Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Analýza bezpečnosti bezdrátových sítí vybraného ISP

Bakalářská práce

Lukáš Janouch

Školitel: Ing. Rudolf Vohnout, Ph.D.

České Budějovice 2018

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

ZADÁVACÍ PROTOKOL BAKALÁŘSKÉ PRÁCE

Student: Lukáš JANOUCH
(jméno, příjmení, tituly)

Obor – zaměření studia: Aplikovaná Informatika - Kriminalisticko-technická činnost v IT

Katedra: Ústav aplikované informatiky

Školitel: Rudolf Vohnout, Ing., Ph.D.
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Garant z PřF: .....
(jméno, příjmení, tituly, katedra – jen v případě externího školitele)

Školitel – specialista, konzultant: .....
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Téma bakalářské práce: *Analýza bezpečnosti bezdrátových sítí vybraného ISP*

Cíle práce:

Hlavní cíl práce:

- Analyzovat a vyhodnotit zabezpečení bezdrátových sítí vybraného komerčního ISP s důrazem na výchozí konfiguraci. Na základě provedeného průzkumu upozornit majitele nevhodně nastavených Wi-Fi sítí na existenci bezpečnostního rizika. Vzhledem ke zjištěným skutečnostem případně navrhnout široce aplikovatelnou změnu vedoucí ke zvýšení zabezpečení.

Úkoly v rámci teoretické části práce:

- Zmapování důvodů nutnosti zabezpečování Wi-Fi sítí
- Vytvoření uceleného přehledu bezpečnostních technik ochrany Wi-Fi sítí a přiblížení jejich slabin
- Představení jednotlivých typů útoků na bezdrátové sítě

Popis práce:

ISP v dnešní době poskytují nejen službu samotného internetového připojení, ale také řešení domácí bezdrátové sítě pro své zákazníky. Výchozí nastavení se v některých případech jeví jako sub-optimální a může vést k bezpečnostním rizikům spojeným s provozováním takové

sítě. Úkolem této práce je tato rizika analyzovat, vyhodnotit a navrhnout globálně aplikovatelné řešení, které povede ke zlepšení tohoto stavu.

Základní doporučená literatura:

WRIGHT Joshua and Johnny CACHE: *Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions 3rd Edition*. McGraw-Hill Education; 3 edition; March 16, 2015. 544 stran. ISBN: 978-0071827638

Financování práce:.....

Vedoucí práce: Rudolf Vohnout podpis : .....

U externích vedoucích fakultní garant práce.....podpis : .....

Garant oboru bak.. studia (nepožaduje se u zaměření „příprava na mag. studium biologie) .....

podpis : .....

Vedoucí katedry: Libor Dostálek podpis .....

Případný souhlas vedoucího ústavu AV .....podpis : .....

V Českých Budějovicích dne 21.2.2017

Převzal/a dne 21.2.2017 podpis : .....

Bibliografické údaje

Janouch L., 2018: Analýza bezpečnosti bezdrátových sítí vybraného ISP. [Analysis of wireless networks security of selected ISP. Bc. Thesis, in Czech.] – 92 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Anotace

Cílem teoretické části této bakalářské práce je vytvořit ucelený přehled týkající se bezpečnosti Wi-Fi sítí. Práce se zabývá tím, proč je nutné Wi-Fi sítě zabezpečovat, jaké možnosti zabezpečení se využívají a v čem tkví jejich případné nedostatky. Na konci teoretického rámce jsou pak rovněž shrnuty známé typy útoků na bezdrátové sítě a možné obrany proti nim. Praktická část práce má za cíl analyzovat a vyhodnotit zabezpečení bezdrátových sítí vybraného komerčního ISP s důrazem na výchozí konfiguraci a na základě zjištěných skutečností navrhnout řešení vedoucí ke zlepšení aktuálního stavu.

Klíčová slova

Wi-Fi, bezpečnost, SSID, defaultní heslo, autentizace, warwalking, slovníkový útok

Annotation

The aim of the theoretical part of this bachelor thesis is to create a comprehensive overview of security of Wi-Fi networks. The thesis deals with issues such as the importance of securing Wi-Fi networks, types of securing and their vulnerabilities. In the end of the theoretic framework, there is a list of common types of attacks on wireless networks and possible defense against them. The aim of the practical part of this thesis is to analyse and evaluate the security of the wireless networks of a chosen commercial ISP with the emphasis on the default configuration and based on the identified facts to propose a solution leading to the improvement of the current state.

Key words

Wi-Fi, security, SSID, default password, authentication, warwalking, dictionary attack

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne

Podpis studenta

.....

Poděkování

Rád bych poděkoval panu Ing. Rudolfu Vohnoutovi, Ph.D. za jeho cenné rady a věcné připomínky během zpracování této bakalářské práce. Poděkování patří též mé rodině za projevenou podporu během studia.

Obsah

1 Úvod 1
2 Důvody nutnosti zabezpečování Wi-Fi sítí 2
2.1 Snížení rychlosti 2
2.2 Odposlech dat a šíření malwaru 3
2.3 Spáchání trestného činu 3
2.3.1 Skutečné případy 4
2.4 Porušení smlouvy s ISP, blokace IP adresy či omezení stahování 4
2.5 Rozdíl mezi domácí a firemní Wi-Fi 5
2.5.1 Případ řešený soudním dvorem EU 5
3 Metody zabezpečení Wi-Fi sítí a jejich slabiny 7
3.1 Změna defaultního SSID a předsdíleného tajemství k Wi-Fi síti 7
3.1.1 Získání informací útočníkem 8
3.1.2 Používání obvyklého SSID 8
3.1.3 Nevhodné generování SSID a hesla výrobcem 9
3.1.4 Tvorba silného předsdíleného tajemství 10
3.2 Změna přístupového hesla do administrace routeru 11
3.3 Filtrování MAC adres 12
3.3.1 Podvržení MAC adresy 12
3.4 Skrytí SSID Wi-Fi sítě 13
3.5 WEP 14
3.6 WPA 15
3.6.1 Integrita dat 15
3.6.2 Šifrování 15
3.6.3 Autentizace 17
3.7 WPA2 19

3.7.1 Autentizace 19
3.7.2 Integrita 19
3.7.3 Šifrování 20
3.7.4 Slabá místa zabezpečení WPA2 21
3.8 První představení zabezpečení WPA3 24
4 Typy útoků na bezdrátové sítě 25
4.1 Odposlech 25
4.2 Falešný přístupový bod – Rogue AP 26
4.3 Man-in-the-Middle (MITM) 27
4.4 Warchalking, wardriving, warwalking 27
4.5 Útok na autentizační mechanismus 28
4.5.1 Slovníkový útok 28
4.5.2 Útok hrubou silou 29
4.5.3 Využití duhových tabulek – Rainbow tables 29
4.5.4 Obrana 30
4.6 DoS útoky 31
5 Současný stav 33
6 Hlavní východisko pro praktickou část 34
6.1.1 Zranitelnost modelu Technicolor TC7200 34
6.1.2 Zranitelnost modelu Ubee EVW3226 35
7 Metodologický postup 36
8 Stanovené cíle a hypotézy 37
9 Praktická část 38
9.1 Dotazníkové šetření 38
9.1.1 Shrnutí dotazníkového šetření 45
9.2 Reálný průzkum 46
9.2.1 Použité zařízení a software 46

9.2.2 Oblast průzkumu 47
9.2.3 Mapování dostupných Wi-Fi sítí 48
9.2.4 Vyfiltrování získaných dat 49
9.2.5 Promítnutí hledaných Wi-Fi sítí do mapy 49
9.2.6 Vyhledání majitele dané Wi-Fi sítě 50
9.2.7 Prověření zranitelnosti 52
9.3 Výsledky průzkumu 54
9.3.1 Wi-Fi sítě od UPC se změněným SSID 55
9.3.2 Prověření zranitelnosti nalezených sítí 57
9.3.3 Poskytnutí pomoci se změnou přednastavených údajů 61
9.3.4 Počet zranitelných zařízení 61
9.3.5 Informování zákazníků o existenci bezpečnostního problému 63
9.4 Žádost o vyjádření zaslaná samotnému UPC 64
9.5 Návrhy vedoucí ke zlepšení stavu 64
10 Závěr 67
Použitá literatura 69
Seznam obrázků 75
Seznam grafů 76
Seznam tabulek 77
Seznam použitých zkratek 78
Seznam příloh 80
Příloha 1: Návod pro modem Technicolor TC7200 81
Příloha 2: Návod pro modem Ubee EVW3226 87

1 Úvod

Využití Wi-Fi sítí, co se týče celosvětového přenosu dat, má na rozdíl od klasického kabelového připojení stále rostoucí tendenci. Za rok 2015 měly Wi-Fi sítě 55,2% podíl z internetového přenosu v rámci celého světa a v roce 2020 bude toto číslo ještě o několik procent vyšší, uvádí průzkum firmy Cisco s názvem *The Zettabyte Era: Trends and Analysis* z června roku 2016. (1) Hlavní předností Wi-Fi a bezdrátových sítí obecně je fakt, že není potřeba klást kabeláž a uživatelé tak mohou využít mobility připojených zařízení. Je nutné si však uvědomit, že tato přednost je v oblasti bezpečnosti naopak nevýhodou. Potencionální útočník se totiž pro vykonání jeho nekalých úmyslů nemusí připojit do sítě fyzicky, ale může se nacházet kupříkladu na ulici vedle domu či v sousedním bytě. Ne všichni vlastníci Wi-Fi sítí si však tuto skutečnost uvědomují a zabezpečení svých sítí podceňují. Uvedená nevědomost je hlavním důvodem vzniku této práce týkající se tématu bezpečnosti Wi-Fi sítí, jejíž cílem je vytvoření uceleného přehledu technik zabezpečování těchto sítí a jejich známých slabin tak, aby si čtenář mohl snadněji udělat představu o tom, jak nejlépe svou bezdrátovou síť zabezpečit.

Zvláštní důraz pak bude kladen především na důležitost změny přednastaveného SSID a přístupového hesla k Wi-Fi síti, což je, ač se jedná o jednu z nejzákladnějších technik v oblasti bezpečnosti, mnohdy opomíjeno. Cílem druhé části práce proto bude zjistit, jak velkou pozornost věnují majitelé Wi-Fi sítí právě změně těchto údajů.

Hlavním podnětem pro vznik této práce bylo především upozornění bezpečnostního analytika Petera Geisslera z počátku roku 2016. Ten přišel s informací o existenci bezpečnostního rizika, jež se týká Wi-Fi sítí jednoho z předních poskytovatelů internetového připojení v České republice, a to konkrétně společnosti UPC. Jedná se o možnost získání přednastaveného hesla z původního SSID u určitých typů modemů[1], jež má UPC ve své nabídce. (2) Z toho důvodu, že v době psaní této bakalářské práce stále existuje poměrně velké množství sítí s uvedenou bezpečnostní trhlinou, se bude druhá část práce zabývat zejména touto problematikou.

[1] Ačkoliv jsou daná zařízení označovaná jako modem, plní nejen funkci modemu, ale i routeru (směrovače) a přístupového bodu.

2 Důvody nutnosti zabezpečování Wi-Fi sítí

Nelze pochybovat o tom, že využití Wi-Fi sítí přináší mnoho výhod, ať již z pohledu snadné instalace dané sítě, nízkých nákladů na její realizaci či následnou mobilitu připojených klientů. I přes množství výhod, které Wi-Fi sítě skýtají, mají ovšem oproti těm kabelovým jednu významnou nevýhodu. Tato nevýhoda spočívá ve fyzické bezpečnosti. Útočník, který chce v rámci kabelové sítě provést kupříkladu odposlech přenášených dat, se musí fyzicky dostat ke kabelům, kterými daná komunikace probíhá. Jedná-li se však o síť bezdrátovou stačí mu pouze to, že je v dosahu signálu a daná síť je zabezpečená buď slabě, nebo není zabezpečená vůbec.

Existuje poměrně velké množství domácích Wi-Fi sítí, které nedisponují žádným zabezpečením a jsou tak volně přístupné komukoliv, kdo se nachází poblíž. Důvody, proč tomu tak je, mohou být různé. Může se jednat o nevědomost nutnosti zabezpečení Wi-Fi sítě, o absenci znalostí potřebných k nastavení své sítě, o pouhou lenost, či o dobrou vůli poskytnout svou Wi-Fi síť ostatním. Ať už je motiv majitelů nezabezpečených Wi-Fi sítí jakýkoliv, v této kapitole budou zmíněny důvody, proč je potřeba své Wi-Fi sítě vhodně zabezpečovat.

2.1 Snížení rychlosti

Kapacita přenosového pásma Wi-Fi sítí má pochopitelně své limity. Aby byla využita maximální možná přenosová rychlost, kterou daná Wi-Fi síť disponuje, musí být v daný okamžik připojeno pouze jedno aktivní zařízení. Je-li totiž k sítí připojeno další zařízení, dojde k rozdělení dostupných zdrojů tak, aby obě zařízení měla v podstatě stejné podmínky. Uživateli, který byl původně na Wi-Fi síti připojen sám, se tak po připojení dalšího klienta sníží rychlost zhruba na polovinu. Toto ovšem platí za předpokladu, že jsou daná zařízení neustále aktivní. V případě, že některý z uživatelů využívá síťové připojení pouze příležitostně, poskytuje router dostupnou šířku pásma především těm, kteří ho v daný okamžik potřebují. Stejně tak je rozdíl v tom, zda dotyčný pouze čte článek na webu, odesílá e-mail či zda sleduje stream v HD kvalitě. Z výše uvedeného každopádně vyplývá, že připojují-li se k domácí síti kromě členů dané domácnosti i další nezvaní hosté, může se tato skutečnost rapidně projevit na dostupné přenosové rychlosti. (3)

2.2 Odposlech dat a šíření malwaru

Útočník připojený do nezabezpečené Wi-Fi sítě rovněž může provádět odposlech dat, která putují po síti a tato data následně analyzovat. Není-li komunikace mezi internetovým prohlížečem a servery šifrovaná, může dotyčný získat obsah odesílaných zpráv, dostat se k informacím o kreditních kartách, přihlašovacím údajům či k jakýmkoliv jiným osobním údajům. (4) Je-li útočník připojen k dané Wi-Fi síti, vzniká navíc hrozba toho, že se dostane do zařízení v ní aktivních, díky čemuž se opět může dostat k důležitým datům – tím spíše obsahuje-li dané zařízení závažné bezpečnostní trhliny. Dalším problémem může být situace, kdy je na zařízení povoleno sdílení souborů v síti. Toho totiž útočník může využít k poměrně snadnému šíření malwaru neboli škodlivého softwaru, jehož cílem může být kupříkladu smazání dat, poškození systému či shromažďování určitých informací. Dotyčný může napadnout i samotný přístupový bod a využít ho k tomu, aby uživatelům, kteří se připojují, vyskočilo okno nabízející aktualizaci určitého softwaru. Neopatrný uživatel, který tuto možnost potvrdí, si místo aktualizace do svého počítače zavede právě zmiňovaný malware. (5)

2.3 Spáchání trestného činu

Pro někoho nemusí být ani doposud uvedené důvody dostatečným motivem si svou síť lépe zabezpečit, jelikož mu snížení dostupné rychlosti příliš nevadí a internet využívá pouze ke čtení na webu, takže o žádná citlivá data v podstatě přijít nemůže. Existuje však další podnět, proč se zabývat bezpečností své Wi-Fi sítě.

Pokud se někdo připojí prostřednictvím určité Wi-Fi sítě, vystupuje pod IP adresou routeru, což znamená, že ať již udělá na internetu cokoliv, stopy povedou právě k majiteli dané sítě. Pachatel tedy může skrze tuto síť kupříkladu vydírat osobu, se kterou se nepohodl, či ji jakýmkoliv jiným způsobem obtěžovat a dopouštět se tak protiprávního jednání. Další situací, která může nastat, je například zneužití sítě útočníkem pro rozesílání spamu, provedení kybernetického útoku, sdílení autorsky chráněných děl, podpora terorismu na sociálních sítích či v různých diskuzích, nebo třeba stahování a šíření dětské pornografie. (6) Vzhledem k tomu, že pachatel daný trestný čin spáchá prostřednictvím cizí Wi-Fi sítě, bude hlavním podezřelým právě její majitel. V takovém případě pak dotyčnému mohou být zabavena všechna zařízení (včetně routeru), která mohla být použita pro spáchání příslušného trestného činu, a to z důvodu následného provedení forenzní analýzy. Jedná-li

se o závaznější zločin, je zde rovněž riziko vzetí do vazby do doby, než se celá situace vyjasní. (7)

2.3.1 Skutečné případy

To, že může být Wi-Fi síť skutečně zneužita nepovolanou osobou ke spáchání trestného činu a hlavním podezřelým se pak stává její majitel, dokazuje hned několik případů, ke kterým došlo ve Spojených státech amerických. Nejčastěji se jednalo právě o síření či stahování velkého množství dětské pornografie.

Dané případy měly téměř stejný průběh, kdy do domu podezřelého vtrhli ozbrojení agenti FBI a majitele Wi-Fi obvinili ze spáchání trestného činu. Vzhledem k povaze daného trestného činu, ze kterého byli dotyční obviněni, asi není potřeba zmiňovat, že se policisté k podezřelým chovali poněkud nevybíravě. Taktéž došlo k zabavení všech zařízení, která mohla být ke spáchání zločinu využita. To může znamenat poměrně velký problém, pokud v nich obviněný má například důležité firemní materiály, které nezbytně potřebuje pro svou práci. Až po provedené forenzní analýze bylo zjištěno, že majitelé daných Wi-Fi sítí daný čin nespáchali a ve většině případů navíc stopy vedly k jejich sousedovi, který byl následně zatčen. Nicméně byla tato situace pro přítomné pravděpodobně velmi nepříjemnou, stresuplnou záležitostí a zřejmě si příště dají větší pozor, jak budou mít svou síť zabezpečenou. (7) (8) Navíc je nutné si uvědomit jednu zcela zásadní skutečnost. Je-li dotyčný obviněn kupříkladu ze stahování nebo šíření dětské pornografie, pravděpodobně se o tom dozví jak jeho příbuzní a známí, tak i širší okolí. Tím může dojít k nenávratnému poškození pověsti obviněného a to i přesto, že po nějakém čase vyjde najevo jeho nevina.

2.4 Porušení smlouvy s ISP, blokace IP adresy či omezení stahování

Ve smlouvě uzavřené s poskytovatelem internetového připojení, neboli s ISP[2], může být navíc uvedeno, že přístup k internetu přes Wi-Fi síť nesmí být sdílen s třetí osobou. V případě absence zabezpečení je možné, že bude tato podmínka porušena. Pokud bude navíc prostřednictvím dané sítě spáchán například již zmiňovaný kybernetický útok, může se stát, že bude síť poskytovatelem odpojena od internetu. (9, s. 288) Ten, kdo zneužije danou Wi-Fi síť kupříkladu k rozesílání SPAMu, nebo se bude nevhodně chovat v diskuzích na sociálních sítích či na jiných webových stránkách, může rovněž zapříčinit

[2] Anglická zkratka odvozená od Internet Service Provider.

uvedení IP adresy v Blacklistu[3], čímž dojde k zablokování přístupu na danou stránku i skutečnému vlastníkovi Wi-Fi sítě. Další problém, jenž může vzniknout provozováním otevřené či nedostatečně zabezpečené Wi-Fi, se týká stahování z určitých úložišť. Některá úložiště mají totiž omezení, kvůli kterému lze z jedné IP adresy provádět ve stejný okamžik pouze jedno stahování a tím pádem se objeví upozornění typu: *„Z této IP adresy právě probíhá stahování, je nutné vyčkat, až bude právě probíhající stahování dokončeno.“* Stejně tak existují webové stránky, na kterých je možné si z určité IP adresy založit pouze jeden účet. Zaregistruje-li se tedy na dané stránce některý z nezvaných hostů, skutečnému vlastníkovi sítě bude tato možnost odepřena.

2.5 Rozdíl mezi domácí a firemní Wi-Fi

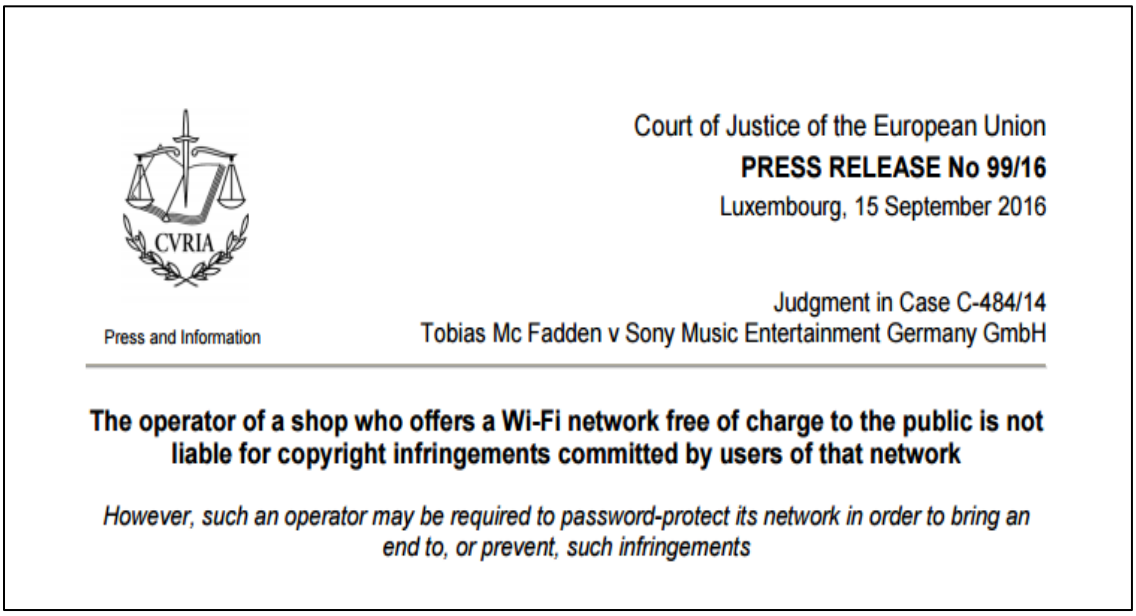
Je potřeba si ovšem uvědomit rozdíl mezi tím, zda bude některý z trestných činů, o kterých se hovořilo v kapitole 2.3, spáchán prostřednictvím domácí Wi-Fi sítě či sítě firemní. Vezmeme-li tedy v potaz, že se jedná o síť nezabezpečenou a tím pádem přístupnou v podstatě komukoliv. U firemní Wi-Fi sítě se totiž předpokládá, že může být využita prakticky kýmkoliv, a proto je na danou firmu nahlíženo jako na oběť, která byla ke spáchání daného zločinu pouze využita. Tím spíše jedná-li se například o internetovou kavárnu. Pokud se však jedná o domácí Wi-Fi síť, její majitel se naopak stává hlavním podezřelým. Přitěžující okolností pro majitele může být navíc to, že je kupříkladu studentem informatiky, IT specialistou či je o něm známo, že se v této oblasti vyzná a tím pádem věděl o možných rizicích otevřené sítě. (10)

2.5.1 Případ řešený soudním dvorem EU

To, že majitel otevřené veřejné sítě, kterou poskytuje široké veřejnosti ve svém baru, obchodu, kavárně či v jiných veřejných prostorách, nezodpovídá za činy, jež uživatelé dané sítě provedou, dokládá případ, který se udál již v roce 2010. Rozsudek k tomuto případu byl vynesen poměrně nedávno, a to v polovině září roku 2016. Soudní dvůr Evropské Unie projednával spor mezi Tobiasem McFaddenem, majitelem obchodu se světelnými a zvukovými aparaturami v Mnichově a mezi společností Sony Music Entertainment Germany. Tato společnost obvinila Tobiase Mcfaddena z toho, že prostřednictvím jeho firemní sítě někdo na internet nahrál album jedné z německých skupin, na které vlastnila autorská práva právě společnost Sony. Rovněž byl vznesen požadavek na uhrazení vzniklé

[3] Blacklistem IP adres se rozumí seznam IP adres, které mají zakázaný přístup.

škody. Soudní dvůr dal ovšem za pravdu McFaddenovi a rozhodl, že majitel otevřené sítě, která je volně přístupná pro veřejnost, není zodpovědný za její zneužití uživateli. (11) Rozhodnutí vydané soudním dvorem je k vidění na obrázku 1 umístěném níže.


Court of Justice of the European Union
PRESS RELEASE No 99/16
Luxembourg, 15 September 2016

Press and Information

Judgment in Case C-484/14
Tobias Mc Fadden v Sony Music Entertainment Germany GmbH

The operator of a shop who offers a Wi-Fi network free of charge to the public is not liable for copyright infringements committed by users of that network

However, such an operator may be required to password-protect its network in order to bring an end to, or prevent, such infringements

Obrázek 1: Rozhodnutí vydané soudním dvorem Evropské Unie. Obrázek převzat z (12)

Součástí rozhodnutí byl však i dodatek, který dává soudům možnost majitelům otevřených firemních Wi-Fi sítí nařídit, aby byla jejich síť zabezpečena heslem, a to v případě že by mělo docházet k obdobnému porušování autorských práv prostřednictvím jejich sítě opakovaně. V takovém případě by se nejprve uživatelé pro přístup na Wi-Fi síť museli autentizovat, čímž by pravděpodobně došlo ke snížení počtu spáchaných trestných činů. (11)

3 Metody zabezpečení Wi-Fi sítí a jejich slabiny

Ještě předtím, než budou představeny jednotlivé metody, které se využívají pro zvýšení bezpečnosti Wi-Fi sítí, je potřeba podotknout, že v některých společnostech se Wi-Fi sítě nepoužívají vůbec. Důvod spočívá právě v tom, že se lze do bezdrátové sítě připojit i z míst vně dané společnosti, čímž vzniká výrazné ohrožení celkové bezpečnosti. Pokud se útočník prostřednictvím Wi-Fi dostane do firemní sítě, může společnosti způsobit finanční ztráty či ve výjimečných případech dokonce zapříčinit její zkrachování. Získání citlivých dat nepovolanou osobou či zajištění nedostupnosti síťových služeb totiž může být pro danou firmu osudné. (13, s. 10) Tvůrci bezpečnostních politik dané firmy tak musí zhodnotit, zda výhody, které Wi-Fi sítě poskytují, převyšují možná bezpečnostní rizika. Je nutné si uvědomit, že i když daná bezdrátová síť disponuje nejmodernějšími bezpečnostními metodami, je možné, že i tyto metody budou v budoucnu prolomeny.

Pokud se ale firma či fyzická osoba rozhodne bezdrátovou síť používat, měla by se seznámit s možnými způsoby, jak rizika v oblasti bezpečnosti co nejvíce eliminovat a zajistit tak pro svou síť co nejlepší ochranu. Následující podkapitoly proto budou pojednávat o jednotlivých bezpečnostních technikách a jejich známých slabinách.

3.1 Změna defaultního SSID a předsdíleného tajemství k Wi-Fi síti

Zkratka SSID je odvozena z anglických slov Service Set Identifier a slouží k identifikaci Wi-Fi sítě. Přístupový bod vysílá signalizační rámce, takzvané beacon rámce, kterými ostatním zařízením oznamuje svou přítomnost. Z těchto rámců mohou jednotlivá zařízení, kromě jiného, zjistit právě zmiňované SSID, potřebné k připojení se do dané sítě. Vzhledem k tomu, že je díky existenci SSID možné zjistit, jaké Wi-Fi sítě jsou dostupné, jeví se jeho vysílání jako velmi užitečné. Z pohledu bezpečnosti je ovšem každá informace, kterou může potencionální útočník o Wi-Fi síti zjistit, nežádoucí. (14, s. 20) V kapitole 3.4 proto bude představen způsob, jakým lze vysílání SSID zakázat a částečně tak zamezit útočníkovi ve zjištění tohoto identifikátoru. O částečnou ochranu se jedná z důvodu toho, že i přes zákaz vysílání existují způsoby, kterými lze SSID dané sítě zjistit.

Tato podkapitola se však zabývá ještě základnějším krokem, který je potřeba učinit pro zvýšení bezpečnosti bezdrátové sítě. Jedná se o změnu přednastaveného SSID, tedy názvu dané sítě, a rovněž náhradu původního předsdíleného tajemství[4] k síti (dále také

[4] Často se používá rovněž anglický termín Pre-shared key nebo zkratka PSK.

„přístupové heslo“ či „heslo“). Jelikož je tato problematika hlavní náplní druhé části této práce, bude jí věnován poměrně velký prostor, aby bylo nastíněno, jak důležitou roli hraje právě změna původního identifikátoru a hesla Wi-Fi sítě. Výjimkou totiž není situace, kdy daná bezdrátová síť sice využívá moderní způsob šifrování, pro přístup k síti je vyžadována autentizace a v rámci bezpečnosti jsou implementovány další ochranné techniky, ale vzhledem k ponechání původního SSID a hesla mohou přijít všechny z těchto ochranných prvků nazmar. Níže jsou proto uvedeny důvody, proč je vhodné si jak přednastavené SSID, tak heslo změnit, a jaké aspekty brát v potaz během jejich tvorby.

3.1.1 Získání informací útočníkem

Přístupové body vysílají název Wi-Fi sítě, respektive SSID, které je definováno již výrobcem. Některé přístupové body šíří SSID, jež obsahuje název společnosti, která dané zařízení vyrobila. Pouze tato skutečnost může znamenat ohrožení bezpečnosti. Pokud totiž útočník zjistí výrobce daného přístupového bodu či se mu podaří určit, o jaký konkrétní model se jedná, může následně realizovat útok na některou ze známých zranitelností, typickou pro daného výrobce či příslušné zařízení. (15) Ačkoliv je tedy nepochybně vhodné si takový název změnit, jedná se pouze o nepatrné zvýšení bezpečnosti, jelikož lze výrobce daného zařízení zjistit i na základě znalosti MAC adresy, která je veřejně vysílaná.

V názvu sítě by se rovněž neměly objevovat osobní informace o daném majiteli. Cokoliv, co se o vlastníkovi sítě záškodník dozví, mu může nepochybně průnik do sítě významně ulehčit. Je-li totiž v názvu sítě uvedeno kupříkladu jméno či příjmení majitele, může útočník jednodušeji odhadnout heslo pro přístup do sítě. Se znalostí identity vlastníka sítě v dnešní době není obtížné získat cenné informace týkající se ať již jeho zaměstnání, koníčků či členů rodiny. Tím spíše, pokud má dotyčný na některé ze sociálních sítí vytvořen profil s nevhodně nastaveným soukromím. V závislosti na získaných informacích pak může útočník při troše štěstí heslo pro přístup do sítě odhadnout. Chce-li se útočník dostat do Wi-Fi sítě konkrétní osoby, přítomnost příjmení v SSID mu navíc ulehčí proces identifikace dané sítě. (16)

3.1.2 Používání obvyklého SSID

Stejně tak je nevhodné používat taková SSID, která jsou hojně rozšířená. Na internetu jsou totiž volně přístupné databáze, které mapují Wi-Fi sítě po celém světě a lze z nich zjistit například právě to, jaké názvy Wi-Fi sítí jsou nejčastější. Tuto informaci pak mohou útočníci zneužít při prolamování hesla do dané sítě a to za podmínky, že se jedná o síť, jejíž

autentizace je založena na před-sdíleném tajemství[5], které musí znát každý uživatel, který se do ní chce připojit. (17). Kryptografická hashovací funkce, která má na starost zašifrování přístupového hesla do nečitelné podoby, totiž využívá SSID jako sůl.[6] Výsledný hash je tak vytvořen nejen z přístupového hesla, ale i z názvu dané sítě. Ačkoliv je vzhledem k jednocestnosti kryptografických hashovacích funkcí prakticky nemožné původní hodnotu hesla zpětně dopočítat, existují takzvané duhové tabulky, které jsou spíše známé pod anglickým názvem Rainbow tables, pomocí nichž lze původní heslo zjistit. Tyto tabulky zjednodušeně řečeno fungují na principu prohledávání sebe samých do doby, než dojde k nalezení hledaného hashe a tím pádem i odpovídajícího hesla. Pokud je tedy název sítě jeden z nejčastěji používaných, může útočník využít již existující duhovou tabulku a nemusí tak plýtvat čas a zdroje při tvorbě své vlastní. (18)

Vzhledem k existenci před-vytvořených duhových tabulek by mělo SSID být co možná nejoriginálnější. Jelikož může být název tvořen až 32 znaky, je v podstatě možné vymyslet i celou větu či neobvyklé slovní spojení, díky čemuž bude zajištěno, že dané SSID není použito v již existujících duhových tabulkách.

3.1.3 Nevhodné generování SSID a hesla výrobcem

Výše zmíněný útok s využitím duhových tabulek ovšem představuje jak časově, tak výpočetně náročnou záležitost a šance na případný úspěch jsou relativně nízké. Pokud se tedy útočník nechce připojit na konkrétní Wi-Fi a stačí mu, když se dostane do jakékoliv sítě, může využít zranitelnosti, která se opět týká původního SSID a hesla. Tuto zranitelnost lze ovšem zneužít pouze u určitých modelů bezdrátových routerů. Někteří výrobci totiž před-sdílené tajemství či SSID generují z MAC adresy daného přístupového bodu, což je značně nezodpovědné. Pokud někdo odhalí, jakým způsobem je heslo generováno, může následně zjistit původní heslo v podstatě do jakékoliv sítě, které se tento problém týká. Obdobným problémem se bude zabývat praktická část této práce, ve které sice nebude řešen přímo případ generování přístupového hesla z MAC adresy přístupového bodu, ale ze sériového čísla.

