UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

BAKALÁŘSKÁ PRÁCE

2016 Milan Zmítko

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Analýza slabin zabezpečení WPA a WPA2

Milan Zmítko

Bakalářská práce

2016

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2015/2016**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Milan Zmítko**
Osobní číslo:	**I11240**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Analýza slabin zabezpečení WPA a WPA2**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je zmapovat slabiny zabezpečení bezdrátové sítě s využitím standardního WPA a WPA2 Personal. Bude provedena podrobná analýza komunikace pomocí Kali Linux a navrhne řešení s využitím konfigurace WPA/WPA2 Enterprise. Práce bude obsahovat tři laboratorní úlohy s podrobným step by step řešením pro simulaci a porovnání použití WPA/WPA2 Personal nebo nasazení WPA/WPA2 Enterprise v podnikové síti.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

*** WRIGHTSON, Tyler. Wireless network security: a beginner's guide. New York: McGraw-Hill, c2012, xvii, 347 p. ISBN 00-717-6094-6.**
*** MILLER, Lawrence. Home Networking Do-It-Yourself For Dummies. 2011. vyd. ISBN 978-0-470-56173-7.**

Vedoucí bakalářské práce: **Ing. Soňa Neradová, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2015**
Termín odevzdání bakalářské práce: **13. května 2016**

Univerzita Pardubice -8- Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Mgr. Josef Horálek, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2016

Prohlášení autora

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

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

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 12. 05. 2016 Milan Zmítko

PODĚKOVÁNÍ

Na tomto místě bych rád poděkoval vedoucí mé bakalářské práce, Ing. Neradové za cenné rady, zprostředkování zapůjčení hardware, trpělivost a podporu během zpracovávání. Dále bych rád poděkoval své partnerce a nejbližší rodině, za plnou podporu.

ANOTACE

Bakalářská práce se zaměřuje na problematiku zabezpečení bezdrátových Wi-Fi sítí, pomocí WPA a WPA2. V práci je popsán vývoj bezdrátových technologií a jsou detailně rozebrána jednotlivá zabezpečení, jejich slabá místa, včetně možných útoků na ně. Práce obsahuje potřebná doporučení pro zabezpečení různých druhů bezdrátové sítě. Praktická část práce se zabývá analýzou paketové komunikace jednotlivých protokolů, a navrhuje zabezpečení pro podnikovou síť.

KLÍČOVÁ SLOVA

Wi-Fi, WPA, WPA2, IEEE, 802.11, 802.1x, zabezpečení, bezdrátové sítě, Kali Linux

TITLE

The analysis of weaknesses of WPA and WPA2.

ANNOTATION

This thesis focuses on the issue of wireless Wi-Fi networks, that used WPA and WPA2. The work describes the development of wireless technologies and there are discussed in detail each security, their weaknesses, including possible attacks on them. The thesis contains the necessary recommendations for securing various types of wireless networks. The practical part deals with the analysis of individual packet communication of each protocols, and suggests security solution for the corporate network.

KEYWORDS

Wi-Fi, WPA, WPA2, IEEE, 802.11, 802.1x, security, wireless networks, Kali Linux

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM TABULEK

SEZNAM ZKRATEK A ZNAČEK

AES	Advanced Encryption Standard
AKM	Auth Key Management
AP	Access Point
ASCII	American Standard Code for Information Interchange
BSS	Basic Service Set
CCMP	Counter Mode with Ciper Block Chaining Message Authentication Code Protocol
CRC	Cyclic Redundancy Check
ČR	Česká republika
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
GSM	Groupe Spécial Mobile
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IV	Initialization vector
LEAP	Lightweight Extensible Authentication Protocol
LTE	Long Term Evolution
MAC	Media Access Control
MIC	Message Integrity Code
MK	Master Key
OSI	Open Systems Interconnection
PEAP	Protected Extensible Authentication Protocol
PN	Packet Number

PSK	Pre-Shared Key
PTK	Pairwise Master Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RFID	Radio Frequency Identification
RSN	Robust Security Network
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
USA	United States of America
VoIP	Voice over Internet Protocol
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
XOR	Exclusive OR

0 ÚVOD

Bezdrátové sítě jsou v dnešní době téměř samozřejmostí každé domácnosti, ale také firmy, nebo restaurace. Od doby, kdy pořízení Wi-Fi směrovače znamenalo investici několika desítek tisíc korun, uběhla již řada let. Nyní je pořízení základního modelu Wi-Fi směrovače otázkou několika stokorun. Jenom těžko budeme hledat místo v městské zástavbě, které by nebylo doslova „prošpikováno“ Wi-Fi sítěmi. Díky snadné instalaci, která nevyžaduje zdlouhavé a nákladné kabelové vedení, je jednoduché Wi-Fi síť v určité lokalitě vytvořit, ale stejně tak jednoduché je ji zrušit, či přemístit. Tento druh mobily je nespornou výhodou Wi-Fi sítí. Pro samé výhody mají bezdrátové Wi-Fi sítě i některé nevýhody. Oproti klasickým kabelovým sítím nedosahují zdaleka takových přenosových rychlostí a je nutné je důsledně zabezpečovat. Právě zabezpečením Wi-Fi sítí se tato práce zabývá do detailů.

Tato práce popisuje historický vývoj Wi-Fi sítí od úplných základů, až do budoucnosti připravovaných technologií. Na několika praktických příkladech z reálného světa je popsáno netradiční využití Wi-Fi sítí, než jen jako pouhé připojení k internetu. Tyto příklady jsou implementovány na konkrétních místech, kde našli své dobré uplatnění.

Práce rozebírá jednotlivé metody a možnosti zabezpečení Wi-Fi sítí do podrobných detailů. Každá z metod zabezpečení je z hlediska bezpečnosti analyzována na slabá místa, z čehož plynou doporučení k použití daného typu zabezpečení. Jak si jsou provozovatelé bezdrátových sítí vědomi, že je nutností zabezpečit jejich sítě a přenášená data, ukazuje analýza oblasti panelového domu. V tomto domě je provedeno měření, za účelem zjistit kolik Wi-Fi sítí je k dispozici a jak dobře jsou jednotlivé sítě zabezpečeny.

Praktická část dále obsahuje laboratorní úlohy, kde je navržena a konfigurována síťová struktura pro jednotlivé druhy zabezpečení. Bezpečnost a proces autentizace klientské stanice je pak analyzován paketovým analyzátorem. S ohledem na provozní náklady a vstupní investice je navrhnuto bezpečné síťové řešení pro podnikovou síť s centralizovanou správou, kde je třeba dbát na bezpeční přenášených dat. Tato data mohou být velmi citlivého charakteru, a proto by bylo nežádoucí, aby si je nezvaný host mohl v nezašifrované podobě číst.

1 BEZDRÁTOVÉ SÍTĚ

Podnět ke vzniku bezdrátových sítí se datuje několik desítek let nazpět. Jednoduchá potřeba přenosu informací na delší vzdálenosti, nebo do odlehlejších koutů naší planety, kde by bylo vybudování klasické metalické sítě ekonomicky a technologicky velmi náročné. To vše dalo základům bezdrátových sítí. Informace jsou v bezdrátových sítích šířeny vzduchem, a to nejčastěji ve formě elektromagnetických vln v různých kmitočtových pásmech. Ke zvýšení efektivity přenosu dat a odolnosti vůči rušení v rámci jednotlivých kmitočtových pásem se aplikuje systém s tzv. rozprostřeným spektrem. Další možností přenosu informací je optické médium, které se však léty příliš neosvědčilo. Přenos pak probíhá mezi jednotlivými účastníky sítě na fyzické vrstvě síťové struktury. (SKELET, 2007)

1.1 Historie

Samotné základy bezdrátového přenosu informací se datují k roku 1895, kdy italský vědec Guglielmo Marconi přenesl informaci pomocí rádia na vzdálenost zhruba dvou kilometrů. Přístroj si rychle nechal patentovat a o rok později se mu povedlo přenést informaci mezi pobřežím a lodí, a to na vzdálenost celých 19 kilometrů. Historicky první transatlantické bezdrátové spojení bylo provedeno 12. prosince 1901. (HISTORY.COM STAFF, 2009)

Další rozvoj bezdrátového přenosu probíhal především na území USA, kde jej využívaly policejní a bezpečnostní složky, ale také námořnictvo a letectvo. Vývoj bezdrátové technologie dále pokračoval během Druhé světové války, kdy byly na bojišti používány ke komunikaci přenosné radiostanice, vyrobené společností Motorola. Vývoj zaznamenávalo především odvětví mobilních radiových přenosů, které jsou podobné dnešním GSM sítím. (KOCMAN, 2000)

Roku 1997 byl přijat standard IEEE 802.11, popisující bezdrátovou komunikaci mezi počítači, který bude dále rozebrán dopodrobna.

1.2 Wi-Fi

Wi-Fi se řadí mezi jednu z nejznámějších forem bezdrátového přenosu dat. Samotný název neměl zpočátku žádným hlubší význam, až po rozmachu Hi-Fi systémů (*Highest Fidelity*) se z něj stala jakási slovní hříčka Wi-Fi (*Wireless Fidelity*), což lze volně přeložit jako bezdrátová věrnost.

Jedná se o soubor standardů IEEE 802.11, které popisují bezdrátovou komunikaci v počítačových sítích. Komunikace probíhá v tzv. bezlicenčním pásmu 2,4 a 5 GHz, ve

kterém je však nutno vzhledem k omezenému množství frekvencí a obrovskému množství vysílajících zařízení dodržovat určitá pravidla. Tyto pravidla pro ČR stanovuje Český telekomunikační úřad. (HRSTKA, c2010-2016)

Obrázek 1 - Logo Wi-Fi

Zdroj: (Wi-Fi Logo, 2013)

1.2.1 Standard IEEE 802.11

První verze tohoto standardu byla vydána v roce 1997. Nabízela přenosové rychlosti maximálně 2 Mb/s. K navýšení přenosové rychlosti došlo s upravenou normou IEEE 802.11 High rate, která umožnovala rychlost až 11 Mb/s. Později byla tato norma přejmenována na IEEE 802.11b, ke kterému došlo v roce 1999. Mezitím již byla delší dobu zpracovávána norma 802.11a, která však byla složitější a vyžadovala tak delší čas pro vlastní spuštění. Další vývoj standardu a jaké změny tyto nové verze přinesly, znázorňuje následující tabulka (Tabulka 1). (HRSTKA, c2010–2016)

Tabulka 1 - Vývoj standardů IEEE 802.11

Standard	Rok uvedení	Novinky
802.11	1997	První verze standardu, která podporuje rychlosti 1 a 2 Mb/s v pásmu 2,4 GHz.
802.11a	1999	Přenos rychlostí až 54 Mb/s v pásmu 5 GHz.
802.11b	1999	Přenos rychlostí až 11 Mb/s v pásmu 2,4 GHz.
802.11g	2003	Přenos rychlostí až 54 Mb/s v pásmu 2,4 GHz.
802.11n	2009	Přenos rychlostí až 600 Mb/s v pásmu 2,4 a 5 GHz.
802.11ad	2012	Přenos rychlostí až 6,933 Gb/s v pásmu 60 GHz.
802.11ac	2013	Přenos rychlostí až 6,933 Gb/s v pásmu 5 GHz.

Zdroj: (HRSTKA, c2010–2016)

Nejnovější standard 802.11ac začal vznikat koncem roku 2008 a měl za cíl přinést vyšší výkonnost souboru základní služby BSS, neboli přístupového bodu AP, který se stará o komunikaci mezi jednotlivými stanicemi. Minimální nároky na počátku celého projektu byly stanoveny alespoň na 1 Gb/s pro AP a minimálně 500 Mb/s pro jednotlivé rádiové spoje. Důvodem k vyšším nárokům na přenosové rychlosti byl především trend stále více se

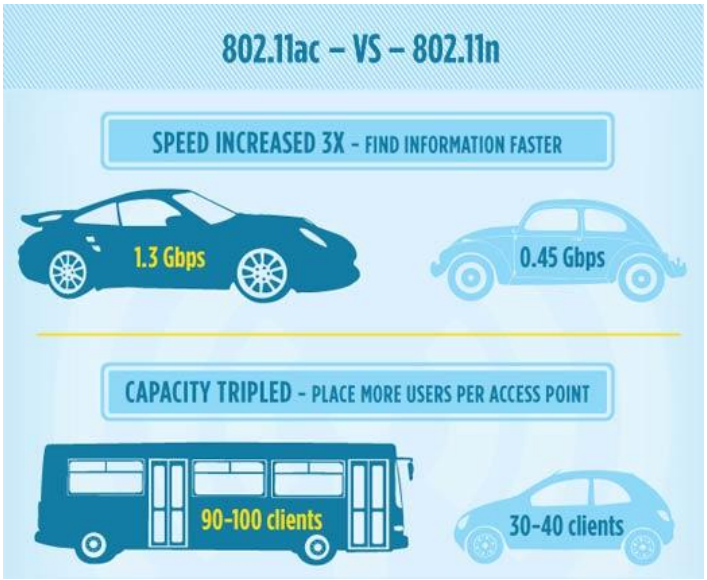
rozšiřujících služeb přenosu videa ve vysokém rozlišení, které vyžaduje také vyšší přenosové kapacity. (GAST, 2013)

Počátkem roku 2014 byl standard spolu s finálními parametry oficiálně spuštěn. Maximální propustnosti tehdejších hi-tech modelů dosahovaly hodnot kolem 1,3 Gb/s (REDAKCE2, 2014). Nyní je již standard 802.11ac zaběhnutý a ze strany uživatelských zařízení stále více podporovaný. Základní modely domácích směrovačů, které plně podporují nejnovější standard, startují na částkách kolem tisíce korun.

Porovnání 802.11n a 802.11ac

Papírově se zdá být nový standard několikanásobně rychlejší, než jeho starší sourozenec 802.11n. V praxi lze sledovat zhruba dvojnásobný nárůst přenosové rychlosti, pokud budeme uvažovat hustou zástavbu a vyšší míru rušení. Mimo zástavbu, s podstatně menším rušením je pak rozdíl výrazně vyšší.

Další velmi důležitý rozdíl je v oblasti maximálního počtu obsluhovaných klientských stanic. Uvažujme konfiguraci 3x3 MIMO a frekvenci 40 MHz. Pakliže standard 802.11n dokázal obsluhovat při dané konfiguraci 30–40 klientů, nový standard při stejné konfiguraci dokáže obsluhovat 90–100 klientských stanic (REDAKCE2, 2014). Rozdíl jak rychlostní, tak kapacitní je pro jednoduché pochopení znázorněn na následujícím obrázku (Obrázek 2).



Obrázek 2 - Porovnání rychlosti a kapacity standardů 802.11ac a 802.11n

Zdroj: (How to Ease the Pain of Slow Wi-Fi, 2016)

Aby bylo možné nových výkonnostních cílů dosáhnout, bylo potřeba zavést určitá vylepšení na fyzické vrstvě, ale i na protokolu řízení přístupu k médiu. Nový standard 802.11ac již pracuje pouze na frekvenčním pásmu 5 GHz, ale díky zpětné kompatibilitě spolupracuje i se starším sourozencem 802.11n, provozovaném ve stejném pásmu. (GAST, 2013)

1.3 Rozdělení Wi-Fi sítí

Wi-Fi sítě lze obecně rozdělit na dva druhy. Prvním je bezdrátová síť, ve které komunikují dvě stanice přímo mezi sebou, kterou pak nazýváme Ad-hoc. Druhou možností jsou infrastrukturní sítě, kde mezi sebou stanice komunikují pomocí přístupového bodu AP (*access point*).

1.3.1 Bezdrátové sítě typu Ad-hoc

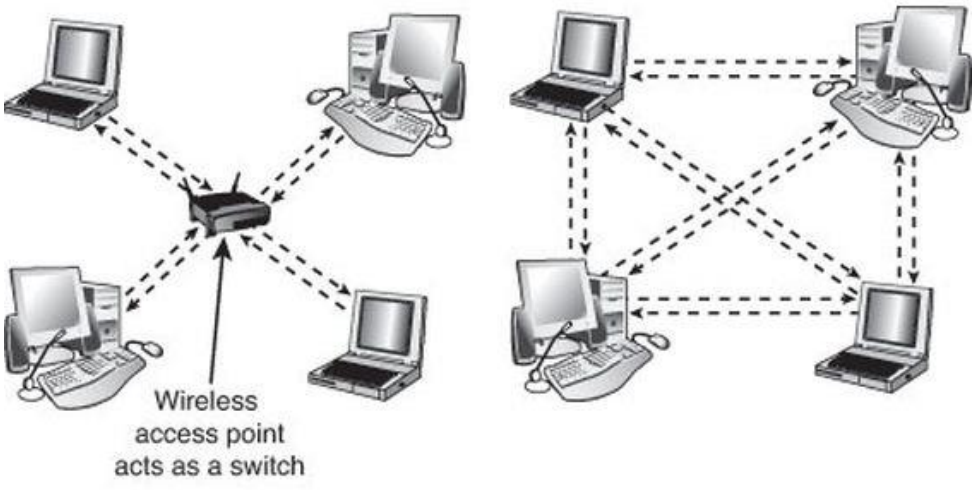
Bezdrátové sítě typu Ad – hoc, nebo také peer-to-peer jsou založeny na principu, že jednotlivé stanice spolu komunikují navzájem. Provoz v takové síti řídí první připojená stanice, která byla do sítě připojena, přičemž při jejím výpadku přebírá řízení jiná, náhodně zvolená stanice v síti. Tato topologie je vhodná zejména pro malé sítě, zahrnující několik málo stanic, kde komunikace probíhá na malé vzdálenosti. (ZHOU, 2012)

Přístup k internetu lze v takové síti sdílet jedině za předpokladu, že jedna stanice je nakonfigurována jako brána (*gateway*). (ZHOU, 2012)

1.3.2 Infrastrukturní bezdrátové sítě

Infrastrukturní sítě se topologicky podobají rychlejším verzím Ethernetové sítě, používající switch, nebo hub. Obsahují jeden, nebo více přístupových bodů AP, které plní funkci přepínače a vysílají svůj identifikátor SSID. Klientská stanice se pak může k vybranému AP libovolně připojovat, popřípadě přepojovat mezi AP se stejným SSID, pro zajištění většího prostorového pokrytí. (WOLIGROSKI, 2011)

Rozdíl mezi uvedenými topologiemi je znázorněn na následujícím obrázku (Obrázek 3).



