802.11 i TKIP* [online]. Trondheim, 2009 [cit. 2015-04-18]. Dostupné z: http://download.aircrack-ng.org/wiki-files/doc/tkip_master.pdf. NTNU.

[38] TEWS, Erik; BECK, Martin. Practical attacks against WEP and WPA. In:*Proceedings of the second ACM conference on Wireless network security*. ACM [online]. 2009. p. 79-86. [cit. 2015-04-18]. Dostupné z: http://dl.aircrack-ng.org/breakingwepandwpa.pdf

[39] Byte-Sized Decryption of WEP with Chopchop. In: *InformIT* [online]. 2004, Jun 9, 2006 [cit. 2015-04-18]. Dostupné z: http://www.informit.com/guides/printerfriendly.aspx?g=security&seqNum=196

[40] OHIGASHI, Toshihiro a Masakatu MORII. A practical message falsification attack on WPA. In: *Procedings of Joint Workshop on Information Security, Cryptography and Information Security Conference System*. [online] 2009 [cit. 2015-04-18]. Dostupné z: http://dl.packetstormsecurity.net/papers/wireless/A_Practical_Message_Falsification_Attack_On_WPA.pdf

[41] FLEISHMAN, G. WiFi "Hole196": major exploit or much ado about little?. In: *ArsTechnica* [online]. 2010 [cit. 2015-04-18]. Dostupné z: http://arstechnica.com/business/2010/07/wifi-hole196-major-exploit-or-much-ado-about-little/

Seznam použitých zkratek

AES	Advanced Encryption Standard
AIFS	Arbitration Interframe Space
ARP	Address Resolution Protocol
BSA	Basic Service Area
BSS	Basic Service Set
CBC-MAC	Cipher Block Chaining MAC
CCM	CTR with CBC-MAC
CCMP	Counter-mode CBC-MAC Protokol
CFP	Contention Free Period
CP	Contention Period
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision avoidance
DCF	Distributed Coordination Function
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIFS	DCF Interframe Space
DoS	Denial of Service
DSSS	Direct-sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LANs
EDCF	Enhanced DCF
ESS	Extended Service Set
FHSS	Frequency-hopping spread spectrum
HCF	Hybrid Coordination Function
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IV	Initialization vector
MAC	Media Access Control
MIC	Message Integrity Code
MIMO	Multiple-input multiple-output
MITM	Man-In-The-Middle
OFDM	Orthogonal frequency-division multiplexing
PCF	Port Coordination Function
PHY	Physical Layer

PN	Packet Number
PSK	Pre-Shared Key
QoS	Quality of Service
RADIUS	Remote Authentication and Dial-In User Service
RC4	Rivest Cipher 4
RSN	Robust Security Network
SSID	Service set identifier
TKIP	Temporal Key Integrity Protocol
TSN	Transition Security Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA	Wi-Fi Protected Access

Seznam použitých obrázků

Obrázek 1: Pokrytí vrstev dle IEEE 802.11, převzato z [4] 2
Obrázek 2: Přístupové metody, převzato z [12] 5
Obrázek 3: Struktura 802.11 sítě, převzato z [3] 10
Obrázek 4: Topologie sítě Ad-hoc, převzato z [3] 12
Obrázek 5: Topologie Infrastrukturní sítě, převzato z [3] 12
Obrázek 6: WEP, převzato z: http://wiki.airdump.cz/Hacking_WiFi_sítí 17
Obrázek 7: WPA, převzato z: http://wiki.airdump.cz/Wi-Fi_Protected_Access 21
Obrázek 8: WPA2, převzato z [23] 25
Obrázek 9: Identifikace bezdrátového adaptéru 42
Obrázek 10: Monitorovací režim na virtuálním rozhraní 42
Obrázek 11: Monitorovací režim na fyzickém rozhraní 42
Obrázek 12: Test injekce paketů 43
Obrázek 13: Monitorování dostupných sítí a klientů 43
Obrázek 14: Duplikace MAC adresy 44
Obrázek 15: Monitorování cíle při ARP injekci 46
Obrázek 16: Zahájení ARP injekce 46
Obrázek 17: Deautentizace klienta 46
Obrázek 18: Intenzivní komunikace mezi přístupovým bodem a útočníkem 47
Obrázek 19: Odhalení WEP klíče 47
Obrázek 20: Monitorování cíle při Chopchop 48
Obrázek 21: Falešná autentizace 49
Obrázek 22: Ověření falešné autentizace 49
Obrázek 23: Potvrzení odchyceného rámce a provedení Chopchop útoku 50
Obrázek 24: Získané soubory po úspěšném Chopchop útoku 50
Obrázek 25: Výstup nástroje tcpdump 50
Obrázek 26: Injekce podvrženého ARP paketu 51
Obrázek 27: Výsledek injekce pomocí Chopchop útoku 52
Obrázek 28: Monitorování sítě s WPA 53
Obrázek 29: Zachycený čtyřcestný handshake 53
Obrázek 30: Prolomení PSK klíče 54
Obrázek 31: Diagram průběhu testování 55

Seznam použitých tabulek

Tabulka 1: Podstatné dodatky k IEEE 802.11 7
Tabulka 2: Porovnání zabezpečení dle vhodnosti použití 27

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2014/2015

Studijní program: Aplikovaná informatika
Forma: Prezenční
Obor/komb.: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Sajvera Miroslav	Štefánikova 316, Hradec Králové - Moravské Předměstí	I1101350

TÉMA ČESKY:

Bezdrátové sítě a jejich zabezpečení

NÁZEV ANGLICKY:

Wireless networks and security

VEDOUCÍ PRÁCE:

Ing. Vladimír Soběslav, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cíl práce: Prozkoumat problematiku bezdrátových sítí se zaměřením na jejich bezpečnost.

Osnova práce:
1.Úvod
2.Standard IEEE 802.11
2.1.Fyzická vrstva PHY
2.2.Podvrstva MAC
2.3.Dodatky
3.Struktura bezdrátové sítě
4.Topologie bezdrátové sítě
5.Zabezpečení
6.Útoky
7.Praktická část
7.1.Otestování zabezpečení
7.2.Vyhodnocení výsledků
8.Závěr

SEZNAM DOPORUČENÉ LITERATURY:

Podpis studenta: Sajvera **Datum:** 28.4.2015

Podpis vedoucího práce: **Datum:** 28.04.2015