Pro lepší představu bude jeden příklad týkající se nevhodného generování SSID a hesla zmíněn již nyní. Konkrétně se jedná o zařízení WR702N společnosti TP-Link. U tohoto modelu je přednastavené heslo k bezdrátové síti totiž vytvořeno z posledních osmi znaků

[5] Princip tohoto způsobu autentizace je rozebrán v podkapitole 3.6.3
[6] Je-li spolu s heslem použita i nějaká sůl, výsledný hash je pro totožná hesla s různou solí odlišná.

MAC adresy a SSID má podobu vycházející z formátu TP-Link_xxxxxx, kde je namísto písmen x použito posledních šest znaků MAC adresy. (19) Tato skutečnost je zachycena na obrázku 2.

Obrázek 2: Odvození SSID a hesla z MAC adresy u routeru TP-Link. *Obrázek převzat z (28)*

Vzhledem k tomu, že lze podobu celého hesla zjistit z posledních 8 znaků MAC adresy routeru, nebude pro kohokoliv problém se do takové sítě dostat. Tím spíše, že je posledních 6 znaků hesla navíc uvedeno i v samotném názvu sítě.

3.1.4 Tvorba silného předsdíleného tajemství

Při tvorbě silného hesla existuje několik základních zásad, které lze využít i při změně původního předsdíleného tajemství k Wi-Fi síti. Prvním důležitým aspektem je délka hesla. Dostatečnou délku hesla je ovšem nutné zkombinovat ještě s dalšími zásadami pro tvorbu hesel. Vhodné je použití jak malých, tak velkých písmen, čísel ale také různých speciálních znaků. Za ideální heslo se dá považovat takové, které je tvořeno náhodnou posloupností různých znaků a je dostatečně dlouhé. Jako minimální délka hesla se obvykle doporučuje 8 či 9 znaků, jako ideální délka se pak zpravidla uvádí 14 a více znaků. Je sice pravdou, že se lidé často snaží vymýšlet taková hesla, která si mohou snadno zapamatovat, což je u náhodné posloupnosti znaků, čísel či speciálních znaků obtížné. Na druhou stranu je však nutné si uvědomit, že heslo k Wi-Fi síti uživatel obvykle zadává pouze při prvním přihlášení z daného zařízení. Při dalších přihlášeních se již zařízení zpravidla připojí automaticky bez nutnosti zadání hesla. Ačkoliv je tedy dlouhé a složité heslo těžší

na zapamatování a rovněž jeho zadávání zabere o něco více času, je to pouze malá daň za výrazné zvýšení celkové bezpečnosti dané sítě.

Při vymýšlení nového hesla je vhodné vyhnout se použití osobních údajů či údajů, které si může kdokoliv zjistit například prostřednictvím sociálních sítí. Rovněž je dobré se vyhnout použití běžně používaných slov a namísto nich volit slova neobvyklá. Hesla, která jsou tvořena ze slov, se kterými se lze setkat prakticky dennodenně, jsou totiž velmi náchylná na prolomení slovníkovým útokem. Stejně tak by se v heslu zcela jistě neměla objevit část názvu Wi-Fi sítě nebo dokonce název celý. Na závěr je ještě potřeba zmínit, že není vhodné mít heslo k Wi-Fi napsané na viditelném místě či uložené v otevřené podobě.[7] Pokud je ovšem nutné heslo písemně poznamenat, ať již z důvodu jeho složitosti či z obavy o jeho zapomenutí, je potřeba se ujistit, že k němu mají přístup pouze ti, kteří jsou oprávněni danou Wi-Fi síť využívat.

3.2 Změna přístupového hesla do administrace routeru

Vzhledem k tomu, že je router vstupní bránou do lokální sítě, je potřeba na jeho zabezpečení klást velký důraz. Kromě změny SSID a přístupového hesla k síti by tak mělo být nepochybně nastaveno i nové heslo pro přístup do administrace routeru. Získání kontroly nad routerem pro útočníka znamená, že má přístup k datům, jež si posílají jednotlivá zařízení v síti, nebo která putují přes router směrem do, respektive ze sítě. V posledních letech jsou právě z tohoto důvodu útoky na routery, ať již drátových či bezdrátových sítí, poměrně časté. Tyto útoky zpravidla fungují na tom principu, že je využita zranitelnost původního hesla k administraci, jelikož se jedná o hesla triviální a navíc snadno zjistitelná z různých volně přístupných databází.

Útok obvykle spočívá v podstrčení javascriptu útočníky na určité webové stránky a to s cílem napadnout počítač uživatele, který infikovanou stránku navštívil. Po té, co je uživatelovo zařízení napadeno, se snaží škodlivý kód připojit na typické lokální IP adresy do administrace routeru, jakou je například adresa 192.168.1.1. V závislosti na tom lze zjistit výrobce routeru nebo dokonce i konkrétní model. Vzhledem k tomu, že výrobci nastavují do administrace obvykle stejná hesla, je získání přístupu do administrace pouze otázkou času. Cíl útoku spočívá ve změně právě používaného DNS serveru na některý, který patří útočníkům. (20) Díky tomuto pak útočníci mohou oběť, která zadá do adresního

[7] Nehovoříme-li tedy o heslu k veřejně přístupné Wi-Fi síti.

řádku například adresu k internetovému bankovnictví, přesměrovat na podvodnou stránku se stejným vzhledem. Zadá-li oběť přihlašovací údaje ke svému bankovnictví, ve skutečnosti je odešle přímo útočníkům, kteří se pak jednoduše dostanou k penězům na účtu. (21) Stejně tak mohou útočníci zajistit, aby byla odesílaná data posílána k cíli přes ně a oni tak mohli danou komunikaci odposlouchávat. Útočníci ale nemusí pouze získávat důležité informace z odesílaných dat, danou síť totiž mohou po ovládnutí routeru například zapojit do DDOS útoku.

Útok však nemusí přijít pouze z vnějšku dané sítě. Pokud síť disponuje slabým zabezpečením či je dokonce otevřená, může se do administrace přihlásit v podstatě kdokoliv, kdo je připojen na dané síti (vezmeme-li tedy v potaz, že nebylo změněno původní heslo k administraci routeru). Ať již se ale jedná o útok realizovaný z vnějšku či zevnitř dané sítě, řešení tohoto problému spočívá v nastavení silného hesla k administraci. Rovněž by mělo dojít ke kontrole toho, zda jsou správně nastaveny DNS servery a zda je aktuální firmware směrovače, čímž lze taktéž zabránit využití některé ze zranitelnosti daného modelu. (22)

3.3 Filtrování MAC adres

Na základě existence MAC adres, tedy jedinečného identifikátoru síťového zařízení, vznikla další metoda pro zvýšení bezpečnosti, kterou je filtrování MAC adres. Jedná se o techniku, kdy je přístup k síti umožněn pouze určitým zařízením v závislosti na jejich MAC adrese, což lze nastavit v administraci routeru. Existují dva různé postupy, které se dají aplikovat. Prvním z nich je použití takzvaného Blacklistu, kdy se specifikují pouze ty MAC adresy, kterým má být přístup do sítě zakázán. Všem ostatním síťovým kartám je pak připojení do Wi-Fi sítě umožněno. Vzhledem k tomu, že se záškodník, kterému je tímto způsobem zamezen přístup do sítě, může pokusit připojit prostřednictvím jiného síťového adaptéru, je vhodnější využívat Whitelist, tedy seznam, ve kterém figurují pouze ty MAC adresy, kterým je přístup povolen. Jakákoliv jiná síťová karta se tedy do sítě nedostane. (23, s. 132)

3.3.1 Podvržení MAC adresy

Filtrování MAC adres by bylo poměrně účinnou metodou za předpokladu nemožnosti MAC adresu síťové karty změnit. Některé síťové karty ovšem disponují ovladačem, který poskytuje možnost změny tohoto identifikátoru. Navíc existuje celá řada volně dostupných programů, které toto taktéž umožňují. Podvržení MAC adresy funguje na tom principu, že

je do odesílaných paketů zapisována jiná MAC adresa, než ta, která byla síťové kartě skutečně přidělena již při výrobě. (24) Vzhledem k absenci šifrování hodnot zdrojové a cílové MAC adresy v paketech není pro útočníka problém v rámci bezdrátové sítě komunikaci mezi autorizovaným zařízením a přístupovým bodem odposlechnout a v závislosti na tom svou MAC adresu změnit. Ať již se tedy router rozhoduje na základě seznamu s povolenými či zakázanými MAC adresami, jedná se o ochranu pouze částečnou, jelikož ji lze poměrně jednoduše obejít. Na druhou stranu však může i tato maličkost potencionálního útočníka odradit a pro jeho nekalou činnost si raději vybere méně zabezpečenou Wi-Fi síť. (14, s. 22)

3.4 Skrytí SSID Wi-Fi sítě

Pro zvýšení bezpečnosti Wi-Fi sítě se často doporučuje skrýt SSID neboli zakázat jeho vysílání. Důvod je prostý, pokud Wi-Fi síť není zobrazena v seznamu dostupných sítí, je méně pravděpodobné, že se na ní připojí nezvaný host. Jedná-li se však o někoho, kdo se do dané sítě chce skutečně dostat, zákaz vysílání SSID není překážkou, která by ho mohla zastavit.

Pokud přístupový bod nevysílá SSID, znamená to, že v beacon rámcích je hodnota SSID nastavena na NULL, jinými slovy tedy v poli pro SSID není v podstatě nic. Avšak zařízení, která se chtějí k síti připojit, musí poslat žádost, ve které je SSID dané sítě uvedeno a název sítě se pak rovněž objevuje v odpovědi přístupového bodu. (25) Tím pádem není pro útočníka žádný problém, aby poměrně snadno a rychle odhalil i skrytou síť. Využít k tomu může například nástroje, jako jsou Kismet, NetStumbler nebo inSSIDer. Podobných nástrojů, jako jsou výše zmiňované, je celé množství a některé z nich jsou dokonce dostupné zcela zdarma. (26)

Zakázáním vysílání SSID navíc vznikají nepříjemnosti, které mohou leckoho od skrytí své sítě odradit. V první řadě zde vzniká nevýhoda ve směru toho, jak rychle je možné se do sítě připojit. Je-li síť zobrazena mezi dostupnými sítěmi, lze se jednoduše připojit zadáním hesla. Pokud je ovšem síť skrytá, musí být kromě hesla zadáno rovněž samotné SSID a použité zabezpečení dané sítě. Některá zařízení mají navíc problém se ke skryté síti vůbec přihlásit. Jedná se především o mobilní telefony s operačním systémem android. (27) Pokud se navíc jedná o velkou firemní síť či jinou síť velkého rozsahu, je tato síť pravděpodobně tvořena více přístupovými body, které jsou rozmístěny tak, aby pokrývaly celou oblast. Je-li ovšem zakázáno vysílání SSID, klient se z beacon rámců nedozví, který přístupový

bod mu nabízí nejsilnější signál. Jinými slovy tedy připojené zařazení nezíská informaci o tom, který z přístupových bodů v daný okamžik poskytuje nejstabilnější připojení. (14, s. 22) Kromě toho se mohou u skryté sítě vyskytnout problémy s automatickým připojením, což vede k nutnosti zadávat výše zmíněné údaje při každém přihlášení.

3.5 WEP

Zkratka WEP je odvozena od anglického sousloví Wired Equivalent Privacy, z čehož se dá odvodit smysl vzniku tohoto protokolu. WEP byl totiž vytvořen z důvodu toho, aby byla bezpečnost v bezdrátových sítích srovnatelná s tou, již lze zajistit v rámci sítí kabelových. Hlavní úloha zabezpečení WEP spočívá v zajištění ochrany přenášených dat proti odposlechu, a to díky jejich zašifrování. Kromě toho se rovněž využívá při autentizaci klientů a pro ověření integrity dat. (14, s. 45–50). Vzhledem k faktu, že tvůrci WEPu nebyli zkušení odborníci na kryptografii ani síťovou bezpečnost obecně, začalo postupem času na povrch vyplývat více a více nedostatků tohoto zabezpečení a v současné době lze WEP prolomit během několika málo minut. Jako mnohem rozumnější alternativa k tomuto zabezpečení se tedy jeví použití WPA, ideálně WPA2.

Jelikož by se v současné době již WEP v žádném případě pro zabezpečení Wi-Fi sítí neměl používat, není nutné tento typ zabezpečení podrobněji představovat a níže tedy bude uveden pouze výčet některých z jeho slabin. (28, s. 9–13), (29), (30), (14, s. 47)

- Použití krátkého šifrovacího klíče, který je navíc statický a nemění se tedy v čase.
- Veškerý přenos je šifrován stejným WEP klíčem (jedná se o přístupové heslo k síti) – se znalostí přístupového hesla tedy lze rozšifrovat veškerou komunikaci na příslušné bezdrátové síti.
- Nesplnění základního požadavku šifry RC4, který říká, že nesmí dojít k zašifrování dvou různých zpráv stejným šifrovacím klíčem – inicializační vektor, který má toto zajistit je příliš krátký (24 bitů) a po určité době se tak začnou hodnoty opakovat.
- Nelze provést automatickou výměnu klíčů – pokud dojde například ve firmě ke ztrátě notebooku některého ze zaměstnanců, musí dojít k manuální výměně klíčů na všech zařízeních.
- Možnost pozměnit kontrolní součet CRC-32 z přenášených dat tak, aby na straně příjemce nebylo odhaleno, že byla narušena integrita přenášené zprávy.
- Absence ochrany proti replay útokům – útočník může opakovaně odesílat totožný požadavek přístupovému bodu, který je nucen odesílat odpovědi, čímž dochází

k tvorbě nových paketů a tedy i použití nových inicializačních vektorů. Tímto způsobem pak může útočník daleko rychleji nasbírat dostatečný počet IV pro dešifrování komunikace.

- Autentizace na základě sdíleného tajemství je pouze jednocestná – přístupový bod sice ověřuje, zda daný klient disponuje přístupovým heslem, ale klient si naopak pravost přístupového bodu ověřit nemůže. Tato skutečnost tedy poskytuje prostor pro tvorbu falešných AP.

3.6 WPA

Vzhledem k existenci řady nedostatků v protokolu WEP bylo potřeba vyvinout alternativní řešení, jež tyto mezery vyplní. Pracovní skupina 802.11i tedy započala vývoj nového bezpečnostního mechanismu, který je dnes známý pod označením WPA2. Výrazným vylepšením v rámci bezpečnosti bezdrátových sítí mělo být především řízení přístupu do sítě a použité šifrování komunikace. Kvůli stále rostoucí nedůvěře v zabezpečení WEP již ovšem nebylo možné čekat na dokončení a ratifikaci[8] WPA2 a proto vznikla jakási podmnožina nazvaná jako WPA, jež zahrnovala již existující implementace, které měly být použity právě v rámci WPA2. Vznik tohoto zabezpečení byl ohlášen Wi-Fi Alliancí[9] 31. října 2002 a během dubna následujícího roku došlo k certifikaci prvních zařízení, jež WPA podporovaly. (14, s. 71), (23, s. 135)

3.6.1 Integrita dat

WPA využívá výrazně bezpečnější způsob kontroly integrity dat, než jakým byl samotný CRC-32 používaný zabezpečením WEP. Konkrétně se jedná o přidání podpory protokolu MIC (Message Integrity Code), který provádí kontrolu integrity pomocí algoritmu Michael. Jde o jednocestnou hashovací funkci, jejímž vstupem je datová část v otevřené podobě, zdrojová a cílová MAC adresa, pořadové číslo paketu a náhodná hodnota. Díky práci se zdrojovou i cílovou adresou je tedy možné provést ověření integrity nejen dat samotných, ale i pravosti MAC adres. (31, s. 97)

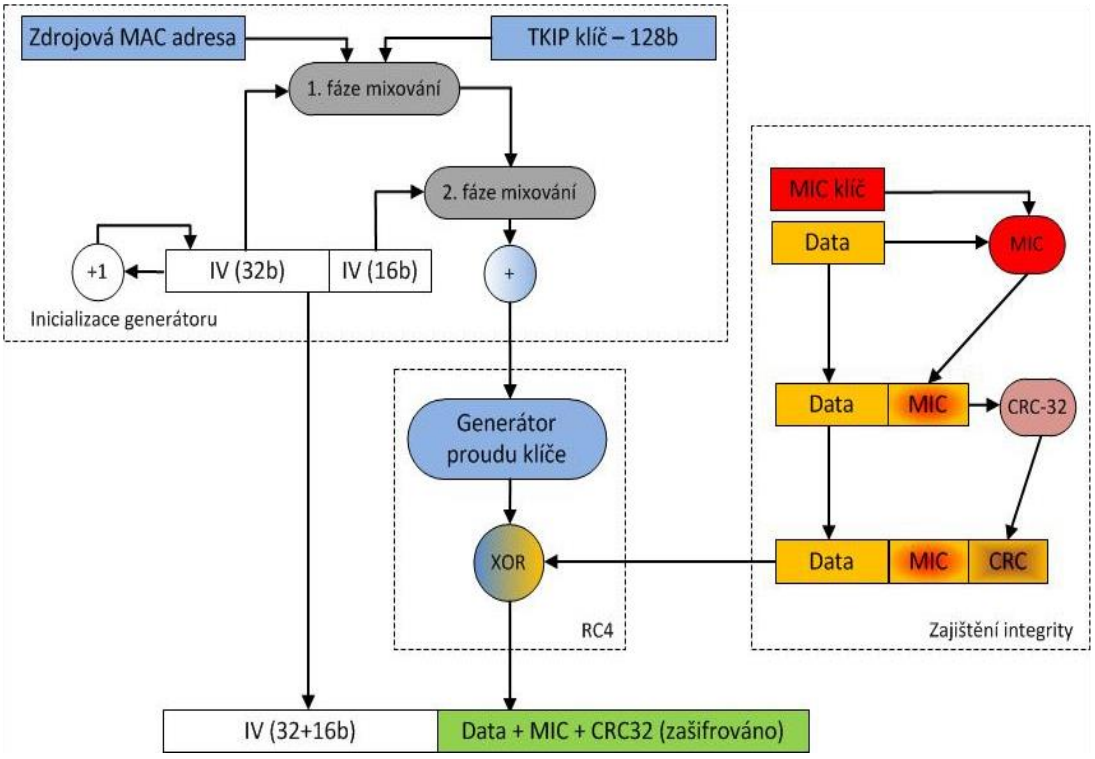
3.6.2 Šifrování

Jelikož je protokol WPA pouze jakousi přechodovou fází mezi WEPem a chystaným zabezpečením WPA2, kladl se důraz na to, aby bylo možné WEP nahradit pouze upgradem

[8] Ratifikací se rozumí potvrzení platnosti, zpravidla velmi důležitého, dokumentu.
[9] Nezisková organizace, kterou tvoří většina výrobců bezdrátových zařízení.

softwaru, respektive firmwaru na daných zařízeních. Pro implementaci WPA tedy není nutné kupovat nové hardwarové prostředky. K tomuto účelu byl využit šifrovací mechanismus TKIP, při jehož návrhu byl sice kladen velký důraz na eliminaci známých slabin WEPu, ovšem za učinění různých kompromisů. Z důvodu zpětné kompatibility byl tedy opět využit šifrovací algoritmus RC4. (14, s. 72–73)

Hlavní rozdíl oproti statickému WEPu ale spočívá v práci s dynamickými klíči, které jsou automaticky nahrazovány každých 10 000 paketů. Vyšší bezpečnost je pak rovněž zajištěna použitím delších, 48 bitů dlouhých, inicializačních vektorů spolu se 128bitovými klíči. Také inicializace algoritmu RC4 je mnohem sofistikovanější a tím pádem i bezpečnější. Na rozdíl od WEPu, kde dochází k pouhému připojení WEP klíče za inicializační vektor, jsou zde definovány dvě fáze, které zajišťují promíchání vstupních hodnot. Nejprve dojde k promíchání 128bitového TKIP klíče s MAC adresou daného zařízení a 32 bity IV. Výsledná hodnota je pak v druhé fázi smíchána znovu se 128bitovým TKIP klíčem a zbývajícími 16 bity inicializačního vektoru. Konečný výstup nabývá délky 128 bitů a je použit pro inicializaci proudové šifry RC4. (28, s. 15) Proces zašifrování dat pomocí protokolu TKIP a zajištění integrity zachycuje obrázek 3.



Obrázek 3: Proces šifrování přenášených dat protokolem TKIP. Převzato z (28, s. 15)

Výše zmíněný protokol TKIP je ovšem v dnešní době považován za zastaralý, a vzhledem k možnosti jeho prolomení byl u zabezpečení WPA2 nahrazen protokolem AES. Každopádně z důvodu zpětné kompatibility existuje i varianta WPA2 zahrnující TKIP.

3.6.3 Autentizace

Zabezpečení WPA nabízí dva možné způsoby řízení přístupu do bezdrátových sítí. Využit může být buď režim s předsdíleným tajemstvím, nebo autentizace realizovaná na základě standardu IEEE 802.1x. První z uvedených technik se používá zpravidla v rámci zabezpečení domácích sítí, a do určité míry je podobná režimu se sdíleným klíčem, který byl využit již WEPem. Z hlediska ochrany sítě se ovšem jedná o mechanismus mnohem sofistikovanější a bezpečnější. Druhá autentizační metoda je pak využívána především v prostředí firemním.

Autentizace s využitím PSK

Jedná se o metodu, kdy je pro autentizaci klientských zařízení použit předsdílený klíč neboli PSK (Pre-Shared key). Uživatelé, kteří se chtějí do dané sítě připojit, musí znát sdílené tajemství, tedy heslo, které může nabývat 8 až 63 znaků. Na základě hodnoty hesla a SSID dojde pomocí kryptografické hashovací funkce k vypočtení 256 bitů dlouhého klíče nazývaného PMK. Z výsledné hodnoty, kterou nabývá klíč PMK, dojde během handshaku mezi klientem a přístupovým bodem k vypočtení klíče PTK, který zajišťuje šifrování komunikace mezi danými zařízeními.[10] K výpočtu PTK je kromě PMK nutná znalost MAC adres komunikujících zařízení a vygenerovaných náhodných čísel zvaných ANonce a SNonce. Jak již bylo řečeno, pro zajištění vyšší bezpečnosti dochází k výměně těchto klíčů každých 10 000 paketů. Klíč PTK navíc není konečnou formou, která je pro zabezpečení komunikace využita. Tento klíč se totiž skládá z více dočasných částí, které mají svou vlastní specifickou funkci. V průběhu použití jsou tyto dočasné klíče aktualizovány a poté, co se klient odpojí, dojde k jejich zrušení. (32)

Autentizace s využitím IEEE 802.1x

Ačkoliv byl protokol 802.1x původně určen pro řízení přístupu v rámci metalických sítí, našel postupem času své využití rovněž v sítích bezdrátových. V součinnosti s protokolem EAP lze provádět autentizaci všemi možnými způsoby, ať už se jedná o využití

[10] Obdobou PTK je pak GTK s tím, že tento typ klíče má své využití při komunikaci typu multicast, respektive broadcast.

uživatelského jména a hesla, autentizaci pomocí certifikátů, tokenů, PKI, čipových karet, biometriky či dalších technik. Vzhledem k tomu, že EAP představuje otevřený standard, není navíc problém do něho v budoucnu implementovat nově vzniklé autentizační metody.

Princip protokolu 802.1x je založen na třech základních komponentách. Jde o žadatele, autentizátor a autentizační server. Žadatelem se rozumí aplikace na straně klienta, který se chce připojit do sítě. Autentizátor představuje aplikaci na síťové straně (přístupovém bodě) povolující či blokující přístup do dané sítě. Posledním ze tří základních komponent je pak autentizační server, který poskytuje autentizační informace autentizátoru. Princip autentizace s využitím 802.1x je následující. Autentizátor vysílá v určitých intervalech žádosti o autentizaci, na něž musí odpovědět každá stanice, jež se chce do sítě připojit. Jednotlivé stanice totiž před úspěšnou autentizací mohou s daným autentizátorem komunikovat jen prostřednictvím protokolu EAP. Veškerá ostatní komunikace je bezpodmínečně blokována. Poté, co jsou uživatelem zadány přihlašovací údaje, dojde k jejich přeposlání autentizátorem směrem k autentizačnímu serveru. Ten uživatelem odeslané informace ověří a na základě toho příslušnému uživateli povolí či zamítne vstup do dané sítě. (14, s. 79–81)

Mód 802.1x mimo jiné rovněž řeší existenci problému, který se týká všech sítí umožňujících připojení na základě znalosti sdíleného tajemství. Vzhledem k tomu, že se v dnešní době téměř každé zařízení připojuje do sítě automaticky, může nastat bezpečnostní problém i v případě, kdy je některému z uživatelů dané zařízení odcizeno. V takovém případě totiž přístup do sítě získá i neautorizovaná osoba. Pokud by se navíc jednalo o zaměstnance, který se prostřednictvím ať už odcizeného mobilního telefonu či notebooku automaticky připojoval do firemní sítě, muselo by po ohlášení krádeže dojít k výměně hesla na všech přístupových bodech dané sítě a na všech klientských zařízeních. Tato skutečnost může být v rámci firemní sítě čítající velké množství zaměstnanců zdlouhavá a především znepokojující. Stejně tak by muselo docházet ke změně hesla pokaždé, když někdo v dané firmě přestane pracovat. Z tohoto důvodu je použití sdíleného hesla pro připojení do firemní sítě, či jiných rozsáhlých sítí, krajně nevhodné a měla by být využita autentizace prostřednictvím mechanismu 802.1x, díky kterému se každý uživatel připojuje na základě znalosti svých vlastních přihlašovacích údajů. (33)

3.7 WPA2

Začátek používání bezpečnostního standardu IEEE 802.11i, který je dnes z důvodu návaznosti na WPA označován jako WPA2, se datuje již k roku 2006. V současné době je toto zabezpečení ve spojení se šifrovacím mechanismem AES stále považováno za nejbezpečnější ze všech nabízených variant. Na rozdíl od WPA je zde AES již povinností, zatímco protokol TKIP představuje pouze možnost zachování zpětné kompatibility. Každopádně je potřeba zmínit, že TKIP ať už v součinnosti s WPA nebo WPA2 je méně bezpečný než modernější AES. (34, s. 34–35) Vzhledem k tomu, že jsou šifrovací algoritmy implementovány již v samotném hardwaru, ať už tedy v přístupových bodech či na síťových kartách jednotlivých zařízení, nebylo možné pro podporu standardu IEEE 802.11i provést pouhou aktualizaci firmwaru. Všechna zařízení, která chtějí být certifikována označením „Wi-Fi“, tak musí od března roku 2006 podporovat standard IEEE 802.11i. Podporu WPA2 bylo navíc nutné zajistit i v operačních systémech koncových stanic. (28, s. 25)

3.7.1 Autentizace

Stejně tak jako tomu bylo u WPA, poskytuje i WPA2 dva základní způsoby autentizace, a to autentizaci s využitím předsdíleného tajemství, neboli WPA2-PSK, či řízení přístupu s existencí autentizačního serveru, také označované jako WPA2-802.1x. V závislosti na vhodnosti použití obou uvedených variant, je první z nich často také označována jako WPA2-Personal a druhá jako WPA2-Enterprise, a to vzhledem k tomu, že implementace infrastruktury 802.1x se obvykle vyplatí spíše jen v rozsáhlejším firemním prostředí, kde se výrazné zvýšení bezpečnosti vyplatí na úkor vyšších nákladů spojených se zavedením této technologie. Naproti tomu přítomnost společného tajemství pro všechna zařízení v síti je pak typická pro osobní, lépe řečeno domácí, bezdrátové sítě. (35)

3.7.2 Integrita

Pro ověření toho, že nebyla narušena integrita přenášené zprávy, je zde opět využit mechanismus nazývaný MIC. Nespoléhá se již ovšem na algoritmus Michael, který byl součástí protokolu TKIP, ale funguje na zcela jiném principu. Pro vypočtení kódu MIC je využit algoritmus CBC-MAC. (14, s. 76) Ten zajišťuje šifrování počátečního Nonce bloku (pseudonáhodné číslo), jež je odvozen z polí Priorita, zdrojová adresa odesílaných dat a

zvýšeného PN[11]. Takto získaný kód je následně připojen k nešifrovaným datům pro šifrování AES v režimu čítače. MIC tedy pracuje stejně jako AES v 128bitových blocích a je postupně vypočten z každého bloku dané zprávy až na její konec, kdy je zjištěna konečná hodnota. Ačkoliv se jedná o hodnotu 128bitovou, první polovina bitů se zahodí a přenáší se tak pouze druhá část, která odpovídá 8 bajtům, tedy velikosti pole MIC. (36, s. 50–51)

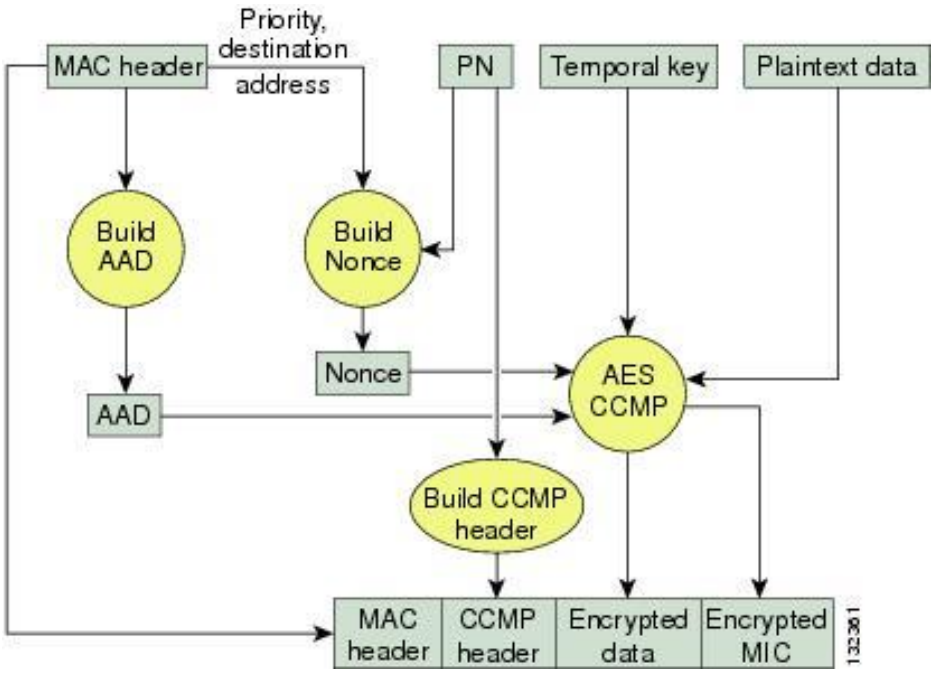
3.7.3 Šifrování

WPA2 zajišťuje šifrování přenášených dat pomocí šifry AES, která byla vytvořena s cílem nahradit dříve používaný algoritmus RC4. AES je úzce spjat s protokolem CCMP, jež slouží jako náhrada za TKIP a ve specifikaci 802.11i pracuje v režimu čítače. Zatímco tento režim slouží k šifrování dat, autentizace a integrita je realizována dle protokolu CBC-MAC. (37, s. 13) Jelikož se stejně jako u RC4, používá totožný klíč jak pro šifrování, tak pro následné dešifrování, spadá AES do šifer se symetrickým klíčem. Výraznou změnou je však upuštění od lineárního způsobu šifrování XORováním každého bajtu dat s náhodnou sekvencí. AES totiž spadá do kategorie blokových šifer, a proto šifrování dat probíhá po 128bitových blocích. Velký rozdíl spočívá také v tom, že se jak pro šifrování, tak zajištění integrity používá stejný klíč, ačkoliv tedy s různými inicializačními vektory. Přesto CCMP disponuje řadou vlastností, které se nacházely i u protokolu TKIP. Jedná se kupříkladu o použití 128 bitů dlouhého dočasného šifrovacího klíče, který je odvozen na základě autentizačního procesu. Stejně tak je zachována obdoba 48bitového inicializačního vektoru, který je zde označován jako „číslo paketu“ neboli PN.

Zjednodušený princip šifrovacího mechanismu AES spočívá v následujícím. Poté co dojde k inicializaci šifry AES, která je založena na inicializačních vektorech a dalších informacích z hlavičky, dojde k vytvoření 128bitového bloku na výstupu. Text v otevřené podobě, který má být zašifrován, je rozdělen na několik bloků o délce 128 bitů. Počet těchto bloků se pochopitelně odvíjí od velikosti dané zprávy. V každém kroku je pak postupně brán jeden blok za druhým a za použití operace XOR je spojen se 128bitovým výstupem získaným v kroku předchozím. Toto se provádí do doby, než dojde k zašifrování celé zprávy. (14, s. 76–77) Protokol CCMP k uživatelským datům navíc vkládá 16 bajtů, které jsou nezbytné pro následné dešifrování či ověření integrity. Prvních 8 bajtů je využito pro sestavení hlavičky CCMP, dalších 8 pak pro pole MIC. Hlavičkou CCMP se rozumí

[11] Zkratka ze slov packet number, jedná se tedy o číslo paketu.

nešifrované pole nacházející se mezi hlavičkou MAC a šifrovanými daty. Je zde uložena 48bitová hodnota PN (Packet Number) a 16bitová hodnota Group Key KeyID[12]. Hodnota PN se pro každá následná data zvýší o jedna. (36, s. 50) Schéma šifrování dat symetrickou blokovou šifrou AES je zachyceno na obrázku 4 níže.