Obrázek 3 - Infrastrukturní topologie (vlevo) vs. Ad-hoc (vpravo).

Zdroj: (WOLIGROSKI, 2011)

Z obrázku je patrné, že v případě infrastrukturní topologie jsou všechna zařízení bezdrátově spojena s AP, který plní funkci přepínače. Veškerá komunikace pak probíhá právě přes AP.

Pokud se zaměříme na Ad-hoc topologii, pak je zřejmé, že zařízení jsou propojena „každý s každým“. Pro komunikaci nepotřebují a nepoužívají žádného „prostředníka“.

2 WI-FI SÍTĚ JAK JE NEZNÁME

Wi-Fi sítě jsou obecně známé jako jedna z nejrozšířenějších metod šíření přístupu k internetu, nebo sdílení dat v lokální, uzavřené síti. Wi-Fi sítě však mají mnohem širší využitelnost, a to i v oborech, kde by to laik ani nečekal. V následujících kapitolách budou uvedeny některé zajímavé možnosti využití Wi-Fi sítí v reálném světě.

2.1 Letiště v Kodani

Na mezinárodním letišti v Kodani byla společností Cisco implementována analytická platforma Cisco Mobile Experience[1]. Technologie zajišťuje monitoring pohybu lidí a na základě získaných dat letiště optimalizuje vytížení svého personálu v jednotlivých segmentech, či zvýšení bezpečnosti. Návštěvníci letiště pak díky speciální aplikaci mohou získat, mimo připojení k internetu, také množství dalších služeb a kratší čekací doby při odletu, nebo příletu. (CISCO SYSTEMS, 2012)

2.2 Muzeum v Atlantě

Společností Cisco a operátorem AT&T byla vytvořena platforma interaktivního průvodce pro návštěvníky Fernbank Museum of Natural History v Atlantě. Návštěvníci tak díky speciální aplikaci ve svém mobilním telefonu mohou zábavnou formou získávat další informace během prohlídky. V aplikaci jsou na základě polohy klientského zařízení zpřístupňovány informace a úkoly, které tak nemusí návštěvník sám složitě vyhledávat. Muzeum získává mnoho spokojených návštěvníků, ale také důležitou zpětnou vazbu na vylepšení expozic. (CISCO SYSTEMS, 2012)

2.3 Masarykův onkologický ústav v Brně

Společnost Cisco stojí také za projektem realizovaném v Masarykově onkologickém ústavu v Brně. Prostřednictvím Wi-Fi sítě a technologie RFID čipů dokáže zdravotnický personál jednoduše lokalizovat polohu vybraných zdravotnických přístrojů a zařízení, ale i pacientů. Ti jsou vybaveni speciálními náramky, díky kterým si mohou přivolat okamžitou pomoc, pouhým stiskem tlačítka na náramku. Tato technologie tak zajišťuje rychlou lokalizaci pacienta v nesnázích, ať už je kdekoliv v dosahu sítě, a to bývá mnohdy otázku života a smrti. (CISCO SYSTEMS, 2012)

[1] Více o Cisco Mobile Experience např. zde: http://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/index.html

2.4 Wi-Fi v železniční dopravě

Wi-Fi sítě našly své uplatnění i v železniční dopravě. Španělský dopravce Renfe, EuskoTren a ETS z Baskicka[2] zavedly systémy, založené na Wi-Fi technologiích do svých souprav. Systém spočívá v mobilní jednotce umístěné přímo ve vlaku a několika pevných přístupových bodů, vytvářejících privátní síť podél trasy. Tyto přístupové body však zdaleka nepokrývají celou trasu, kudy vlak jede. Touto metodou se přenáší pouze objemná data s nízkou prioritou jejich včasného doručení do řídícího centra. Mobilní jednotka ukládá potřebná data během jízdy, jako například záznamy bezpečnostních kamer, audiozáznamy z kabiny a další objemná data. Při průjezdu pokrytou oblastí jsou tato data přenesena do sítě řídícího centra. Důležitá data, jako třeba poloha a chybová hlášení jsou pak přenášena v reálném čase, pomocí jiných bezdrátových technologií (*např. mobilní sítě*). Tato data však již nejsou objemově náročná (*řádově kB*). Výhodou tohoto řešení jsou vstupní a provozní náklady, které jsou díky použité Wi-Fi technologii velmi nízké. (SALABERRIA, CARBALLEDO a PERALLOS, 2012, s. 469–488)

2.5 Volání z mobilních telefonů

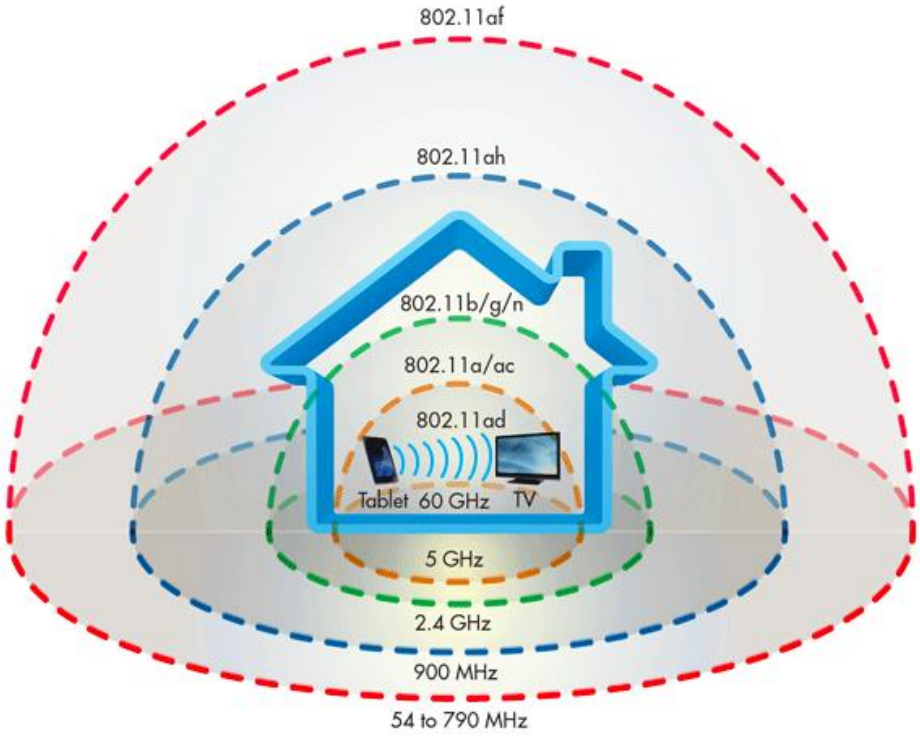
Jelikož jsou Wi-Fi sítě velmi rozšířené, přičemž vysoký podíl tvoří Wi-Fi sítě veřejné (*např. restaurace s volným přístupem k internetu*), rozhodl se tuzemský operátor T-Mobile toho využít a v místech se zhoršeným signálem mobilní sítě umožnuje automatické uskutečnění hovoru přes Wi-Fi síť. Tím je zachována kvalita a dostupnost spojení. Tuto službu spustil T-Mobile na přelomu roku 2015–2016 a prozatím je dostupná pouze pro vybrané chytré mobilní telefony, které tuto funkci umožnují ze strany hardware a operačního systému. (T-MOBILE CZECH REPUBLIC, 2015)

Velkou novinkou je tato funkce pouze pro laickou veřejnost. Mnohem déle totiž funguje služba Skype[3] a VoIP telefonie. Tato služba funguje na podobném principu. Využívá Wi-Fi sítě, pevné Ethernetové připojení, nebo mobilní datové sítě, přes které jsou uskutečněny hovory a posílány SMS, nebo MMS zprávy. Službu nabízí řada virtuálních operátorů, včetně možnosti přenést si své stávající mobilní číslo. Rozdílem jsou několikanásobně nižší účtované částky a podpora ze strany téměř všech „chytrých“ mobilních telefonů. (KELLY, 2005)

[2] Baskicko – území mezi Španělskem a Francií, zahrnující několik autonomních společenství.
[3] Skype – program, který umožňuje VoIP telefonii, chatování a přenos souborů, již od roku 2003.

2.6 Budoucnost a vývoj Wi-Fi

Budoucnost Wi-Fi sítí je pravděpodobně velmi zajímavá a bude docházet k dalším vylepšením protokolů, převážně pak k většímu rozprostření do různých frekvenčních pásem. Níže jsou popsány chystané standardy, jejich výhody a nevýhody. Pro názornost jsou na obrázku (Obrázek 4) graficky znázorněny připravované standardy, spolu se stávajícími.



Obrázek 4 - 802.11 současnost a budoucnost

Zdroj: (LINK LABS, 2015)

2.6.1 802.11ah

Jedná se o připravovaný standard, který funguje na frekvenci 900 MHz. Tato frekvence je vhodná ke snížení energetické náročnosti jednotlivých zařízení a pro přenášení dat na delší vzdálenosti. Výhodou je lepší prostupnost signálu překážkami, než u vysokofrekvenčních přenosů. Vhodné zejména pro menší datové toky, které mohou vysílat na delší vzdálenosti. (LINK LABS, 2015)

2.6.2 802.11af

Tento standard počítá s nevyužitým frekvenčním spektrem u televizorů. Využívají se tzv. bílé mezery. Vzhledem k tomu, že kmitočty se pohybují mezi 54 MHz a 790 MHz, lze tento rozsah použít pro energeticky nenáročná zařízení a na větší vzdálenosti, podobně jako 802.11ah. Nízká úroveň rušení může znatelně navýšit výkon celé soustavy a přenosové

vzdálenosti tak mohou být až několik kilometrů, při zachování vysokorychlostního přenosu. Jedná se stále pouze o návrh a nevýhodou může být horší dostupnost zmíněných bílých mezer. Tento problém by mohl nastat hlavně ve větších městech. (LINK LABS, 2015)

2.6.3 802.11ad

Na rozdíl od předchozích standardů je 802.11ad vhodný spíše na krátké vzdálenosti, ale při velmi vysokých rychlostech. Pracuje ve frekvenčním pásmu 60 GHz, které je kompletně volné a bezlicenční. Využití nalezne především ve vnitropodnikových sítích, které vyžadují velmi vysoké rychlosti na krátké vzdálenosti. Nevýhody jsou prozatím: velmi nákladná výroba podporujících čipů a špatná prostupnost překážkami, kvůli vysokofrekvenčnímu 60 GHz pásmu. (LINK LABS, 2015)

2.6.4 Rozšíření Wi-Fi pokrytí

Dostupnost připojení k internetu není vždy samozřejmostí. V řídce obydlených zemích se mnohdy poskytovatelům nevyplatí budovat nákladnou mobilní, nebo jinou bezdrátovou síť, a tyto oblasti pak bývají „odříznuté“ od sítě internetu. Novinkou, kterou plánuje zavést společnost Facebook jsou bezpilotní letouny (*tzv. drony*), poháněné solární energií, které vydrží ve vzduchu až několik měsíců. Díky těmto dronům by bylo možné takto „odříznuté“ oblasti jednoduše zasíťovat Wi-Fi, nebo LTE připojením. Facebook nyní zlepšuje své letouny a laserový komunikační systém, který spojuje jednotlivé letouny mezi sebou a pozemskými stanicemi. Tato služba by byla následně nabídnuta místním telekomunikačním operátorům, kteří by tak mohli jednoduše, bez dalších nákladů rozšířit úroveň pokrytí složitých oblastí. (WILLIAMS, 2016)

Následující obrázek (Obrázek 5) zachycuje drona Aquila společnosti Facebook.

Obrázek 5 - Dron Aquila společnosti Facebook

Zdroj: (HERN, 2015)

Dron Aquila má tvar písmene „V“. Celý jeho povrch je složen ze solárních panelů, které mají za úkol napájet celý stroj. Rozpětí křídel činí 40 metrů (pro představu dopravní letadlo Boeing 737 má rozpětí křídel zhruba 35 metrů). Stroj drží ve vzduchu čtyři elektromotory, které pohání vrtule. Laserový zaměřovací a GPS navigační systém určuje dráhu letu a koordinuje pohyb jednotlivých dronů mezi sebou. (WILLIAMS, 2016)

3 ZABEZPEČENÍ BEZDRÁTOVÝCH SÍTÍ

Bezdrátové sítě se za posledních několik let staly téměř samozřejmostí každé domácnosti, firmy, nebo restaurace. Masivní rozšíření těchto technologií si vyžádalo řešení otázky zabezpečení přenášených dat a bezpečnosti sítě všeobecně. U klasických metalických sítí postačí odepřít přístup ke kabeláži, nebo jednotlivým síťovým prvkům, což u bezdrátových sítí zdaleka nestačí.

Tak jako se chytá prach na nábytku, nebo pyl na parapetu, tak i datové pakety přenášené vzduchem lze jednoduše a kýmkoliv zachytit. Toto je největší slabina bezdrátových sítí, proto je třeba bezpečnosti sítě a přenášeným datům věnovat zvýšenou pozornost.

Při budování bezdrátové sítě je třeba dbát zvýšené opatrnosti a nepodcenit fázi návrhu. Správná volba jednotlivých komponent a aplikace zabezpečovacích mechanismů je rozhodujícím faktorem pro bezchybný a bezpečný chod. Samozřejmě jinak tomu je v domácí síti, která slouží pro přístup k internetu, nebo firemní síti, kde se přenáší důvěrná data a jejich únik by mohl mít destruktivní dopad na celou společnost.

Ve firemní praxi bývá zavedena centrální správa jednotlivých prvků s možností monitoringu sítě. Bez centrální správy je téměř nemožné objevit například pirátský přístupový bod AP. Ten by mohl být do sítě podstrčen a odposlouchávat, popřípadě přesměrovávat veškerou důvěrnou komunikaci.

WRIGHTSON (2012, s. 53) ve své knize rozděluje bezpečnost bezdrátových sítí do dvou kategorií:

- autorizace - řídí oprávněnost přístupu jednotlivých uživatelů do sítě,
- šifrování - zabezpečuje přenášená data před odposlechem.

3.1 Autorizace (autentizace)

Ověřovací proces je velmi důležitý. Je třeba si uvědomit, že během autentizace se ověřuje, jestli ono zařízení je tím, za které se vydává. Výsledkem tohoto rozhodovacího procesu je úspěšné, či neúspěšné připojení klienta k síti. Autentizaci zajistí údaje (typicky heslo, nebo certifikát), které mohou vlastnit pouze uživatelé s oprávněním přístupu.

WRIGHTSON (2012, s. 53–54) uvádí nejčastější metody autentizace:

- WEP klíč,
- WPA Pre-Shared klíč,
- autentizace do centrální databáze,

- Two-factor autentizace.

3.2 Šifrování (encryption)

Šifrování je proces, který mění data do takové podoby, která je pro neoprávněnou osobu nečitelná. Chrání tak přenášená data proti přečtení. Tento proces musí být vratný, aby bylo možné z takto změněných dat získat zpět data původní. Šifrování tedy musí být obousměrný proces. Návrat dat do původní podoby pak nazýváme dešifrováním.

WRIGHTSON (2012, s. 55) popisuje dva hlavní systémy šifrování dat, a to:

- Shared-key,
- Public key.

3.2.1 Shared-key

Shared-key lze přeložit jako sdílený klíč. Jedná se o šifrovací metodu, jejíž kořeny sahají do dávné minulosti. Byla používána již v dobách Římanů. Shared-key zná zdrojová i cílová stanice a používá stejný klíč k šifrování, ale i dešifrování dat. Někdy bývá toto šifrování označováno jako symetrické. Symetrický klíč může být pro každou relaci komunikace rozdílný, ten pak nazýváme klíčem sezení (*session key*). (WRIGHTSON, 2012, s. 55)

3.2.2 Public key

Public key lze přeložit jako veřejný klíč. Jedná se o asymetrickou šifrovací metodu, kde se používá jiný klíč pro šifrování a jiný klíč pro dešifrování dat. Asymetrické šifry používají soukromý (*private*) a veřejný (*public*) klíč. Zpráva je šifrována veřejným klíčem a pouze ten, kdo zná asociovaný soukromý klíč, dokáže tuto zprávu dešifrovat. Na pozadí těchto operací jsou složité matematické výpočty. Asymetrické šifrování je považováno za velmi silnou šifrovací metodu. (WRIGHTSON, 2012, s. 55)

Následující tabulka (Tabulka 2) popisuje obecné výhody šifrovacích systémů.

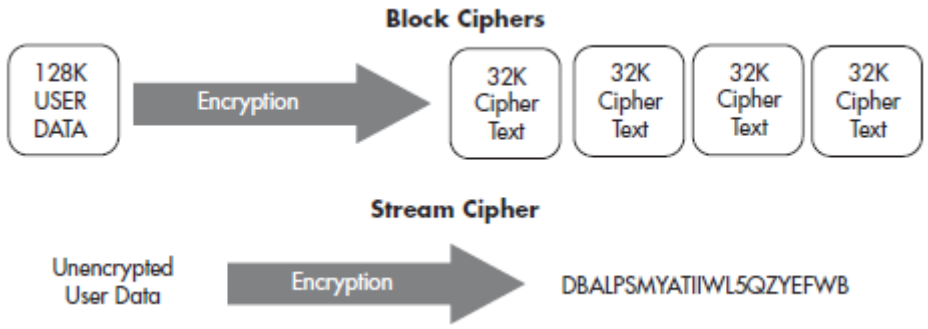
Tabulka 2 – Porovnání šifrování Shared-key a Public key

Technologie	Výhody
Shared-key	• Rychlost • Nízká výpočetní náročnost • Velmi jednoduché
Public key	• Mnohem bezpečnější

Zdroj: (WRIGHTSON, 2012, s. 55)

3.2.3 Proudová šifra vs. bloková šifra

Proudové a blokové šifry jsou základní metody pro šifrování dat. Proudová šifra typicky šifruje data bajt po bajtu a zašifrovaný výstup má stejnou, nebo velmi podobnou délku, jako nešifrovaný vstup. Naopak při blokovém šifrování jsou zpracovávány bloky dat o pevné délce, a ty jsou následně šifrovány. Pro příklad je na následujícím obrázku (Obrázek 6) znázorněno šifrování 128bajtového textu blokovou a proudovou šifrou. (WRIGHTSON, 2012, s. 56)



Obrázek 6 - Bloková vs. proudová šifra

Zdroj: (WRIGHTSON, 2012, s. 56)

3.3 Omezení vysílacího signálu

Základním předpokladem realizace útoku na bezdrátovou síť je nacházet se v dosahu vysílaného signálu. Správně navržená bezdrátová síť by neměla vyzařovat vysílací signál zbytečně mimo požadovanou oblast. Správným rozmístěním aktivních prvků sítě a nastavením jejich vysílacího výkonu, lze částečně eliminovat fyzický přístup potencionálního útočníka k zabezpečované síti. Pokus o útok „útočníka amatéra“ tady na 99 % končí. Profesionál se však vybaví dostatečně silnou směrovou anténou a tento druh „zabezpečení“ pak ztrácí smysl. (WRIGHTSON, 2012, s. 145)

3.4 Zákaz vysílání SSID

Další metodou, jak potencionálnímu útočníkovi ztížit přístup do sítě je zakázat vysílání SSID[4] přístupovému bodu. Takto nastavené zařízení pak nešíří svůj identifikátor „do prostoru“, a není tak viditelné v seznamu dostupných sítí. Stanice, která se k takové síti připojuje, musí pro úspěšné připojení znát skryté SSID přístupového bodu. Tento způsob je jednoduchý, ale stejně tak je jednoduché jej obejít. Vzhledem k tomu, že během procesu připojování stanice je

[4] SSID – řetězec ASCII znaků, který je maximálně 32 znaků dlouhý. Slouží k identifikaci zařízení v síti Wi-Fi.

SSID přenášeno v nezašifrované podobě, je tak lehce zjistitelné během odposlechu komunikace. (WRIGHTSON, 2012, s. 146)

3.5 Zákaz DHCP

DHCP, neboli dynamické přidělování IP adres zrychluje proces připojení nového zařízení k síti a automatizuje správu adresního prostoru. Tak jako jej zjednodušuje běžnému uživateli, který je v síti autorizovaný, tak i potencionálnímu útočníkovi, který díky DHCP nemusí znát rozsahy přidělovaných IP adres. Pokud je DHCP na směrovači zakázáno a IP adresy jsou přidělovány ručně (*staticky*), pak je pro útočníka mnohem složitější získat právě takovou IP adresu, která do sítě patří. IP adresy mohou být dále asociovány s MAC adresami, což přístup ještě více ztíží. (WRIGHTSON, 2012, s. 50)

3.6 Filtrování MAC adres

Každý síťový prvek a zařízení připojované do sítě má svou unikátní adresu, tzv. MAC adresu. Většina moderních síťových prvků umožňuje spravovat seznam MAC adres a filtrovat MAC adresy s právem přístupu k síti. Tím je možné omezit přístup neautorizovaných zařízení. Tento druh zabezpečení je náročný na správu, jelikož je potřeba udržovat aktuální seznam povolených MAC adres na všech aktivních zařízeních sítě. Bezpečí takové řešení nezajistí, jelikož zkušený útočník dokáže jednoduše přenastavit svou MAC adresu na některou z autorizovaných adres. Takový druh zabezpečení je vhodný spíše jako doplňkový, zejména pro malou domácí síť, do které se připojují stále stejná zařízení. (WRIGHTSON, 2012, s. 146)

4 POKROČILÉ METODY ZABEZPEČENÍ

4.1 WEP

WEP je zabezpečovací mechanismus, který je součástí původního standardu 802.11 od roku 1999. WEP poskytuje šifrování dat na druhé vrstvě OSI[5] modelu (*linková vrstva*). K šifrování je použita proudová šifra RC4[6] a systém sdíleného klíče (*shared-key*). Pro šifrování dat je k dispozici 40bitový, nebo 104 bitů dlouhý WEP klíč. (WRIGHTSON, 2012, s. 56)

WEP klíč je konfigurován administrátorem a je uložen v samotném zařízení. Jeho distribuci WEP neřeší, což je velkou slabinou tohoto systému. Obecně platí, že čím delší je přístupové heslo, tím silnější je zabezpečení. V případě WEP proto není žádný důvod pro použití 40bitového klíče, snad jen že kratší heslo se lépe pamatuje. (WRIGHTSON, 2012, s. 57)

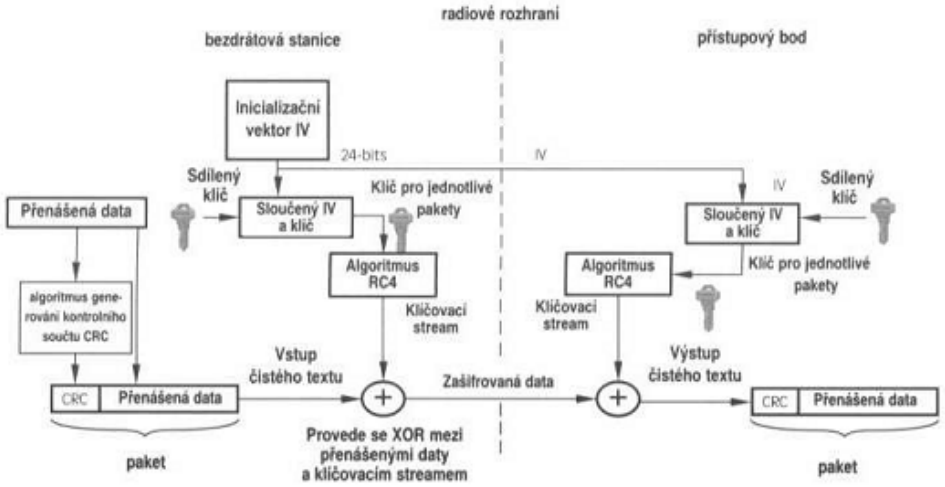
WRIGHTSON (2012, s. 57) popisuje fáze šifrování následujícím způsobem:

1. Přenášeným datům je vypočten kontrolní součet CRC. Sloučením dat a CRC vzniká datový paket.
2. Je generován 24bitový inicializační vektor IV, který je sloučen s WEP klíčem.
3. Sloučený IV s WEP klíčem se zašifruje RC4 šifrou.
4. Provede se logická operace XOR mezi výsledkem RC4 a šifrovaným paketem.

Takto upravená data jsou zaslána na cílovou stanici, prostřednictvím bezdrátového spojení, na které jsou následně dešifrována do původní podoby.

Průběh šifrování je znázorněn na následujícím obrázku (Obrázek 7).

[5] OSI – standardizovaný referenční model počítačových sítí. Rozděluje komunikaci do sedmi vrstev, které jsou na sobě nezávislé a nahraditelné.
[6] RC4 – kryptografický algoritmus, který se používá pro šifrování přenosu. Je jednoduchý a velmi rychlý.



Obrázek 7 - Průběh šifrování WEP

Zdroj: (SKELET, 2007)

Algoritmus RC4, který je používán pro šifrování dat je sám o sobě velmi robustní, avšak jeho implementace v případě WEP je poněkud nešťastná. WRIGHTSON (2012, s. 57) uvádí další implementace proudové šifry RC4:

- WPA,
- TLS/SSL,
- Microsoft Point-to-Point Encryption,
- Remote Desktop Protocol,
- některé implementace SSH,
- některé implementace Kerberos.

WEP zajišťuje integritu dat pomocí algoritmu CRC-32, který vypočítává kontrolní součet, a je bohužel velmi jednoduchý. Takto chráněné zprávy lze díky jednoduchosti algoritmu pozměnit, včetně jejich kontrolního součtu. Cílová stanice pak nemůže jednoduše rozpoznat, jestli se nejedná o podvržený, nebo jakkoliv jinak pozměněný paket.

4.1.1 Slabiny WEP

Zabezpečení WEP je dávno překonané a v dnešní době je otázkou několika minut jej prolomit. Pokud bude útočník odposlouchávat provoz na síti a odchytá dostatečný počet paketů, může specializovaným software (*např.: aircrack -ng*) vypočítat tajný klíč. Slabé místo je právě v IV, který je pouze 24 bitů dlouhý, čili má 16 777 216 unikátních kombinací. To na vytížené síti způsobí, že se IV začnou velmi rychle opakovat. Logickými výpočty tak lze dopočítat WEP klíč. Provoz na síti může útočník aktivně vytvářet opakovanou deautentizací

některého zařízení, které se následně opětovně autentizuje. Tím útočník získává další cenné rámce s tajným klíčem, pro jeho následný matematický výpočet. (WRIGHTSON, 2012, s. 60–61)

Jakmile se útočník autentizuje k AP, může proniknout hlouběji do sítě, nebo odchytávat dešifrovaný provoz na síti. Jelikož každý uživatel sítě používá stále stejný WEP klíč, může útočník dešifrovat jakoukoliv komunikaci, kteréhokoliv účastníka sítě. (WRIGHTSON, 2012, s. 62)

4.2 WPA

WPA zcela nahrazuje původní standard WEP. Tento novější systém existuje ve dvou variantách, a to WPA a WPA2. WPA měl za úkol rychle nahradit nedostatečné zabezpečení WEP, mezitím co byl WPA2 dále vyvíjen. Zpětná kompatibilita se zařízeními podporující WEP je zajištěna díky použitému šifrování TKIP, které tak jako WEP pracuje s proudovou šifrou RC4. Stačí tak pouze aktualizovat firmware na bezdrátových zařízeních. Z pohledu bezpečnosti řeší WPA spoustu bezpečnostních slabin WEP. (WRIGHTSON, 2012, s. 64)

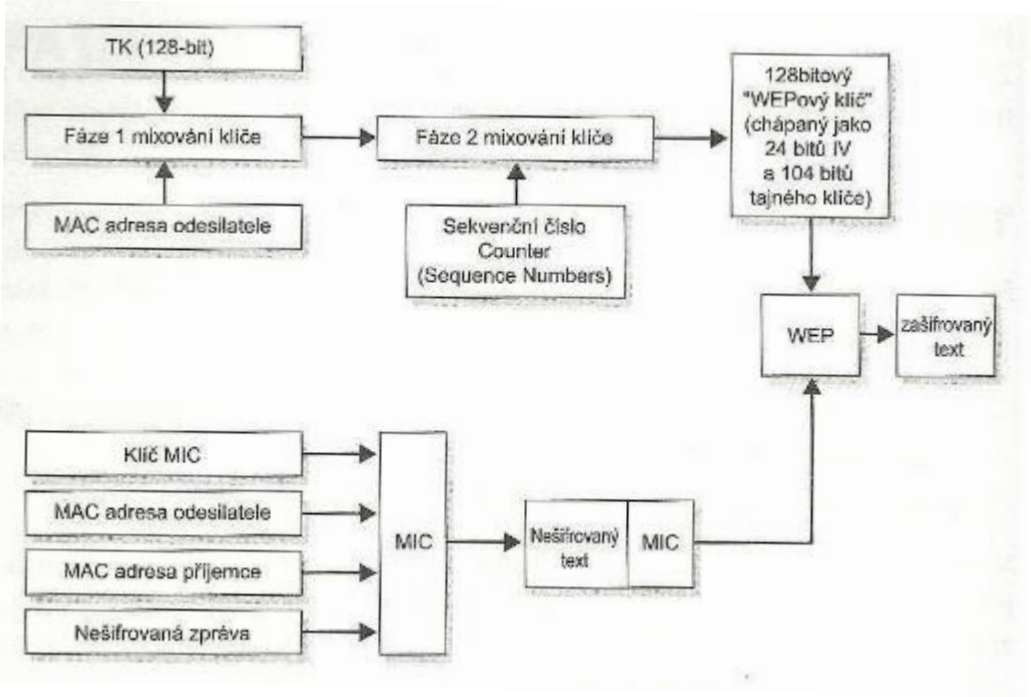
TKIP si nově uchovává pořadová čísla rámců a používá pro každý paket jiný klíč, který je vytvořen z tzv. základního klíče PTK, cílové MAC adresy a pořadového čísla rámce. Rámce, které nezapadají do číselné řady, jsou jednoduše ignorovány. Tímto způsobem lze eliminovat útoky typu replay[7], které jsou založeny na opětovném použití, již použitého rámce. PTK je generován při každém připojení klienta k AP. Vzniká hashováním pořadového čísla relace a inicializačního vektoru. Inicializační vektor je nově 48 bitů dlouhý, což znamená zhruba 281 bilionů unikátních kombinací, proti 16 milionům u WEP. Unikátnost šifrovacího klíče je zajištěna náhodným číslem, které je při každé relaci inkrementováno. Používá se jak pro tvorbu IV, tak pro PTK. (BARKEN, 2004)

WPA zajištuje integritu dat jednocestným hashovacím algoritmem zvaným Michael, nebo také MIC. MIC pracuje s počítadlem rámců, cílovou a zdrojovou MAC adresou. Výstup algoritmu je 8 bajtů dlouhý a je následně připojen k přenášeným datům. MIC je mnohem složitější podvrhnout, naproti CRC u zabezpečení WEP. (BARKEN, 2004)

Dalo by se zjednodušeně říct, že TKIP provádí bezpečnější variantu toho, co prováděl WEP.

[7] Replay – typ útoku, který se snaží využít jeden a ten samý rámec několikrát, pro získání více IV, a tím větší a rychlejší šanci dopočítat tajný klíč.

Na následujícím obrázku (Obrázek 8) je znázorněn průběh šifrování pomocí WPA.



Obrázek 8 - WPA šifrování

Zdroj: (BARKEN, 2004)

WRIGHTSON (2012, s. 64) popisuje dva způsoby autentizace WPA:

- WPA-PSK,
- WPA-Enterprise.