Obrázek 4: Schéma šifrování dat symetrickou blokovou šifrou AES. *Obrázek převzat z (38, s. 13 – kapitola 4)*

3.7.4 Slabá místa zabezpečení WPA2

Vzhledem k tomu, že je zabezpečení WPA2 spolu s šifrovacím mechanismem AES stále nejpřijatelnější dostupnou variantou z pohledu bezpečnosti Wi-Fi sítí, budou v této kapitole rozebrána zranitelná místa tohoto typu zabezpečení. Ačkoliv ještě donedávna bylo zabezpečení WPA2 považováno za zcela bezpečné – bez přítomnosti jakýchkoliv významnějších zranitelných míst, v době, kdy byla napsána podstatná část teoretického rámce této bakalářské práce, se začaly objevovat zprávy o tom, že zabezpečení WPA2 bylo prolomeno. V závislosti na tomto zjištění tak byla tato kapitola doplněna o útok zvaný KRACK, který využil doposud neznámé zranitelnosti tohoto zabezpečení.

Slabé přístupové heslo

Prvním způsobem, jak prolomit zabezpečení WPA2 spočívá ve zjištění přístupového hesla k Wi-Fi síti. Ať již je tohoto docíleno pomocí slovníkového útoku, útoku hrubou silou či

[12] Je zde uložena hodnota indexu klíče.

dojde k prostému uhádnutí hesla, nedá se získání přístupového hesla považovat za slabinu samotného WPA2. Mnohdy dojde k prolomení hesla z důvodu toho, že si uživatel nastavil velmi slabé heslo, které je obsaženo v prakticky každém slovníku či si pouze nezměnil heslo vygenerované výrobcem.

Wi-Fi Protected Setup (WPS)

Ani druhá uvedená zranitelnost se netýká přímo zranitelnosti samotného WPA2, ale funkce zvané WPS, která je dostupná nejen u přístupových bodů využívajících zabezpečení WPA2, ale i u těch, jejichž bezpečnost zajišťuje starší verze WPA. Hlavní smysl WPS spočívá v poskytnutí většího komfortu v rámci připojování nových zařízení k Wi-Fi síti. Technologie WPS totiž umožňuje jednotlivá zařízení k síti připojit bez nutnosti zadávání přístupového hesla. Existují dva základní přístupy, kterými tohoto lze docílit. První z nich je použití dvojice tlačítek, z nichž jedno je umístěno přímo na routeru a druhé se nachází v zařízení, které chceme připojit. Druhé zmiňované tlačítko ovšem nemusí být na zařízení přítomno fyzicky, může se jednat pouze o jeho softwarovou reprezentaci. Po stisknutí obou zmíněných tlačítek dojde k připojení daného zařízení k Wi-Fi síti. Druhý přístup pak spočívá v zadání PINu, který je obvykle uveden přímo na štítku příslušného routeru. Vzhledem k tomu, že je tento PIN obvykle osmimístný a pochopitelně tvořen pouze z čísel, je jeho zadávání, oproti klasickému heslu, mnohdy daleko jednodušší. (39)

Ačkoliv tedy WPS uživatelům přináší vyšší komfort v oblasti autentizace, je tomu tak na úkor bezpečnosti. Tato technologie totiž spoléhá na to, že je router umístěn v místě, ke kterému nemá přístup neoprávněná osoba. Pokud tomu tak ovšem není, může se k síti připojit v podstatě kdokoliv, ať již za pomocí stisknutí tlačítka či zadání PINu. V případě zadávání PINu se navíc nabízí další možnost napadení. Útočník se nemusí k routeru dostat fyzicky, ale může se pokusit realizovat útok hrubou silou a PIN uhodnout. (40) Vzhledem k tomu, že mnoho zařízení využívajících WPS nekontroluje zadaný PIN jako celek, ale nejprve dojde ke kontrole toho, zda se shodují první čtyři číslice a až poté ověřují shodu dalších čtyř, může útočník po neúspěšném pokusu z odpovědi routeru zjistit informaci o tom, jaká část PINu byla chybná. Na základě toho se z původního počtu 2^8 možných kombinací dostáváme na daleko přijatelnější hodnotu $2x2^4$. Poslední číslice navíc zpravidla reprezentuje kontrolní součet předchozích 7 čísel, čímž je hledání správného PINu ještě více usnadněno. (41, s. 4–6)

S přihlédnutím na skutečnost, že je funkce WPS nejen implementována ve valné většině dostupných routerů, ale navíc je mnohdy v defaultním nastavení routeru aktivní, nemělo by být toto bezpečnostní riziko přehlíženo. Kromě toho není výjimkou, že daný router nedisponuje žádnou či pouze slabou ochranou proti opakovanému zadávání nesprávného PINu, a tak lze poměrně jednoduše realizovat útok hrubou silou. Pokud tedy není funkce WPS uživateli využívána či není možné router dostatečně zabezpečit, ať již proti fyzickému přístupu neoprávněných osob, tak proti útoku hrubou silou, měla by být bezpodmínečně vypnuta. (41, s. 1, s. 9)

KRACK

Dne 16. října 2017 se prakticky ve všech technicky zaměřených mediích začaly objevovat zprávy o tom, že zabezpečení WPA2 bylo prolomeno. Dosaženo toho bylo pomocí útoku KRACK, jehož autorem je Mathy Vanhoef, bezpečnostní expert ze skupiny Imec-DistriNet působící na Katolické univerzitě v belgické Lovani. Nutno podotknout, že KRACK nepředstavuje pouze jeden typ útoku, ale reprezentuje různé verze, jejichž cílem je podvržení šifrovacího klíče. Útočník díky tomuto útoku může přenášená data nejen číst, ale při špatné konfiguraci sítě dokonce i pozměňovat. Hlavní podstata útoku KRACK spočívá v napadení čtyřcestného handshaku, který je součástí autentizace jak u zabezpečení WPA2, tak i staršího WPA. Bezpečnostní problém se navíc netýká pouze domácích sítí využívajících režim s předsdíleným tajemstvím, tedy režimu PSK, ale i sítí firemních, které využívají mód Enterprise.

KRACK se zaměřuje na to, že pro zachování bezpečnosti šifrování v rámci Wi-Fi sítí je bezpodmínečně nutné, aby nedocházelo k opakovanému používání šifrovacích klíčů. Bezpečnostní problém spočívá v tom, že protokol WPA či WPA2 umožnuje opakování zpráv odeslaných v rámci handshaku. Není totiž výjimkou, že se během přenosu od jednoho zařízení k druhému některá ze zpráv ztratí a je tak nutné celou akci opakovat. Útok tedy vhodnou manipulací a znovu používáním již odeslaných zpráv handshaku docílí toho, že klientské zařízení oběti použije klíč, který již byl k šifrování komunikace využit. Opakovaným posíláním zprávy obsahující šifrovací klíč a resetováním parametrů nonce a replay counter je totiž docíleno toho, že klient reinstaluje svůj současný klíč a nahradí ho tím, který je podvržen útočníkem. (42)

Pozitivní je alespoň skutečnost, že lze tuto zranitelnost záplatovat pouhou aktualizací firmwaru a není tak nutné všechna zařízení, kterých se problém týká, nahrazovat. Záleží

ovšem na jednotlivých výrobcích, jak rychle a zda vůbec všechna svá zařízení zazáplatují. Některé firmy, jako například Microsoft, uvedly ihned v den zveřejnění tohoto útoku, že byly o nastalé situaci informovány předem a svá zařízení již zabezpečily prostřednictvím aktualizací. Je tedy potřeba, aby uživatelé v případě dostupnosti nových aktualizací svá zařízení záplatovali. Do té doby je vhodné používat protokoly typu HTTPS, které šifrují komunikaci mezi odesílatelem a příjemcem nezávisle na tom, jaké zabezpečení je použito například v rámci domácí Wi-Fi sítě. (43) (44)

3.8 První představení zabezpečení WPA3

Během psaní této bakalářské práce, konkrétně 8. ledna roku 2018, rovněž přišla Wi-Fi Alliance se zprávou, že v současné době pracuje na novém zabezpečení, které v budoucnu nahradí WPA2. Toto zabezpečení nese označení WPA3 a blíže by mělo být představeno v průběhu roku 2018. Nelze pochybovat o tom, že jedním z hlavních impulzů, pro učinění tohoto kroku, bylo zveřejnění útoku KRACK, který odhalil zranitelnost zabezpečení WPA2. Wi-Fi Aliance slibuje s příchodem WPA3 znatelné zlepšení ve třech oblastech, a to v rámci konfigurace zařízení, šifrování dat a autentizace. Postupné uvádění zařízení certifikovaných jako WPA3 na trh, ovšem neznamená, že bude podpora mechanismu WPA2, který se v současné době využívá v miliardách zařízení, zcela ukončena. Wi-Fi Alliance uvádí, že zabezpečení WPA2 se bude i nadále vylepšovat, aby byla zajištěna bezpečnost všech zařízení, které tento bezpečnostní mechanismus využívají. (45)

Ačkoliv zatím nejsou známy bližší podrobnosti ohledně chystaných vylepšení, měly by být přidány čtyři nové prvky, které zajistí vyšší bezpečnost Wi-Fi sítí. První, poměrně výrazná změna, se má týkat toho, že bude komunikace šifrovaná i v rámci otevřených sítí, ve kterých není potřeba zadávat přístupové heslo. To znamená, že přenášená data nebude moci odposlechnout každý, kdo je připojen ke stejné síti, jako tomu bylo doposud. Další ochranný prvek pak bude zajišťovat vyšší bezpečnost především těch sítí, jež mají nastaveno slabé přístupové heslo. Systém totiž bude blokovat pokusy o slovníkový útok či útok hrubou silou. Rovněž bude zlepšen proces konfigurace zabezpečení těch zařízení, která mají omezené grafické rozhraní či ho nemají vůbec. Jedná se především o zvýšení bezpečnosti různých domácích spotřebičů, které využívají internet, ale vzhledem k jejich jednoduchosti je lze poměrně snadno napadnout. Poslední oznámený bezpečnostní prvek se pak týká šifrování. WPA3 bude podporovat 192bitové šifrování za využití algoritmů vyvinutých americkou vládní organizací CNNS. (46)

4 Typy útoků na bezdrátové sítě

Útok na bezdrátovou síť může být realizován mnoha způsoby, které lze rozdělit do dvou základních skupin. Do první skupiny spadají útoky pasivního rázu a do druhé pak jejich pravý opak, tedy útoky aktivní. Typickým příkladem pasivního útoku je situace, kdy útočník odposlouchává danou komunikaci, aniž by do ní nějak zasahoval. V praxi však útočník pro splnění svého cíle mnohdy kombinuje více útoků najednou. Často je tedy například proveden nejprve odposlech a až po té realizován některý z útoků aktivních, jakým je kupříkladu pozměnění obsahu odchycené zprávy. Níže budou představeny základní typy útoků na bezdrátové sítě a techniky obrany proti nim.

4.1 Odposlech

Hlavní podstata odposlechu neboli sniffingu spočívá ve sběru paketů putujících po síti a jejich následné analýze. Pro odposlech dat v bezdrátových sítích není vzhledem k přenosu dat prostřednictvím rádiových vln potřeba, aby byl útočník v síti přítomen fyzicky. Má-li navíc k dispozici výkonnou parabolickou anténu, může odposlech provádět i z úctyhodné vzdálenosti a o něco snížit riziko jeho odhalení. Aby bylo možné tento útok provést, je zapotřebí přepnout síťovou kartu z režimu promiskuitního do monitorovacího. Tím se docílí toho, že daná síťová karta přijímá veškerou komunikaci, která probíhá na síti a nikoliv tedy jen tu, která je adresována přímo jí. Vzhledem k tomu, že navíc existuje celá řada nástrojů pro monitoring sítě, je tato hrozba poměrně reálnou záležitostí.

Není-li komunikace v rámci dané sítě šifrovaná, může si útočník kupříkladu přečíst obsah posílaných zpráv či získat přihlašovací údaje, které nejsou směrem k serveru přenášeny pomocí protokolů jako jsou SSL a TLS. Přítomnost zabezpečení WEP a WPA s protokolem TKIP ovšem rovněž není, vzhledem k možnosti jejich prolomení, nijak významnou ochranou proti odposlechu. Vhodné je tedy přinejmenším použití zabezpečení WPA2 (WPA) spolu s protokolem AES. I zde je ovšem možné odposlech realizovat, a to na základě znalosti přístupového hesla a informací získaných z handshaku mezi konkrétním zařízením a přístupovým bodem. Ideální je tak použití mechanismu 802.1x, kde je autentizace realizována oproti autentizačnímu serveru. Vzhledem k tomu, že se zde klíče generují mimo jiné na základě přihlašovacích údajů konkrétního uživatele, je provedení odposlechu na této síti prakticky nemožné. Vhodnou ochranou domácí sítě pro zamezení odposlechu zevnitř sítě může být taktéž například použití zařízení, které vysílá více SSID. Díky tomu lze zajistit, aby členové dané domácnosti nevyužívali stejnou síť jako případní

hosté, a nebyla tak ohrožena jejich bezpečnost. Je-li naopak potřeba předejít odposlechu při komunikaci na ne příliš důvěryhodné Wi-Fi síti, za ideální volbu se dá označit použití šifrovaného tunelu VPN. (35)

4.2 Falešný přístupový bod – Rogue AP

Pod pojmem falešný přístupový bod se obecně rozumí bezdrátový přístupový bod připojený k podnikové síti, a to bez vědomí síťového správce. Ať již je takovýto přístupový bod do sítě nainstalován zaměstnancem bez postranních úmyslů či záškodníkem, který chce ohrozit síťovou bezpečnost, může falešný přístupový bod způsobit značné potíže. Připojením neautorizovaného přístupového bodu k podnikové síti totiž vzniknou zadní vrátka, která umožní přístup k této síti z vnějšího prostředí. Důvodem je skutečnost, že se útočníkovi naskýtá možnost obejít všechna kabelová bezpečnostní opatření, jakými jsou například firewally nebo systémy řízení síťového přístupu (NAC). (47) Přesto však existuje způsob, jak přítomnost falešných přístupových bodů odhalit a následně je automaticky zablokovat. Jedná se o síťové zařízení WIPS, jehož hlavní podstatou je kontrola rádiového spektra a portů přepínače, díky čemuž je schopno vyhledávat neautorizované přístupové body. (48)

Tvorba falešných přístupových bodů se však netýká pouze narušení bezpečnosti podnikových sítí. Útočník může realizovat také útok zvaný Evil Twin AP, který spočívá ve vytvoření Wi-Fi sítě, která je nakonfigurována stejně jako síť původní. (49) To znamená použití shodného SSID, typu zabezpečení (WEP, WPA, WPA2) a šifrovacího algoritmu (TKIP, AES). Navíc je ovšem nezbytné, aby byl signál falešného přístupového bodu silnější, než signál pravého AP. Pro úspěšnou asociaci oběti tedy útočník musí znát heslo k dané síti, které nastaví na podvrženém AP. V opačném případě nebude úspěšný handshake a klient se nepřipojí. Výjimkou jsou samozřejmě otevřené sítě, k jejichž připojení není potřeba znát žádné heslo. Tento útok lze tedy poměrně snadno realizovat například ve veřejně přístupných Wi-Fi sítích, ať už otevřených či s heslem, které lze získat na požádání. Tato problematika se ale pochopitelně netýká jen veřejných sítí, nýbrž i sítí domácích, ke kterým se přihlašuje více uživatelů a některý z nich se rozhodne odposlouchávat ostatní účastníky.

Možnou obranou proti existenci stejně nakonfigurovaných přístupových bodů je použití autentizačního mechanismu 802.1x, který neověřuje pouze připojující se zařízení, ale rovněž zajišťuje důvěryhodnost přístupových bodů použitím certifikátů. Uživatelé

připojující se na neznámou Wi-Fi síť by se opět v rámci bezpečnosti měli přihlašovat pouze na stránky zabezpečené protokolem HTTPS, nebo ještě lépe se na veřejných sítích nepřihlašovat vůbec. Nemá-li ale dotyčný jinou možnost, samozřejmostí by mělo být použití šifrovaného spojení VPN.

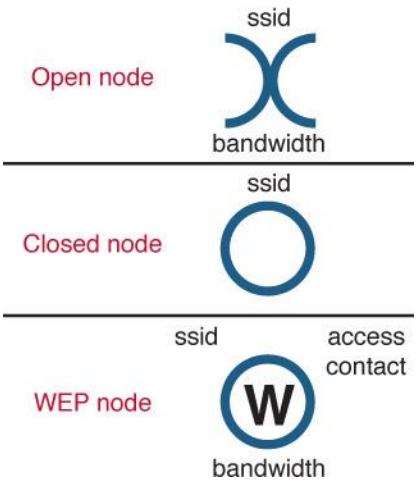
4.3 Man-in-the-Middle (MITM)

Princip útoku Man-in-the-Middle vyplývá již z názvu. Jde o techniku, kdy se útočník snaží dostat mezi zařízení, která spolu komunikují a jejich komunikaci následně zprostředkovávat. Kromě odposlechu se pak může záškodník pokusit procházející data modifikovat, nebo dokonce vkládat vlastní pakety. (50) Ideální je tedy pro útočníka situace, kdy jsou data k serveru přenášená pomocí nešifrovaných protokolů, a to prostřednictvím nezabezpečené Wi-Fi sítě. S ohledem na možnost dešifrování komunikace ostatních uživatelů na síti, a to i v rámci WPA/WPA2-PSK díky znalosti hesla a odchycení informací z handshaku, není tento útok aktuální pouze u veřejně přístupných sítí. Příkladem útoku MITM je v podstatě i falešný přístupový bod, zmíněný v předchozí kapitole, jež je nakonfigurovaný tak, aby byl prakticky nerozeznatelný od pravého přístupového bodu.

Ochranu proti MITM útokům lze opět zajistit díky využití tunelu VPN. Omezením používání neznámých Wi-Fi sítí, u kterých si nelze být jistý tím, kudy vlastně komunikace putuje, lze pochopitelně taktéž výrazně snížit pravděpodobnost vzniku MITM útoku. Jelikož útočník nemusí komunikaci pouze odposlouchávat, ale například se oběť může pokusit přesměrovat na podvrženou stránku internetového bankovnictví, měly by být neznámé sítě ideálně využívány pouze ke čtení na webu či posílání dat, jejichž zachycení nám nezpůsobí žádné nepříjemnosti. V každém případě je pak vhodné se vyhnout zadávání důležitých přihlašovacích údajů.

4.4 Warchalking, wardriving, warwalking

Pojem warchalking byl vytvořen britským designerem Mattem Jonesem již v roce 2002. Jedná se o činnost, jejíž podstata spočívá v mapování existujících Wi-Fi sítí, a to pomocí předem stanovených značek. Vzhledem k tomu, že v dané době ještě nebyly bezdrátové sítě rozšířeny tak masivně, jako je tomu dnes, měli walkchalkeři upozorňovat především na přítomnost volně přístupných Wi-Fi sítí. (51) Některé z používaných značek zachycuje obrázek 5, který se nachází na následující straně.



Obrázek 5: Warchalking značky. *Obrázek převzat z (52)*

Postupem času již lokalizace Wi-Fi sítí nespočívala pouze v kreslení značek na chodníky či zdi domů. Vzhledem k existenci nástrojů pro vyhledávání Wi-Fi sítí, jako je NetStumbler pro operační systém Windows nebo Kismet pro linuxové distribuce, vznikly techniky jako wardriving, warbiking, warflying či warwalking. Podstata uvedených technik je stejná a liší se pouze tím, zda jsou sítě vyhledávány při jízdě autem, na kole, během letu či za chůze. Pomocí nástrojů pro vyhledávání sítí jsou pak ve spolupráci s GPS zařízením nalezené Wi-Fi sítě ukládány do online map a databází, díky čemuž je možné získat poměrně přesnou polohu dané sítě a informace o jejím zabezpečení. Ačkoliv je hlavním cílem tvorby těchto map a databází poskytnutí informací o tom, kde všude se nachází volně přístupné Wi-Fi sítě a jedná se o činnost legální, tyto poznatky může rovněž využít útočník pro vyhledávání napadnutelných sítí patřících firmám či domácnostem.

4.5 Útok na autentizační mechanismus

Útokem na autentizační mechanismus se v prostředí Wi-Fi sítí obvykle rozumí prolomení sdíleného hesla k dané Wi-Fi síti. Vzhledem k tomu, že zabezpečení jako WPA či WPA2 eliminují nedostatky zastaralého WEPu, prostor pro realizaci různých typů útoků je značně omezen. Přesto však i tyto normy obsahují několik slabých míst, která mohou být zneužita. Jedním z nich je útok na autentizaci typu PSK, který lze provést hned několika způsoby.

4.5.1 Slovníkový útok

Tento typ útoku je založen na postupném zkoušení hesel uložených v určitém seznamu, také označovaném jako slovník. Útočník si může takovýto slovník vytvořit buď sám, na základě zjištěných informací o dané oběti, nebo může využít některý z již existujících

slovníků, jež jsou volně dostupné na internetu. Obvykle jsou v nich uvedena nejčastěji používaná hesla, která jsou známa díky kompromitaci mnoha databází s přístupovými údaji uživatelů. Pro realizaci slovníkového útoku je zapotřebí nejprve odposlechnout handshake mezi přístupovým bodem a připojujícím se klientem, který obsahuje pro útočníka nezbytné informace.[13] Jelikož handshake probíhá v době připojování klienta, má útočník dvě možnosti. Buď bude pasivně vyčkávat, až se některý z klientů připojí, nebo některého z již připojených klientů deautentizuje, čímž si vynutí jeho opětovné přihlášení. (53) Po té přichází na řadu ověření toho, zda se hledané heslo nachází v použitém slovníku. V případě úspěchu získává útočník přístup k celé síti. Tento typ útoku využívá především toho, že mnoho uživatelů volí lehce zapamatovatelná hesla, která lze poměrně snadno odhadnout a často se tedy v daných slovnících nachází.

4.5.2 Útok hrubou silou

Namísto zkoušení slov z určitého slovníku se může útočník pokusit uhodnout heslo hrubou silou. Toto hádání spočívá v tom, že jsou postupně zkoušeny všechny variace znaků, které mohly být použity. Prvním důvodem nepoužitelnosti tohoto způsobu je ovšem fakt, že počet možných variací roste exponenciálně vzhledem k délce hesla. (54) Druhý problém pak spočívá v tom, že autentizace typu PSK využívá pro vytvoření hashe z hesla funkci HMAC-SHA1, jejíž výstup je zpravidla odvozen na základě 4096 iterací, díky čemuž je proces zjišťování původního hesla výrazně zpomalen. (55, s. 153) Aby měl útočník 100% jistotu, že vyzkoušel všechna možná hesla, musel by použít velká a malá písmena, čísla, ale i všechny speciální znaky. Vezmeme-li navíc v potaz, že je heslo tvořeno minimálně osmi znaky a útočník s největší pravděpodobností jeho skutečnou délku nezná, nestihl by celý prostor vyčerpat ani za celý svůj život. Ačkoliv u výše zmíněného slovníkového útoku není jistota, že je heslo ve slovníku obsaženo, jedná se oproti útoku hrubou silou o techniku daleko rychlejší, efektivnější a s vyšší šancí na úspěch v rozumném čase.

4.5.3 Využití duhových tabulek – Rainbow tables

Vzhledem k tomu, že předchozí zmíněné útoky fungují na principu, kdy je nejprve vzat řetězec v otevřené podobě, následně dojde k jeho zahashování a výsledný hash je porovnán s hashem hesla skutečného, dochází kvůli této činnosti ke znatelnému zatížení procesoru a celý proces ověření shody trvá výrazněji déle. Z tohoto důvodu vznikla myšlenka, předvypočítat si jakousi tabulku, která bude obsahovat dvojici řetězec (heslo)

[13] Nehovoříme-li tedy o situaci, kdy jsou hesla ze slovníku zkoušena online přímo oproti autentizační autoritě.

a odpovídající hash, díky čemuž nebude potřeba během procesu porovnání vypočítávat hash z každého kandidáta na heslo. (55, s. 159) Díky tomu by bylo teoreticky možné vytvořit tabulku založenou na útoku hrubou silou, která by zahrnovala variace všech znaků, jež mohly být použity, přičemž by ke každému řetězci byl přiřazen výsledný hash. Problém ovšem spočívá v tom, že pokud by tato tabulka zahrnovala například jen hesla tvořená osmi znaky, a to za použití malých písmen a číslic, odpovídala by její velikost zhruba 2,8 terabytům. Při zvětšení délky hesla na deset znaků a přidání velkých písmen by velikost takovéto tabulky sahala až k miliónu terabytů. Jelikož však délka skutečného hesla není známa a je potřeba počítat i s možností, že obsahuje speciální znaky, v současné době není možné takovouto tabulku uložit. (56, s. 99–100)

Text výše však nepojednává přímo o duhových tabulkách, ale pouze o myšlence, ze které tato technika vychází. Ačkoliv musí být i zde nejprve vygenerována tabulka, pomocí které lze k příslušnému hashi dohledat odpovídající heslo, výsledná velikost tabulky, která zahrnuje výše zmiňovanou množinu možných znaků, je již přijatelnější. Na první pohled duhové tabulky rovněž používají pouze dva sloupce, první pro potenciální hesla a druhý pro odpovídající hashe. Ve skutečnosti je ovšem jejich činnost založena na mnohem sofistikovanějším mechanismu s přítomností daleko většího počtu sloupců, které lze během hledání odpovídajícího hashe zpětně zrekonstruovat.

Každopádně je potřeba připomenout jednu zásadní skutečnost. V autentizaci typu PSK není výsledný hash generován pouze z hesla, ale také z přidané soli, kterou je zde SSID sítě. Pokud si tedy útočník nevytvoří tabulku svou, což ho bude stát spoustu času a zdrojů, bude muset použít nějakou již existující. Ty ovšem pochopitelně nemůžou zahrnovat všechna existující SSID, ale pouze ty nejčastěji používané.

4.5.4 Obrana

Ochránit Wi-Fi síť před tím, aby útočník mohl provést úspěšný útok na autentizační mechanismus, ovšem není nikterak složité. Je-li nastaveno dostatečně silné heslo, a to například dle doporučení zmíněných v kapitole 3.1.4, jsou útočníkovy šance na úspěch výrazným způsobem sníženy. Zvýšení bezpečnosti se ovšem netýká pouze nastavení silného přístupového hesla. Druhým aspektem, kterým je nutné se zabývat, je zmiňované použití SSID jako soli při tvorbě výsledného hashe. Pokud Wi-Fi síť nese co možná nejoriginálnější název, dochází k odstranění hrozby, že útočník využije některou již existující duhovou tabulku.

4.6 DoS útoky

V kybernetické bezpečnosti je kladen důraz na splnění tří hlavních cílů, a to zajištění dostupnosti, integrity a důvěryhodnosti informací. Útoky typu DoS mají přes rozdílný způsob provedení stejný cíl, který spočívá v narušení prvního zmiňovaného cíle, tedy v omezení dostupnosti informací. Přesněji řečeno se jedná o omezení dostupnosti služeb, což ale obecně nepříznivě ovlivní i dosažitelnost s nimi spojených informací. Toho lze docílit na základě přetížení jedné z částí daného systému. Ať už útočník využije nedostatečné výpočetní kapacity, operační paměti, či síťového pásma, výsledkem je úplná či částečná nedostupnost určité služby. (57, s. 38–39)

Příkladem DoS útoku na bezdrátovou síť je opakující se deautentizace připojených klientů. Tento útok využívá toho, že komunikace mezi přístupovým bodem a jednotlivými uživateli není do úspěšné asociace klienta šifrovaná. Řídicí rámce, které zajišťují například právě autentizaci a následnou asociaci daných zařízení jsou tak posílány v otevřené podobě a jejich obsah lze jednoduše odposlechnout. Pokud tedy útočník nějakou dobu zachytává provoz na síti, může zjistit, které stanice jsou k ní připojeny a na základě jejich MAC adresy provést jejich deautentizaci. Tu provede pomocí řídícího rámce, jehož obsahem bude oznámení o ukončení spojení mezi danou stanicí a přístupovým bodem. Přístupový bod této žádosti vyhoví a danou stanici tak deautentizuje. Vzhledem k tomu, že si toto odhlášení daná stanice ve skutečnosti nevyžádala, ihned se znovu připojí. Útočník ale může zajistit, aby se deautentizační rámec posílal ve smyčce a tím pádem nebude síť pro příslušného uživatele dostupná. Útočník se navíc může pokusit tímto způsobem deautentizovat všechna zařízení na síti tím, že bude zaslaný řídící rámec typu broadcast. Zde ovšem může narazit na to, že mnohé přístupové body hromadný rámec tohoto typu zahodí. (58)

Standard 802.11 ani 802.11i nenabízí proti útokům typu DoS žádný způsob obrany. Naštěstí však existují možnosti, pomocí kterých lze DoS útokům do jisté míry čelit. Jednou z nich je použití systému WIDS, který monitoruje bezdrátovou síť, na základě čehož generuje podrobné zprávy například o kvalitě signálu, využití pásma či poměru úrovně signálu a šumu (Signal-to-Noise Ratio). Systém WIDS je schopen odhalit probíhající DoS útok a informovat o něm správce sítě. Tento systém ovšem není schopen proti probíhajícím útokům zakročit a jeho úkolem je tedy o existenci problému informovat. (59, s. 24) Jako vhodnější pomocník v boji proti DoS útokům se tedy jeví systém WIPS, který funguje na obdobném principu, ale navíc umí automaticky vykonat protiopatření, která znemožní

další průběh probíhajícího útoku. (60) Absenci bezpečnostního mechanismu, který by znemožnil vykonání alespoň některých typů DoS útoků, si uvědomovala i standardizační skupina 802.11. Na základě toho byl v roce 2009 vydán dodatek nesoucí označení 802.11w, který eliminuje možnost zneužití řídících rámců, čímž řeší kupříkladu zmiňovaný deautentizační útok. Vzhledem k tomu, že rámce poslané útočníkem nejsou patřičně podepsány, stanice a přístupové body pracující podle tohoto standardu příslušné rámce automaticky zahazují. Skutečnost je ovšem taková, že mnoho zařízení ani v současné době tento protokol nepodporuje a nejedna sít je tak stále zranitelná i proti velmi známým a jednoduše realizovatelným typům DoS útoků. (58)

Pro realizaci útoku DoS ovšem nemusí být využity pouze vrstvy jako je linková, síťová či aplikační, útočník může narušit přímo fyzické médium. V prostředí kabelových sítí se může jednat například o prosté přerušení síťového kabelu, čímž opět dojde k naplnění podstaty DoS útoku, tedy k znepřístupnění určité služby. Co se týče útoku na fyzickou vrstvu u bezdrátových sítí, může se jednat o úmyslné rušení kanálu či poškození přístupového bodu. Vhodnou ochranou je zde tedy strategické rozmístění přístupových bodů do výšky či na místa, která nejsou volně přístupná. Rovněž by měl být kladen důraz na vhodnou volbu topologie z hlediska co nejnižší dostupnosti signálu vně danou oblast. Je potřeba se zabývat tím, jaký typ antén bude použit a jak budou v dané oblasti rozmístěny. Pomocí použití stínění v podobě specializovaných nátěrových barev, tapet či záclon na okna, které zabraňují v šíření radiofrekvenčních signálů, lze zabránit nejen dostupnosti Wi-Fi sítě mimo požadovanou oblast, ale i úmyslnému rušení kanálu z vnějšku sítě. (59, s. 24–25)

5 Současný stav

Ačkoliv by v současné době mělo být zajištěno, že poskytovatelé internetového připojení zákazníkům nabízí certifikovaná Wi-Fi zařízení, která podporují nejmodernější dostupná zabezpečení, je možné se stále setkat s Wi-Fi sítěmi, které používají již dávno prolomené bezpečnostní mechanismy. Tato skutečnost je zřejmě dána tím, že přechod ze zastaralého protokolu WEP či WPA na modernější WPA2 se již neobejde bez výměny hardwaru, a tak se někteří poskytovatelé Wi-Fi sítí pravděpodobně rozhodli ušetřit finance na úkor bezpečnosti svých zákazníků a zranitelná zařízení nenahradili. Pokud se tedy daný zákazník o bezpečnost své Wi-Fi sítě nezajímá, nemusí si být této skutečnosti vůbec vědom. Kvalitnější poskytovatelé ovšem naštěstí dbají na to, aby byly jejich bezdrátové sítě co možná nejbezpečnější a využití WPA2 je tak zpravidla jakýsi standard.

Vzhledem k tomu, že v době, kdy začala vznikat tato bakalářská práce, neměl protokol WPA2 sám o sobě v podstatě žádnou známou zranitelnost a za největší slabinu sítí s tímto zabezpečením se tak dalo považovat slabé přístupové heslo, zabývá se praktická část práce právě důležitostí změny přednastaveného hesla spolu s SSID. Na významnosti změny těchto údajů se nic nemění ani přesto, že během psaní této práce došlo ke zveřejnění útoku KRACK, který využil do té doby neznámé zranitelnosti protokolu WPA2 a později byla dokonce představena nová verze zabezpečení nesoucí označení WPA3, která by mimo jiné měla ošetřit právě i problém týkající se nastavení slabého přístupového hesla. Zranitelnost WPA2 lze ovšem eliminovat pouhou aktualizací firmwaru, a tak nebude nutné postižená zařízení nahrazovat a budou se i nadále využívat. I kdyby ovšem v budoucnu mělo postupně docházet k výměně zařízení s mechanismem WPA2 za ta, která již budou využívat WPA3, zcela jistě tato obměna nenastane ze dne na den. Vezmeme-li navíc v potaz, že i dnes se na některých sítích používá WEP či WPA, pravděpodobně ani zabezpečení WPA2 v dohledné době jen tak nevymizí a problém týkající se používání defaultního přístupového hesla a SSID tak bude stále aktuální.