4.2.1 WPA-PSK

WPA-PSK, označovaný také jako WPA-Personal, je založen na přednastaveném MK klíči. Ten je sdílený všemi zařízeními, které se chtějí do sítě připojit. MK si lze představit jako heslo, které je složeno z ASCII znaků, nebo hexadecimálních číslic. Heslo poté musí všichni klienti, kteří se pokouší o připojení k síti zadat do svého zařízení. Tento systém autentizace a distribuce klíčů je velmi podobný tomu, jaký používá WEP. Rozdíl je v délce klíče, který je nyní 256 bitů dlouhý. TKIP dále hodnotu MK použije pouze během první fáze autentizace, ze kterého jsou odvozeny další potřebné klíče. Ty jsou pak matematickými operacemi měněny. (WRIGHTSON, 2012, s. 64)

WPA-PSK je vhodné řešení pro domácnosti, nebo malé kancelářské sítě, které sestávají z několika málo klientských stanic. (WRIGHTSON, 2012, s. 64)

4.2.2 WPA-Enterprise

WPA-Enterprise je mnohem složitějším řešením. Vyžaduje podstatně více konfigurace, a zároveň další připojená zařízení. Novým prvkem Enterprise konfigurace je autentizační server (*typicky RADIUS server*). Některé moderní přístupové body lze nakonfigurovat na funkci RADIUS serveru. Ten se spolu s protokolem EAP stará o ověření jednotlivých uživatelů. EAP definuje formát rámců a způsob zapouzdření. (WRIGHTSON, 2012, s. 64–65)

EAP protokol existuje v několika variantách, z nichž nejdoporučovanější je EAP-TLS. Ten vyžaduje pro autentizaci uživatele oboustranný certifikační proces. WRIGHTSON (2012, s. 143–145) uvádí další varianty EAP:

- **EAP-TTLS** – zjednodušená verze EAP-TLS, kde klient nepoužívá certifikát, ale heslo.
- **PEAP** – zabezpečená verze EAP, které stejně jako TTLS vyžaduje certifikát pouze na straně serveru a klient využívá své přihlašovací jméno a heslo. Za protokolem PEAP stojí firmy Cisco a Microsoft.
- **LEAP** – odlehčená verze EAP od firmy Cisco. Používá opět přihlašovací jméno a heslo, ale již úplně bez certifikátů. Lze použít pouze pro Cisco výrobky.

WPA-Enterprise je vhodný zejména pro větší firemní sítě. Počáteční složitější konfigurace se navrací v podobě jednodušší správy a vyšší mírou zabezpečení.

WRIGHTSON (2012, s. 64–65) uvádí příklad firmy, ve které je použit systém WPA-PSK. Pro přístup do sítě je zvolen MK klíč. Pokud má firma 100 zaměstnanců a jeden z nich opouští firmu, pak je nutno vzhledem k bezpečnosti změnit klíč na přístupovém bodu a na zbývajících 99 stanicích. Důvodem je, že by bývalý zaměstnanec mohl heslo zneužít a připojit se libovolně do firemní sítě, nebo heslo dále šířit. WPA-Enterprise tento problém odstraňuje, jelikož každý uživatel má svůj uživatelský účet, vedený u autentizačního serveru. Pokud zaměstnanec opustí firmu, pak stačí jeho účet jednoduše zablokovat u autentizačního serveru.

4.2.3 Slabiny WPA

Největší slabinou WPA zabezpečení je možný útok na PSK. Pokud administrátor zvolí příliš krátké, nebo slabé heslo, je možné jej tzv. slovníkovým útokem zjistit. Pro tento typ útoku stačí dostatečně velký slovník klíčů (běžně k dispozici ke stažení) a odposlechnout autentizační rámce tzv. WPA handshake. Ten si může útočník snadno vynutit zasláním deautentizačního rámce některé ze stanic, která následně provede novou autentizaci a zašle cenný WPA handshake. Pokud se klíč shoduje s některým z klíčů ve slovníku, pak je otázkou

několika minut (záleží na velikosti slovníku a výpočetním výkonu), než bude klíč rozluštěn. (WRIGHTSON, 2012, s. 65–66)

Další možností je útok na TKIP, který má své kryptografické nedostatky. Tyto nedostatky paradoxně nahrazují nedostatky WEP. Martin Beck a Erik Tews zveřejnili roku 2008 tzv. Beck-Tews útok, který umožňuje útočníkovi odhadovat následující bajty paketu. Celý paket je možné uhodnout za necelých 12 minut. Jakmile má útočník celý paket, má i klíč k jeho sestavení. Na základě tohoto klíče může sestavit své vlastní pakety. Ač má WPA ochranu proti opakování (*replay*), je možné zneužitím služby QoS tuto ochranu obejít. Toshihiro Ohigashi a Masakatu Morii zjednodušili a zrychlili Beck-Tews útok, bez nutnosti povoleného QoS. (WRIGHTSON, 2012, s. 69)

4.3 WPA2

WPA2, nebo také standard 802.11i je novým nástupcem WPA. WPA2 byl schválen roku 2004 a nyní je léty prověřený, dodnes ničím nenahrazený. Využívá velmi robustní šifrování AES. Kvůli zpětné kompatibilitě podporuje volitelně i starší TKIP. (WRIGHTSON, 2012, s. 65)

AES je symetrický, blokový šifrovací algoritmus, který využívá 128 bitů, 192 bitů, nebo 256 bitů dlouhý šifrovací klíč. Tato šifra šifruje bloky dat o velikosti 128 bitů. (WRIGHTSON, 2012, s. 65). WRIGHTSON (2012, s. 65) definuje části režimu AES-CCMP následovně:

- Hlavička MAC – obsahuje zdrojovou a cílovou MAC adresu.
- CCMP hlavička – obsahuje 48bitové číslo paketu PN, inicializační vektor IV a ID klíče.
- Odesílaná paketová data.
- MIC pro zajištění integrity dat.

Tak jako WPA, nabízí i WPA2 dva možné režimy Personal a Enterprise, které již byly popsány v kapitole 4.2.1 a 4.2.2.

4.3.1 Slabiny WPA2

WPA2 jako takové je považováno za neprolomitelné. Problém může nastat pouze implementaci na daném systému, nebo v konfiguraci ověřovacího serveru (u varianty Enterprise). Dalším rizikem je u varianty Personal PSK klíč. Nedostatečně složitý a dlouhý klíč může být napadnutelný slovníkovým útokem (jako u WPA). Doporučuje se tedy volit klíč takový, aby byl zcela unikátní, dostatečně dlouhý (doporučeno 20 a více ASCII znaků) a kombinující čísla, písmena a speciální znaky.

5 ANALÝZA OBLASTI A METOD ZABEZPEČENÍ

V rámci této práce je provedena analýza zabezpečení Wi-Fi sítí v místě mého bydliště. Cílem této části je poukázat na to, jak moc si jsou lidé vědomi bezpečnostních rizik nezabezpečené, nebo špatně zabezpečené Wi-Fi sítě. K těmto účelům poslouží Kali Linux a nástroj airodump -ng[8]. V kapitole 5.1 je popsáno konkrétní místo, kde byla analýza provedena. Následující kapitola 5.2 popisuje postup získání potřebných dat a kapitola 5.3 shrnuje analytická data, ze kterých vychází graf a shrnutí (kapitola 5.4).

5.1 Situace

Analyzovaná oblast je panelový dům, který má dohromady 14 podlaží. Celkem se v něm nachází 76 bytových jednotek. Půdorysně je dům čtvercový.

Monitorovací stanice je umístěna v 11 nadzemním podlaží, přibližně uprostřed půdorysného průřezu. Jako monitorovací stanice byl zvolen starší notebook Fujitsu Siemens AmiloPro V3505 a Kali Linux, jako obslužný software.

Monitorování bylo provedeno ve všední den, okolo 21 hodiny.

5.2 Postup získání dat

- Spustíme monitorovací stanici s OS Kali Linux.
- Spustíme terminál, pro zadávání příkazů.
- Pomocí následujícího příkazu vypneme bezdrátové Wi-Fi rozhraní wlan0: `ifconfig wlan0 down`.
- Zadáním příkazu `iwconfig wlan0 mode monitor` přepneme rozhraní wlan0 do promiskuitního (*monitorovacího*) modu.
- Příkazem `ifconfig wlan0 up` povolíme zpět rozhraní wlan0.
- Příkazem `airodump –ng mon0` spustíme nástroj airodump –ng na rozhraní mon0.
- Dostáváme výpis dostupných Wi-Fi sítí, včetně detailních informací o nich, viz. Příloha A.

[8] Airodump -ng je nástroj programu Aircrack, který umožňuje zachytávat pakety.

5.3 Analytická data

Následující tabulka (Tabulka 3) je výtahem důležitých dat z Přílohy A.

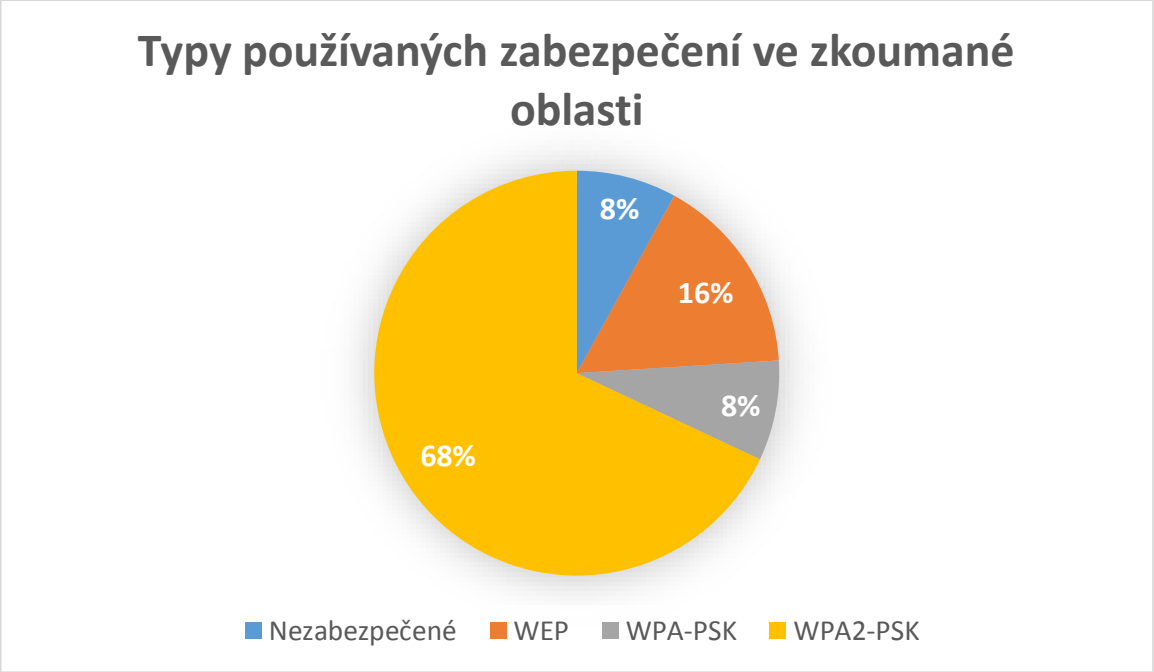
Tabulka 3 – Analytická data oblasti

ESSID	Kanál	Šifrování	Šifra	Autentizace
MaMi	11	WPA2	CCMP	PSK
Kuka	3	WPA2	CCMP	PSK
Bartonova	6	WPA2	CCMP	PSK
WifiDoma62	11	WPA2	CCMP	PSK
lachmanova	1	WPA	CCMP	PSK
ACAB	7	WEP	WEP	
zemlicka	5	WEP	WEP	SKA
SATnet_Zaip_S_Studanka	7	OPN		
Lefik	6	WPA2	CCMP	PSK
Dubina_P	11	WPA2	CCMP	PSK
UPC1889582	11	WPA2	CCMP	PSK
Novakova	3	WPA2	CCMP	PSK
Zabarela	6	WPA2	CCMP	PSK
SATnet_Zaip_S_Dubina	8	OPN		
hugovychodni	1	WEP	WEP	
Egovi	1	WPA2	CCMP	PSK
Elias	13	WPA2	CCMP	PSK
Wifi_Dum	1	WPA2	CCMP	PSK
MeteorCS_205_02	10	WEP	WEP	
Pitrovi	2	WPA2	CCMP	PSK
Pokolnet	13	WPA2	CCMP	PSK
SATnet_Havlinova	1	WPA2	CCMP	PSK
Koudy	9	WPA2	CCMP	PSK
dlink-st	11	WPA2	CCMP	PSK

Zdroj: vlastní

5.4 Shrnutí zkoumané oblasti

V návaznosti na tabulku (Tabulka 3) je možno sestavit následující graf (Obrázek 9).



Obrázek 9 - Typy používaných zabezpečení ve zkoumané oblasti

Zdroj: vlastní

Z tabulky (Tabulka 3) a grafu na obrázku (Obrázek 9) je patrné že:

- V analyzované oblasti bylo zachyceno vysílání celkem 26 přístupových bodů.
- 68 % sítí bylo zabezpečeno WPA2-PSK.
- Nedostatečně zabezpečeno bylo 16 % sítí, a to pomocí dávno překonaného WEP.
- 8 % sítí bylo zabezpečeno WPA-PSK, který je však podobně jako WEP překonaný.
- 8 % sítí bylo úplně nezabezpečeno.
- Dvě sítě měly skryté vysílání SSID.
- Každý přístupový bod měl změněné SSID (*žádné výchozí SSID např.: tp-link, dlink, apod.*), takže uživatel takového zařízení evidentně měnil nastavení jeho nastavení.
- O přístupovém bodu „UPC1889582“ lze s jistotou říct, že byl přednastaven poskytovatelem internetového připojení UPC.
- Sítě SATnet_Zaip_S_Studanka a SATnet_Zaip_S_Dubina jsou na první pohled otevřené sítě, avšak k přístupu do sítě je třeba předplatit si tarif u provozovatele SATnet, a následně se k síti autorizovat.
- Síť MeteorCS_205_02 je chráněna WEP, avšak pro úspěšné připojení je třeba další autorizace vůči AP, kterou klient získá po předplacení tarifu u provozovatele Meteor CS.

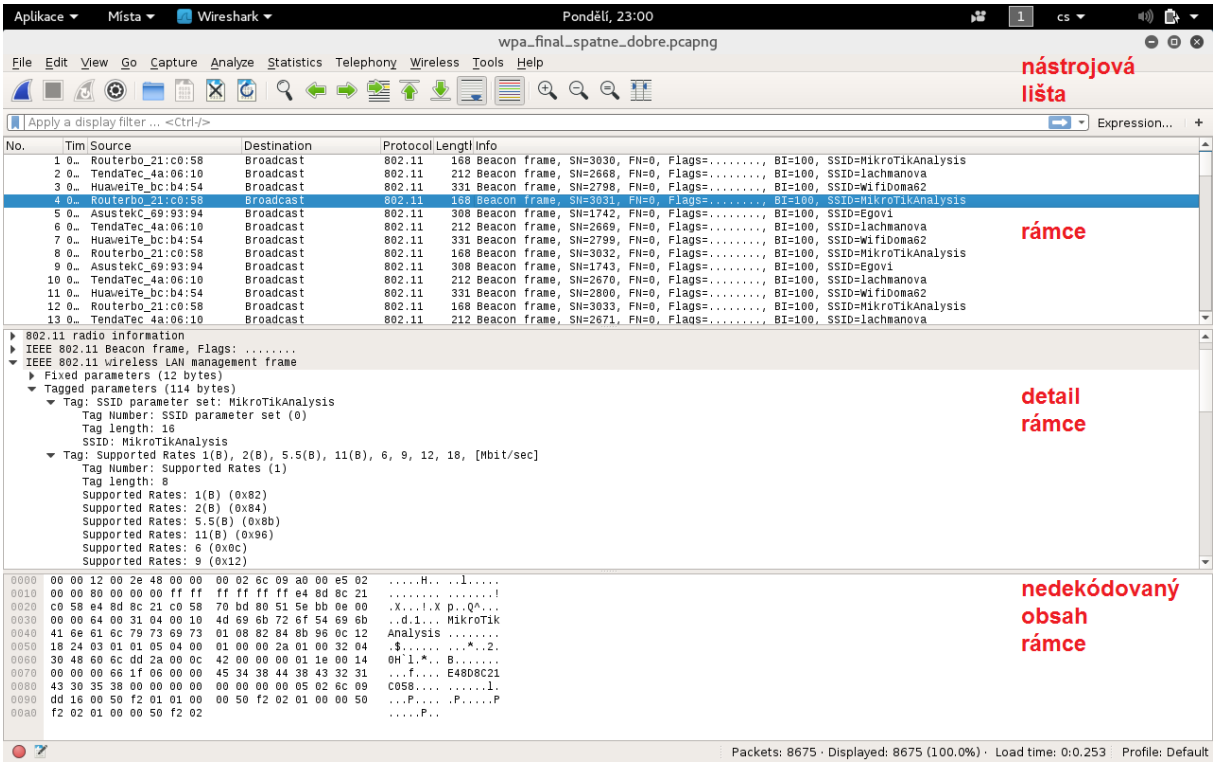
Obecně lze říct, že provozovatelé domácích AP již řeší zabezpečení své bezdrátové sítě, až na některé výjimky. Co však již moc neřeší, tak to je vysílací výkon. To může způsobit určité bezpečnostní riziko, nebo také nestabilní připojení kvůli velkému rušení ostatními stanicemi, ale také spotřebiči v domácnostech, jako jsou mikrovlnné trouby, apod.

Co se týká provozovatelů Wi-Fi sítí SATnet a Meteor CS, nepodařilo se mi získat informace o způsobu další autorizace. Oba provozovatelé na dotaz způsobu autorizace předplacených klientů shodně odpověděli, že tyto „důvěrné“ informace nemohou z bezpečnostních důvodů poskytnout.

6 ANALÝZA KOMUNIKACE

Následující kapitoly praktické části práce se zaměřují na modelové situace jednotlivých typů zabezpečení. Pro každý typ zabezpečení je navržena analyzovaná síťová struktura, popsány jednotlivé prvky struktury, stručná konfigurace zařízení, a následně je provedena samotná analýza komunikace. Výsledkem jsou tři laboratorní úlohy, na kterých je znázorněno, jak jednoduché je zachytávat „cizí“ paketová data. Pokud bude síť nezabezpečena, nebo jen slabě zabezpečena, může případný útočník síť snadno napadnout a číst přenášená dešifrovaná data (*hesla, emaily, apod.*).

Pro účely analýzy komunikace je použit program Wireshark[9], kterým jsou zachytávány pakety zkoumaných protokolů, a ty jsou dále analyzovány. Rozhraní programu Wireshark je zobrazeno a stručně popsáno na následujícím obrázku (Obrázek 10).



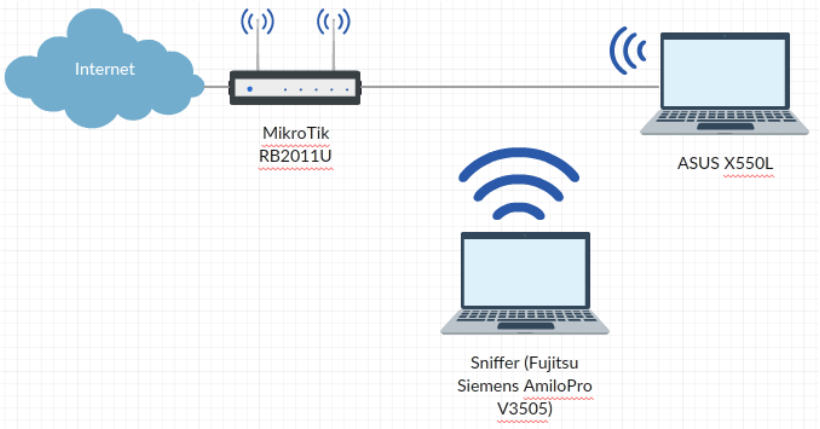
Obrázek 10 - Wireshark rozhraní

Zdroj: vlastní

[9] Wireshark – jedná se o protokolový analyzátor, resp. paketový sniffer. Prostřednictvím síťového rozhraní, které podporuje monitorovací mód, dokáže odchytávat veškerou komunikaci na tomto rozhraní a následně ji přehledně zobrazovat.

6.1 WPA-Personal

Následující obrázek (Obrázek 11) znázorňuje topologickou strukturu sítě, která je použita pro analýzu provozu, při použití WPA-Personal (*WPA-PSK*). Ve struktuře je použit směrovač MikroTik RB2011U, dále jen přístupový bod AP. Notebook klientské stanice ASUS X550L, který se autentizuje k přístupovému bodu a pirátský notebook Fujitsu Siemens AmiloPro V3505, který odchytává provoz na síti, za účelem další analýzy komunikace.



Obrázek 11 - Modelová situace WPA-Personal

Zdroj: vlastní

6.1.1 Použité prvky a jejich konfigurace

MikroTik RB2011U – přístupový bod

Název ve Wiresharku: Routebo_21:c0:58.

MAC adresa zařízení: E4:8D:8C:21:C0:58.

Konfigurace bezdrátové sítě:

- Mode: ap bridge (mód přístupového bodu).
- Band: 2GHz-B/G (vysílá v pásmu 2GHz, protokol 802.11b a 802.11g).
- Channel width: 20MHz (šířka pásma).
- SSID: MicroTikAnalysis (identifikátor SSID).
- Security profile: (profil zabezpečení)
    - Mode: dynamic keys (dynamicky měněné klíče).
    - Authentication types: WPA PSK (typ autentizace WPA Pre-Shared klíč).
    - Unicast Ciphers: tkip (unicast šifrování TKIP).
    - Group Ciphers: tkip (group šifrování TKIP).
    - WPA Pre-Shared key: 123456789 (sdílený klíč).

- Group Key Update: 00:05:00 (změna group-key každých 5 minut).
- Hide SSID: false (skrývání SSID vypnuto).

ASUS X550L – klient

Název ve Wiresharku: Azurewav_84:e9:f7.

MAC adresa zařízení: 54:27:1E:84:E9:F7.

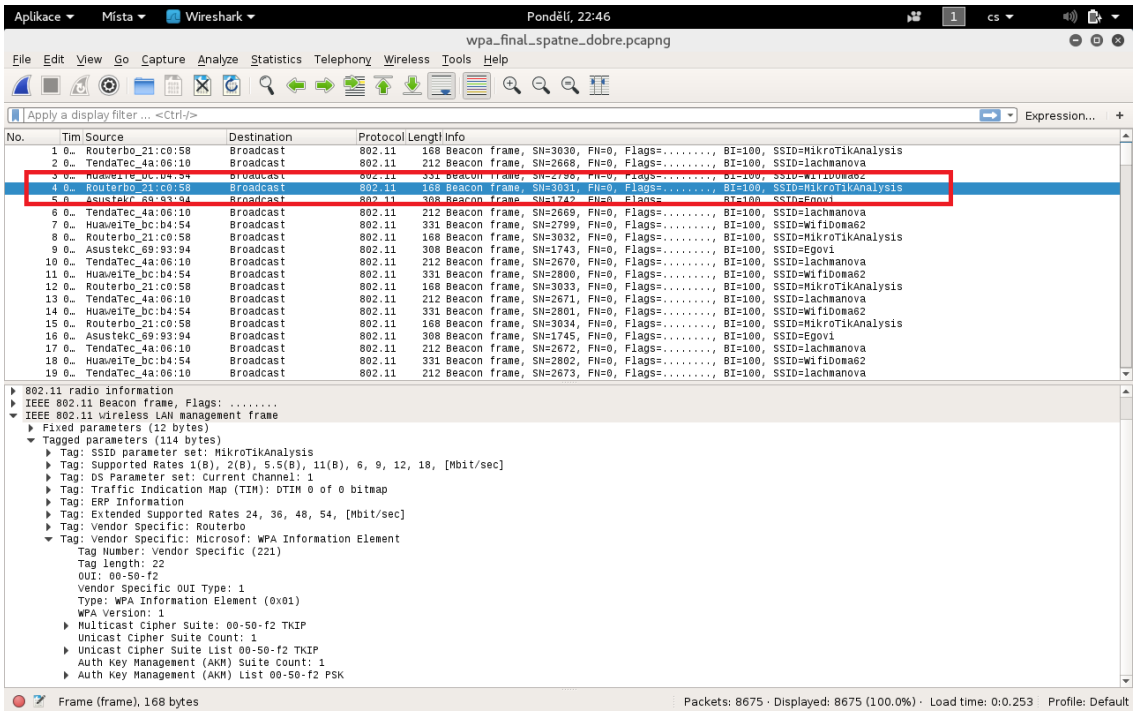
Notebook klientské stanice s operačním systémem Microsoft Windows 8.1, který se bezdrátově připojuje k AP.

Fujitsu Siemens AmiloPro V3505 – sniffer

Pirátská stanice s předinstalovaným operačním systémem Kali Linux a nástrojem Wireshark, který poslouží pro odposlech komunikace mezi klientem a AP. Síťová karta Wi-Fi umožňuje tzv. monitorovací mód, kdy je možný odposlech veškeré komunikace.

6.1.2 Rozbor komunikace WPA-Personal

Spustíme program Wireshark příkazem `wireshark` v terminálu, nebo poklepáním na ikonu. Vybereme rozhraní (*wlan0*), na kterém chceme odchytávat paketová data a spustíme monitoring (*capture*). Nyní již odchytáváme všechny pakety, jak můžeme vidět na následujícím obrázku (Obrázek 12).

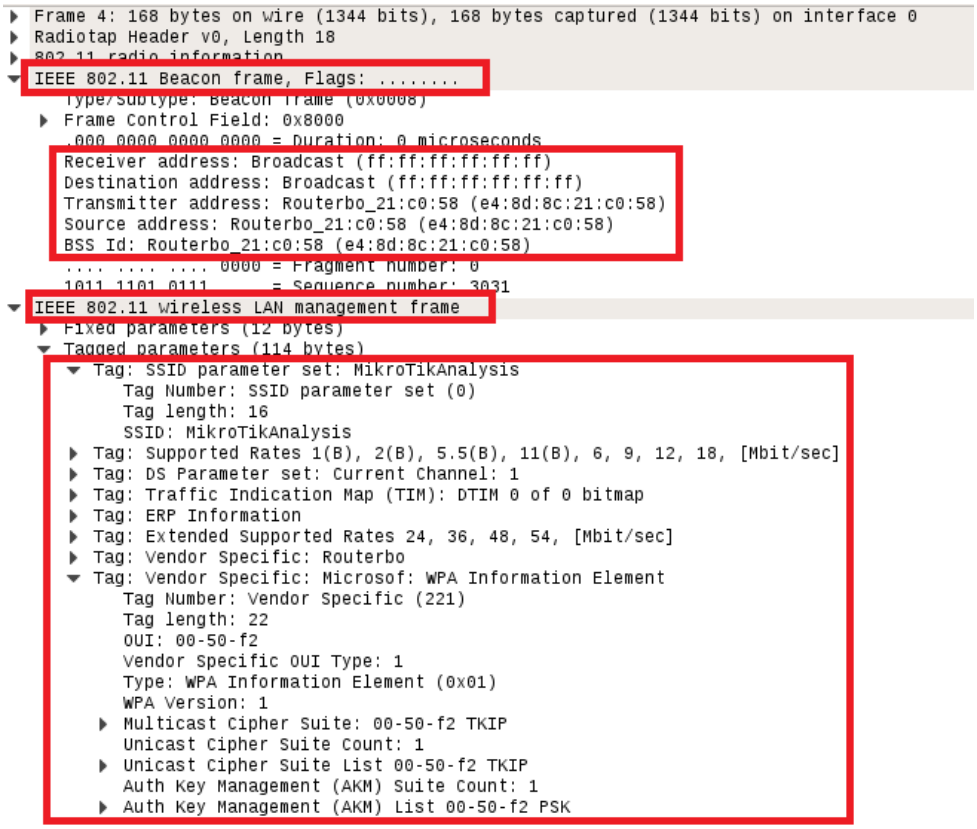


Obrázek 12 - WPA-PSK beacon frames

Zdroj: vlastní

Na obrázku (Obrázek 12) dále můžeme sledovat, že každý dostupný přístupový bod vysílá opakovaně rámec typu beacon (*zvýrazněno červeně*), kterým vlastně do prostoru (*broadcast*) říká „jsem tu“. Tento rámec s sebou nese všechny důležité informace o AP, jako například: SSID, MAC adresu, datové propustnosti, kanál, šifrovací metody a mnohé další.

Detailní pohled na rámec typu beacon je na obrázku (Obrázek 13).

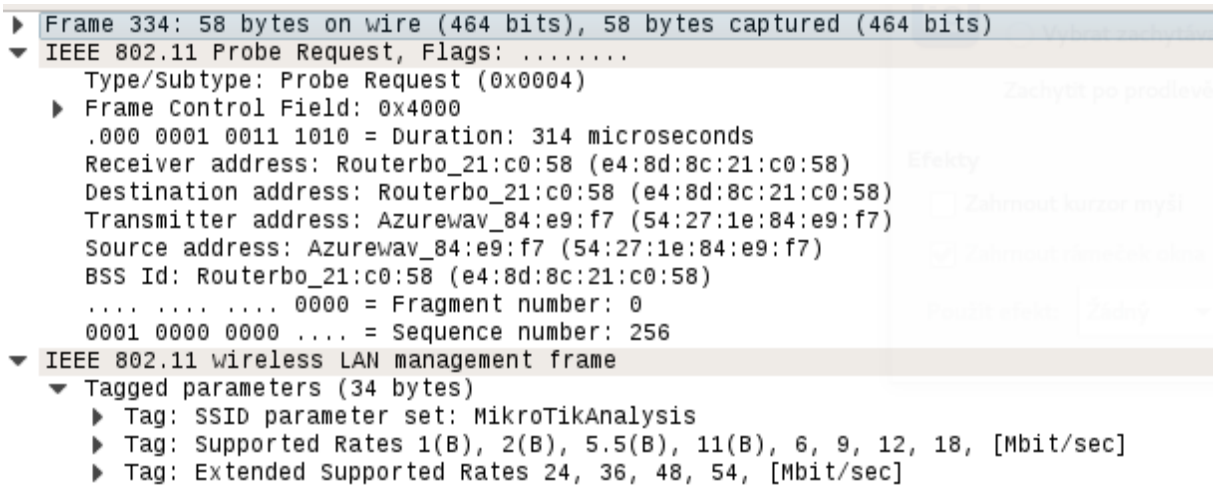


Obrázek 13 - Beacon frame

Zdroj: vlastní

Zde je zřejmé, že původcem rámce je náš AP v síti MikroTikAnalysis, který má MAC adresu e4:8d:8c:21:c0:58. BSS Id je Routerbo_21:C0:58, což je identifikátor zařízení. Cílová adresa rámce je ff:ff:ff:ff:ff:ff (*broadcast*). AP vysílá na kanálu (*channel*) 1. Maximální propustnost je 54 Mbit/s, přičemž šifrování je WPA-TKIP. Autentizaci zajišťuje sdílený klíč (*PSK*).

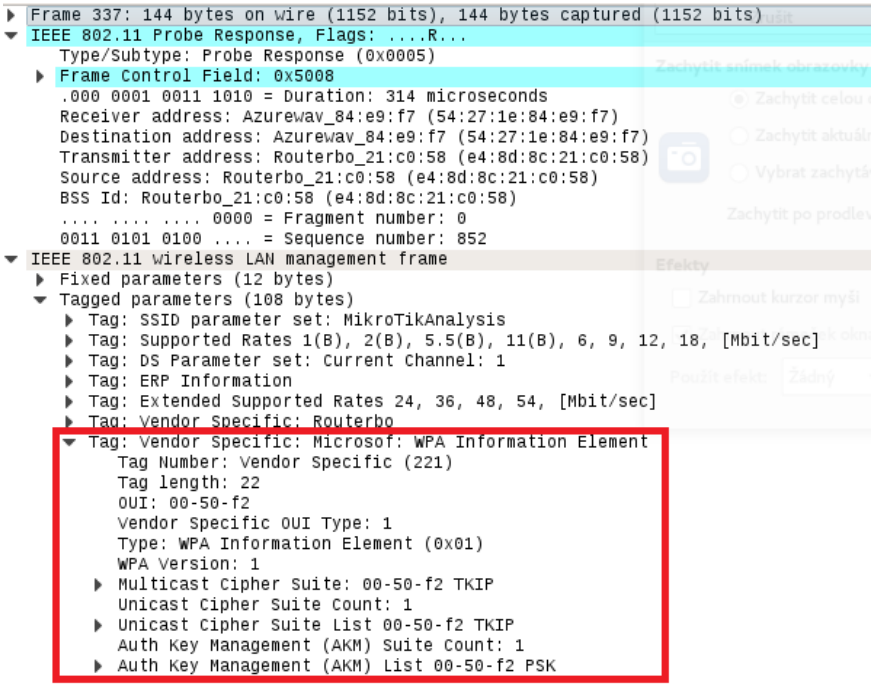
Pokud se klientská stanice bude chtít připojit k vybranému AP, zašle rámec typu probe request (*požadavek na prozkoumání*) na adresu vybraného AP. Jeho úkolem je získat informace od daného AP. Rámec je detailně zachycen na následujícím obrázku (Obrázek 14).



Obrázek 14 - Probe request

Zdroj: vlastní

AP, který obdrží rámec probe request, odpoví rámcem typu probe response (*odpověď na prozkoumání*) zpět, na původní zdrojovou (*source*) adresu. Následující obrázek (Obrázek 15) zachycuje rámec probe response.

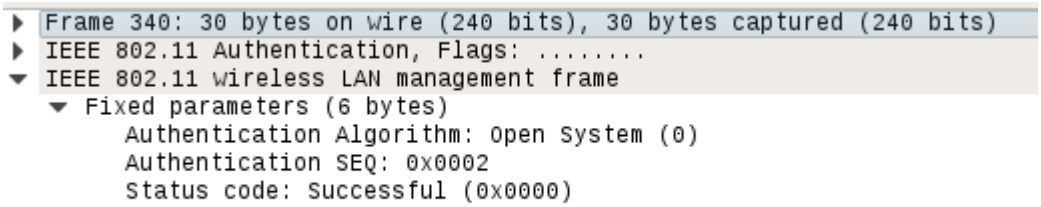


Obrázek 15 - Probe response

Zdroj: vlastní

Rámec probe respone, podobně jako rámec beacon, obsahuje detaily o přístupovém bodu. Popisuje datové propustnosti, šifrovací a autentizační metody, správu klíčů, aktuální vysílací kanál a mnohé další.