6 Hlavní východisko pro praktickou část

V lednu roku 2016 zveřejnil bezpečnostní analytik Peter Geissler, v internetovém prostředí spíše známý jako Blasty, informaci o existující zranitelnosti jednoho ze zařízení, které má v nabídce poskytovatel internetového připojení UPC. Zároveň navíc dodal, že se problém může týkat i dalších typů zařízení, jež daný poskytovatel využívá pro realizaci bezdrátových sítí. Uvedená zranitelnost spočívá v možnosti získání přednastaveného hesla na základě znalosti původního SSID. Přestože je ve skutečnosti k zisku správného přístupového hesla nutná znalost sériového čísla daného routeru, díky existenci vztahu mezi defaultním SSID a příslušným sériovým číslem, lze vygenerovat několik potencionálních kandidátů na přístupové heslo a následně jen vyzkoušet, zda je některé z nich platné. (2) Dle vyjádření UPC by se problém měl týkat dvou z jimi nabízených zařízení, a to konkrétně modelů Ubee EVW3226 a Technicolor TC7200. (61) Jedná se tedy o ty Wi-Fi sítě, jejichž původní SSID je tvořeno z deseti znaků. První tři znaky reprezentuje trojice písmen UPC a na následujících sedmi pozicích se pak nacházejí čísla.

6.1.1 Zranitelnost modelu Technicolor TC7200

Peter Geissler při své analýze zjistil, že jediným vstupem algoritmu, který je zodpovědný za výpočet defaultního přístupového hesla ale i SSID, je právě sériové číslo daného routeru. V případě znalosti sériového čísla tak není problém zjistit i odpovídající přístupové heslo. Vzhledem k tomu, že pro zjištění sériového čísla by musel mít útočník fyzický přístup k danému zařízení, nepředstavuje použití tohoto údaje k vygenerování přístupového hesla tak zásadní nebezpečí. Pokud by totiž měla neautorizovaná osoba fyzický přístup k routeru, zřejmě by se nezaobírala zjišťováním sériového čísla, ale rovnou by se zaměřila na defaultní heslo, které je na daném zařízení rovněž zpravidla uvedeno. Problém je ale v tom, že existuje již zmiňovaná souvislost mezi původním SSID sítě a sériovým číslem routeru, díky čemuž se Peteru Geisslerovi podařilo implementovat algoritmus, který projde všechna možná sériová čísla daného modelu routeru a vybere jen ta, ke kterým je přiřazeno hledané SSID. Jelikož je sériové číslo jediným vstupem algoritmu, který má na starost generování přístupového hesla, není pak již problém na základě znalosti zjištěných sériových čísel a znalosti algoritmu použitého pro generování přístupových hesel dopočítat i odpovídající přístupová hesla. (2)

6.1.2 Zranitelnost modelu Ubee EVW3226

Ačkoliv bylo v předchozím textu zmíněno, že má UPC ve své nabídce dva typy routerů, u nichž lze původní přístupové heslo zjistit, kód pro výpočet několika kandidátů na heslo, se kterým přisel Peter Gaissler, lze uplatnit pouze na router s označením Technicolor TC7200. Zařízení Ubee EVW3226 totiž nevyužívá pro výpočet defaultního hesla a SSID ten samý algoritmus, který je využit v rámci Technicoloru. Touto skutečností se začala zabývat i dvojice bezpečnostních expertů ze Slovenska, která se rozhodla analyzovat firmware routeru Ubee EVW3226 a zjistit princip generování SSID a přístupového hesla i v tomto zařízení.

Prvním důležitým krokem, který bylo potřeba vykonat, bylo získání práv roota, aby mohlo na daném zařízení dojít ke stažení a následné analýze firmwaru. Vzhledem k tomu, že již v této době měl router Ubee EVW3226 několik známých zranitelností a jednou z nich bylo právě nedostatečné zabezpečení administrátorského rozhraní, nebyl pro dvojici větší problém práva roota získat. (62) Využili k tomu navíc již existující návod, který jim umožnil získat kontrolu nad zařízením díky vložení USB disku, na němž se nacházelo několik jednoduchých skriptů. Na základě analýzy firmwaru došli ke zjištění, že i tento typ routeru využívá algoritmus, jehož jediným vstupem je sériové číslo daného zařízení. Na rozdíl od Technicoloru je ale zranitelnost routeru Ubee EVW3226 ještě o něco závažnější. Sériové číslo lze totiž odvodit z MAC adresy daného zařízení, a to pouhým snížením posledního bajtu MAC adresy o hodnotu tři – jedná-li se o Wi-Fi síť běžící v pásmu 2.4 GHz, a o hodnotu jedna – pracuje-li dané zařízení v pásmu 5 GHz. Díky této skutečnosti tak není potřeba zkoušet několik potenciálních kandidátů na heslo, jako je tomu u Technicoloru TC7200. Se znalostí skutečného sériového čísla lze vygenerovat jedno jediné odpovídající defaultní přístupové heslo. (63)

7 Metodologický postup

Na základě informací uvedených na předchozích stránkách nelze pochybovat o tom, že nevhodné generování přístupového hesla a SSID může představovat velké bezpečnostní riziko. Pokud by ale byla změna těchto údajů běžnou praxí, nemuselo by se jednat o problém až tak velkého rozsahu. Z tohoto důvodu bylo prostřednictvím dotazníku zjištěno, jak velkou pozornost věnují vlastníci Wi-Fi sítí nejen změně přednastaveného hesla, ale i změně SSID či přihlašovacích údajů k administraci routeru. Ačkoliv si lze na základě odpovědí jednotlivých respondentů udělat určitou představu o tom, jak moc závažným bezpečnostním nedostatkem je nevhodné generování těchto údajů, skutečný stav se pochopitelně může od získaných dat razantně lišit. Proto bylo nezbytné rovněž provést reálný průzkum, díky čemuž mohlo dojít k porovnání toho, zda data získaná z dotazníku alespoň přibližně korespondují se skutečným stavem.

- **Dotazníkové šetření**

Pro získání představy o tom, zda vlastníci Wi-Fi sítí považují změnu SSID a přístupového hesla za důležitou a zda si tyto údaje na své síti změnili, posloužil dotazník v elektronické podobě. Struktura dotazníku byla vytvořena tak, aby mohla být získaná data porovnána s těmi, jež byly nabyty v rámci reálného průzkumu.

- **Reálný průzkum v Českých Budějovicích**

Již během tvorby samotného dotazníku byla zahájena hlavní část této bakalářské práce, kterou bylo vyhledávání Wi-Fi sítí od poskytovatele UPC, jež vysílají zmiňované problematické SSID. Nejprve byl vybrán software vhodný pro vyhledávání daných Wi-Fi sítí a následně došlo k vyhodnocení toho, jakým způsobem budou identifikováni majitelé zachycených sítí. V případě, že byl majitel sítě úspěšně nalezen, byl o existujícím bezpečnostním nedostatku informován a s jeho souhlasem došlo k ověření toho, zda se zranitelnost týká i jeho Wi-Fi sítě. V případě potřeby byl dotyčnému rovněž poskytnut postup, jak si své přednastavené přístupové heslo k Wi-Fi síti a SSID může změnit.

- **Analýza získaných dat**

Po ukončení sběru dat za pomocí dotazníkového šetření a reálného průzkumu, došlo k jejich vyhodnocení a poznatky získané oběma metodami byly následně porovnány.

8 Stanovené cíle a hypotézy

V rámci druhé části bakalářské práce byly stanoveny cíle, které povedou k potvrzení či vyvrácení hypotéz, jež jsou uvedeny níže.

Cíl 1) Zjistit, zda je SSID, které se skládá z UPC + 7 čísel, měněno častěji, než jiné typy SSID od UPC. A to vzhledem k tomu, že se bezpečnostní problém týká pouze SSID tvořeného zkratkou UPC následovanou sedmi čísly.

Hypotéza 1) *SSID, jež je tvořeno zkratkou UPC a sedmi čísly je měněno častěji, než jiná SSID od poskytovatele UPC.*

Cíl 2) Zjistit, zda UPC problém týkající se možnosti zjištění přednastaveného hesla z původního SSID či MAC adresy u určitých směrovačů napravilo a jakým způsobem.

Hypotéza 2) *Stále existují směrovače, u nichž je možné na základě znalosti SSID či MAC adresy zjistit původní přístupové heslo k dané Wi-Fi síti.*

Cíl 3) Zjistit, zda odpovědi uvedené v dotazníku korespondují s reálnou situací.

Hypotéza 3) *Ve skutečnosti nebudou v provedeném průzkumu majitelé Wi-Fi sítí klást na změnu SSID a hesla takový důraz, jako tomu bude v dotazníkovém šetření.*

Cíl 4) Zjistit, zda se majitelé, jichž se tento problém týká, o bezpečnostním riziku dozvěděli.

Hypotéza 4) *Většina majitelů otestovaných Wi-Fi sítí ani po roce a půl od zveřejnění bezpečnostního problému nebude tušit, že jejich síť obsahuje příslušnou zranitelnost.*

9 Praktická část

9.1 Dotazníkové šetření

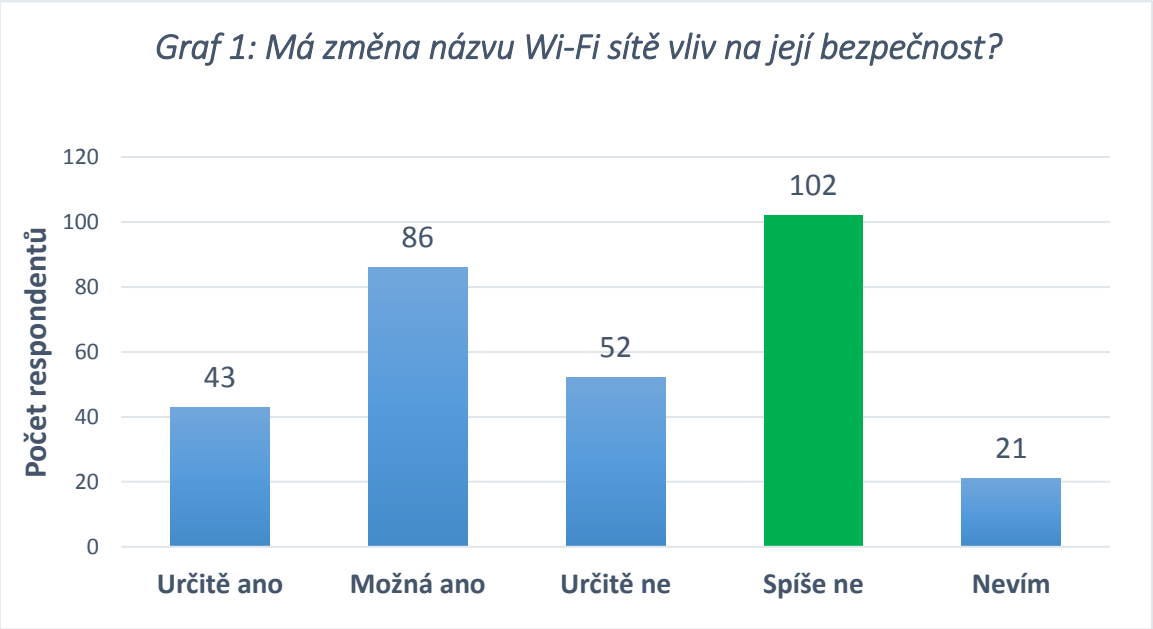
Dotazníkové šetření proběhlo v termínu od 5. března do 3. dubna 2018, a to v elektronické podobě. Dotazník zahrnoval celkem 12 otázek, z nichž 10 bylo uzavřených, 1 polouzavřená a 1 otevřená. První čtyři otázky dotazníku měly za cíl rozdělit respondenty do skupin na základě jejich pohlaví, věku, dosaženého vzdělání a dle toho, zda někdy studovali či pracovali v IT oblasti. Otázky číslo pět až jedenáct se pak již týkaly samotného zabezpečení Wi-Fi sítě. Dvanáctá a zároveň poslední otázka sloužila ke zjištění poskytovatele Wi-Fi sítě, respektive poskytovatele internetového připojení daného respondenta. Tato informace byla využita především k tomu, aby mohli být od ostatních respondentů odlišeni ti, co mají Wi-Fi síť od UPC a jejich odpovědi pak porovnány s daty zjištěnými v reálném průzkumu. Dotazník vyplnilo celkem 304 respondentů s tím, že návratnost dotazníků činila 70,2 %.

Ačkoliv došlo k rozdělení jednotlivých respondentů do skupin na základě prvních čtyř otázek, díky čemuž mohlo být vyhodnoceno, zda má ať již věk, pohlaví, dosažené vzdělání či zkušenosti v IT vliv na to, jak se dotyční v dané oblasti orientují a jak velký důraz kladou na zabezpečení své Wi-Fi sítě, budou na následujících stránkách uvedeny výsledky pouze těch otázek, které se týkají výhradně zabezpečení Wi-Fi sítí. První čtyři otázky byly spíše doplňujícího charakteru a nejsou pro potřeby této práce nezbytné. V případě zájmu je ovšem možné navštívit odkaz uvedený níže, na kterém se nachází vyhodnocený dotazník a lze se podívat i na výsledky prvních čtyř otázek. Kromě toho je navíc možné využít funkci zvanou „Zjišťování závislostí odpovědí“, která se na dané webové stránce nachází pod vyhodnocenými odpověďmi respondentů. Pomocí této funkce lze vhodným nastavením filtrů zjistit například to, jak na konkrétní otázku odpovídali kupříkladu pouze muži ve věku 26-35 let, kteří uvedli jako nejvyšší dosažené vzdělání střední školu s maturitou a nikdy nestudovali ani nepracovali v IT oblasti. Vyhodnocený dotazník je volně dostupný na následující adrese:

https://www.vyplnto.cz/realizovane-pruzkumy/zabezpeceni-wi-fi-site/

<u>Otázka č. 1:</u> Myslíte si, že může mít změna názvu Wi-Fi sítě vliv na její bezpečnost?

Cílem první otázky týkající se bezpečnosti bylo zjistit, zda podle dotazovaných může mít změna názvu Wi-Fi sítě vliv na její zabezpečení. Respondent si mohl vybrat z pěti nabízených možností, a to buď určitě ano, možná ano, určitě ne, spíše ne a nevím. Výsledky této otázky byly následující: 102 dotazovaných zvolilo možnost spíše ne, 86 možná ano, 52 určitě ne, 43 určitě ano a zbylých 21 pak uvedlo možnost nevím. Ačkoliv se 154 respondentů, tedy nepatrná většina, přiklonilo k názoru, že změna SSID vliv na bezpečnost nemá, opačného názoru bylo 129 dotazovaných a mezi oběma skupinami tak nebyl příliš velký rozdíl. Níže je zobrazen graf s výsledky k této otázce.



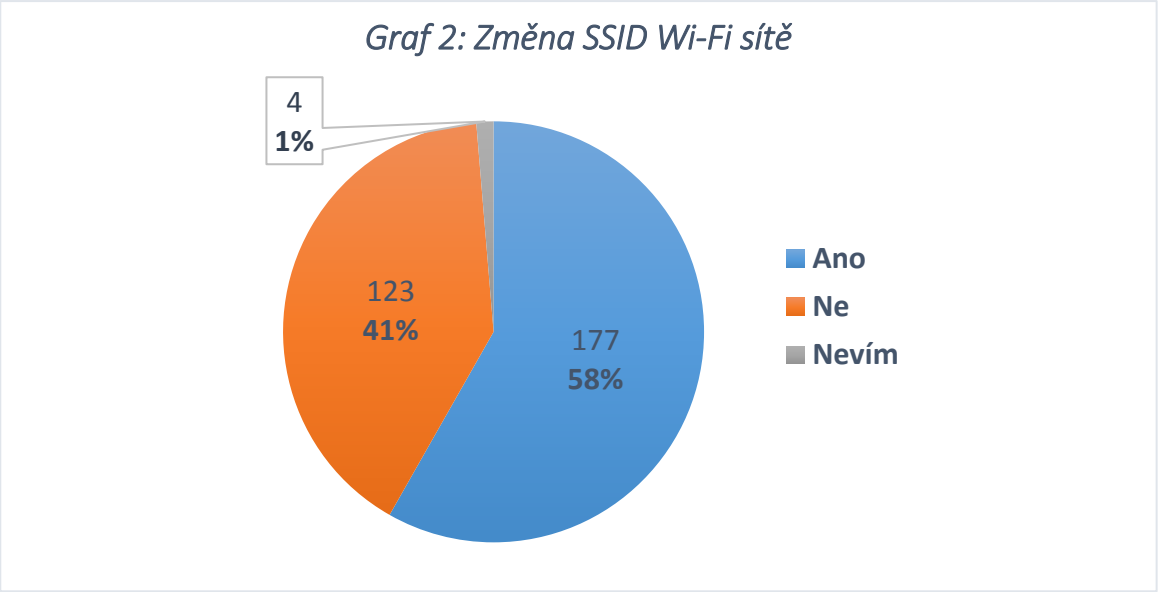
Je sice pravdou, že nezměněné SSID samo o sobě neznamená téměř žádné bezpečnostní riziko. V případě, že však nedojde ani ke změně přístupového hesla, může původní SSID určitý bezpečnostní problém představovat. Důkazem tohoto je mimo jiné průzkum, který byl proveden v rámci této práce a bude blíže představen na následujících stránkách. Stejně tak může nastat případ uvedený v podkapitole 3.1.3, kdy byla část hesla uvedena přímo v původním názvu Wi-Fi sítě.

Ponechání původního SSID či nastavení nového názvu nevhodným způsobem ovšem může v určitých případech znamenat jisté ohrožení bezpečnosti i v případě, že bylo přístupové heslo změněno. Některé z existujících důvodů byly zmíněny již v kapitole 3.1, která pojednává o změně defaultního SSID a před-sdíleného tajemství k Wi-Fi síti. Pro připomenutí se jedná například o situaci, kdy je na Wi-Fi síti nastaven hojně používaný

název, díky čemuž se útočník může pokusit heslo prolomit za využití již existujících duhových tabulek. Stejně tak je vhodné se vyvarovat například uvedení příjmení v názvu Wi-Fi sítě či jakýchkoliv jiných informací, dle kterých by mohl útočník zjistit, komu daná síť patří. Díky znalosti identity vlastníka sítě je totiž mnohdy možné, například prostřednictvím sociálních sítí zjistit, jaké má dotyčný záliby či jak se jmenují členové jeho rodiny, což může útočníkovi výrazně pomoci ke zjištění nastaveného přístupového hesla. I volba vhodného SSID tak skutečně může zajistit o něco vyšší bezpečnost dané Wi-Fi sítě.

<u>Otázka č. 2:</u> Změnil/a jste si název Vaší Wi-Fi sítě?

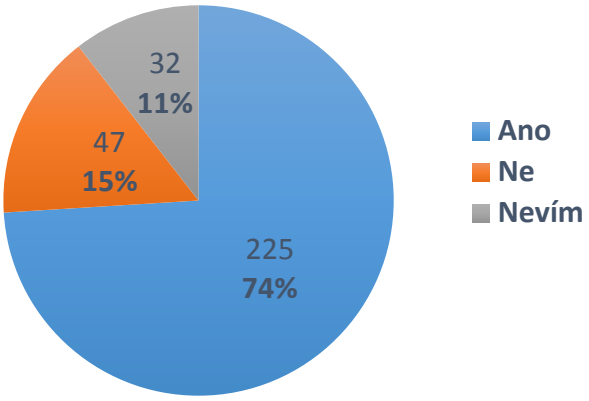
Na předchozí otázku navazovala otázka číslo dva, ve které bylo zjištěno, kolik respondentů si název sítě skutečně změnilo. Změnu SSID dle výsledků provedlo 177 dotazovaných, což odpovídá zhruba 58 %. Název sítě si naopak nezměnilo 123 respondentů, tedy přibližně 41 % z celkového počtu. Pouze 4 účastníci průzkumu si pak nebyli jisti, zda si název své sítě změnili či nikoliv.



<u>Otázka č. 3:</u> Myslíte si, že je ponechání přístupového hesla přednastaveného výrobcem bezpečnostní riziko?

Sedmá otázka sloužila ke zjištění toho, zda účastníci průzkumu považují ponechání přístupového hesla, které přednastavil výrobce, za bezpečnostní riziko. Většina respondentů uvedla, že se o bezpečnostní riziko jedná a heslo by tedy mělo být změněno. Konkrétně tuto možnost zvolilo 225 dotazovaných. Naopak 48 respondentů bylo toho názoru, že hesla od výrobce jsou dostatečně silná a není tak potřeba je měnit. Ve zbylých 32 dotaznících pak byla u této otázky označena možnost nevím.

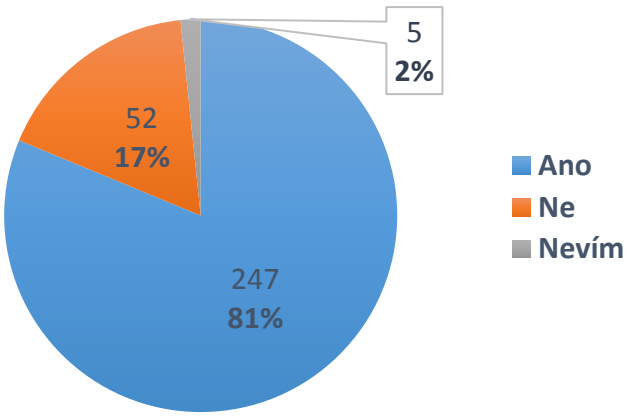
Graf 3: Představuje přednastavené přístupové heslo bezpečnostní riziko?



<u>Otázka č. 4:</u> Změnil/a jste si přístupové heslo k Vaší Wi-Fi síti?

V otázce číslo čtyři pak měli dotazovaní uvést, zda si přístupové heslo k Wi-Fi síti skutečně změnili. Celkem 247 z nich uvedlo, že si původní heslo změnili. Nové heslo si nenastavilo 52 respondentů a zbylých 5 si již nevybavilo, zda ke změně hesla došlo či nikoliv. Z výše uvedeného vyplývá, že počet těch, kteří si heslo změnili je ještě o něco vyšší, než počet těch, kteří v předešlé otázce uvedli, že je dle nich ponechání výrobcem představeného hesla bezpečnostní riziko. Nelze tedy pochybovat o tom, že někteří z těch, kteří v předchozí otázce uvedli, že se o bezpečnostní riziko nejedná či zvolili možnost nevím, si i přesto heslo změnili. Ať již si ale dotyční změnili heslo z důvodu vyšší bezpečnosti či pouze pro lepší zapamatování, je výsledných 81 % nepochybně velmi vysokým číslem. Pochopitelně ale změna hesla ještě nutně nemusí znamenat zvýšení bezpečnosti. V případě nastavení krátkého hesla s využitím omezené množiny použitých znaků může být dané heslo ještě zranitelnější, než heslo původně nastavené.

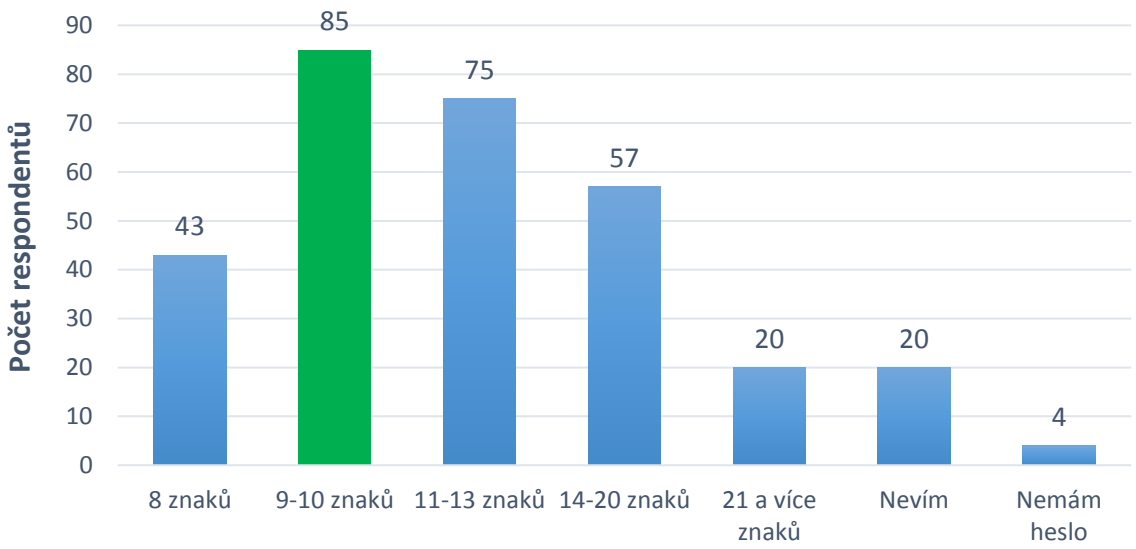
Graf 4: Změna přednastaveného přístupového hesla



<u>Otázka č. 5:</u> Jak dlouhé je přístupové heslo k Vaší Wi-Fi síti?

V páté otázce měli respondenti zvolit jednu z uvedených možností na základě toho, jak dlouhé je přístupové heslo k jejich Wi-Fi síti. Výsledky této otázky jsou zobrazeny prostřednictvím grafu 5. Pozitivním zjištěním byla především skutečnost, že heslo dlouhé 8 znaků, bylo uvedeno pouze ve 43 případech. Nejčastěji se objevovala odpověď 9-10 znaků a s rostoucím počtem znaků v rámci jednotlivých kategorií, které byly na výběr, pak naopak klesal počet respondentů, kteří danou možnost zvolili. Celkem 20krát se objevila odpověď nevím a 4 účastníci průzkumu uvedli, že nemají nastavené žádné přístupové heslo. Jeden z těchto čtyř ovšem uvedl, že mechanismy typu WPA jsou k ničemu a on osobně namísto toho pro zajištění bezpečnosti své sítě využívá technologii zvanou IPsec.

Graf 5: Délka přístupového hesla k Wi-Fi síti

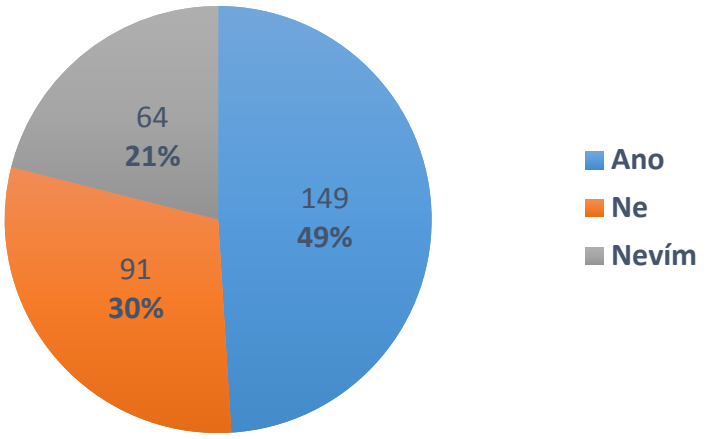


Pokud budeme brát v potaz pouze výsledky těch respondentů, kteří v předešlé otázce uvedli, že si přístupové heslo ke své Wi-Fi síti změnili, byly výsledky následující. Z celkového počtu 247 dotazovaných si dle výsledků dotazníku nastavilo heslo delší než 8 znaků hned 207 z nich. Respondentů, kteří si heslo sice změnili, ale nově opět nastavili heslo s minimální požadovanou délkou, tedy osmi znaky, se v průzkumu objevilo 33. Ze zbylých 7 respondentů si pak 6 účastníků průzkumu nebylo schopno vybavit, jak je jejich nově zvolené heslo dlouhé a jednou se objevila odpověď, že po změně není vyžadováno vůbec žádné přístupové heslo.

<u>Otázka č. 6:</u> Změnil/a jste si přístupové údaje k administraci routeru?

Cílem šesté otázky bylo zjistit, kolik z dotazovaných si změnilo přístupové údaje do administrace routeru. Zde již byla situace o poznání horší, než u změny samotného přístupové hesla k Wi-Fi síti. Přenastavením těchto údajů si byla jista necelá polovina respondentů. Téměř třetina dotazovaných pak uvedla, že ke změně přístupových údajů k administraci routeru nedošlo. Poměrně velký počet dotazovaných, zhruba 21 % z celku, si pak již tuto skutečnost nevybavil. Výsledky této odpovědi zachycuje graf 6.

Graf 6: Změna přístupových údajů k administraci routeru



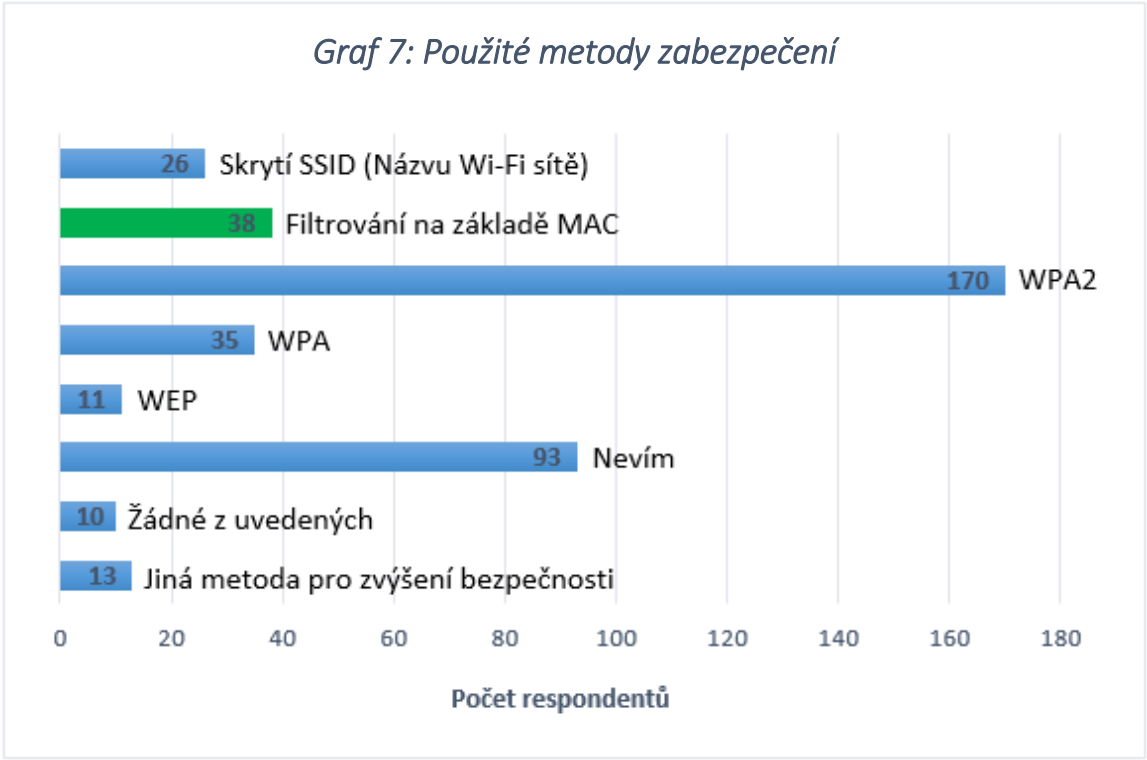
V celkovém počtu 149 respondentů, kteří si přístupové údaje k administraci routeru změnili, byla naprostá většina těch, kteří v otázce číslo 8 uvedli, že si změnili přístupové heslo ke své bezdrátové síti. Našlo se ale 8 dotazníků, ve kterých bylo uvedeno, že ke změně přístupového hesla sice nedošlo, ale údaje k administraci routeru byly naopak změněny.

<u>Otázka č. 7:</u> Z uvedených metod zabezpečení vyberte ty, které používáte v rámci Vaší Wi-Fi sítě.

V předposlední otázce měli respondenti z nabízených metod vybrat ty, které používají pro zabezpečení jejich vlastní Wi-Fi sítě. Na výběr měli následující možnosti: skrytí SSID, filtrování na základě MAC adresy, WEP, WPA či WPA2. Dotazovaní mohli rovněž zvolit odpověď nevím či zaškrtnout možnost žádné z uvedených. Jelikož se jednalo o polouzavřenou otázku, mohl respondent popřípadě uvést ještě některou jinou, jím využívanou techniku pro zvýšení bezpečnosti své Wi-Fi sítě. Z grafu 7, který je umístěn na následující straně, je patrné, že ačkoliv nejvíce respondentů uvedlo, že jejich síť disponuje zabezpečením WPA2, někteří z dotazovaných stále používají méně bezpečný mechanismus

WPA či dokonce zastaralý WEP. Každý osmý respondent uvedl, že je přístup k jeho síti filtrován na základě MAC adresy zařízení, jež se chce připojit. Skrytí názvu sítě pak uvedlo jen 26 dotazovaných. Poměrně velký počet účastníků průzkumu naopak vůbec nevěděl, jakým způsobem je jejich Wi-Fi síť zabezpečena. Pouze 10krát se v této otázce vyskytla odpověď, že dotyčný nevyužívá žádné z uvedených metod zabezpečení. 13 respondentů pak doplnilo svou vlastní odpověď, ve které zmínili zcela jinou techniku, kterou využívají pro zabezpečení své Wi-Fi sítě. Ani jeden ovšem nepatřil k těm, kteří uvedli, že nepoužívají žádné z uvedených zabezpečení. Ti, co využili možnost vlastní odpovědi, uvedli například oddělení sítě pro hosty, zapínání Wi-Fi sítě pouze v případě potřeby, pravidelnou kontrolu logů routeru či dálkový monitoring sítě prostřednictvím aplikace, která umožnuje nejen zjistit, jaká zařízení jsou aktuálně připojená, ale nabízí i možnost vybraná zařízení odpojit nebo dokonce zablokovat.