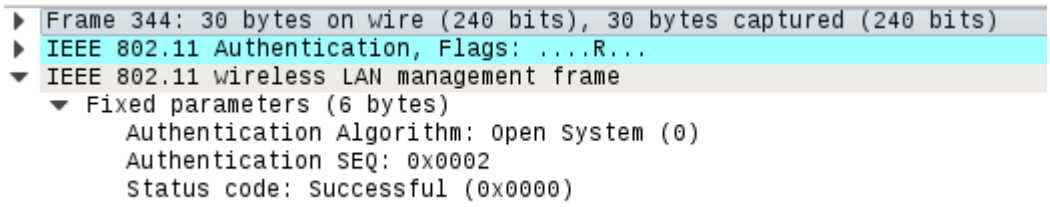
Proces autentizace, kdy AP buď přijme, nebo odmítne identitu klienta, začíná zasláním rámce authentication request (*autentizační požadavek*) přístupovému bodu (Obrázek 16).



Obrázek 16 - Authentication frame

Zdroj: vlastní

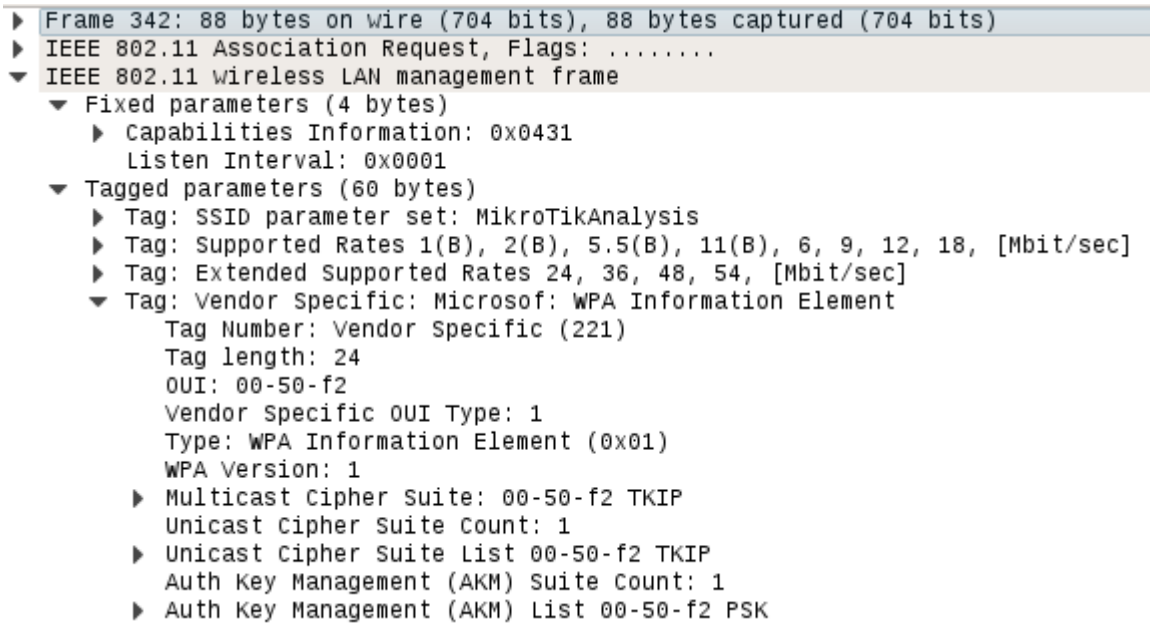
Odpovědí přístupového bodu je rámec authentication acceptance (*přijetí autentizace*), který je na následujícím obrázku (Obrázek 17).



Obrázek 17 - Authentication acceptance frame

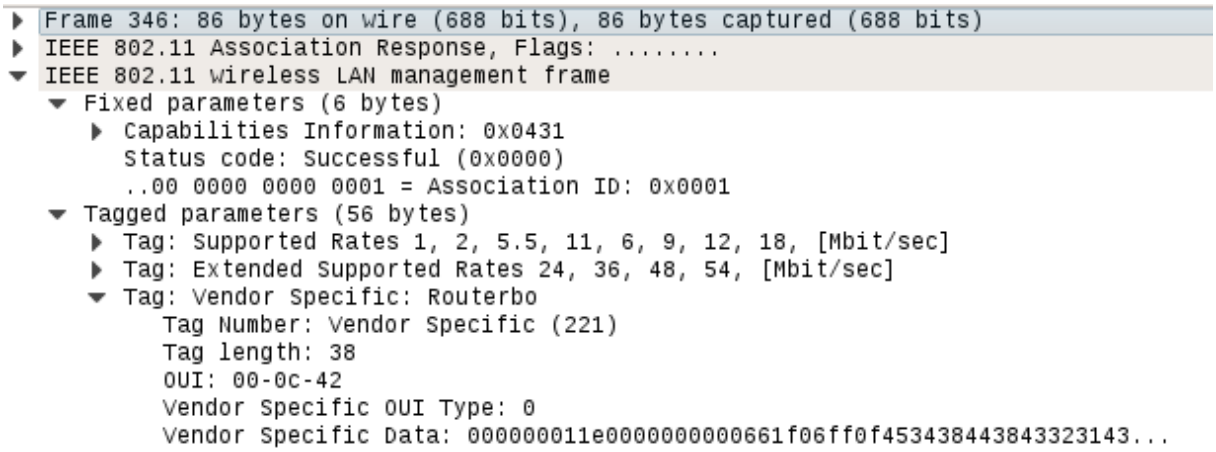
Zdroj: vlastní

Přidružení přístupového bodu a klienta zajišťují asociační rámce. Přístupový bod si tak alokuje potřebné zdroje pro klienta a následně se synchronizují. Klient zašle rámec association request (*požadavek k asociaci*) směrem k přístupovému bodu (Obrázek 18), který odpovídá rámcem association response (*odpověď na asociaci*). Rámec association response je zachycen na obrázku (Obrázek 19).



Obrázek 18 - Association request

Zdroj: vlastní



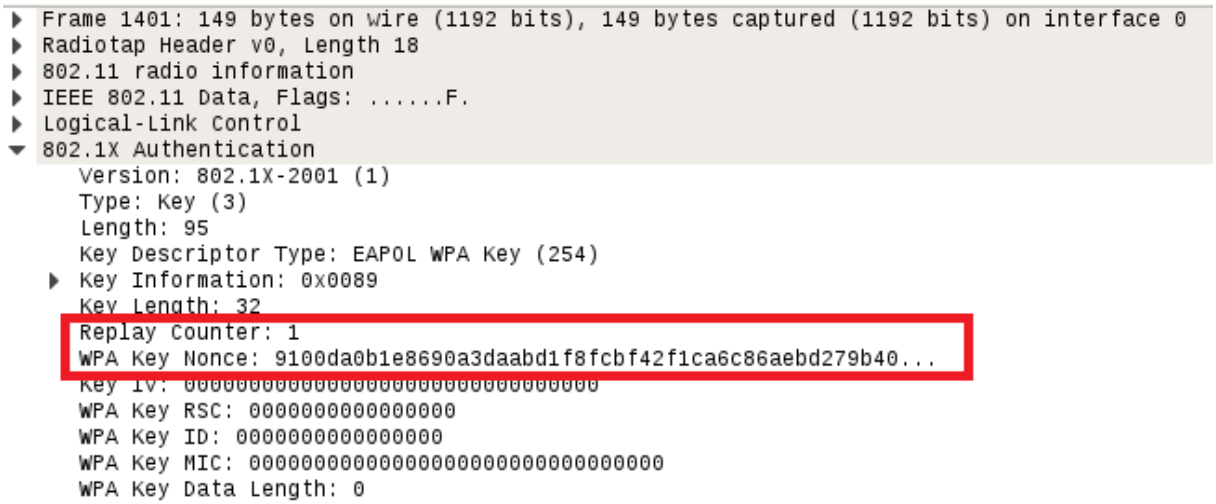
Obrázek 19 - Association response

Zdroj: vlastní

Pokud je požadavek na asociaci přijat a zařízení jsou úspěšně asociována (*přidružena*), pak si AP rezervuje paměťový prostor a stanoví asociační ID klientské stanici.

Následující čtyři pakety tvoří WPA handshake (*potřesení rukou*), při kterém jsou dohodnuta šifrovací pravidla další komunikace. Z předdefinovaného PSK klíče je odvozen klíč PTK, přičemž PSK je zde použit pouze jako PMK klíč. Proces funguje principem dotaz-odpověď. První zašle AP rámec s hodnotou WPA key nonce (*náhodné 256bitové číslo*) ke klientské

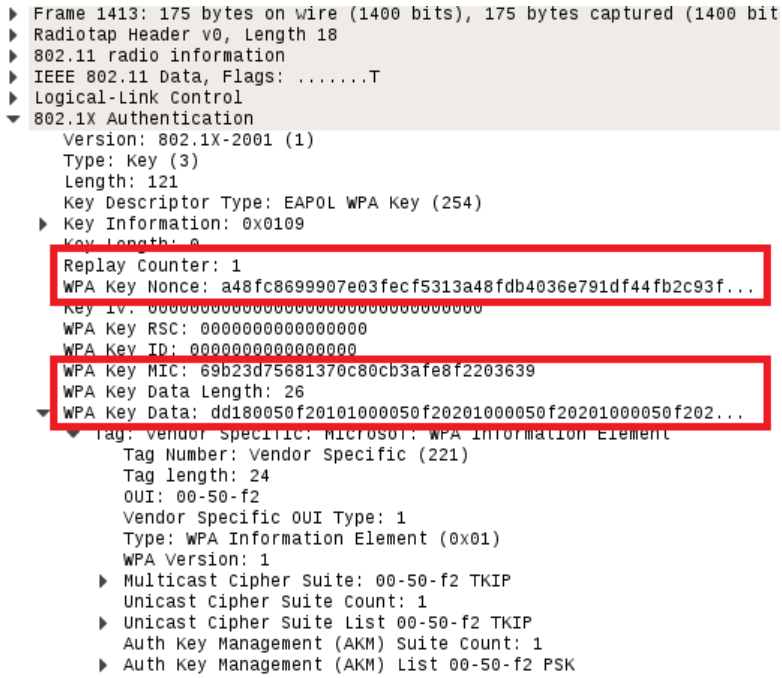
stanici. Rámec dále obsahuje informace o šifrovacích metodách, počítadlo opakování, ale také druh konstruovaného klíče (Obrázek 20).



Obrázek 20 - WPA handshake 1

Zdroj: vlastní

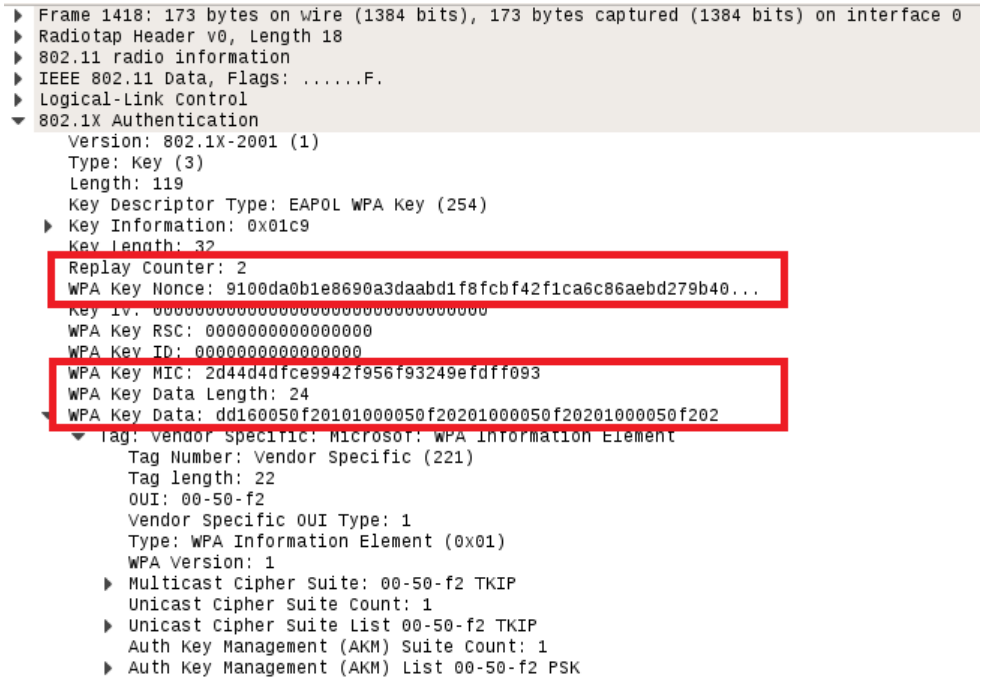
Nyní má klientská stanice vše potřebné pro konstrukci PTK klíče. Klient odpovídá rámcem, ve kterém připojuje svoji hodnotu WPA key nonce, vypočítaný MIC (*integrita*) a WPA key (Obrázek 21). Hodnota počítadla replay (*sekvence*) zůstává stejná.



Obrázek 21 - WPA handshake 2

Zdroj: vlastní

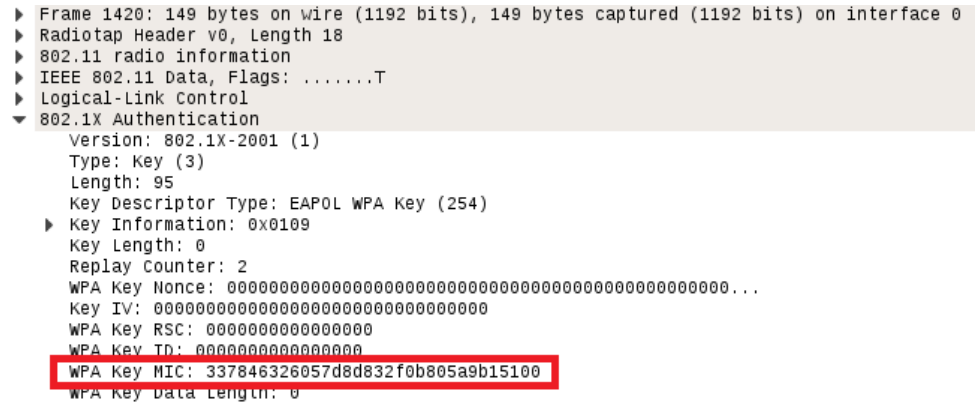
AP vytvoří rámec s novým MIC a novým WPA key, přičemž hodnotu nonce použije původní (Obrázek 20). Počítadlo replay se nyní zvyšuje (*druhá fáze*). Na následujícím obrázku (Obrázek 22) je zachycen zmíněný rámec.



Obrázek 22 - WPA handshake 3

Zdroj: vlastní

Klientská stanice vypočítá nový MIC a odpoví akceptačním rámcem (Obrázek 23).



Obrázek 23 - WPA handshake 4

Zdroj: vlastní

Od této chvíle jsou všechna přenášená data šifrována, přičemž každý datový rámec s sebou nese TKIP informace (*inicializační vektor*) a zašifrovaná data (Obrázek 24).

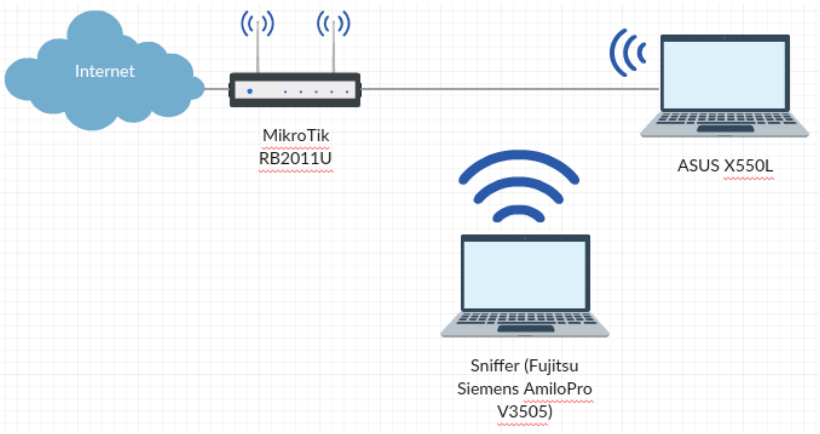
```
▼ TKIP parameters
      TKIP Ext. Initialization Vector: 0x000000000001
      Key Index: 0
Data (151 bytes)
   Data: 9e2977bd757957115c3d5e74ebeaffc9797fdde56bf2ebec...
```

Obrázek 24 - WPA zašifrovaná data

Zdroj: vlastní

6.2 WPA2-Personal

Následující obrázek (Obrázek 25) znázorňuje topologickou strukturu sítě, která je použita pro analýzu provozu, při použití WPA2-Personal (*WPA2-PSK*). Ve struktuře je použit směrovač MikroTik RB2011U, dále jen přístupový bod AP, notebook klientské stanice ASUS X550L, který se autentizuje k přístupovému bodu a pirátský notebook Fujitsu Siemens AmiloPro V3505, který odchytává provoz na síti, za účelem další analýzy komunikace.