Graf 7: Použité metody zabezpečení



<u>Otázka č. 8:</u> Uveďte prosím poskytovatele Vašeho Wi-Fi připojení, respektive poskytovatele internetu.

Poslední otázka byla otevřenou a sloužila v podstatě pouze k tomu, aby byly v rámci dotazníkového šetření odlišeni od ostatních respondentů ti, kteří mají Wi-Fi síť od UPC. Není tedy potřeba uvádět, kolik z dotazovaných uvedlo kterého poskytovatele a stačí zmínit, že se poskytovatel UPC objevil v odpovědích hned 75krát. V některých z těchto

odpovědí ovšem figuroval, zřejmě z důvodu vlastnictví více Wi-Fi sítí, ještě jiný poskytovatel internetového připojení. Tyto odpovědi proto nebyly brány v potaz. Stejně tak se našlo několik respondentů, kteří uvedli, že poskytovatelem jejich internetového připojení je sice UPC, ale Wi-Fi síť si již poskytují sami. Ani tyto odpovědi tak nebyly do výsledného počtu započítány a z uvedených 75 dotazovaných tak zůstalo 68 z nich. Odpovědi těchto 68 respondentů budou porovnány s poznatky získanými z reálného průzkumu. Ačkoliv je pravdou, že se i mezi těmito respondenty mohou najít tací, kteří k provozu své bezdrátové sítě nepoužívají zařízení poskytované samotným UPC, ale mohou mít své vlastní, tato skutečnost s největší pravděpodobností nebude mít vliv na to, zda si dotyčný svou Wi-Fi síť lépe zabezpečil či nikoliv. Pokud si totiž dotyčný bude chtít změnit přístupové heslo k Wi-Fi síti, zřejmě nebude hrát velkou roli, zda má svůj vlastní router či využívá ten, který mu poskytlo UPC.

9.1.1 Shrnutí dotazníkového šetření

Výsledky tohoto dotazníku se nepochybně dají považovat za příznivé, a to především s ohledem na to, že zhruba 81 % dotazovaných uvedlo, že si změnili přístupové heslo ke své Wi-Fi síti. Vzhledem k tomu, že by v současné době mělo být například využití WPA2 standardem, není takový problém, že téměř třetina dotazovaných nevěděla, jakým zabezpečením jejich Wi-Fi síť disponuje. Úplným základem je totiž právě to, aby si jednotlivý vlastníci změnili přednastavené přístupové heslo, což v tomto průzkumu dle uvedených odpovědí učinil úctyhodný počet dotazovaných. Změnu SSID pak sice potvrdilo výrazněji méně respondentů, něco málo přes 58 %, ale i tento výsledek se však dá považovat za velmi úspěšný. Přijatelný byl rovněž počet těch, kteří si byli jisti změnou přístupových údajů k administraci routeru, jelikož tuto skutečnost uvedl téměř každý druhý účastník dotazníkového šetření.

Je ovšem potřeba zmínit, že přibližně čtvrtina dotazovaných uvedla, že mají zkušenosti v IT oblasti, ať již v rámci práce či studia, což nepochybně do jisté míry ovlivnilo získané výsledky. Nelze taktéž pochybovat o tom, že dotazník tohoto tématu vyplní především ti, kteří mají o této oblasti nějaké povědomí a naopak ti, kteří se o bezpečnost své sítě vůbec nezajímají, se pak pravděpodobně nebudou zdržovat vyplňováním dotazníku týkajícího se obdobného tématu. Z tohoto důvodu tak musí být výsledky tohoto dotazníkového šetření brány s určitou rezervou a směrodatnější tak nepochybně budou poznatky získané z reálného průzkumu, který bude představen na následujících stránkách.

9.2 Reálný průzkum

V závislosti na objevení bezpečnostní trhliny u některých routerů společnosti UPC, která spočívá v možnosti zjištění původního hesla k Wi-Fi síti díky znalosti přednastaveného SSID či MAC adresy daného zařízení, byl proveden průzkum, jehož podstatou bylo vyhledat co největší množství Wi-Fi sítí s tímto bezpečnostním nedostatkem. Dalším úkolem pak bylo identifikovat vlastníky těchto sítí, informovat je o dané skutečnosti a s jejich souhlasem pak případně existenci zranitelnosti prověřit. Výsledky získané na základě tohoto průzkumu pak byly porovnány s tím, co bylo zjištěno prostřednictvím elektronického dotazníku.

9.2.1 Použité zařízení a software

Ačkoliv pro operační systémy Windows a Linux existuje řada poměrně sofistikovaných nástrojů, jako je například aircrack-ng, InSSIDer či Kismet, které by v této práci nepochybně našli své uplatnění, vzhledem k povaze daného průzkumu by bylo využití notebooku značně nepraktické, a tak byl pro potřeby praktické části práce upřednostněn mobilní telefon Huawei P9 Lite s operačním systémem Android. Na základě této volby se pak tedy odvíjel i výběr samotného softwaru, jež byl nezbytný pro mapování dostupných Wi-Fi sítí, nalezení příslušných majitelů a rovněž prověření toho, zda je daná síť zranitelná či nikoliv. Níže je uvedena bližší specifikace použitého mobilního telefonu a seznam aplikací, které byly v rámci průzkumu využity.

Specifikace mobilního telefonu:

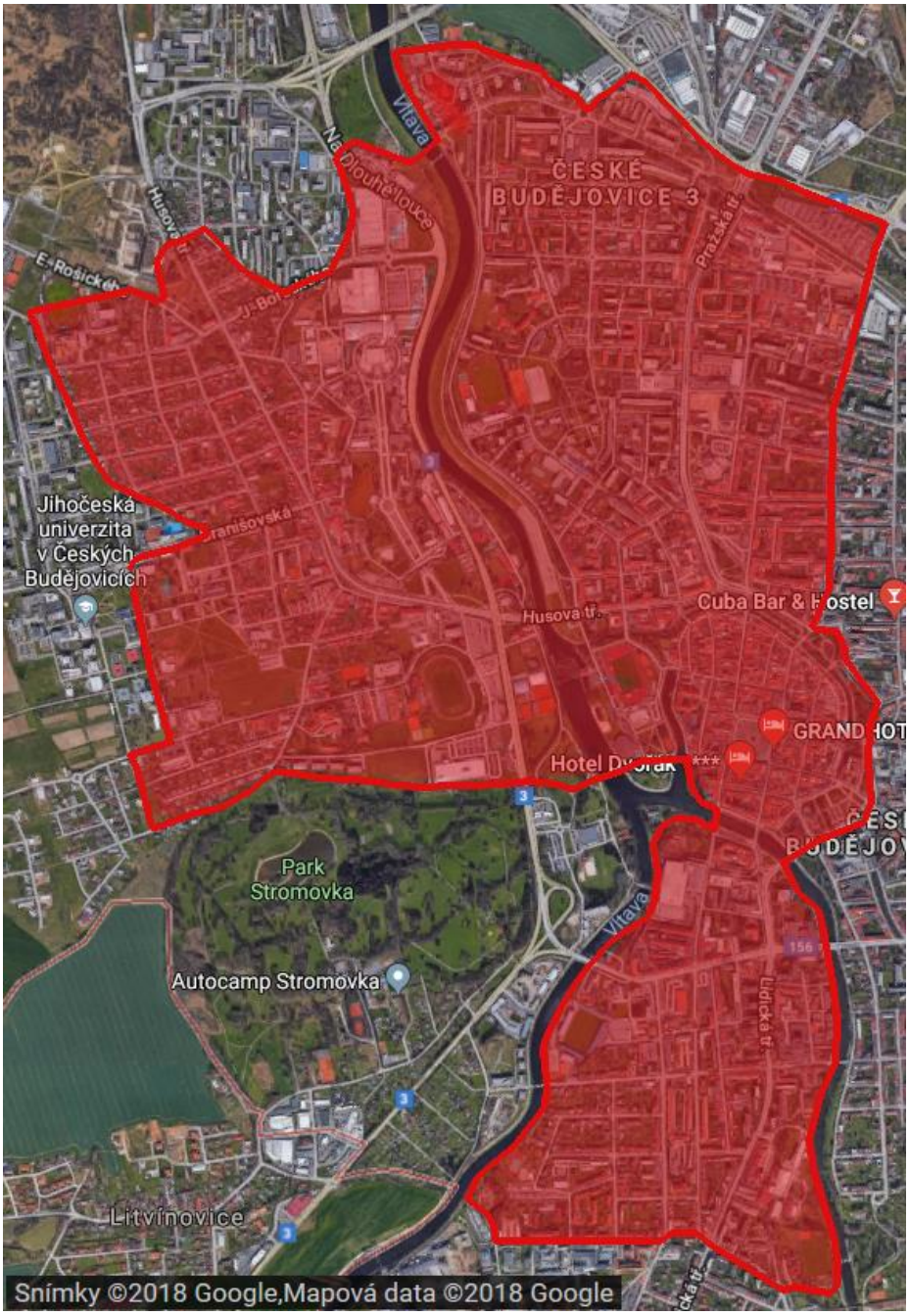
- **Operační systém** - Android 7.0 Nougat
- **Procesor** - HiSilicon Kirin 650 (4 jádra 2,0 GHz + 4 jádra 1,7 GHz, 64 bitů)
- **Paměť RAM** - 2 GB
- **Grafické jádro** - Mali-T830MP

Použité aplikace:

- **WiGLE WiFi Wardriving** - mapování dostupných Wi-Fi sítí
- **Google Earth** - promítnutí hledaných Wi-Fi sítí do mapy
- **WiFiAnalyzer** - vyhledání majitele dané Wi-Fi sítě
- **UPC Keygen, WIBR+** - prověření zranitelnosti dané Wi-Fi sítě

9.2.2 Oblast průzkumu

Po volbě vhodného zařízení a výběru vyhovujících aplikací již nic nebránilo tomu, aby byl samotný průzkum zahájen. K jeho provedení došlo v krajském městě Jihočeského kraje, tedy v Českých Budějovicích. Konkrétně se jednalo o městské části České Budějovice 1, 2, 3 a 7, kde by dle dostupnosti služeb UPC, měla být koncentrace Wi-Fi sítí od tohoto poskytovatele nejvyšší. Přesná oblast, ve které byly jednotlivé Wi-Fi sítě zachytávány, je vyznačena červenou barvou na obrázku 6.

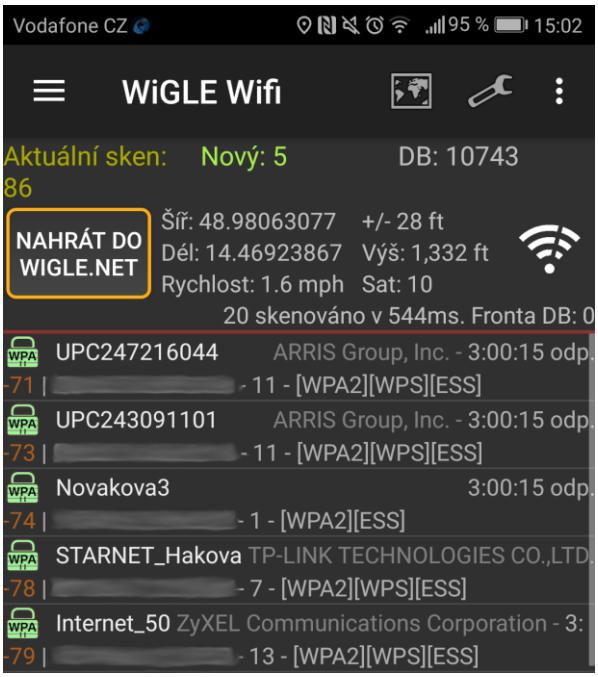


Obrázek 6: Oblast prováděného průzkumu. Screenshot převzat z (64)

9.2.3 Mapování dostupných Wi-Fi sítí

První krok, který bylo potřeba učinit, spočíval ve zmapování co možná největšího počtu Wi-Fi sítí od UPC v předem vybrané oblasti. Cílem ovšem nebylo vyhledat pouze ty Wi-Fi sítě, jejichž SSID obsahuje sedm číslic. Vzhledem ke stanoveným cílům a hypotézám bylo potřeba najít veškeré Wi-Fi sítě, které spadají pod tohoto poskytovatele. K danému účelu byla využita technika zvaná warwalking, která spočívá v tom, že se dotyčná osoba pohybuje v určité oblasti a pomocí k tomu určeného nástroje zachytává dostupné Wi-Fi sítě. Vyhledané sítě a informace o nich jsou pak zpravidla ukládány do veřejně přístupné databáze a stejně tak je jejich přibližná poloha zanesena do mapy. Velmi významnou roli v této oblasti hraje projekt zvaný wigle.net, který je založen právě na zachytávání Wi-Fi sítí jednotlivými uživateli po celém světě a jejich následném ukládání do centrální databáze. Zachycené sítě lze pak posléze promítnout do mapy a získat tak jejich přibližnou polohu. V současné době databáze čítá více než 400 milionů unikátních Wi-Fi sítí po celém světě.

V rámci tohoto projektu je volně dostupná i aplikace pro operační systém Android, zvaná WiGLE WiFi Wardriving. Pro mapování dostupných Wi-Fi sítí ve vybrané oblasti byla v tomto průzkumu zvolena právě tato aplikace, a to především z důvodu toho, že umožnuje získaná data exportovat do souborového formátu CSV nebo KML, což bylo velmi přínosné pro následné vyhledávání konkrétních sítí. Na obrázku 7 níže je zachycen scan dostupných sítí pomocí této aplikace.



Obrázek 7: Screenshot z aplikace WiGLE WiFi Wardriving

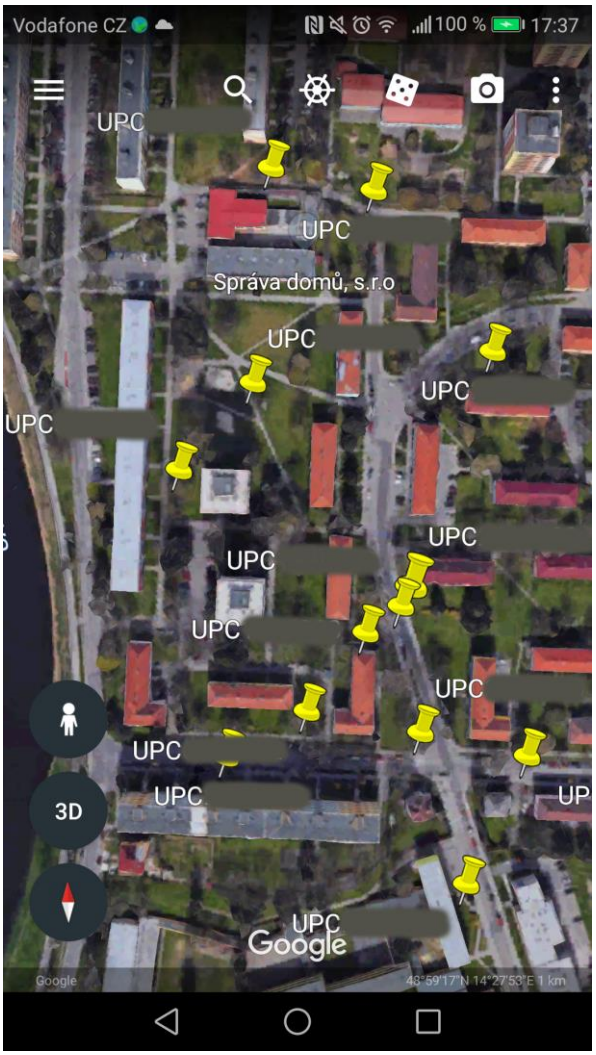
9.2.4 Vyfiltrování získaných dat

Poté, co bylo zachyceno dostatečné množství Wi-Fi sítí, bylo potřeba vybrat pouze ty sítě, které spadají pod poskytovatele UPC a pro následné prověření zranitelnosti pak především ty, jež splňují podmínku, že je jejich název tvořen ze zkratky UPC následovanou sedmi čísly. Právě v tuto chvíli přišla vhod možnost, kterou nabízí aplikace WiGLE WiFi Wardriving, tedy export dat ve formátu CSV. Takto získaný soubor pak stačí jednoduše otevřít například v Excelu, což bylo učiněno i v tomto případě, a vyfiltrovat pouze potřebné Wi-Fi sítě, ať již dle prefixu MAC adresy či na základě přítomnosti písmen UPC v názvu sítě.

Rovněž ale bylo nutné se zbavit duplicitních záznamů, které vznikly z důvodu toho, že aplikace WiGLE WiFi Wardriving obvykle pro určení přesnější polohy zaznamená danou Wi-Fi síť hned několikrát. Zaznamenané informace jsou odeslány na server a na základě porovnání dat odeslaných všemi uživateli, jež tuto síť zachytili, dochází ke zpřesnění polohy Wi-Fi sítě. Během jednoho uživatelského skenu dostupných sítí tak může vzniknout více záznamů vztahujících se k jedné konkrétní síti. Tyto záznamy se liší souřadnicemi místa, ve kterém byla síť zachycena a rovněž sílou signálu. Počet duplicitních dat byl navíc umocněn tím, že vzhledem k velikosti oblasti průzkumu muselo být vyhledávání sítí rozděleno do delšího časového úseku. Bylo tedy vždy nezbytné zahájit sken Wi-Fi sítí v místě, kde byl ukončen předchozí sběr dat a některé, již objevené sítě, tak pochopitelně byly zaznamenány znovu.

9.2.5 Promítnutí hledaných Wi-Fi sítí do mapy

Jelikož aplikace WiGLE WiFi Wardriving využívá GPS, jsou součástí získaných dat již zmíněné souřadnice místa, kde byla daná síť zachycena. Nabízí se zde tedy možnost promítnout nalezené Wi-Fi sítě do mapy a značně tak ulehčit proces zpětného dohledávání místa, kde byla konkrétní síť zachycena. Právě k tomuto účelu slouží formát KML, který umožňuje prezentaci geografických dat. Po vyfiltrování zachycených sítí v předchozím kroku tak stačilo překonvertovat formát CSV do formátu KML a výsledný soubor pak nahrát do aplikace Google Earth, s jejíž pomocí lze zobrazit jednotlivé Wi-Fi sítě na mapě. Na následující straně je screenshot z aplikace Google Earth, na kterém jsou zachyceny některé z hledaných Wi-Fi sítí. Z názvů jednotlivých sítí byla ponechána jen úvodní zkratka „UPC“ a zbylá část byla zakryta.

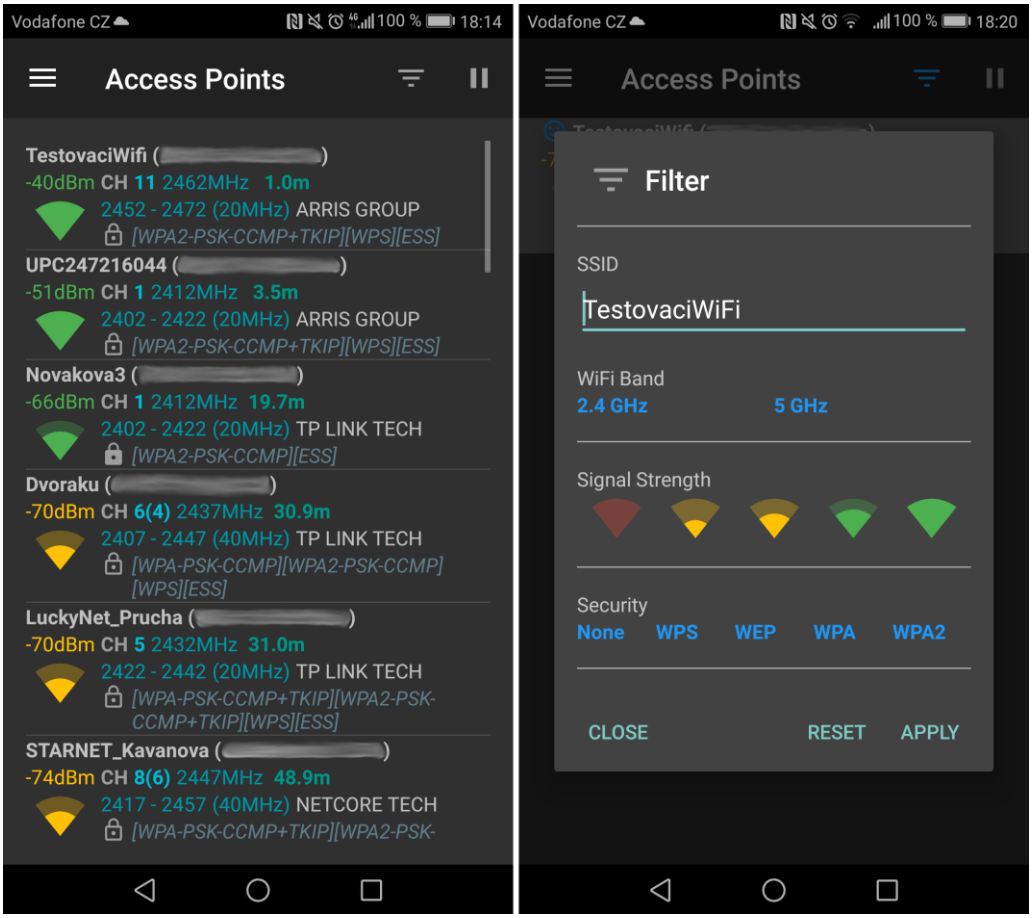


Obrázek 8: Screenshot z aplikace Google Earth - hledané Wi-Fi sítě

9.2.6 Vyhledání majitele dané Wi-Fi sítě

Ačkoliv došlo díky aplikaci Google Earth k získání polohy všech hledaných Wi-Fi sítí, v souboru předaném této aplikaci byly uvedeny pouze souřadnice bodu, ve kterém byla síla signálu dané Wi-Fi sítě při jejím zachycení nejsilnější. Zařízení, které danou síť vysílá, se tak sice bude nacházet někde v blízkém okolí, ale pro vyhledání příslušného majitele sítě je zapotřebí určit, odkud přesně je daný signál vysílán. Jelikož z veřejně dostupných zdrojů není možné zjistit, ať již na základě názvu dané sítě či MAC adresy přístupového bodu, komu daná Wi-Fi síť patří, byla síla signálu jedinou možností, jak příslušného majitele vyhledat. Pro tento účel tak bylo potřeba použít aplikaci, která je schopna zjistit a zobrazit několik základních údajů, a to název dané Wi-Fi sítě, MAC adresu přístupového bodu, výrobce příslušného zařízení a aktuální sílu signálu. Pochopitelně se dalo předpokládat, že se na daném místě bude vyskytovat až několik desítek dostupných Wi-Fi sítí, a tak bylo

rovněž vhodné, aby daná aplikace disponovala i filtrem, který by zajistil zobrazení informací jen o právě hledané Wi-Fi síti. Jednou z volně dostupných aplikací pro operační systém android, která všechny výše zmíněné podmínky splňuje, je WiFiAnalyzer, který byl použit i v rámci této práce. Jak je patrné z levé části obrázku 9, aplikace WiFiAnalyzer zobrazuje seznam aktuálně dostupných Wi-Fi sítí a u každé z nich je pak, kromě jiného, informace o aktuální síle signálu spolu s odhadovanou vzdáleností příslušného routeru od místa, kde se dotyčná osoba právě nachází. Pravá část obrázku pak zachycuje filtr, který má tato aplikace k dispozici. Filtrování lze realizovat na základě použitého typu zabezpečení, síly signálu, pásma či SSID. Právě poslední z uvedených možností, tedy filtrování dle názvu sítě, je ideální v případě, kdy je potřeba nalézt konkrétní Wi-Fi síť a je nežádoucí, aby se v seznamu dostupných sítí objevovala jakákoliv jiná bezdrátová síť.



Obrázek 9: Screenshoty z aplikace WiFiAnalyzer

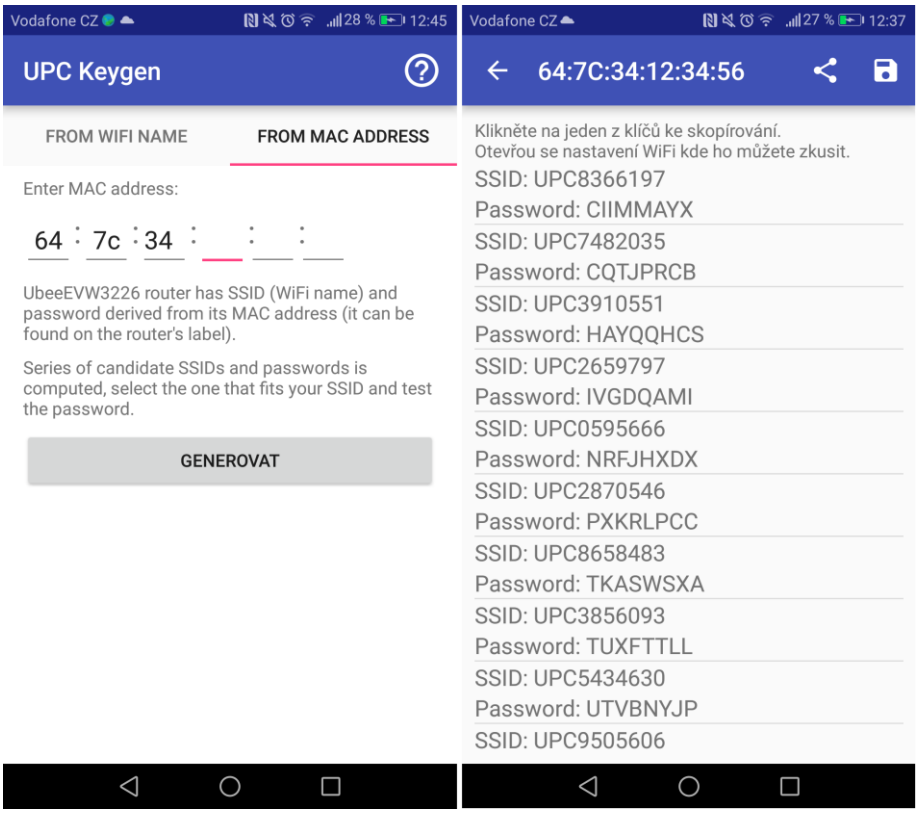
Vyhledání příslušného majitele dané Wi-Fi sítě ovšem byla poměrně náročná záležitost. Nejprve bylo nutné prozkoumat blízké okolí a na základě sledování změn v síle signálu určit, z jakého směru je daná síť vysílána. Díky tomuto snažení bylo zjištěno, z jakého objektu je signál vyzařován. Mnohdy se ovšem jednalo o budovu s více vchody, a proto

bylo zapotřebí nejprve zjistit, který z nich je ten správný. Ať již ale měl daný dům více vchodů či nikoliv, bylo nutné prostřednictvím domovního zvonku kontaktovat některého z obyvatelů a s jeho svolením získat přístup do vnitřních prostor. V případě, že byl zvolen správný vchod, stačilo již jen určit, u kterého z bytů je signál nejsilnější. Ne vždy se ovšem potenciální vlastník sítě nacházel doma, a tak bylo nutné se na dané místo opakovaně vracet a snažit se dotyčného zastihnout v různou dobu. V některých případech navíc nebylo patrné, u kterých bytových dveří je signál nejvýraznější, a proto bylo nezbytné zazvonit i u sousedních bytů či dokonce v přilehlých patrech a dopátrat se tak skutečného majitele.

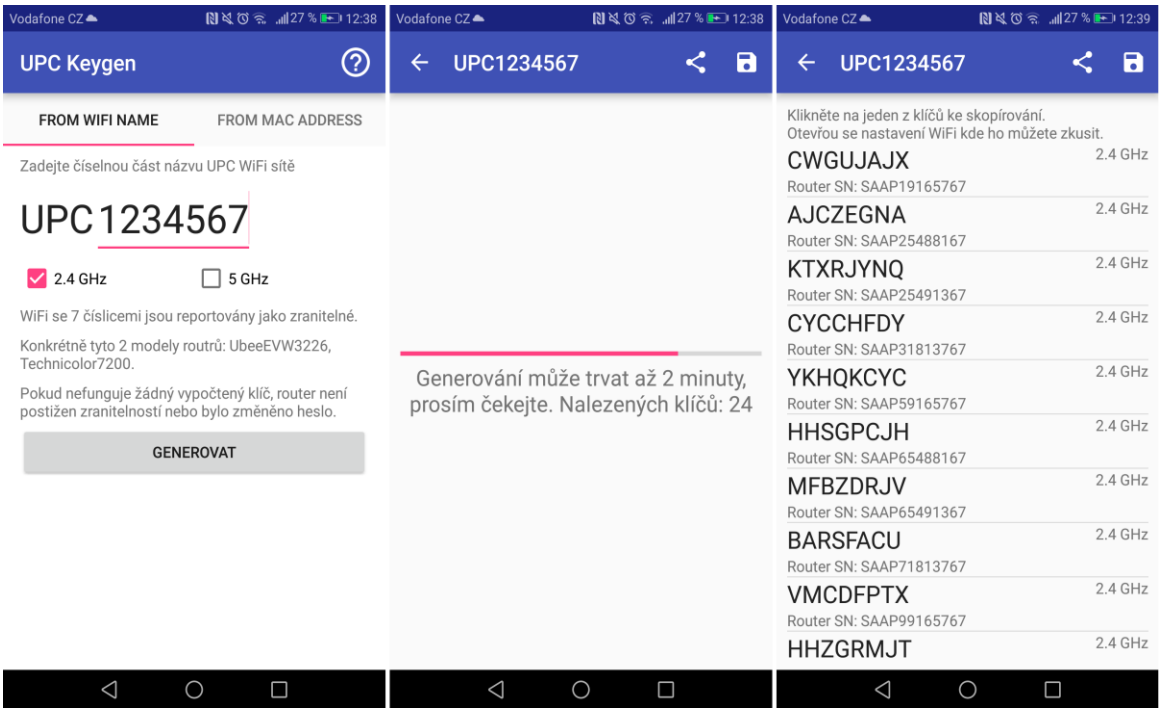
9.2.7 Prověření zranitelnosti

V případě, že k nalezení skutečného majitele došlo, byl dotyčný informován o možné zranitelnosti jeho bezdrátové sítě a bylo mu doporučeno změnit si přednastavené přístupové heslo a SSID – ačkoliv tedy název sítě po změně hesla není již nezbytně nutné měnit. Pokud s tím majitel dané sítě souhlasil, došlo rovněž k ověření toho, zda je jeho Wi-Fi síť zranitelná či nikoliv. K tomuto účelu byly použity dvě volně dostupné aplikace. První z nich nese název Keygen for UPC routers (UPC Keygen) a jejími autory jsou již zmiňovaní slovenští bezpečnostní experti, kteří při tvorbě této aplikace vycházeli z Geisslerova algoritmu, jež využívá zranitelnosti routeru Technicolor TC7200. Navíc pak ještě přidali možnost zjištění původního přístupového hesla pro model Ubee EVW3226.

Screenshoty z této aplikace jsou umístěny na následující straně. Na obrázku 10 je zachycen proces vygenerování hesel pro model Ubee EVW3226 a na obrázku 11 pak pro model Technicolor TC7200. Z levé části obrázku 10 je patrné, že uživatel musí zadat pouze druhou polovinu MAC adresy routeru, jelikož hodnota prefixu u routerů Ubee EVW3226 je vždy stejná. Po zadání MAC adresy lze vygenerovat seznam sítí obdobný tomu, který je zobrazen na screenshotu vpravo. V daném seznamu pak již jen stačí vyhledat záznam, ve kterém je SSID příslušné sítě a tím zjistit i odpovídající přístupové heslo. U modelu Technicolor TC7200 je potřeba zadat SSID dané sítě, nikoliv MAC adresu zařízení. Jelikož není problém zjistit, zda daná Wi-Fi síť vysílá v pásmu 2,4 či 5 GHz, je zbytečné, aby aplikace generovala hesla pro obě uvedená pásma a bylo tak potřeba vyzkoušet více kandidátů. Stačí tedy označit pouze jedno z uvedených pásem, jako je tomu na obrázku 11. Po stisknutí tlačítka generovat dojde k vygenerování potenciálních kandidátů, což je obvykle záležitost několika málo vteřin. Na posledním ze tří přiložených screenshotů je pak zachycena část seznamu hesel, které je potřeba postupně vyzkoušet.