Obrázek 25 - Modelová situace WPA2-Personal

Zdroj: vlastní

6.2.1 Použité prvky a jejich konfigurace

MikroTik RB2011U – přístupový bod

Název ve Wiresharku: Routebo_21:c0:58.

MAC adresa zařízení: E4:8D:8C:21:C0:58.

Konfigurace bezdrátové sítě:

- Mode: ap bridge (mód přístupového bodu).
- Band: 2GHz-B/G (vysílá v pásmu 2GHz, protokol 802.11b a 802.11g).
- Channel width: 20MHz (šířka pásma).

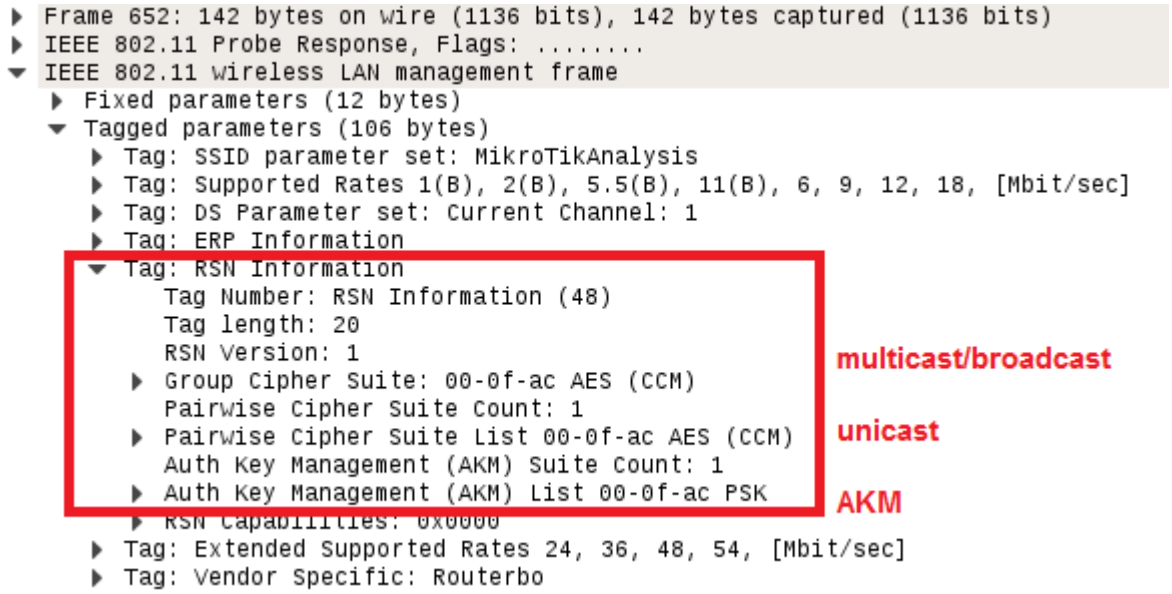
- SSID: MicroTikAnalysis (identifikátor SSID).
- Security profile: (profil zabezpečení)
    - Mode: dynamic keys (dynamicky měněné klíče).
    - Authentication types: WPA2 PSK (typ autentizace WPA Pre-Shared klíč).
    - Unicast Ciphers: tkip (unicast šifrování AES CCMP).
    - Group Ciphers: tkip (group šifrování AES CCMP).
    - WPA Pre-Shared key: 123456789 (sdílený klíč).
    - Group Key Update: 00:05:00 (změna group-key každých 5 minut).
    - Hide SSID: false (skrývání SSID vypnuto).

Konfigurace klientské a pirátské stanice je stejná, jako u WPA-Personal (kapitola 6.1.1).

6.2.2 Analýza komunikace WPA2-Personal

Celý proces autentizace a asociace je prakticky totožný s procesem WPA-Personal, proto se nebudeme zabývat psaním toho samého znovu, nýbrž budou vypíchnuty rozdíly.

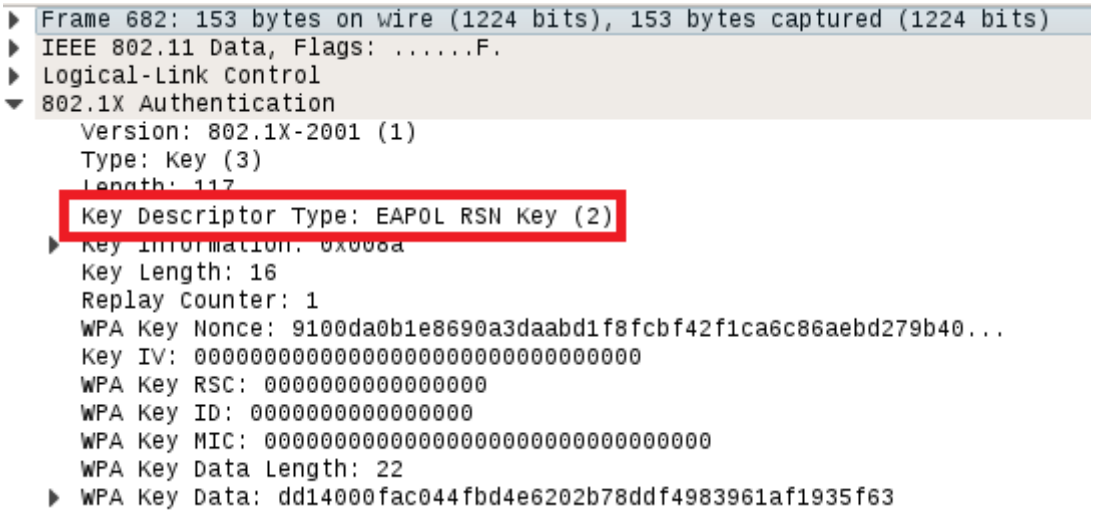
Rámce probe request/response a association request/response nově obsahují informační složku RSN (*protokol pro vytvoření bezpečné komunikace protokolu 802.11*), která zahrnuje šifrovací sady pro unicast (*jeden klient*), multicast (*skupina klientů*) a broadcast (*veřejné*) vysílání. RSN dále obsahuje informace AKM (*systém distribuce klíčů*). Rámec probe response, při použití WPA2-Personal je zachycen na následujícím obrázku (Obrázek 26).



Obrázek 26 - WPA2 včetně RSN

Zdroj: vlastní

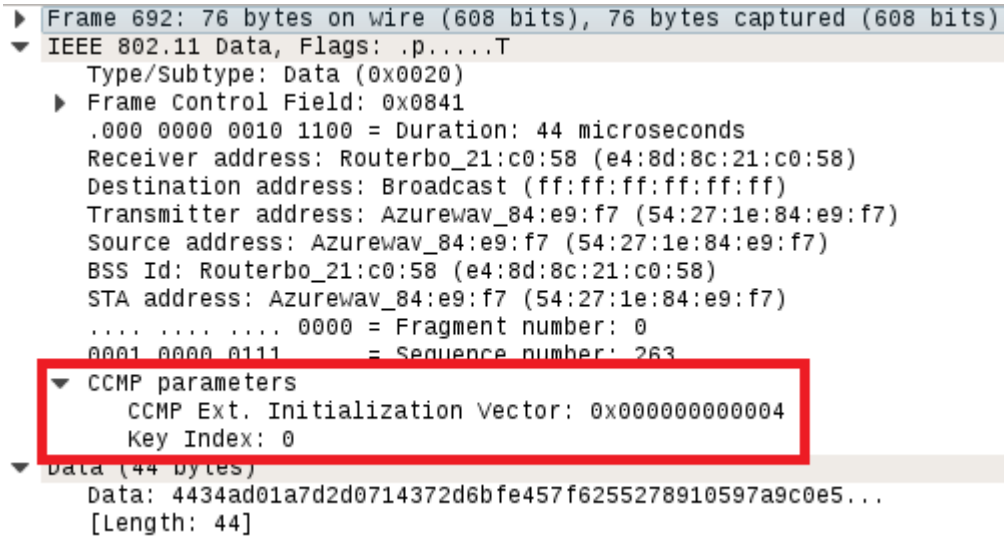
Dále WPA2 pozměňuje rámce pro WPA handshake, konkrétně hodnotu deskriptoru klíče. WPA používá EAPOL WPA Key (254), kdežto WPA2 používá EAPOL RSN Key (2). Rozdíl znázorňuje obrázek (Obrázek 27).



Obrázek 27 - WPA2 handshake

Zdroj: vlastní

Datové pakety potom neobsahují informační složku TKIP (*pokud není TKIP zvoleno, jako kompatibilní šifrovací metoda*), nýbrž složku CCMP, konkrétně pak inicializační vektor (Obrázek 28).



Obrázek 28 - WPA2 datový paket s CCMP

Zdroj: vlastní

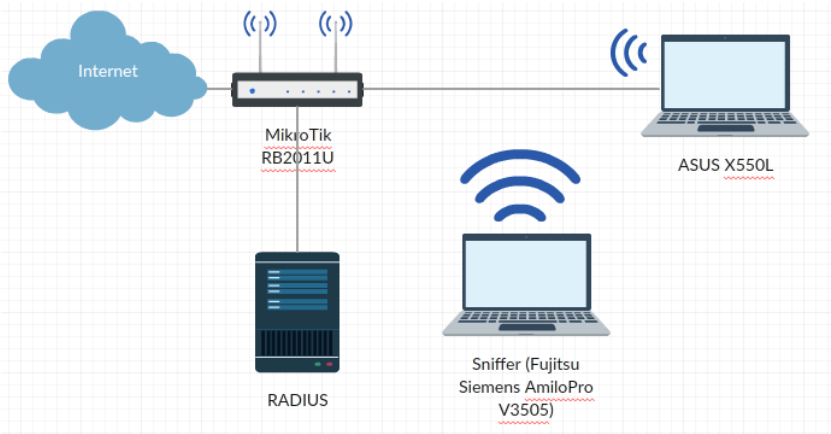
6.3 Shrnutí WPA a WPA2-Personal

Co se týká bezpečnosti, tak je v dnešní době varianta WPA-PSK-TKIP nedostatečným řešením i co se domácí sítě týče. TKIP lze s trochou úsilí velmi jednoduše prolomit. Pokud se jedná o podnikovou síť, kde se přenáší extra citlivá data, pak je tento typ zabezpečení zcela nevhodný. Když se vrátíme k analýze komunikace, tak v případě slovníkového útoku na PSK stačí odchytat dostatečný počet WPA handshake a bezpečnostní problém je na světě. Pokud zvolí administrátor heslo dostatečně silné, je stále ve hře varianta útoku na TKIP, která počítá s hádáním bajtů. Tyto útoky byly popsány v kapitole 4.2.3.

WPA2 ve variantě WPA2-PSK-AES-CCMP je velmi robustní řešení. Nepodcení-li administrátor sítě „sílu“ hesla (*délka a kombinace nesouvisejících znaků*), pak je vlastně nemožné toto zabezpečení prolomit. Z pohledu podnikové sítě, je řešení WPA2-Personal vhodné spíše pro malé sítě, nebo kanceláře. Kvůli sdílení jednoho klíče (*hesla*) všemi uživateli, je složitá správa všech zařízení sítě. Pokud jeden ze zaměstnanců opouští firmu, je nutné z bezpečnostního hlediska přenastavit sdílený klíč, a to na všech zařízeních sítě. Malý podnik s 5 stanicemi se s tímto vypořádá, ale pro větší podniky by bylo řešení bez centrální správy velmi složité na údržbu.

6.4 Návrh bezpečné podnikové sítě

Dostáváme se k řešení zabezpečení pro větší a velké podnikové sítě. Pro tuto variantu je nutná centrální správa uživatelských účtů, a je proto vhodné nasadit zabezpečení WPA2-Enterprise, kdy je místo sdíleného klíče autentizován každý uživatel svými vlastními údaji (*typicky jméno a heslo, nebo certifikát*). O autentizaci uživatele rozhodne autentizační server, se kterým komunikuje přístupový bod během pokusu o autentizaci klienta.

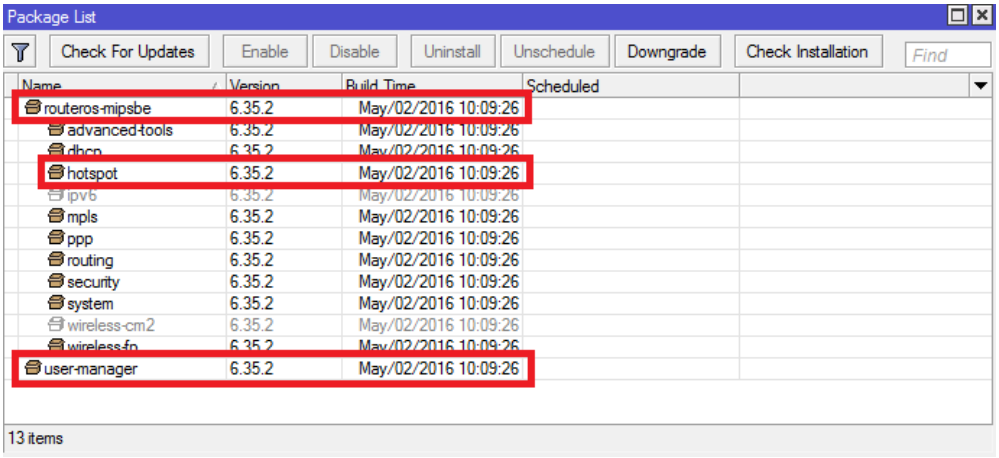


Obrázek 29 - WPA2-Enterprise

Zdroj: vlastní

Předchozí obrázek (Obrázek 29) zachycuje modelovou situaci zapojení pro WPA2-Enterprise.

Pro sestavení uvedeného řešení byl použit směrovač MikroTik RB2011U. MikroTik na svých webových stránkách nabízí ke stažení extra balíčky, díky kterým směrovač MikroTik získá nějaké extra funkce. Pro naši simulaci bylo potřeba aktualizovat hlavní systém RouterOS na verzi 6.35.2 a doinstalovat správu uživatelských účtů (*jeden z extra balíčků*). Funkcionalita hotspotu a podpora RADIUS serveru je k dispozici v základním balíčku RouterOS. Nainstalované balíčky, které jsou důležité pro laboratorní zapojení, jsou zvýrazněny na obrázku (Obrázek 30).

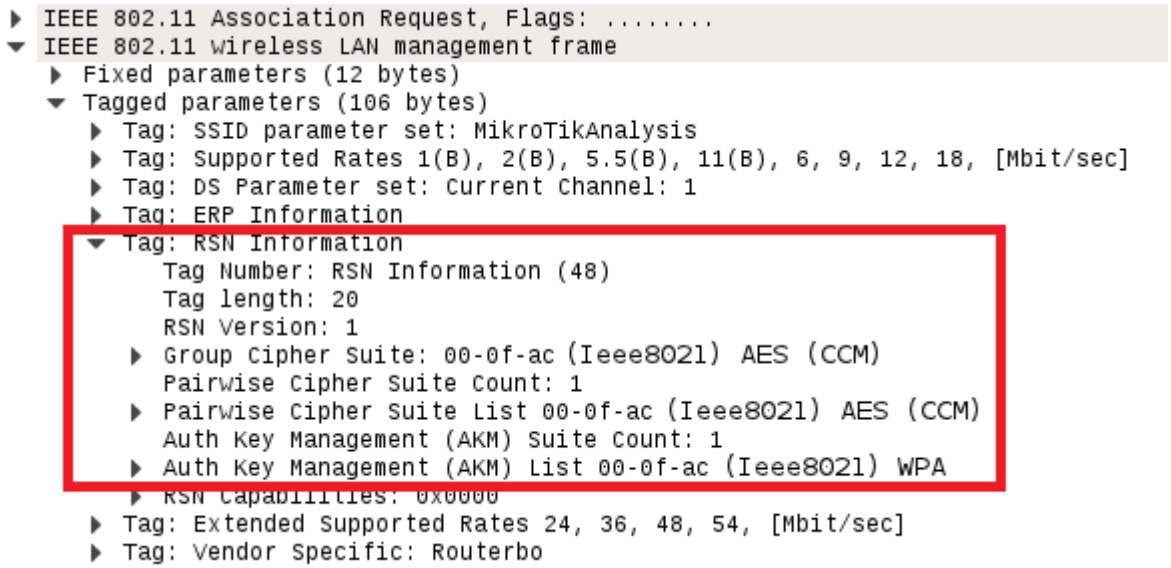


Obrázek 30 - WPA2-Enterprise a potřebné balíčky

Zdroj: vlastní

Jelikož Enterprise řešení umožňuje oba druhy šifrování, může i přístupový bod nabízet jak TKIP, tak AES šifrování. V RSN složce rámců, které vysílá AP, jsou informace o podporovaném šifrování obsaženy.

Klientská stanice si vybere některé z nabízeného šifrování a odesílá tuto informaci v RSN složce asociačního rámce. Rámec s RSN složkou vybraného šifrování je zachycen na obrázku (Obrázek 31).