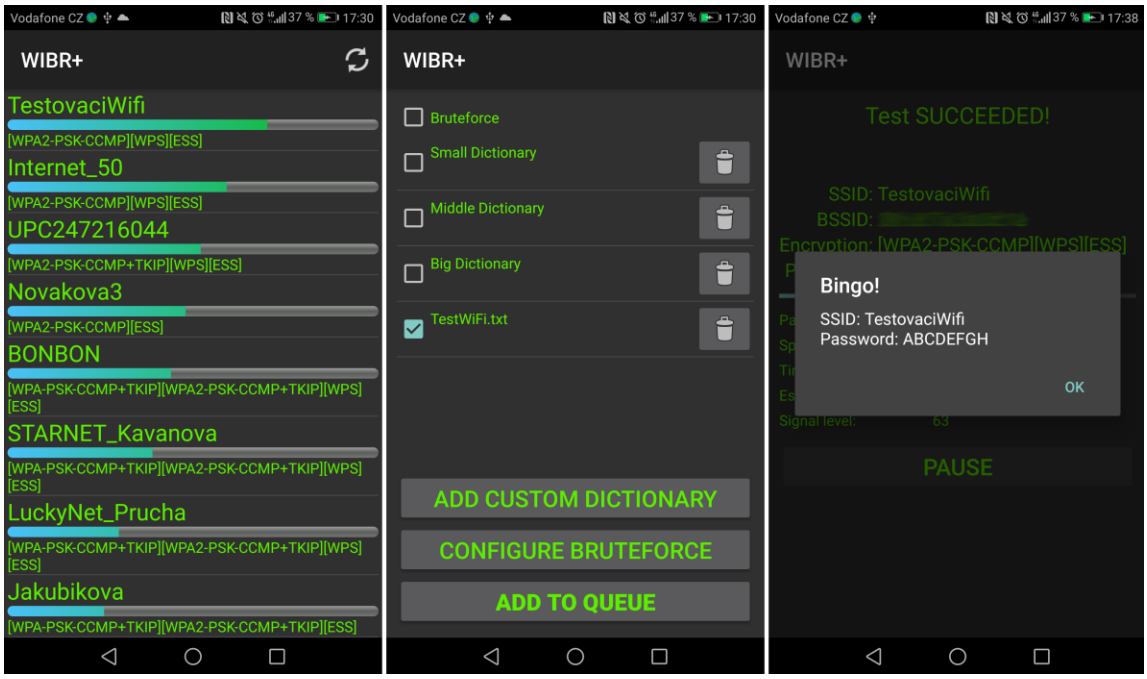


Obrázek 10: Screenshoty z aplikace UPC Keygen (Ubee EVW3226)



Obrázek 11: Screenshoty z aplikace UPC Keygen (Technicolor TC7200)

Ačkoliv počet kandidátů vygenerovaných na základě zadaného SSID není příliš vysoký a obvykle se pohybuje od 20 do 30 hesel, ruční zadávání by bylo časově poměrně náročnou záležitostí. Z tohoto důvodu přišla vhod aplikace WIBR+, která umí vyzkoušet hesla z předem vytvořeného slovníku. Jelikož se ale seznam vygenerovaných hesel liší na základě zadaného SSID, bylo potřeba pro každou z hledaných Wi-Fi sítí vytvořit vlastní slovník. V případě, že s tím majitel Wi-Fi sítě souhlasil, pak tedy stačilo předat aplikaci odpovídající slovník a počkat, až dojde k vyzkoušení jednotlivých hesel a bude zjištěno, zda je některé z nich platné. Zjištění přístupového hesla k Wi-Fi síti pomocí aplikace WIBR+ je znázorněno na obrázku 12. Nejprve je potřeba vybrat Wi-Fi síť, která má být otestována, následně zvolit příslušný slovník a pak již jen vyčkat, zda se skutečné přístupové heslo v daném slovníku nachází či nikoliv.



Obrázek 12: Screenshoty z aplikace WIBR+

9.3 Výsledky průzkumu

Sběr Wi-Fi sítí byl realizován především v termínu od 10. do 30. října 2017 a celkem bylo prostřednictvím aplikace WiGLE WiFi Wardriving vytvořeno 46 026 záznamů. Vzhledem k tomu, že většina sítí byla zaznamenána hned několikrát, byl počet unikátních Wi-Fi sítí po odstranění duplicitních záznamů roven číslu 10 629. Z tohoto počtu spadalo 253 Wi-Fi sítí pod poskytovatele UPC, což bylo možné určit na základě nezměněného SSID. Pro účely této práce bylo ovšem zapotřebí vybrat pouze ty sítě, jež měly za zkratkou UPC sedm čísel. Tuto podmínku splňovalo celkem 110 nalezených Wi-Fi sítí.

9.3.1 Wi-Fi sítě od UPC se změněným SSID

S ohledem na to, že výše uvedených 253 Wi-Fi sítí od UPC zahrnuje pouze ty sítě, které neměly změněné SSID, byl počet nalezených sítí, spadajících pod tohoto poskytovatele, ještě o něco vyšší. Na základě existence projektu Wifileaks, který je v podstatě obdobou projektu wigle.net, lze i navzdory změněnému SSID zjistit, které sítě jsou s největší pravděpodobností rovněž poskytované UPC. Na stránkách projektu Wifileaks[14] jsou totiž pravidelně zveřejňovány soubory v datovém formátu .tsv, které zahrnují všechny zmapované Wi-Fi sítě v České republice od samotného vzniku tohoto projektu. Jelikož naposledy nahrané soubory čítají více jak dva a půl milionu doposud zachycených Wi-Fi sítí, je možné zjistit, jaké prefixy MAC adresy využívají Wi-Fi sítě od UPC. Ve výsledném souboru, který byl vygenerován aplikací WiGLE WiFi Wardriving, pak tedy bylo nutné se pokusit vyhledat všechny prefixy, které byly dle Wifileaks obsazené sítěmi od UPC a z nalezených sítí pak odstranit již zmiňovaných 253 sítí, které měly původní SSID. Díky tomuto pak s největší pravděpodobností zůstaly pouze Wi-Fi sítě poskytované společností UPC, jejichž název byl změněn.

Ačkoliv se lze setkat hned s několika typy SSID, které jsou charakteristické pro Wi-Fi sítě od UPC, pro každý typ jsou vyhrazeny určité prefixy MAC adresy, a tak mohlo být u sítí se změněným názvem zjištěno, jakého typu bylo původní SSID. Díky tomu bylo následně vyhodnoceno, u kterého z nich byl u zachycených sítí měněn název nejčastěji. Zjištěné poznatky jsou uvedeny v tabulce 1 a pro lepší představu pak prezentovány prostřednictvím grafu 8, který se nachází na následující straně.

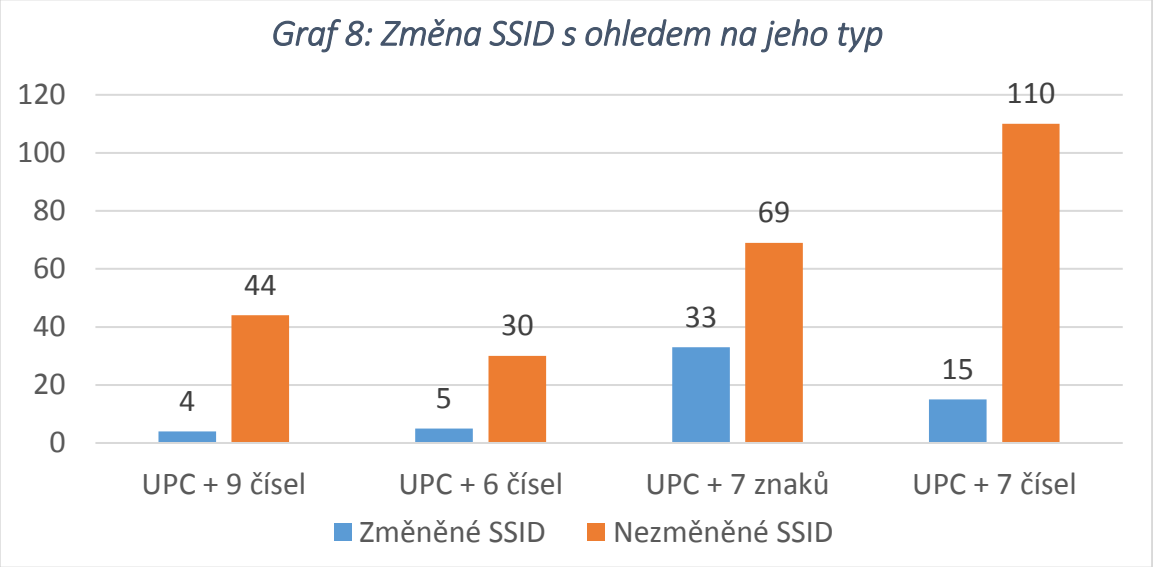
Typ SSID	Počet zachycených sítí	Nezměněné SSID	Změněné SSID
UPC + 9 čísel	48	44 (91,67 %)	4 (8,33 %)
UPC + 6 čísel	35	30 (85,71 %)	5 (14,29 %)
UPC + 7 znaků	102	69 (67,65 %)	33 (32,35 %)
UPC + 7 čísel	125	110 (88 %)	15 (12 %)
Celkem	310	253 (81,61 %)	57 (18,39 %)

Tabulka 1: Změna SSID na základě typu

[14] Webové stránky projektu Wifileaks jsou dostupné na adrese www.wifileaks.cz

Z tabulky 1 je patrné, že bylo nalezeno celkem 310 Wi-Fi sítí od UPC, z nichž nebylo SSID změněno ve 253 případech. Ke změně názvu naopak došlo u 57 sítí, což činí zhruba 18 %. Je tedy zřejmé, že byl zjištěný výsledek, v porovnání s tím, co vyplynulo z dotazníkového šetření, o poznání horší. V dotazníku totiž změnu přednastaveného SSID potvrdilo přibližně 57 % respondentů. Pokud se pak zaměříme pouze na ty, kteří ve dvanácté otázce uvedli jako poskytovatele bezdrátového připojení UPC, z celkového počtu 68 dotazovaných si název sítě změnilo hned 41 z nich, tedy zhruba 60 %.

Co se týče změny SSID v rámci jednotlivých skupin, nejméně si dle průzkumu mění SSID ti, jejichž název sítě je tvořen ze zkratky UPC následovanou devíti čísly. Ze 48 zachycených sítí byl název změněn pouze 4krát. Nejčastěji byl tento identifikátor naopak změněn u sítí s původním názvem ve tvaru UPC a sedm znaků. Jedná se o Wi-Fi sítě, které mají na posledních sedmi pozicích názvu kromě čísel rovněž i písmena. Z celkového počtu 102 sítí byl název změněn téměř u každé třetí Wi-Fi sítě. Překvapivým zjištěním pak byla skutečnost, že ze 125 nalezených sítí, které dle prefixu spadaly do skupiny těch, jež mají v původním názvu pouze sedm čísel, došlo ke změně SSID jen v 15 případech. To odpovídá zhruba 12 % a jedná se tak o druhý nejhorší výsledek ze všech uvedených typů.



V tuto chvíli je vhodné připomenout jeden z cílů praktické části této práce, který spočíval ve zjištění toho, zda je SSID, které se skládá ze zkratky UPC + 7 čísel, měněno častěji, než jiné typy SSID od UPC. Na základě tohoto cíle měla být vyřešena následující hypotéza:

Hypotéza 1) *SSID, jež je tvořeno zkratkou UPC a sedmi čísly je měněno častěji, než jiná SSID od poskytovatele UPC.*

Jelikož byl uvedený typ SSID měněn naopak téměř v nejmenší míře, v rámci tohoto průzkumu se výše uvedená hypotéza nepotvrdila, a to i navzdory tomu, že se o existujícím problému, který se týká právě tohoto typu názvu, psalo na mnoha webech, které se zabývají oblastí počítačů a informačních technologií obecně. Navíc rovněž i samotné UPC po odhalení tohoto problému uvedlo, že byli příslušní zákazníci, kterých se vzniklá zranitelnost týká, o daném problému informováni, respektive jim byla prostřednictvím vyúčtování několikrát po sobě doporučena změna přednastaveného přístupového hesla k jejich bezdrátové síti. Tehdejší tiskový mluvčí UPC David Frodl navíc uvedl, že poskytovatel nemá na podobu hesel ani na způsob, jakým dochází k jejich generování žádný vliv, jelikož je za toto zodpovědný samotný výrobce daných zařízení. (65)

9.3.2 Prověření zranitelnosti nalezených sítí

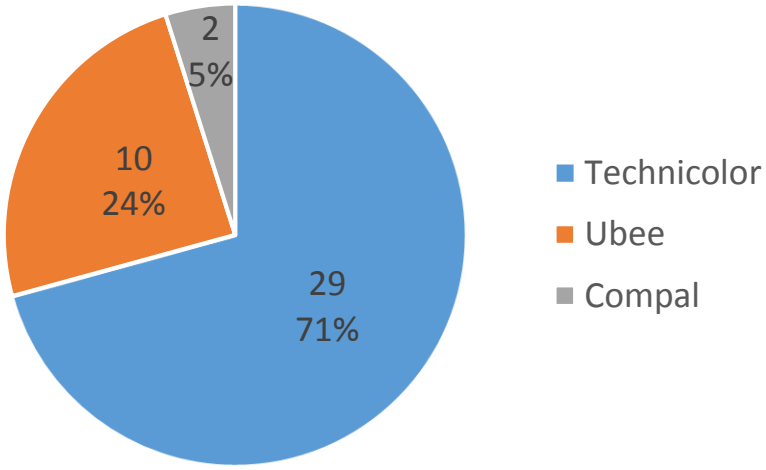
Z celkového počtu 110 Wi-Fi sítí, jejichž název obsahoval 7 číslic a tím pádem se na ně vztahovala zjištěná zranitelnost, byla v 79 případech Wi-Fi síť vysílána zařízením Technicolor TC7200, v 28 případech zařízením Ubee EVW3226 a třikrát se jednalo o router výrobce Compal Broadband Networks. Poslední tři uvedená zařízení ovšem spadají do skupiny těch sítí, jejichž původní název obsahuje nejen čísla, ale i písmena a při tvorbě SSID tak s největší pravděpodobností pouze došlo k tomu, že nebylo vygenerováno ani jedno písmeno, ale pouze samá čísla. Těchto zařízení by se tak daná zranitelnost týkat neměla.

Samotný proces hledání jednotlivých majitelů 110 nalezených Wi-Fi sítí probíhal během února a března roku 2018, tedy s určitým časovým odstupem od doby, kdy byly tyto sítě zachyceny. Tato skutečnost měla za následek to, že několik málo Wi-Fi sítí, se zpětně nepodařilo dohledat, jelikož již zřejmě neexistovaly.

Ačkoliv bylo vynaloženo značné úsilí, aby byl počet prověřených sítí co možná největší, pochopitelně se dalo předpokládat, že se zranitelnost podaří ověřit jen u určité části z celkového počtu. Bylo totiž nutné nejen určit konkrétní objekt, ze kterého je daná Wi-Fi síť vysílána, ale rovněž získat souhlas majitele dané Wi-Fi sítě k tomu, aby mohla být zranitelnost otestována. Třebaže se ve valné většině případů na základě síly signálu podařilo určit konkrétní byt či rodinný dům, ne vždy se podařilo potenciálního majitele zastihnout, a to i přes to, že ve všech případech došlo k opakovaným pokusům o jeho kontaktování. Vyhledání konkrétního majitele bylo značně ztíženo i tím, že nejednou došlo k situaci, kdy bylo dle signálu patrné, z jakého bytu je bezdrátová síť vysílána a rovněž se

podařilo některého z obyvatelů příslušného bytu zastihnout, ale dotyčný uvedl, že Wi-Fi síť od UPC nemá. Bylo tak nutné ověřit, zda příslušná síť skutečně nepatří někomu jinému, což zpravidla znamenalo pouze investovaný čas navíc bez valného úspěchu. Našli se rovněž tací, kteří sice sdělili, že mají Wi-Fi síť od UPC či dokonce potvrdili, že je hledaná Wi-Fi síť jejich, ale s prověřením toho, zda je jejich síť zranitelná, již nesouhlasili. Výsledkem tak bylo to, že z celkového počtu 110 sítí, se podařilo vyhledat majitele a získat souhlas k otestování jeho Wi-Fi sítě ve 41 případech. V grafu 9 níže jsou zobrazeny počty úspěšně ověřených routerů na základě výrobce daného zařízení.

Graf 9: Úspěšně ověřená zařízení



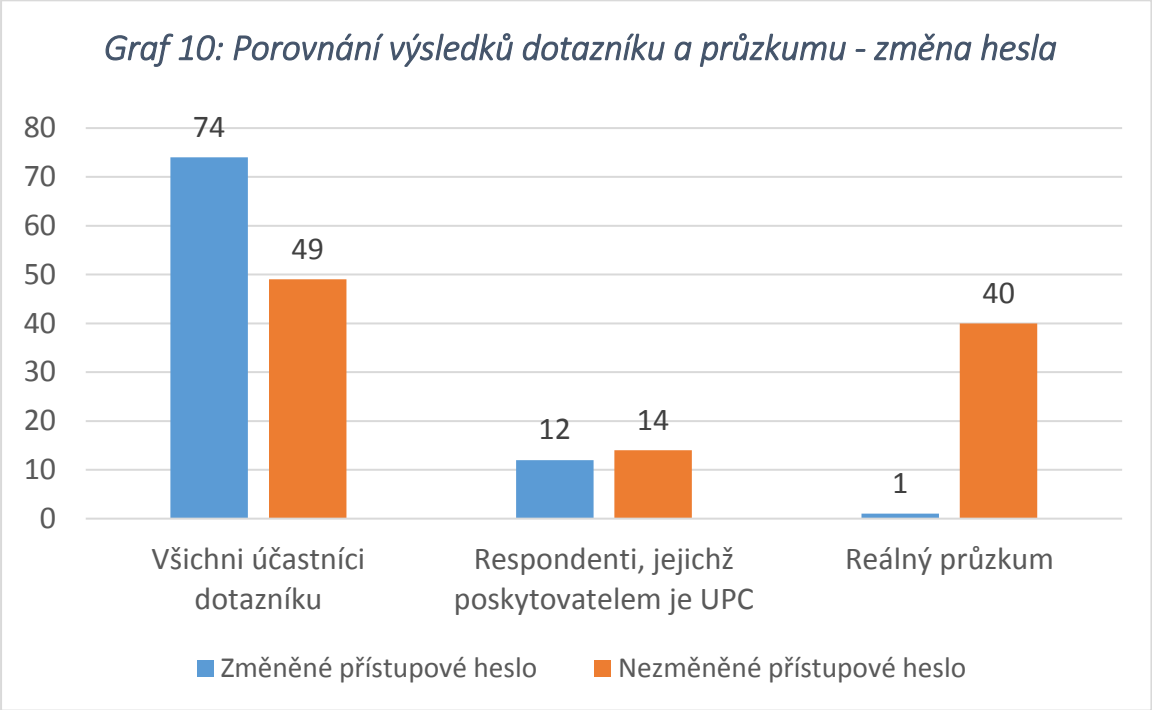
Z grafu 9 je patrné, že bylo otestováno nejvíce routerů typu Technicolor TC7200. Tato skutečnost nebyla velkým překvapením, jelikož Wi-Fi sítí vysílaných prostřednictvím tohoto zařízení bylo v průzkumu nalezeno nejvíce. Routerů Ubee EVW3226 pak bylo otestováno zhruba třikrát méně. Poměrně velkým úspěchem ovšem bylo to, že se podařilo prověřit zranitelnost hned u dvou ze tří nalezených zařízení výrobce Compal Broadband Networks.

Na základě otestování zranitelnosti u všech 41 sítí došlo ke zjištění hesla ve 36 případech. Přístupové heslo se tedy nepodařilo zjistit pouze u 5 Wi-Fi sítí. Nebylo to ovšem z důvodu toho, že by si všichni majitelé těchto sítí změnili své přístupové heslo. Ve dvou případech se totiž jednalo o zařízení Compal, na které by se daná zranitelnost vztahovat neměla. Vzhledem k tomu, že si ani jeden z majitelů těchto dvou Wi-Fi sítí nebyl vědom toho, že

by si přístupové heslo měnil, s největší pravděpodobností se tento bezpečností problém daného typu routeru skutečně netýká. Je to ovšem pochopitelné už jen na základě skutečnosti, že u tohoto typu zařízení je SSID generováno nejen z čísel, ale i z písmen, a tak není pochyb o tom, že je původní název sítě vytvořen za pomocí jiného algoritmu, než toho, který je využit u Technicoloru TC7200 či Ubee EVW3226.

U dvou Wi-Fi sítí, kterých by se ovšem již tento bezpečnostní problém týkat měl, nebylo heslo rovněž odhaleno ani přesto, že oba vlastníci shodně uvedli, že si původní přístupové heslo nezměnili. Jelikož se v obou případech jednalo o zařízení Technicolor TC7200 a prefix MAC adres daných sítí byl stejný, je možné, že tato zařízení mají méně běžný prefix sériového čísla, který není aplikací UPC Keygen podporován. Ta totiž u routeru Technicolor TC7200 bere v potaz pouze sériová čísla, která začínají prefixem SAAP, SAPP či SBAP. Pokud tedy existuje ještě některý jiný, ne tak rozšířený, prefix sériového čísla pro tento model routeru, aplikace UPC Keygen pro dané zařízení odpovídající přístupové heslo nevygeneruje. Poslední Wi-Fi síť, u které nebylo původní heslo platné, byla síť vysílaná zařízením Ubee EVW3226. Jelikož u tohoto typu routeru lze vygenerovat na základě znalosti MAC adresy pro dané SSID jedno konkrétní přístupové heslo, bylo sice původní heslo zjištěno, ale vlastník sítě uvedl, že si nastavil heslo nové. I přesto bylo heslo vygenerované aplikací UPC Keygen pro jistotu vyzkoušeno. Dle očekávání ale bylo vyhodnoceno jako neplatné.

Z doposud uvedeného tak vyplývá, že ačkoliv se z celkového počtu úspěšně otestovaných sítí nepodařilo přístupové heslo zjistit u pěti Wi-Fi sítí, pouze u jediné z nich to bylo z důvodu změny přednastaveného přístupového hesla. Z celkového počtu 41 Wi-Fi sítí tak ke změně došlo pouze v jednom jediném případě. Pro porovnání dat získaných z dotazníku s těmi, které byly zjištěny na základě reálného průzkumu, je na následující straně uveden graf číslo 10. Jelikož byly vyhledáváni majitelé pouze těch bezdrátových sítí, které neměly změněné SSID, bylo potřeba pro porovnání dat do grafu promítnout jen odpovědi těch respondentů, kteří v dotazníku uvedli, že si název své Wi-Fi sítě nezměnili.



V první kategorii jsou zahrnuti všichni dotazovaní, kteří sdělili, že si SSID své sítě nezměnili. Do druhé kategorie pak spadají pouze ti, kteří v dotazníku kromě nezměněného SSID uvedli, že je poskytovatelem jejich bezdrátového připojení UPC. Poslední dva sloupce pak reprezentují výsledky získané z reálného průzkumu. Z grafu je patrné, že z celkového počtu 123 respondentů, kteří si nezměnili své SSID, si heslo změnilo 74 z nich, což činí zhruba 60 %. U těch, kteří spadají pod poskytovatele UPC je pak situace o něco horší, jelikož si z celkového počtu 26 dotazovaných heslo změnilo pouze 12. To odpovídá přibližně 46 %. I to je ovšem velmi dobrý výsledek v porovnání s tím, co bylo zjištěno díky skutečnému průzkumu. V tom totiž došlo k nastavení nového přístupového hesla pouze v jednom případě z celkového počtu 41 Wi-Fi sítí.

Na základě uvedených poznatků je nyní možné potvrdit či vyvrátit další dvě stanovené hypotézy, které byly následující:

Hypotéza 2) *Stále existují zařízení, u nichž je možné na základě znalosti SSID či MAC adresy zjistit původní přístupové heslo k dané Wi-Fi síti.*

Hypotéza 3) *Ve skutečnosti nebudou v provedeném průzkumu majitelé Wi-Fi sítí klást na změnu SSID a hesla takový důraz, jako tomu bude v dotazníkovém šetření.*

Cílem, ke kterému se vztahovala první z uvedených hypotéz, bylo zjistit, zda UPC danou zranitelnost již napravilo a pokud ano, jakým způsobem k tomu došlo. Jelikož se i po dvou

letech od zveřejnění problému stále vyskytují Wi-Fi sítě s touto zranitelností, byla hypotéza číslo 2 potvrzena a problém tedy stále přetrvává. Dalším cílem pak bylo zjistit, zda odpovědi uvedené v dotazníku alespoň přibližně korespondují s tím, co bylo zjištěno na základě reálného průzkumu. Jelikož bylo u nalezených sítí SSID měněno daleko v menší míře a výsledky týkající se změny hesla byly u otestovaných sítí v porovnání s dotazníkovým šetřením ještě daleko horší, byla potvrzena i hypotéza číslo 3. Ta totiž předpokládala, že majitelé Wi-Fi sítí nebudou ve skutečnosti na změnu těchto údajů klást takový důraz, jako tomu bude u provedeného dotazníkového šetření.

9.3.3 Poskytnutí pomoci se změnou přednastavených údajů

Jelikož se dalo předpokládat, že ne všichni vyhledaní majitelé budou schopni si přístupové heslo a SSID změnit, nemělo by pouhé doporučení na změnu hesla tak velký efekt. Z tohoto důvodu byl pro oba z uvedených modelů routerů, tedy jak pro Technicolor TC7200, tak pro Ubee EVW3226, vytvořen návod na změnu těchto údajů. Tento návod byl po ověření zranitelnosti jednotlivým vlastníkům předáván v tištěné podobě. Oba návody jsou uvedeny na konci práce jako přílohy.

Ačkoliv bylo předání návodu většinou naprosto dostačující, ve čtyřech případech si nalezení majitelé nebyli jisti tím, zda si budou schopni nové heslo a SSID nastavit sami, a tak požádali o poskytnutí pomoci s přenastavením jejich sítě. Dotyčným tak bylo názorně ukázáno, jak se dostanou do administrace routeru a kde je možné nastavit si jak nové přístupové heslo, tak název Wi-Fi sítě. Poté, co si dotyčný heslo změnil, bylo ještě nutné odpovídající heslo nastavit ve všech zařízeních, které se k dané síti připojovaly. Nutnost nastavení nového přístupového hesla i v zařízeních, které se k Wi-Fi síti připojují, byla pro jistotu uvedena i v předávaných návodech.

9.3.4 Počet zranitelných zařízení

Pro vytvoření představy o tom, jakého množství zařízení se může problém řešený v této práci týkat, bude na následující straně uvedena tabulka, která byla vytvořena na základě dat získaných z projektu Wifileaks. Konkrétně byl k tomuto účelu použit soubor z dubna roku 2018, který čítá 2 829 276 zaznamenaných Wi-Fi sítí.[15] V daném souboru byly vyhledány jen ty prefixy, na kterých se vyskytují Wi-Fi sítě od UPC, které mají v názvu za zkratkou tohoto poskytovatele 7 čísel a mělo by se tak jednat o zranitelné sítě, jež vysílá zařízení

[15] Použitý soubor je volně přístupný na následující adrese: download.wifileaks.cz/data

Technicolor TC7200 či Ubee EVW3226. Jednotlivé prefixy a počty nalezených sítí se změněným či nezměněným SSID jsou zachyceny v tabulce 2 níže. Zelenou barvou jsou označeny ty prefixy, které byly zachyceny i během průzkumu a alespoň na jednom zařízení s tímto prefixem došlo k úspěšnému zjištění hesla. Žlutě je označen zmiňovaný prefix, kterým disponovaly dvě otestované sítě, jež by měly být rovněž zranitelné, ale heslo se zjistit nepodařilo. Modrá barva je použita u těch prefixů, které se během průzkumu buď nepodařilo otestovat či vůbec nebyly zachyceny.

Prefix	Celkový počet sítí	Defaultní SSID	Změněné SSID
08:95:2a	608	433	175
44:32:c8	5 023	4189	834
58:23:8c	8 312	7188	1 124
64:7c:34	14 317	11734	2 583
80:c6:ab	559	441	118
88:f7:c7	20 522	17557	2 965
8c:04:ff	2 486	2114	372
b0:c2:87	57	34	23
c4:27:95	11 597	9664	1933
cc:03:fa	68	30	38
cc:35:40	2 077	1792	285
e0:88:5d	84	48	36
fc:94:e3	266	178	88
Celkem	**65 976**	**55 402 (84 %)**	**10 574 (16 %)**

Tabulka 2: Prefixy zranitelných zařízení

Je potřeba podotknout, že do sítí s defaultním SSID byly započítány i ty sítě, které sice měly název upravený, ale i v novém názvu se objevovalo původní SSID, a to buď celé, nebo jeho část. Jednalo se například o případy, kdy byl původní název ponechán a za něj bylo přidáno jméno či příjmení. K zahrnutí těchto sítí mezi ty s defaultním SSID tak došlo z toho důvodu, že jsou dané sítě zranitelné navzdory provedené změně názvu. Takových sítí bylo ovšem naprosté minimum, a tak jejich započítání mezi sítě s defaultním SSID nehraje téměř žádnou roli. Každopádně z tabulky 2 vyplývá, že bylo na území České

republiky doposud zachyceno téměř 66 tisíc Wi-Fi sítí, kterých se daný problém týká. Za zmínku stojí skutečnost, že si SSID změnilo přibližně 16 % z celkového počtu, což se téměř neliší od výsledku, kterého bylo dosaženo během skutečného průzkumu. V něm bylo SSID z celkového počtu nalezených sítí od UPC změněno zhruba u 18 % sítí. U těch, které měly v názvu sedm čísel, došlo ke změně názvu přibližně ve 12 %. Pokud by s průzkumem alespoň přibližně korespondovala i změna přístupového hesla u Wi-Fi sítí s nezměněným SSID, znamenalo by to, že bylo doposud zachyceno okolo 50 000 zařízení, u kterých by mohla být zranitelnost, vzhledem k nezměněnému přístupovému heslu, zneužita (-počítáme-li tedy pouze ty prefixy, u nichž byla zranitelnost skutečně ověřena a jsou v tabulce označeny zelenou barvou).

Pochopitelně je ale potřeba brát v potaz, že se jedná o Wi-Fi sítě zachycené za několik posledních let, a tak některé z nich již nemusí a pravděpodobně ani nebudou existovat. Na druhou stranu je potřeba zmínit, že nepochybně existují i další Wi-Fi sítě, které ještě nebyly nikým zachyceny a v celkovém počtu tak nejsou zahrnuty. Změna SSID navíc nutně nezaručuje, že si vlastník sítě změnil i přístupové heslo. Sítě s prefixem 64:7c:34, který odpovídá zařízením Ubee EVW3226, tak mohou být zranitelné i přes změněný název, jelikož u tohoto typu routeru dochází ke zjištění přednastaveného hesla na základě znalosti MAC adresy, nikoliv názvu sítě.

9.3.5 Informování zákazníků o existenci bezpečnostního problému

V kapitole 9.3.1 pojednávající o Wi-Fi sítích poskytovatele UPC se změněným SSID byla vyvrácena hypotéza, která předpokládala, že bude problémové SSID měněno častěji než ostatní typy. Tato hypotéza vycházela z toho, že se jednotliví vlastníci o existenci problému mohli dočíst například na internetu a na základě tohoto zjištění si raději své SSID spolu s přístupovým heslem změnili – tím spíše, když UPC údajně jednotlivé zákazníky o nutnosti změny těchto údajů několikrát informovalo prostřednictvím vyúčtování. Během prováděného průzkumu si ovšem jednotliví vlastníci nebyli vědomi toho, že by byli na vzniklou situaci upozorněni a nikdo z nich netušil, že tato zranitelnost existuje. V provedeném průzkumu tak tímto byla potvrzena poslední stanovená hypotéza, která zněla následovně:

Hypotéza 4) *Většina majitelů otestovaných Wi-Fi sítí ani po roce a půl od zveřejnění bezpečnostního problému nebude tušit, že jejich síť obsahuje příslušnou zranitelnost.*

Je tedy otázkou, zda byli dotyční vlastníci prostřednictvím vyúčtování informováni pouze o tom, že si mají přednastavené údaje změnit, či byl uveden i důvod, proč je potřeba tento krok učinit. Pokud by totiž byla spolu s doporučením na změnu hesla stručně představena i příslušná zranitelnost, zřejmě by změnu těchto údajů provedl větší počet vlastníků daných sítí, než v případě pouhého konstatování, že je na jejich zařízení potřeba nastavit nové přístupové heslo.

9.4 Žádost o vyjádření zaslaná samotnému UPC

Ačkoliv se UPC k problému vyjádřilo prakticky ihned po zveřejnění problému, tedy v lednu roku 2016, od této doby uplynuly již více jak dva roky a situace se nijak razantně nezměnila. Proto došlo k odeslání žádosti o vyjádření k současné situaci na dva kontaktní e-maily uvedené na stránkách UPC. První žádost byla směřována samotnému tiskovému mluvčímu UPC Jaroslavu Kolárovi a druhá byla odeslána prostřednictvím formuláře na webových stránkách této společnosti. V žádosti byly stručně shrnuty poznatky získané z průzkumu a následně byl položen dotaz, zda UPC v současné době pracuje na nějakém řešení, jak tento bezpečnostní problém odstranit. Vzhledem k tomu, že si jednotliví majitelé existence zranitelnosti nebyli vědomi, byla rovněž položena otázka, jakým konkrétním způsobem byli zákazníci, jichž se daný problém týká, o situaci informováni. Bohužel se však ani po více jak dvou týdnech od prvního kontaktování nepodařilo vyjádření získat. První žádost o vyjádření směřována tiskovému mluvčímu Jaroslavu Kolárovi zůstala bez odpovědi. O několik dní později tedy byla odeslána zpráva prostřednictvím formuláře. Na tuto zprávu sice přišla druhý den odpověď, ve které stálo, že byl dotaz přesměrován ke kompetentnímu oddělení, od té doby již ovšem uplynul více jak týden a žádné vyjádření doposud rovněž nepřišlo.