Obrázek 31 - WPA2-Enterprise asociační rámec

Zdroj: vlastní

Přístupový bod obsahuje RADIUS klienta, který slouží pro komunikaci s RADIUS serverem. Klientská stanice předá své údaje (*jméno, heslo, certifikát*) RADIUS klientu. Poté proběhne proces ověření uživatele mezi RADIUS klientem a RADIUS serverem. Celá komunikace je šifrována a výsledkem je přijetí (*autentizace*), nebo nepřijetí (*deautentizace*) klientské stanice protokolem EAP. Pokud je stanice přijata, pak proběhne tradiční WPA handshake (*popsáno v kapitole 6.1.2*), pro zajištění šifrování přenášených dat. Pokud by byly zjištěny autentizační údaje některého z klientů sítě, pak nemá útočník šanci dešifrovat paketová data jiného uživatele, ač se nachází ve stejné síti.

V našem případě nebylo potřeba dalších zařízení, jelikož použitý směrovač podporuje funkci RADIUS serveru „sám na sobě“, takže stačilo pouze nastavit celou konfiguraci, spustit RADIUS server a RADIUS klienta. V administraci RADIUS serveru pak jednoduše přidávat/mazat jednotlivé uživatele.

Řešení s použitím WPA2-Enterprise je sice náročnější na prvotní konfiguraci, avšak centralizace a zjednodušení následné správy tyto prvotní investice hravě převáží. Při důsledné konfiguraci a údržbě je toto řešení na velmi vysoké úrovni zabezpečení, a proto je v podnikové praxi hojně využíváno. Příkladem tohoto zabezpečení je třeba síť eduroam, která je dostupná na mnoha místech republiky (*převážně univerzitách*) a studenti se mohou se svými údaji kdekoliv hravě připojit.

7 ZÁVĚR

Cílem práce bylo zmapovat slabiny zabezpečení bezdrátových Wi-Fi sítí, které využívají zabezpečení WPA-Personal, WPA2-Personal a navrhnout bezpečné řešení s využitím WPA2-Enterprise pro podnikovou síť.

V úvodní části práce byl zpracován historický vývoj bezdrátových technologií a byla provedena rešerše zabezpečení bezdrátových Wi-Fi technologií, až po zkoumané zabezpečení WPA a WPA2. Byly uvedeny netradiční příklady využití Wi-Fi sítí z reálného života, než je jen pouhé připojení k internetu, které jsou zajímavou ukázkou dalšího využití těchto technologií. Co se týče budoucnosti, byly uvedeny připravované novinky a nastíněn možný další vývoj Wi-Fi sítí.

Dále byly rozpracovány obecné pojmy zabezpečení a jejich základní implementace v bezdrátových Wi-Fi sítích. Po základních zabezpečovacích metodách byly rozpracovány pokročilé metody zabezpečení. Každé z uvedených zabezpečení bylo do detailu rozebráno a byla analyzována slabá místa těchto zabezpečení. Na základě slabin bylo doporučeno, či nedoporučeno takové zabezpečení používat, popřípadě za jakých podmínek.

V praktické části práce bylo provedeno měření v panelovém domě, za účelem zjistit míru zabezpečení dostupných sítí. Výsledkem byla statistika použitých zabezpečovacích metod a míry uvědomění administrátorů sítí o nezbytnosti dostatečného zabezpečení jejich Wi-Fi sítí.

Součástí praktické částí byla paketová analýza jednotlivých zabezpečení, obsahující návrh bezpečné podnikové sítě. Pro každý typ zabezpečení byla navrhnuta a simulována určitá topologická struktura. Následovala podrobná paketová analýza provozu, během procesu autentizace klientské stanice k přístupovému bodu. Shrnutí jednotlivých zabezpečení obsahovalo potřebná doporučení o vhodnosti použití jednotlivých zabezpečení v různých segmentech. Cílem poslední části bylo navrhnout bezpečné síťové řešení pro podnikovou síť. Byl proveden návrh topologie sítě a popsány další prvky sítě, které předchozí praktické úlohy nepotřebovaly. Byl popsán proces komunikace a autentizace klientské stanice k autentizačnímu serveru a zdůrazněny bezpečnostní důvody pro nasazení tohoto řešení v podnikovém prostředí.

8 POUŽITÁ LITERATURA

BARKEN, Lee, 2004. *Wi-Fi: jak zabezpečit bezdrátovou síť*. Brno: Computer Press, 2004. ISBN 80-251-0346-3.

CISCO SYSTEMS, 2012. New Cisco Solution Helps Service Providers & Enterprises Deliver Exciting, Profitable Mobile Experiences with Advanced Location-Based Wi-Fi Technology. In: *Cisco's The Network* [online]. SAN JOSE, CA, Nov. 15, 2012 [cit. 2016-04-14]. Dostupné z: http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1105153

GAST, Matthew, 2013. *802.11ac: A Survival Guide* [online]. Sebastopol: O'Reilly Media, 2013 [cit. 2016-04-13]. ISBN 978-144-93-4314-9. Dostupné z: http://chimera.labs.oreilly.com/books/1234000001739/index.html

HERN, Alex, 2015. *Facebook launches Aquila solar-powered drone for internet access*. In: The Guardian: Technology [online]. 31 July 2015 [cit. 2016-05-02]. Dostupné z: https://www.theguardian.com/technology/2015/jul/31/facebook-finishes-aquila-solar-powered-internet-drone-with-span-of-a-boeing-737

HISTORY.COM STAFF, 2009. *Guglielmo Marconi*. In: HISTORY.com [online]. A+E Networks, 2009 [cit. 2016-04-13]. Dostupné z: http://www.history.com/topics/inventions/guglielmo-marconi

How to Ease the Pain of Slow Wi-Fi. IT BusinessEdge [online]. 2016 [cit. 2016-05-02]. Dostupné z: http://www.itbusinessedge.com/slideshows/how-to-ease-the-pain-of-slow-wi-fi-05.html

HRSTKA, Jaroslav, c2010–2016. *Gigabitová místní rádiová síť*. In: NETGURU [online]. c2010–2016 [cit. 2016-05-01]. Dostupné z: http://www.netguru.cz/odborne-clanky/gigabitova-mistni-radiova-sit.html

KELLY, Timothy V., 2005. *VoIP For Dummies*. Indianapolis: Wiley Publishing, Inc., September 2005. ISBN 978-0-7645-8843-3.

KOCMAN, Rostislav, 2000. *Jak se Motorola stala Motorolou*. In: IDNES.cz [online]. 21. listopadu 2000 [cit. 2016-04-28]. Dostupné z: http://mobil.idnes.cz/jak-se-motorola-stala-motorolou-da0-/mob_tech.aspx?c=A001120_0024392_mob_aktuality

LINK LABS, 2015. *Examining The Future Of WiFi: 802.11ah HaLow, 802.11ad (& Others)*. In: Link Labs [online]. August 12, 2015 [cit. 2016-04-17]. Dostupné z: http://www.link-labs.com/future-of-wifi-802-11ah-802-11ad/

REDAKCE2, 2014. *Více než 1 Gbit/s na bezdrátové síti? Díky standardu 802.11ac je to možné!*. In: BusinessIT [online]. Srpen 2014 [cit. 2016-05-01]. Dostupné z: http://www.businessit.cz/cz/vice-nez-1-gbit-s-na-bezdratove-siti-diky-standardu-802-11ac-je-to-mozne.php

SKELET, 2007. *Bezdrátové sítě*. Bezdrátové sítě [online]. 2007-06-24 [cit. 2016-05-07]. Dostupné z: http://bezdratovesite.wz.cz/

T-MOBILE CZECH REPUBLIC, 2015. *T-Mobile představuje Wi-Fi volání jako první v ČR*. In: T-Mobile t-press: Tiskové centrum [online]. 04. 11. 2015 [cit. 2016-05-08]. Dostupné z: https://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/t-mobile-predstavuje-wi-fi-volani-jako-prvni-v-cr.html

Wi-Fi Logo, 2013. *Famous Logos: The most famous logos and brands in the world* [online]. 23 Apr 2013 [cit. 2016-05-07]. Dostupné z: http://www.famouslogos.org/logos/wi-fi-logo

SALABERRIA, Itziar, Roberto CARBALLEDO a Asier PERALLOS, 2012. *Wireless Technologies in the Railway: Train-to-Earth Wireless Communications*. In: Wireless Communications and Networks - Recent Advances [online]. University of Deusto (Spain): InTech, March 14, 2012, s. 469-491 [cit. 2016-04-14]. ISBN 978-953-51-0189-5. Dostupné z: http://www.intechopen.com/books/wireless-communications-and-networks-recent-advances/wireless-technologies-in-the-railways-train-to-earth-wireless-communications

WILLIAMS, Martyn, 2016. *Internetové připojení kdekoli pomocí dronů? Facebook začne testovat novou technologii už letos*. In: CIO Business World [online]. 23.02.2016 [cit. 2016-04-17]. Dostupné z: http://businessworld.cz/net/internetove-pripojeni-kdekoli-pomoci-dronu-facebook-zacne-testovat-novou-technologii-uz-letos-12803

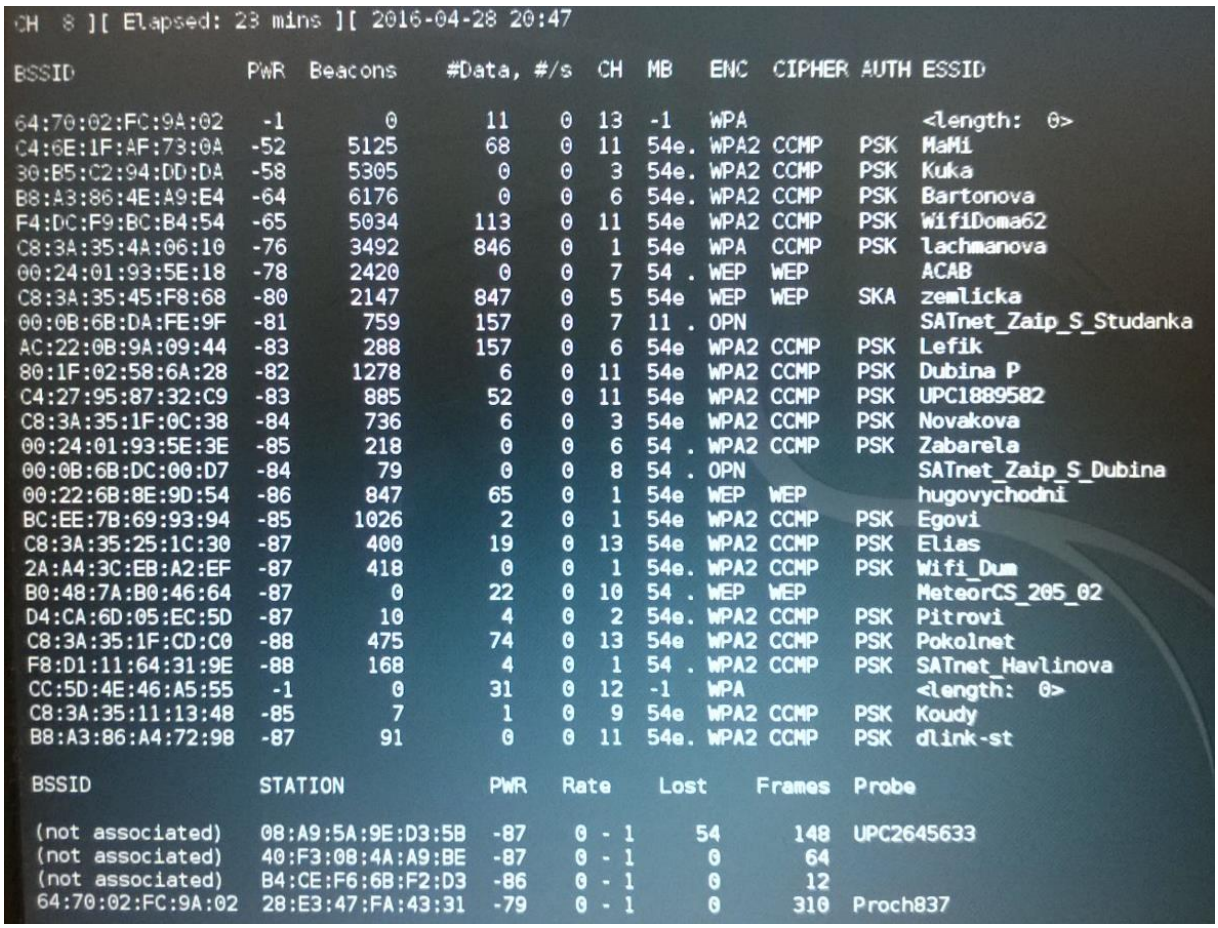
WOLIGROSKI, Don, 2011. *LAN 102: Network Hardware And Assembly: Wireless Network Logical Topologies*. In: Tom's Hardware [online]. Purch Group, Inc., November 1, 2011 [cit. 2016-04-13]. Dostupné z: http://www.tomshardware.com/reviews/local-area-network-gigabit-ethernet,3035-7.html

WRIGHTSON, Tyler, 2012. *Wireless network security: a beginner's guide*. New York: McGraw-Hill, c2012. ISBN 00-717-6094-6.

ZHOU, Hongbo (ed.), 2012. *Wireless Ad-Hoc Networks* [online]. Slippery Rock University: InTech, December 12, 2012 [cit. 2016-04-13]. ISBN 978-953-51-0896-2. Dostupné z: http://www.intechopen.com/books/wireless-ad-hoc-networks

9 PŘÍLOHY

Příloha A – výpis programu airodump -ng



```
CH  8 ][ Elapsed: 23 mins ][ 2016-04-28 20:47

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

64:70:02:FC:9A:02   -1        0       11    0  13  -1   WPA                <length:  0>
C4:6E:1F:AF:73:0A  -52     5125       68    0  11  54e. WPA2 CCMP   PSK  MaMi
30:B5:C2:94:DD:DA  -58     5305        0    0   3  54e. WPA2 CCMP   PSK  Kuka
B8:A3:86:4E:A9:E4  -64     6176        0    0   6  54e. WPA2 CCMP   PSK  Bartonova
F4:DC:F9:BC:B4:54  -65     5034      113    0  11  54e  WPA2 CCMP   PSK  WifiDoma62
C8:3A:35:4A:06:10  -76     3492      846    0   1  54e  WPA  CCMP   PSK  lachmanova
00:24:01:93:5E:18  -78     2420        0    0   7  54 . WEP  WEP         ACAB
C8:3A:35:45:F8:68  -80     2147      847    0   5  54e  WEP  WEP    SKA  zemlicka
00:0B:6B:DA:FE:9F  -81      759      157    0   7  11 . OPN              SATnet_Zaip_S_Studanka
AC:22:0B:9A:09:44  -83      288      157    0   6  54e  WPA2 CCMP   PSK  Lefik
80:1F:02:58:6A:28  -82     1278        6    0  11  54e  WPA2 CCMP   PSK  Dubina P
C4:27:95:87:32:C9  -83      885       52    0  11  54e  WPA2 CCMP   PSK  UPC1889582
C8:3A:35:1F:0C:38  -84      736        6    0   3  54e  WPA2 CCMP   PSK  Novakova
00:24:01:93:5E:3E  -85      218        0    0   6  54 . WPA2 CCMP   PSK  Zabarela
00:0B:6B:DC:00:D7  -84       79        0    0   8  54 . OPN              SATnet_Zaip_S_Dubina
00:22:6B:8E:9D:54  -86      847       65    0   1  54e  WEP  WEP         hugovychodni
BC:EE:7B:69:93:94  -85     1026        2    0   1  54e  WPA2 CCMP   PSK  Egovi
C8:3A:35:25:1C:30  -87      400       19    0  13  54e  WPA2 CCMP   PSK  Elias
2A:A4:3C:EB:A2:EF  -87      418        0    0   1  54e. WPA2 CCMP   PSK  Wifi_Dum
B0:48:7A:B0:46:64  -87        0       22    0  10  54 . WEP  WEP         MeteorCS_205_02
D4:CA:6D:05:EC:5D  -87       10        4    0   2  54e. WPA2 CCMP   PSK  Pitrovi
C8:3A:35:1F:CD:C0  -88      475       74    0  13  54e  WPA2 CCMP   PSK  Pokolnet
F8:D1:11:64:31:9E  -88      168        4    0   1  54 . WPA2 CCMP   PSK  SATnet_Havlinova
CC:5D:4E:46:A5:55   -1        0       31    0  12  -1   WPA                <length:  0>
C8:3A:35:11:13:48  -85        7        1    0   9  54e  WPA2 CCMP   PSK  Koudy
B8:A3:86:A4:72:98  -87       91        0    0  11  54e. WPA2 CCMP   PSK  dlink-st

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   08:A9:5A:9E:D3:5B  -87    0 - 1     54       148  UPC2645633
(not associated)   40:F3:08:4A:A9:BE  -87    0 - 1      0        64
(not associated)   B4:CE:F6:6B:F2:D3  -86    0 - 1      0        12
64:70:02:FC:9A:02  28:E3:47:FA:43:31  -79    0 - 1      0       310  Proch837
```