9.5 Návrhy vedoucí ke zlepšení stavu

Je sice pravdou, že generování přístupových hesel či SSID k dané Wi-Fi síti má na starost výrobce příslušného zařízení, samotný poskytovatel ovšem nepochybně může ovlivnit, jaká zařízení má ve své nabídce a po zjištění existence zranitelnosti některého z nabízených modelů by měla být situace napravena například aktualizací firmwaru či výměnou příslušných zařízení za jiná. Samotný zákazník totiž většinou neovlivní, jaké zařízení mu bude přiděleno a poskytovatel by se tak měl postarat o bezpečnost jím nabízeného řešení. Nebereme-li tedy v potaz, že zákazník může jemu přidělené zařízení přepnout do bridge

módu, vypnout vysílání Wi-Fi sítě a připojit svůj vlastní router, který danou zranitelností nedisponuje.

Pochopitelně ale mají na zjištěném stavu značný podíl i samotní vlastníci, kteří si nezměnili alespoň přístupové heslo ke své Wi-Fi síti, čímž by zranitelnost eliminovali. Vzhledem k tomu, že jsou vygenerovaná hesla náhodnou posloupností znaků, ovšem měli někteří vlastníci otestovaných sítí falešný pocit bezpečí, že je heslo dostatečně složité a není tak možné jej zjistit. Na základě této skutečnosti si pak dotyční přístupové heslo nezměnili.

Není tedy pochyb o tom, že je nutné změnu přednastavených údajů důrazně doporučit například již při samotné instalaci dané sítě technikem. Z důvodu toho, že ne všichni si musí s přenastavením své sítě poradit, bylo by ideálním řešením, kdyby došlo ke změně přednastavených údajů samotným technikem, respektive za jeho asistence, aby byli dotyční schopni případnou změnu hesla v budoucnu provést sami. Problém s používáním původních přístupových hesel by mohl být vyřešen také tím, že by byla změna hesla, názvu sítě a případně i přihlašovacích údajů k administraci routeru vynucena při úplně prvním připojení libovolného zařízení k danému přístupovému bodu. Dotyčný by tak musel nejprve tyto údaje nastavit a až poté by mu byl povolen přístup k internetu. Pochopitelně by ale muselo být zobrazené uživatelské rozhraní dostatečně přehledné a srozumitelné, aby bylo i méně zdatným uživatelům zřejmé, jakou změnu přesně provádí a byli si tak vědomi toho, že minimálně zadané přístupové heslo budou využívat pro připojení každého nového zařízení a je tedy nutné si jej poznamenat.

Výše zmíněné návrhy na zlepšení situace ovšem neřeší příčinu vzniklého problému, ale pouze jeho následek. Je potřeba se tedy zabývat tím, proč vlastně dochází ke generování hesel takovým způsobem, jako tomu je právě u zařízení Technicolor TC7200 či Ubee EVW3226. Ke generování přístupových hesel ze sériového čísla dochází především z důvodu ulehčení procesu výroby. Je pochopitelně výhodnější, když jsou všechna zařízení v podstatě stejná a není potřeba je přizpůsobovat zakázce. Jedinečnost daných zařízení je pak zajištěna přítomností sériového čísla a MAC adresy. Tyto údaje jsou obvykle zapsány do EEPROM paměti, odkud si je při procesu generování defaultního přístupového hesla načte firmware daného zařízení. Jelikož není sériové číslo zjistitelné bez fyzického přístupu k danému zařízení, není generování přístupového hesla na základě využití tohoto identifikátoru samo o sobě nebezpečné. Problém je ovšem v tom, že například u zařízení

Ubee EVW3226 je ze sériového čísla generováno nejen přístupové heslo, ale i SSID, a to za využití téměř identického algoritmu.

Je tedy nezbytné se vyvarovat použití prakticky totožné funkce pro generování jak přístupového hesla, tak SSID, aby nebylo možné heslo odhalit na základě znalosti názvu sítě a použitého algoritmu. Obecně by neměla existovat žádná korelace mezi vygenerovaným přístupovým heslem a některým z veřejně zjistitelných identifikátorů, jakým je například SSID či MAC adresa daného zařízení, což představuje výrazné ohrožení bezpečnosti. Nutné je ovšem navíc klást velký důraz na zabezpečení zařízení jako takového, aby nenastala situace, kdy neoprávněná osoba získá nejen přístup k firmwaru daného zařízení, ale může provést jeho následnou analýzu, respektive odhalit princip generování přístupových hesel.

Vzhledem k tomu, že zranitelnost řešená v této práci byla odhalena právě na základě analýzy funkce, která generuje přístupová hesla, nabízí se jedna možnost, jak tuto zranitelnost eliminovat. Řešení by mohlo spočívat v tom, že by náhodně vygenerované heslo bylo rovnou zapsáno do EEPROM paměti, tak jako sériové číslo či MAC adresa daného zařízení. Příslušný firmware by si pak toto heslo načetl jako je tomu například u sériového čísla. Tím pádem by daný firmware nemusel obsahovat žádnou funkci pro generování původního přístupového hesla a nebylo by tak možné pomocí reversního inženýrství zjistit, jakým způsobem jsou hesla generována, k čemuž došlo u obou modelů představených v této práci. I přesto, že by SSID mohlo být i nadále generované ze sériového čísla či MAC adresy daného zařízení, nehrozilo by již, že na základě znalosti těchto identifikátorů dojde ke zjištění odpovídajícího přístupového hesla.

10 Závěr

První část bakalářské práce měla za cíl vytvořit ucelený přehled dostupných informací v oblasti zabezpečování Wi-Fi sítí. V této části práce byly nejprve uvedeny důvody nutnosti zabezpečování Wi-Fi sítí, aby si čtenář mohl udělat představu o tom, jaká rizika nevhodně zabezpečená bezdrátová síť skýtá a proč je nutné bezpečnosti své sítě věnovat zvýšenou pozornost. Následně došlo k představení jednotlivých metod, jež se využívají ke zvýšení bezpečnosti Wi-Fi sítě a rovněž byly uvedeny slabiny těchto technik. V závěru teoretické části práce pak byly shrnuty známé typy útoků na bezdrátové sítě a možné obrany proti nim.

Hlavní náplní praktické části této bakalářské práce pak bylo analyzovat a vyhodnotit zabezpečení bezdrátových sítí vybraného poskytovatele internetového připojení, s důrazem kladeným na výchozí konfiguraci, kterou představuje přednastavené přístupové heslo a SSID Wi-Fi sítě. Na základě zjištěných skutečností pak měla být případně navržena široce aplikovatelná změna vedoucí ke zvýšení bezpečnosti. Vzhledem k existenci zranitelnosti některých zařízení, která využívá pro realizaci bezdrátových sítí společnost UPC, byl pro účely této části práce vybrán právě tento poskytovatel.

Jelikož daná zranitelnost spočívá v nevhodném generování přístupového hesla k Wi-Fi síti, které lze zjistit na základě znalosti SSID, bylo nejprve prostřednictvím dotazníku v elektronické podobě zjištěno, zda vlastníci Wi-Fi sítí považují změnu těchto údajů za důležitou, a zda ji na svém zařízení provedli. Poznatky získané v dotazníku pak byly vyhodnoceny a porovnány s výsledky skutečného průzkumu, který spočíval v prověření zabezpečení bezdrátových sítí poskytovatele UPC. V rámci tohoto průzkumu nejprve došlo k ověření toho, zda se i po roce a půl od upozornění Petera Geisslera na existenci bezpečnostního problému vyskytují Wi-Fi sítě, které touto zranitelností trpí. Podstatou průzkumu nebylo pouze konstatování, zda je problém stále aktuální či nikoliv. Na základě průzkumu bylo možné reálně ověřit, zda majitelé věnují zabezpečení své Wi-Fi sítě dostatečnou pozornost, či se naopak spíše spoléhají na to, že je jejich bezdrátová síť dostatečně zabezpečena samotným výrobcem, respektive poskytovatelem daného zařízení.

Ačkoliv v dotazníkovém šetření změnu přednastaveného přístupového hesla potvrdilo 81 % respondentů a celkově z dotazníku vyplynulo, že majitelům Wi-Fi sítí není bezpečnost jejich bezdrátové sítě lhostejná, získané poznatky v podstatě vůbec nekorespondovaly s tím, co bylo zjištěno na základě provedeného průzkumu. Zásadním

zjištěním byla skutečnost, že ze 41 prověřených sítí si změnil původní přístupové heslo pouze jediný vlastník, a jelikož daná zranitelnost skutečně nebyla odstraněna, drtivá většina otestovaných sítí tak byla stále zranitelná.

Přestože UPC uvedlo, že byli majitelé příslušných sítí o problému informováni prostřednictvím vyúčtování, během provedeného šetření si nikdo z vlastníků zranitelných sítí nebyl vědom toho, že by byl na danou skutečnost upozorněn. To pochopitelně neznamená, že UPC dotyčné o nutnosti změny přednastavených údajů skutečně neinformovalo, ale jak je patrné, způsob kterým byli dotyční upozorněni, nebyl zřejmě příliš efektivní. Názorná demonstrace možnosti zjištění přístupového hesla k Wi-Fi síti tak splnila svůj účel a dle reakcí jednotlivých vlastníků otestovaných Wi-Fi sítí nelze pochybovat o tom, že si dotyční dle poskytnutého návodu minimálně přístupové heslo k síti změnili a zranitelnost tak odstranili.

V práci bylo rovněž nastíněno, jak velkého počtu Wi-Fi sítí na území České republiky se může daná zranitelnost týkat. Na základě dat získaných z projektu Wifileaks bylo zjištěno, že v průběhu posledních několika let bylo v České republice zachyceno přibližně 66 tisíc Wi-Fi sítí, které jsou dle prefixu MAC adresy zranitelné. Vzhledem k tomu, že z tohoto počtu bylo SSID změněno pouze u 16 % sítí, bylo by u více než 55 tisíc zařízení možné přinejmenším vygenerovat kandidáty na přístupové heslo a následně je vyzkoušet.

Z provedeného průzkumu bylo patrné, že pouhé doporučení změny hesla, které může být například uvedeno na dokumentech dodaných k danému zařízení, či realizované prostřednictvím e-mailu, je nedostačující. Na základě toho byly v poslední kapitole naznačeny možnosti, prostřednictvím kterých by mohlo dojít ke zlepšení současného stavu. Toho by mohlo být docíleno nejen zajištěním změny přednastavených údajů samotným poskytovatelem, ale především upuštěním od současného způsobu generování hesel, který využívají někteří výrobci.

Použitá literatura

(1) VNI Complete Forecast Highlights Tool. In: *Cisco* [online]. 2016 [cit. 2017-02-28]. Dostupné z: http://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html

(2) GEISSLER, Peter. UPC%07d WiFi WPA2 key recovery service. In: *Haxxin* [online]. 2016 [cit. 2017-01-14]. Dostupné z: https://haxx.in/upc-wifi/

(3) ANDREW, Jacob. Do Multiple Users Using the Internet Affect Speed?. In: *Tech in our everyday life* [online]. b.r. [cit. 2016-11-16]. Dostupné z: http://techin.oureverydaylife.com/multiple-users-using-internet-affect-speed-3650.html

(4) JEŽDÍK, Pavel. Jak zabezpečit domácí Wi-Fi. In: *Eurosignal* [online]. 2016 [cit. 2016-11-16]. Dostupné z: http://www.eurosignal.cz/rady-a-tipy/jak-zabezpecit-domaci-wi-fi/

(5) Rizika použití veřejných wifi sítí – proč se jich nemusíte bát. In: *Kaspersky Lab* [online]. b.r. [cit. 2016-11-16]. Dostupné z: http://www.kaspersky.com/cz/internet-security-center/internet-safety/public-wifi-risks

(6) KSCHANG, . 6 Reasons Why You Should Secure Your Unsecured Wi-Fi Wireless Network. In: *HubPages* [online]. b.r., Updated on March 3, 2015 [cit. 2016-11-16]. Dostupné z: http://hubpages.com/technology/6-Reasons-Why-You-Should-Secure-Your-Wi-Fi-Network

(7) CHENG, Jacqui. FBI child porn raid a strong argument for locking down WiFi networks. In: *Ars Technica* [online]. 2011 [cit. 2017-02-28]. Dostupné z: https://arstechnica.com/tech-policy/2011/04/fbi-child-porn-raid-a-strong-argument-for-locking-down-wifi-networks/

(8) TRANG, Do. Police: Man Uses Neighbor's Unsecured Wi-Fi Connection To Download, Distribute Child Pornography. In: *CBS Philly* [online]. 2016 [cit. 2017-02-28]. Dostupné z: http://philadelphia.cbslocal.com/2016/09/12/unsecured-wifi-child-pornography/

(9) HAROLD, Davis. *Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě*. Praha: Grada, 2006. ISBN 80-247-1421-3.

(10) ČERMÁK, Miroslav. Je lepší provozovat Wi-Fi síť v otevřeném nebo zabezpečeném módu?. In: *Clever and Smart* [online]. 2015 [cit. 2016-11-17]. Dostupné z: http://www.cleverandsmart.cz/je-lepsi-provozovat-wi-fi-sit-v-otevrenem-nebo-zabezpecenem-modu/

(11) METELKA, Jan. Nové pojetí odpovědnosti provozovatelů wi-fi sítí. In: *Epravo.cz* [online]. 2016 [cit. 2016-11-17]. Dostupné z:

http://www.epravo.cz/top/clanky/nove-pojeti-odpovednosti-provozovatelu-wi-fi-siti-103325.html

(12) ČÍŽEK, Jakub. Soudní dvůr EU: Provozovatel otevřené Wi-Fi není zodpovědný za stahování warezu. In: *Živě.cz* [online]. 2016 [cit. 2016-11-17]. Dostupné z: http://www.zive.cz/bleskovky/soudni-dvur-eu-provozovatel-otevrene-wi-fi-neni-zodpovedny-za-stahovani-warezu/sc-4-a-184237/default.aspx

(13) NEOH, Dany. Corporate Wireless LAN: Know the Risks and Best Practices to Mitigate them. In: *SANS* [online]. 2003 [cit. 2016-11-23]. Dostupné z: https://www.sans.org/reading-room/whitepapers/wireless/corporate-wireless-lan-risks-practices-mitigate-1350

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

(15) How to secure your home wireless network router. In: *Computer Hope: Free computer help and information* [online]. b.r. [cit. 2016-11-23]. Dostupné z: http://www.computerhope.com/issues/ch001289.htm

(16) GREENBAUM, Dave. Don't Use Personal Information in Your Wi-Fi Network Name. In: *Life hacker* [online]. 2014 [cit. 2016-11-26]. Dostupné z: http://lifehacker.com/don-t-use-personal-information-in-your-wi-fi-network-na-1661652496

(17) O'DONNELL, Andy. How to Beef Up Security on Your Home Wireless Network. In: *Lifewire: Tech untangled* [online]. b.r., October 17, 2016 [cit. 2016-11-26]. Dostupné z: https://www.lifewire.com/how-to-beef-up-security-on-your-home-wireless-network-2487660

(18) O'DONNELL, Andy. Is Your Wireless Network's Name a Security Risk?. In: *Lifewire* [online]. b.r., Updated October 17, 2016 [cit. 2016-12-06]. Dostupné z: https://www.lifewire.com/is-your-wireless-networks-name-a-security-risk-2487658

(19) SZCZYS, Mike. TP-LINK's WiFi Defaults to Worst Unique Passwords Ever. In: *Hackaday* [online]. 2016 [cit. 2016-12-06]. Dostupné z: http://hackaday.com/2016/01/27/tp-links-wifi-defaults-to-worst-unique-passwords-ever/

(20) Masívny útok na domáce routery neprístupné z Internetu, cez prehliadač Chrome. In: *Digitálný Svet pod lupou* [online]. 2015 [cit. 2016-11-28]. Dostupné z: http://www.dsl.sk/article.php?article=17043&hot=5

(21) HOROWITZ, Michael. Home routers can be dangerous. VERY dangerous. In: *Michael Horowitz: Comments on computers from a long-time computer nerd* [online]. 2007 [cit. 2016-11-28]. Dostupné z: http://michaelhorowitz2.blogspot.cz/2007/03/home-routers-can-be-dangerous-very.html

(22) LELL, Jakob. Real-World CSRF attack hijacks DNS Server configuration of TP-Link routers. In: *Jakob Lell's Blog: technology changes – insecurity remains*

[online]. 2013 [cit. 2016-11-28]. Dostupné z: http://www.jakoblell.com/blog/2013/10/30/real-world-csrf-attack-hijacks-dns-server-configuration-of-tp-link-routers-2/

(23) ZANDL, Patrick. *Bezdrátové sítě WiFi: praktický průvodce*. Brno: Computer Press, 2003. ISBN 80-7226-632-2.

(24) MARTASW, . Jak prolomit ochranu filtrování MAC adres. In: *Marťas bloguje: Všem a o všem* [online]. 2013 [cit. 2016-11-28]. Dostupné z: http://martasw.cz/svet_it/prolomeni_ochrany_mac

(25) DAVIES, Joe. Non-broadcast Wireless Networks with Microsoft Windows. In: *Microsoft: TechNet* [online]. b.r., Updated: April 19, 2007 [cit. 2016-11-29]. Dostupné z: https://technet.microsoft.com/en-us/library/bb726942.aspx#EDAA

(26) KILIÁN, Karel. Jak ochránit svou Wi-Fi před sousedy a zvědavci?. In: *Svět Androida* [online]. 2016 [cit. 2016-11-29]. Dostupné z: https://technet.microsoft.com/en-us/library/bb726942.aspx#EDAA

(27) HEDDINGS, Lowell. Debunking Myths: Is Hiding Your Wireless SSID Really More Secure?. In: *How-To Geek* [online]. 2014 [cit. 2016-11-29]. Dostupné z: http://www.howtogeek.com/howto/28653/debunking-myths-is-hiding-your-wireless-ssid-really-more-secure/

(28) VANĚK, Tomáš. Zabezpečení bezdrátových sítí IEEE 802.11. In: *Cedupoint: Continuing Education Point* [online]. České vysoké učení technické v Praze Fakulta elektrotechnická, b.r. [cit. 2017-03-05]. Dostupné z: http://data.cedupoint.cz/oppa_e-learning/2_KME/043.pdf

(29) ARP Request Replay Attack. In: *Aircrack-ng* [online]. 2010 [cit. 2017-03-24]. Dostupné z: https://www.aircrack-ng.org/doku.php?id=arp-request_reinjection

(30) ROBERTS, Eric. 802.11b Security Mechanisms. In: *Stanford Engineering: Computer Science* [online]. 2006 [cit. 2017-03-14]. Dostupné z: https://cs.stanford.edu/people/eroberts/courses/soco/projects/2003-04/wireless-computing/sec_80211.shtml#top

(31) PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. Vyd. 1. Brno: CP Books, 2005. ISBN 80-251-0791-4.

(32) MOSKOWITZ, Robert. Weakness in Passphrase Choice in WPA Interface. In: *Wi-Fi Net News: Daily reporting on wireless data networking* [online]. 2003 [cit. 2017-03-10]. Dostupné z: http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html

(33) GEIER, Eric. Zabezpečte si Wi-Fi v režimu enterprise. In: *ComputerWorld* [online]. 2015 [cit. 2017-03-21]. Dostupné z: http://computerworld.cz/internet-a-komunikace/zabezpecte-si-wi-fi-v-rezimu-enterprise-51826

(34) SALAZAR, Jordi. Bezdrátové sítě. In: *TECHpedia* [online]. České vysoké učení technické v Praze, b.r. [cit. 2017-03-12]. Dostupné z: http://techpedia.fel.cvut.cz/single/?objectId=50

(35) NOVÁK, Michal. Odposlouchávání a prolamování Wi-Fi sítí zabezpečených pomocí WPA2. In: *Root.cz* [online]. 2017 [cit. 2017-03-21]. Dostupné z: https://www.root.cz/clanky/odposlouchavani-a-prolamovani-wi-fi-siti-zabezpecenych-pomoci-wpa2/

(36) PETROVIČ, Michal a Martin ŠIMEK. *Bezdrátové sítě*. Plzeň: Západočeská univerzita, 2013. ISBN 978-80-261-0225-0.

(37) LEHEMBRE, Guillaume. Wi-Fi security – WEP, WPA and WPA2. In: *Hervé Schauer Consultants: Network Security Consultants* [online]. 2005 [cit. 2017-03-10]. Dostupné z: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf

(38) *Enterprise Mobility 4.1 Design Guide: Chapter 4 - Cisco Unified Wireless Network Architecture—Base Security Features* [online]. Cisco Systems, 2008 [cit. 2018-01-12]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.pdf

(39) HOFFMAN, Chris. Wi-FI Protected Setup (WPS) is Insecure: Here's Why You Should Disable It. In: *How-To Geek* [online]. b.r. [cit. 2018-01-15]. Dostupné z: https://www.howtogeek.com/176124/wi-fi-protected-setup-wps-is-insecure-heres-why-you-should-disable-it/

(40) MACICH, Jiří. Bezpečné WiFi není žádná věda, přesvědčte se. In: *DigiRoom.cz* [online]. b.r. [cit. 2018-01-15]. Dostupné z: https://digiroom.digizone.cz/clanky/bezpecne-wifi-neni-zadna-veda/

(41) VIEHBÖCK, Stefan. Brute forcing Wi-Fi Protected Setup: When poor design meets poor implementation. In: *Sviehb.wordpress.com* [online]. Version 3. b.r. [cit. 2018-01-15]. Dostupné z: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

(42) VANHOEF, Mathy. Key Reinstallation Attacks: Breaking WPA2 by forcing nonce reuse. In: *Krackattacks.com* [online]. b.r. [cit. 2018-01-15]. Dostupné z: https://www.krackattacks.com/

(43) GOODIN, Dan. Serious flaw in WPA2 protocol lets attackers intercept passwords and much more. In: *Ars Technica* [online]. b.r. [cit. 2018-01-15]. Dostupné z: https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/

(44) CVE-2017-13080 | Windows Wireless WPA Group Key Reinstallation Vulnerability: Security Vulnerability. In: *Microsoft TechNet* [online]. b.r., 10/18/2017 [cit. 2018-01-15]. Dostupné z: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080

(45) Wi-Fi Alliance® introduces security enhancements: New Wi-Fi® security features available in 2018. In: *Wi-Fi Alliance: The worldwide network of companies that brings you Wi-Fi®* [online]. b.r., January 8, 2018 [cit. 2018-01-12]. Dostupné z: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements

(46) NG, Alfred. Your local public Wi-Fi network may be a whole lot safer soon: New technology coming to Wi-Fi later this year vows to keep your traffic private even on a public network. In: *Cnet.com* [online]. b.r., January 8, 2018 [cit. 2018-01-12]. Dostupné z: https://www.cnet.com/news/public-wifi-ces-wpa3-security-privacy-online-traffic-safe/

(47) *RogueAP: Eliminate Rogues APs once and for all* [online]. 2009 [cit. 2017-03-16]. Dostupné z: http://www.rogueap.com/

(48) GOPINATH, K. a Chaskar HEMANT. All You Wanted to Know About WiFi Rogue Access Points. In: *RogueAP: Eliminate Rogue APs once and for all* [online]. 2009 [cit. 2017-03-16]. Dostupné z: http://www.rogueap.com/rogue-ap-docs/RogueAP-FAQ.pdf

(49) CHAUDHARY, Shashwat. Evil Twin Tutorial. In: *KaliTutorials* [online]. b.r. [cit. 2018-04-14]. Dostupné z: http://www.kalitutorials.net/2014/07/evil-twin-tutorial.html

(50) Man-in-the-middle útok. In: *Wiki.airdump.cz* [online]. b.r., 5. 1. 2008 [cit. 2018-04-15]. Dostupné z: http://wiki.airdump.cz/Man-in-the-middle_%C3%BAtok

(51) Warchalking. In: *Správa sítě: Slovník pojmů* [online]. b.r. [cit. 2017-03-16]. Dostupné z: http://www.sprava-site.eu/warchalking/

(52) CompTIA Network+ N10-006 Cert Guide (2015): Chapter 8. Wireless LANs. In: *Computer science, Programming, Web, Software* [online]. b.r. [cit. 2018-04-12]. Dostupné z: http://apprize.info/network/comptia/8.html

(53) Wireless Hacking Basics WPA Dictionary Attack, Handshake, Data Capture, Part 5. In: *WirelesSHack* [online]. 2015 [cit. 2017-03-21]. Dostupné z: http://www.wirelesshack.org/wireless-hacking-basics-wpa-dictionary-attack-handshake-data-capture-part-5.html

(54) ČERMÁK, Miroslav. Lámání hesel. In: *Clever and Smart* [online]. 2010 [cit. 2017-03-21]. Dostupné z: http://www.cleverandsmart.cz/lamani-hesel/

(55) WRIGHT, Josua a Johnny CACHE. *Hacking Exposed Wireless: Wireless Security Secrets & Solutions*. Third Edition. McGraw-Hill Education, 2015. ISBN 978-0-07-182762-1.

(56) ZELINKA, Ivan. Moderní metody v počítačové a komunikační bezpečnosti pro integrovanou výuku VUT a VŠB -TUO. In: *DataAnalysis.vsb.cz* [online]. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava, 2014 [cit. 2017-03-21]. Dostupné z: http://dataanalysis.vsb.cz/data/OPVK_PVBPS.pdf

(57) BAŠTA, Pavel a Zuzana DURAČINSKÁ. DDoS – sofistikovaný útok nebo služba na objednávku?. *IT Systems*. 2015, **17**(42015), 38-39. ISSN 1802-615X.

(58) ČÍŽEK, Jakub. Vyrobili jsme si rušičku Wi-Fi. Stačil běžný laptop a hackerský Kali Linux. In: *Živě.cz* [online]. 2016 [cit. 2017-03-23]. Dostupné z: http://www.zive.cz/clanky/vyrobili-jsme-si-rusicku-wi-fi-stacil-bezny-laptop-a-hackersky-kali-linux/sc-3-a-181832/default.aspx

(59) COMPTON, Stuart. 802.11 Denial of Service Attacks and Mitigation. In: *SANS: The most trusted source for information security training, certification, and research.* [online]. 2007 [cit. 2017-03-23]. Dostupné z: https://www.sans.org/reading-room/whitepapers/wireless/80211-denial-service-attacks-mitigation-2108

(60) Wireless Intrusion Prevention System (WIPS). In: *WatchGuard: Smart Security, Simply Done.* [online]. b.r. [cit. 2017-03-23]. Dostupné z: http://www.watchguard.com/wgrd-products/access-points/wips

(61) Pozor, WiFi heslá na UPC modemoch nie sú bezpečné. Urýchlene si ho zmeňte. In: *DSL.sk: Digitální Svět pod Lupou* [online]. b.r. [cit. 2018-04-11]. Dostupné z: http://www.dsl.sk/article.php?article=17885

(62) Multiple critical vulnerabilities in Ubee EVW3226 Advanced wireless voice gateway. In: *SecurityFocus* [online]. b.r. [cit. 2018-04-11]. Dostupné z: https://www.securityfocus.com/archive/1/538560

(63) KLINEC, Dušan a Miroslav SVÍTOK. UPC UBEE EVW3226 WPA2 Password Reverse Engineering, rev 3. In: *0xDEADCODE* [online]. b.r. [cit. 2018-04-11]. Dostupné z: https://deadcode.me/blog/2016/07/01/UPC-UBEE-EVW3226-WPA2-Reversing.html

(64) Mapová data ©2018 Google. *Mapy Google* [online]. b.r. [cit. 2018-04-17]. Dostupné z: https://www.google.cz/maps/place/%C4%8Cesk%C3%A9+Bud%C4%9Bjovice/@48.9744773,14.4728679,4286m/data=!3m1!1e3!4m5!3m4!1s0x47734fb43a5f629b:0x400af0f6614de80!8m2!3d48.9756578!4d14.480255

(65) SLÍŽEK, David. Máte router od UPC? Změňte si výchozí heslo k wi-fi, není bezpečné. In: *Lupa.cz* [online]. b.r. [cit. 2018-04-11]. Dostupné z: https://www.lupa.cz/clanky/mate-router-od-upc-zmente-si-vychozi-heslo-k-wi-fi-neni-bezpecne/

Seznam obrázků

Obrázek 1: Rozhodnutí vydané soudním dvorem Evropské Unie 6

Obrázek 2: Odvození SSID a hesla z MAC adresy u routeru TP-Link 10

Obrázek 3: Proces šifrování přenášených dat protokolem TKIP 16

Obrázek 4: Schéma šifrování dat symetrickou blokovou šifrou AES 21

Obrázek 5: Warchalking značky 28

Obrázek 6: Oblast prováděného průzkumu 47

Obrázek 7: Screenshot z aplikace WiGLE WiFi Wardriving 48

Obrázek 8: Screenshot z aplikace Google Earth 50

Obrázek 9: Screenshoty z aplikace WiFiAnalyzer 51

Obrázek 10: Screenshoty z aplikace UPC Keygen (Ubee EVW3226) 53

Obrázek 11: Screenshoty z aplikace UPC Keygen (Technicolor TC7200) 53

Obrázek 12: Screenshoty z aplikace WIBR+ 54

Seznam grafů

Graf 1: Má změna názvu Wi-Fi sítě vliv na její bezpečnost? 39

Graf 2: Změna SSID Wi-Fi sítě 40

Graf 3: Představuje přednastavené přístupové heslo bezpečnostní riziko? 41

Graf 4: Změna přednastaveného přístupového hesla 41

Graf 5: Délka přístupového hesla k Wi-Fi síti 42

Graf 6: Změna přístupových údajů k administraci routeru 43

Graf 7: Použité metody zabezpečení 44

Graf 8: Změna SSID s ohledem na jeho typ 56

Graf 9: Úspěšně ověřená zařízení 58

Graf 10: Porovnání výsledků dotazníku a průzkumu - změna hesla 60

Seznam tabulek

Tabulka 1: Změna SSID na základě typu 55

Tabulka 2: Prefixy zranitelných zařízení 62

Seznam použitých zkratek

Zkratka	Plné znění	Význam
SSID	Service Set Identifier	Identifikátor Wi-Fi sítě
MAC	Media Access Control	Jednoznačný identifikátor síťového zařízení
DNS	Domain Name System	Hierarchický systém doménových jmen
WEP	Wired Equivalent Privacy	Soukromí ekvivalentní drátovým sítím
AP	Access Point	Přístupový bod
CRC	Cyclic redundancy check	Cyklický redundantní součet
IV	Initialization vector	Inicializační vektor
WPA(2)	Wi-Fi Protected Access	Chráněný přístup k Wi-Fi
MIC	Message Integrity Code	Kód pro ověření integrity zprávy
TKIP	Temporal Key Integrity Protocol	Bezpečnostní protokol používaný zabezpečením WPA
AES	Advanced Encryption Standard	Standard pokročilého šifrování
PSK	Pre-Shared key	Předsdílený klíč
PMK	Pairwise Master Key	Hlavní párový klíč
PTK	Pairwise Transient Key	Přechodný párový klíč
PKI	Public Key Infrastructure	Infrastruktura veřejných klíčů
EAP	Extensible Authentication Protocol	Rozšiřitelný autentizační protokol
CBC-MAC	Cipher Block Chaining-Message Authentication Code	Řetězení šifrového textu-Autentizační kód zprávy

XOR	Exclusive disjunction	Exkluzivní (úplná) disjunkce
PN	Packet Number	Číslo paketu
KRACK	Key Reinstallation Attacks	Útoky znovuzavedením klíče
WPS	Wi-Fi Protected Setup	Chráněné nastavení Wi-Fi
PIN	Personal identification number	Osobní identifikační číslo
HTTPS	Hypertext Transfer Protocol Secure	HTTP spolupracující s protokolem SSL či TLS
CNNS	Committee on National Security Systems	Americká vládní organizace
VPN	Virtual private network	Virtuální privátní síť
WIPS	Wireless intrusion prevention system	Systém prevence průniku u bezdrátových sítí
NAC	Network Access Control	Řízení síťového přístupu
MITM	Man-in-the-Middle	Člověk uprostřed – typ útoku
HMAC-SHA	Keyed-hash Message Authentication Code-Secure Hash Algorithm	Typ autentizačního kódu zprávy – Hashovací algoritmus
DoS	Denial of service	Odepření služby – typ útoku
WIDS	Wireless Intrusion Detection System	Systém detekce průniku u bezdrátových sítí
IPsec	IP security	Bezpečnostní rozšíření protokolu IP
CSV	Comma-separated values	Hodnoty oddělené čárkami (souborový formát)
KML	Keyhole Markup Language	Datový formát založený na XML
EEPROM	Electrically Erasable Programmable Read-Only Memory	Elektronicky vymazatelná paměť pouze pro čtení

Seznam příloh

Příloha 1: Návod pro modem Technicolor TC7200

Příloha 2: Návod pro modem Ubee EVW3226

Příloha 1: Návod pro modem Technicolor TC7200

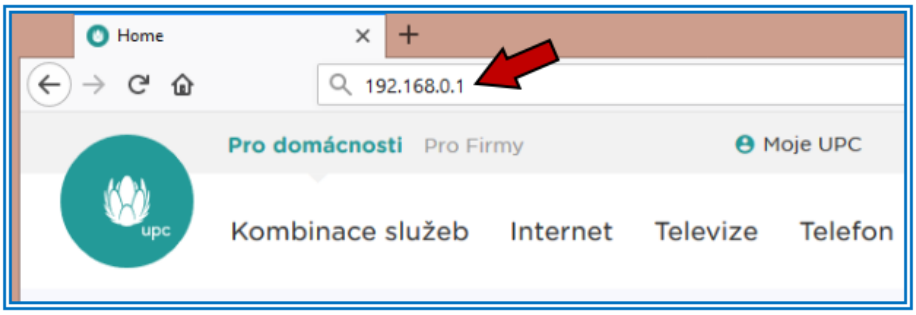
Návod na změnu názvu Wi-Fi sítě a hesla

(pro router TECHNICOLOR TC7200)

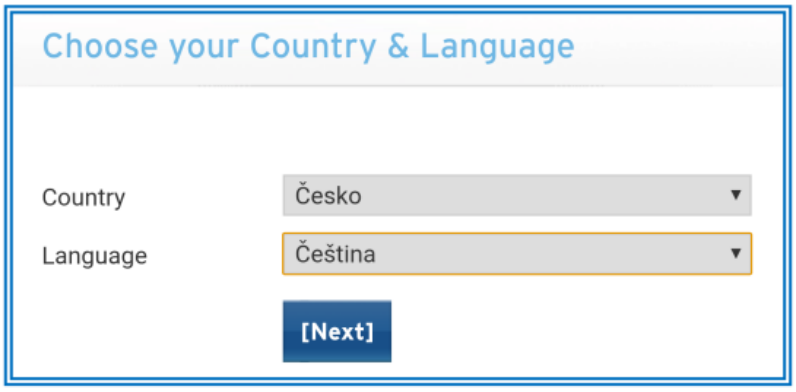
1) Připojte se k dané Wi-Fi síti prostřednictvím notebooku, mobilního telefonu či jiného bezdrátového zařízení s Wi-Fi adaptérem

2) Po připojení Vašeho zařízení zapněte libovolný webový prohlížeč (Mozilla Firefox, Google Chrome, Internet Explorer, Opera, či jiný Vámi používaný)

3) Ve webovém prohlížeči napište do adresního řádku následující adresu: 192.168.0.1 a stiskněte klávesu enter.

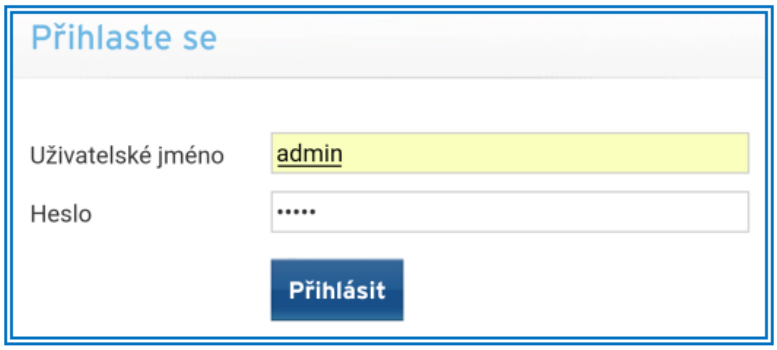


4) Po zadání výše zmíněné adresy se zobrazí okénko s volbou země a jazyka použitého v administraci routeru. V políčku **Country** (země) zvolte Česko a v políčku **Admin language** (jazyk administrace) vyberte možnost Čeština. Následně stiskněte tlačítko **[Next]** (dále).

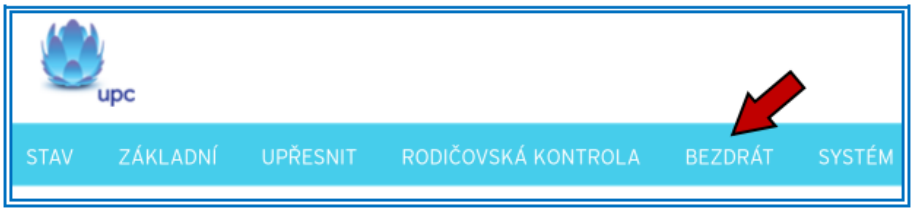


1

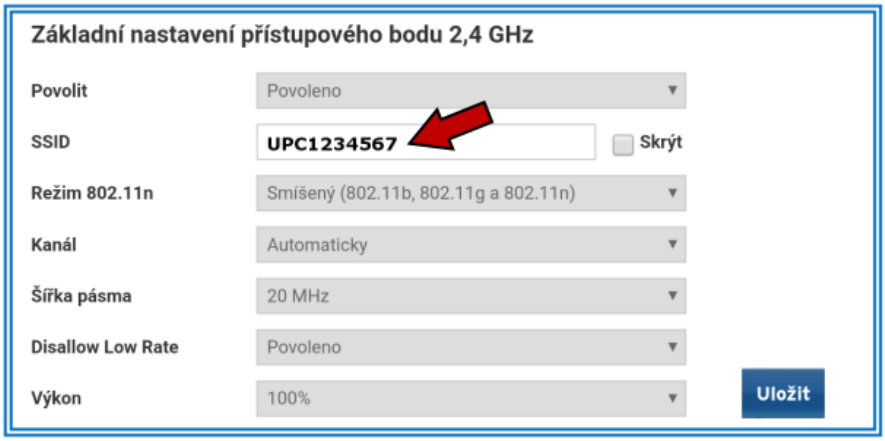
5) Poté, co stisknete tlačítko **Continue** se objeví nové okénko, ve kterém bude nutné zadat uživatelské jméno a heslo k administraci routeru. Zadejte uživatelské jméno **admin** a heslo **admin**. Následně stiskněte tlačítko **Přihlásit**.



6) Po přihlášení vyberte záložku **Bezdrát (Bezdrátové připojení).**

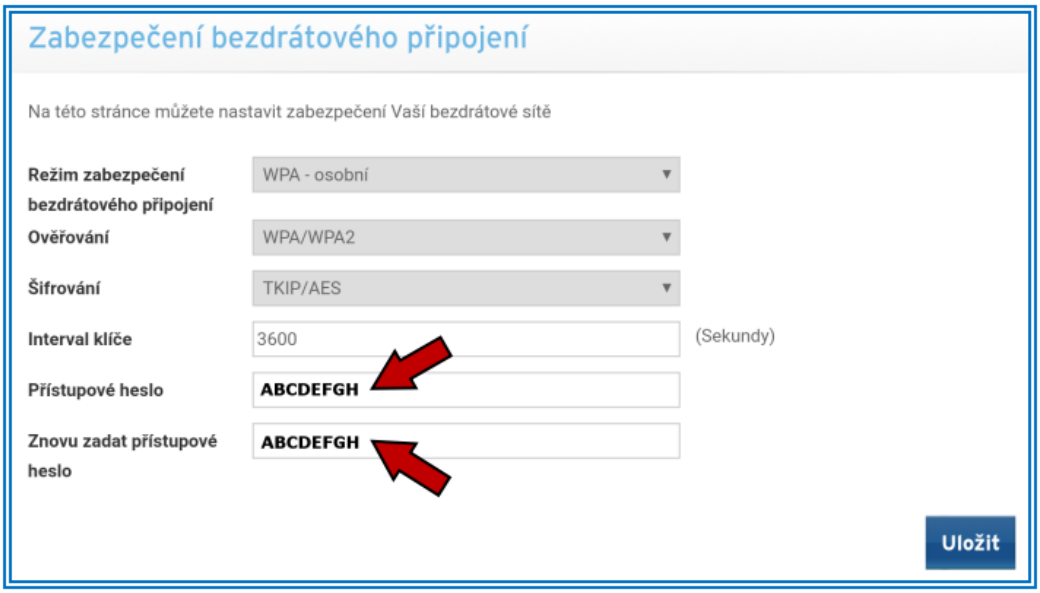


7) Následně najděte řádek označený jako SSID. Jedná se o řádek, ve kterém je uveden současný název vaší Wi-Fi sítě. Vymyslete si nový název pro Vaši Wi-Fi síť. Následně smažte současný název a uveďte namísto něj Váš nový název. Poté stiskněte tlačítko **Uložit**.



8) Jakmile úspěšně změníte název Wi-Fi sítě, je potřeba rovněž změnit přístupové heslo k Vaší Wi-Fi síti. To se opět provádí v záložce Bezdrát. Po levé straně klikněte na možnost **Zabezpečení**.

9) Poté, co kliknete na možnost **Zabezpečení**, se Vám zobrazí informace o zabezpečení bezdrátového připojení. V kolonce **Přístupové heslo** vymažte dosavadní heslo. Vymyslete si heslo nové a to uveďte do kolonky, ve které se nacházelo heslo původní. Nově zvolené heslo napište ještě jednou do kolonky **Znovu zadat přístupové heslo**. Nakonec stiskněte tlačítko **Uložit**.



10) V posledním kroku se odhlaste z administrace routeru kliknutím na tlačítko **Odhlásit**, které se nachází v pravém horním rohu.

Návod na změnu přístupového hesla k Vaší Wi-Fi síti v jednotlivých zařízeních

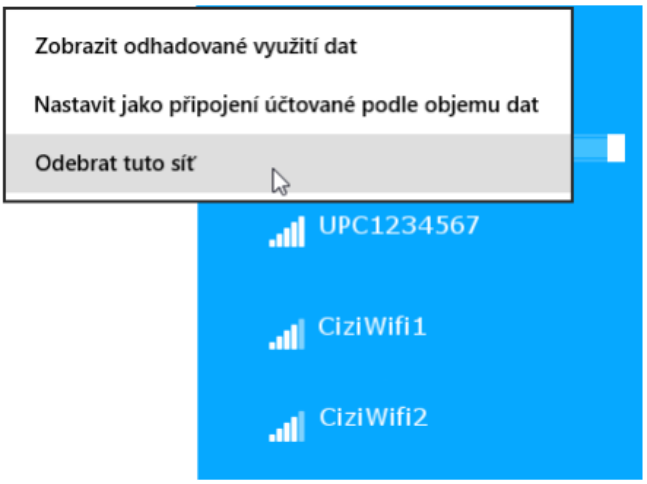
Po úspěšné změně přístupového hesla k Vaší Wi-Fi síti bude rovněž potřeba nové heslo nastavit i v zařízeních, se kterými se k Vaší Wi-Fi síti připojujete (ať již na notebooku či mobilním telefonu). Pokud se totiž například Váš notebook po zapnutí připojuje k Wi-Fi síti automaticky, bude mít uložené staré heslo, které je po Vaší změně již neplatné, a tím pádem bude připojení k Wi-Fi síti neúspěšné.

Níže bude uveden návod, jak nastavit nové heslo na notebooku a mobilním telefonu. Uvedený postup se ovšem může lišit v závislosti na tom, jaký je v notebooku či mobilním telefonu nainstalovaný operační systém. Princip by ovšem měl být obdobný.

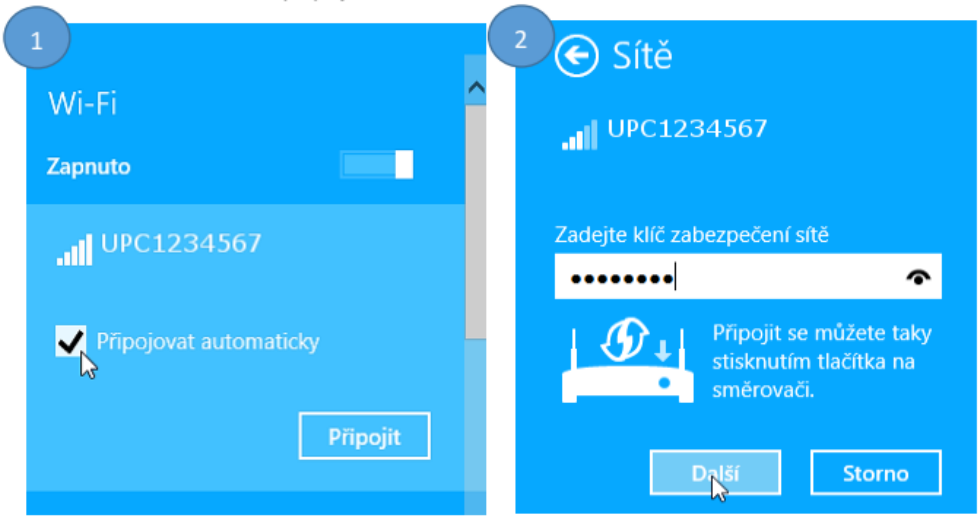
Změna přístupového hesla k Wi-Fi síti na notebooku (operační systém Windows 8.1)

1. V pravém dolním rohu obrazovky klikněte levým tlačítkem myši na ikonku Wi-Fi sítě.

2. Po kliknutí se Vám zobrazí seznam dostupných Wi-Fi sítí. Mezi zobrazenými sítěmi nalezněte tu Vaši a klikněte na ni pravým tlačítkem. Následně z uvedených možností vyberte **Odebrat tuto síť.**

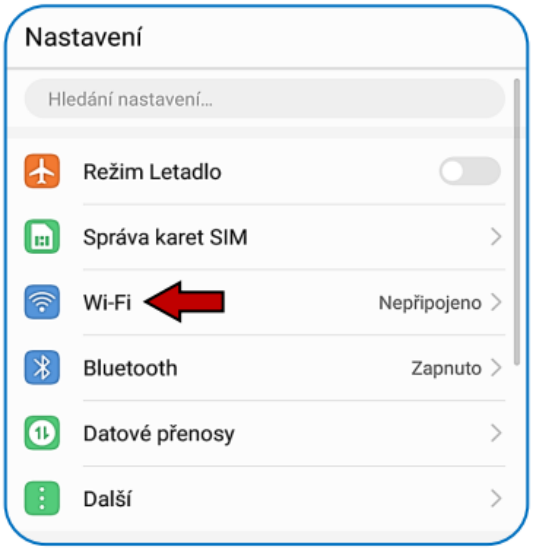


3. Nyní v seznamu dostupných sítí klikněte na Vaši Wi-Fi síť levým tlačítkem myši. Políčko **Připojovat automaticky** nechte zaškrtnuté a následně klikněte na tlačítko **Připojit**. Zobrazí se Vám okénko pro zadání hesla. Do tohoto okénka uveďte to heslo, které jste si dle předchozího návodu nově nastavili v administraci routeru. Poté klikněte na tlačítko **Další** a budete připojeni k síti.



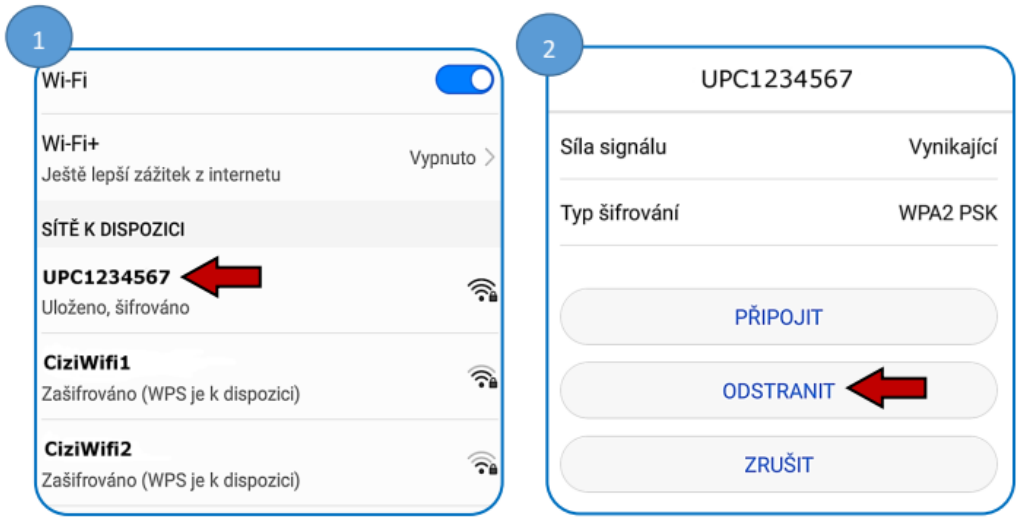
Změna přístupového hesla k Wi-Fi síti na mobilním telefonu (operační systém Android)

1. Jděte do **Nastavení** mobilního telefonu a vyberte z nabídky sekci **Wi-Fi**.



5

2. Po kliknutí na sekci Wi-Fi se zobrazí seznam dostupných sítí. Vyhledejte Vaši Wi-Fi síť a klikněte na ni (Obrázek 1). Po kliknutí na danou síť se zobrazí okénko, ve kterém vyberete možnost **Odstranit** (Obrázek 2).



3. Nyní v seznamu dostupných sítí klikněte znovu na Vaši Wi-Fi síť. Zobrazí se okénko, ve kterém bude potřeba zadat heslo. Do políčka uveďte to heslo, které jste si dle předchozího návodu nově nastavili v administraci routeru. Po zadání hesla stiskněte tlačítko **Připojit**.

Příloha 2: Návod pro modem Ubee EVW3226

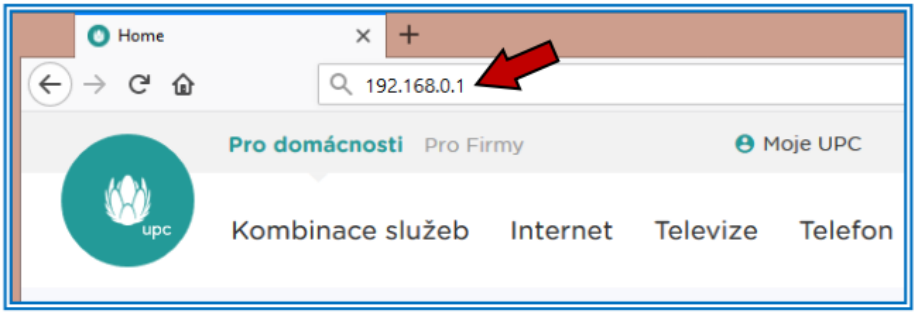
Návod na změnu názvu Wi-Fi sítě a hesla

(pro router UBEE EVW3226)

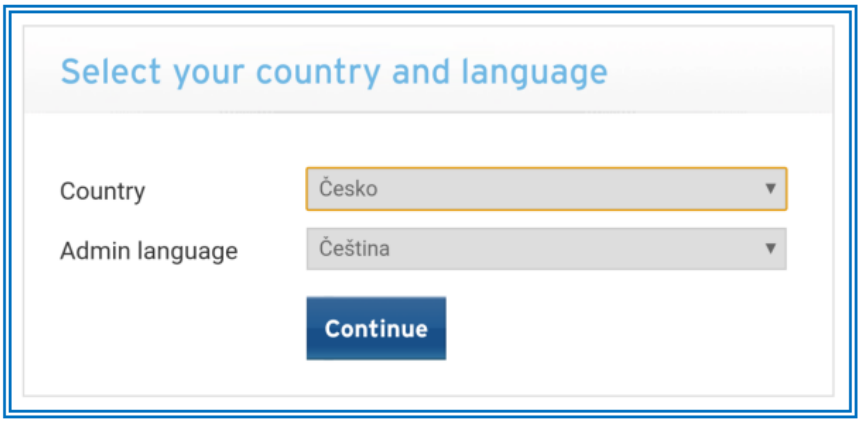
1) Připojte se k dané Wi-Fi síti prostřednictvím notebooku, mobilního telefonu či jiného bezdrátového zařízení s Wi-Fi adaptérem

2) Po připojení Vašeho zařízení zapněte libovolný webový prohlížeč (Mozilla Firefox, Google Chrome, Internet Explorer, Opera, či jiný Vámi používaný)

3) Ve webovém prohlížeči napište do adresního řádku následující adresu: 192.168.0.1 a stiskněte klávesu enter.

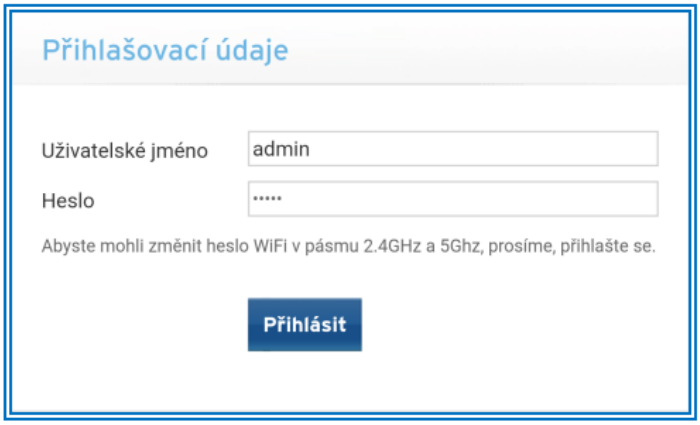


4) Po zadání výše zmíněné adresy se zobrazí okénko s volbou země a jazyka použitého v administraci routeru. V políčku **Country** (země) zvolte Česko a v políčku **Admin language** (jazyk administrace) vyberte možnost Čeština. Následně stiskněte tlačítko **Continue** (pokračovat).



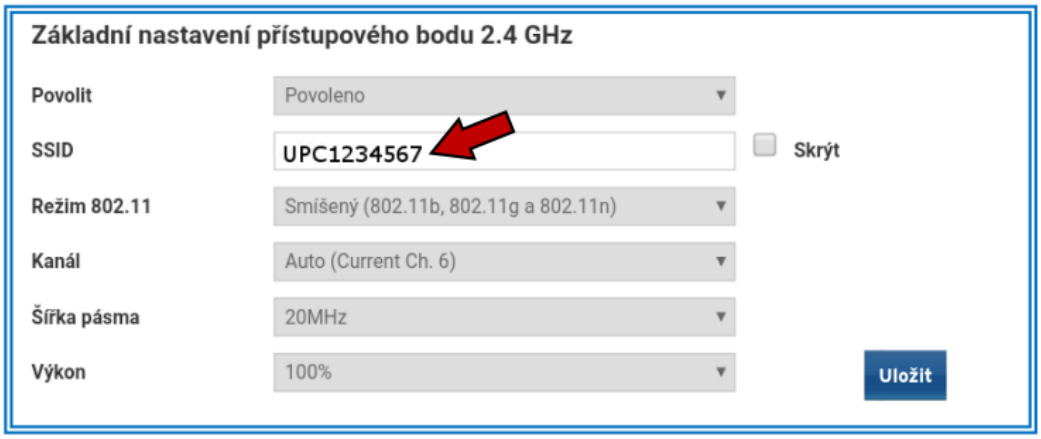
1

5) Poté, co stisknete tlačítko **Continue** se objeví nové okénko, ve kterém bude nutné zadat uživatelské jméno a heslo k administraci routeru. Zadejte uživatelské jméno **admin** a heslo **admin**. Následně stiskněte tlačítko **Přihlásit**.



6) Po přihlášení vyberte záložku **Bezdrátové připojení (Bezdrát).**

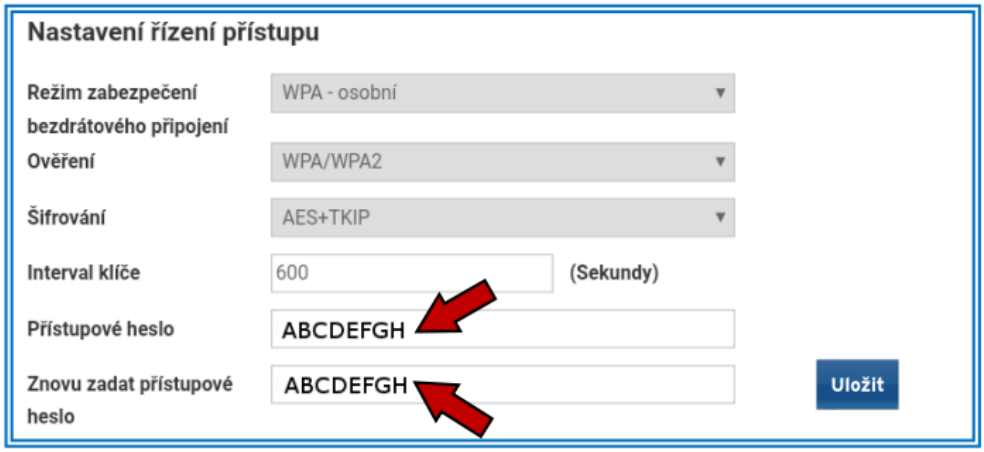
7) Následně najděte řádek označený jako SSID. Jedná se o řádek, ve kterém je uveden současný název vaší Wi-Fi sítě. Vymyslete si nový název pro Vaši Wi-Fi síť. Následně smažte současný název a uveďte namísto něj Váš nový název. Poté stiskněte tlačítko **Uložit**.



2

8) Jakmile úspěšně změníte název Wi-Fi sítě, je potřeba rovněž změnit přístupové heslo k Vaší Wi-Fi síti. To se opět provádí v záložce Bezdrátové připojení. Po levé straně klikněte na možnost **Zabezpečení**.

9) Poté, co kliknete na možnost **Zabezpečení**, se Vám zobrazí informace o zabezpečení bezdrátového připojení. V kolonce **Přístupové heslo** vymažte dosavadní heslo. Vymyslete si heslo nové a to uveďte do kolonky, ve které se nacházelo heslo původní. Nově zvolené heslo napište ještě jednou do kolonky **Znovu zadat přístupové heslo**. Nakonec stiskněte tlačítko **Uložit**.



10) V posledním kroku se odhlaste z administrace routeru kliknutím na tlačítko **Odhlásit**, které se nachází v pravém horním rohu.

3

Návod na změnu přístupového hesla k Vaší Wi-Fi síti v jednotlivých zařízeních

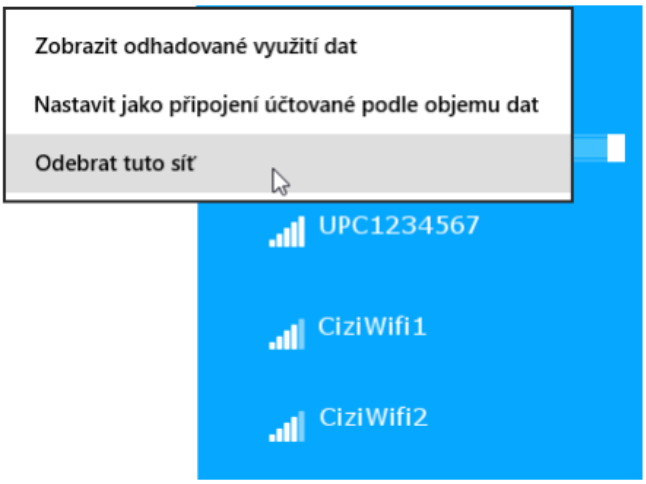
Po úspěšné změně přístupového hesla k Vaší Wi-Fi síti bude rovněž potřeba nové heslo nastavit i v zařízeních, se kterými se k Vaší Wi-Fi síti připojujete (ať již na notebooku či mobilním telefonu). Pokud se totiž například Váš notebook po zapnutí připojuje k Wi-Fi síti automaticky, bude mít uložené staré heslo, které je po Vaší změně již neplatné, a tím pádem bude připojení k Wi-Fi síti neúspěšné.

Níže bude uveden návod, jak nastavit nové heslo na notebooku a mobilním telefonu. Uvedený postup se ovšem může lišit v závislosti na tom, jaký je v notebooku či mobilním telefonu nainstalovaný operační systém. Princip by ovšem měl být obdobný.

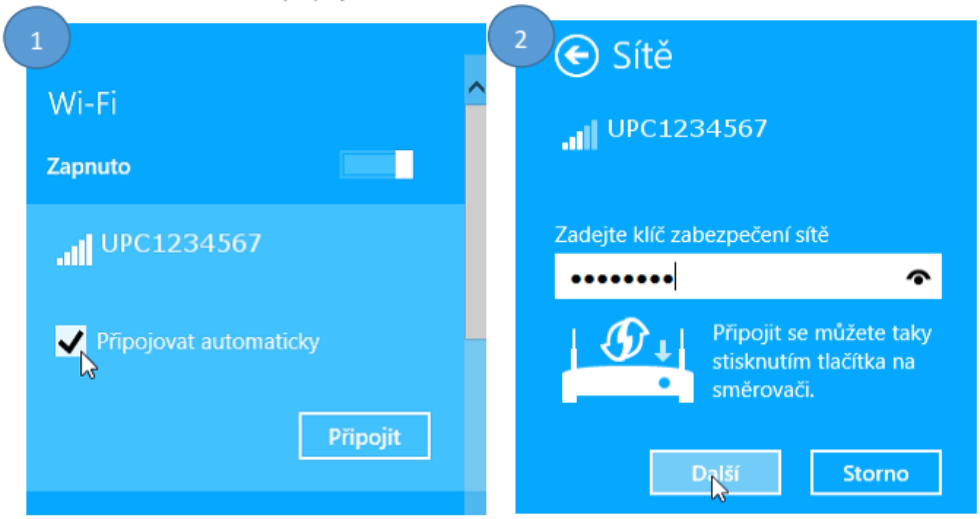
Změna přístupového hesla k Wi-Fi síti na notebooku (operační systém Windows 8.1)

1. V pravém dolním rohu obrazovky klikněte levým tlačítkem myši na ikonku Wi-Fi sítě.

2. Po kliknutí se Vám zobrazí seznam dostupných Wi-Fi sítí. Mezi zobrazenými sítěmi nalezněte tu Vaši a klikněte na ni pravým tlačítkem. Následně z uvedených možností vyberte **Odebrat tuto síť.**

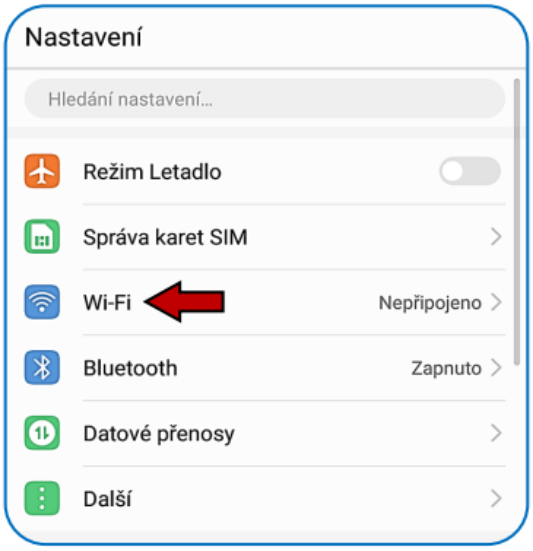


3. Nyní v seznamu dostupných sítí klikněte na Vaši Wi-Fi síť levým tlačítkem myši. Políčko **Připojovat automaticky** nechte zaškrtnuté a následně klikněte na tlačítko **Připojit**. Zobrazí se Vám okénko pro zadání hesla. Do tohoto okénka uveďte to heslo, které jste si dle předchozího návodu nově nastavili v administraci routeru. Poté klikněte na tlačítko **Další** a budete připojeni k síti.

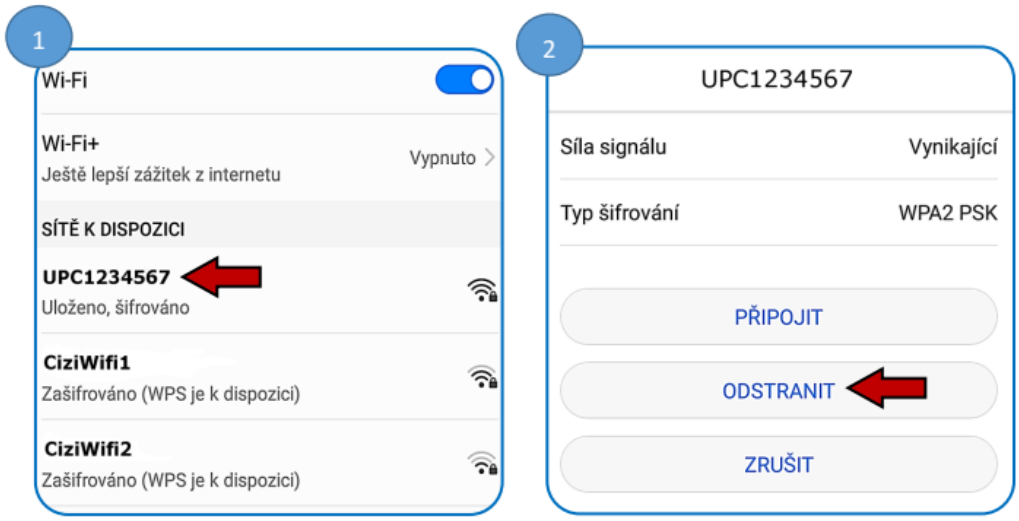


Změna přístupového hesla k Wi-Fi síti na mobilním telefonu (operační systém Android)

1. Jděte do **Nastavení** mobilního telefonu a vyberte z nabídky sekci **Wi-Fi**.



2. Po kliknutí na sekci Wi-Fi se zobrazí seznam dostupných sítí. Vyhledejte Vaši Wi-Fi síť a klikněte na ni (Obrázek 1). Po kliknutí na danou síť se zobrazí okénko, ve kterém vyberete možnost **Odstranit** (Obrázek 2).



3. Nyní v seznamu dostupných sítí klikněte znovu na Vaši Wi-Fi síť. Zobrazí se okénko, ve kterém bude potřeba zadat heslo. Do políčka uveďte to heslo, které jste si dle předchozího návodu nově nastavili v administraci routeru. Po zadání hesla stiskněte tlačítko **Připojit**.