Zjištění reálného stavu zabezpečení bezdrátových Wi-Fi přenosů ve vybrané oblasti

Finding out the real state of wireless security of Wi-Fi transmissions in selected areas

Bc. Petr Svoboda

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Petr SVOBODA**
Osobní číslo:	**A09401**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Zjištění reálného stavu zabezpečení bezdrátových Wi-Fi přenosů ve vybrané oblasti**

Zásady pro vypracování:

1. **Vysvětlete pojem Wi-Fi síť a přínosy při jejím užívání.**
2. **Definujte hrozby napadení Wi-Fi sítí a možnou obranu.**
3. **Ve vybrané lokalitě zjistěte používaná zabezpečení v domácnostech a ve firemním sektoru.**
4. **Zjistěte a zhodnoťte právní podmínky užití Wi-Fi ve firmách PKB.**
5. **Užitím dotazníků prověřte základní znalosti uživatelů, týkající se problematiky Wi-Fi sítí.**
6. **Graficky znázorněte výstupní informace, které byly v průběhu vypracování získány.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **MA, Jianfeng. Security access in wireless local area networks : from architecture and protocols to realization. Beijing : Higher Education Press, 2009. 431 s. ISBN 978-3-642-00941-9.**
2. **LUDVÍK, Miroslav; ŠTĚDROŇ, Bohumír. Teorie bezpečnosti počítačových sítí. 1. vyd. Kralice na Hané : Computer Media, 2008. 98 s. ISBN 978-80-86686-35-6.**
3. **GORANSSON, Paul; GREENLAW, Raymond. Secure roaming in 802.11 networks [online]. Oxford : Newnes, [cit. 2011-01-19]. 343 s. Dostupné z WWW: [http://www.sciencedirect.com/science/book/9780750682114]. ISBN 9780750682114.**
4. **SOSINSKY, Barrie. Mistrovství – počítačové sítě : [vše, co potřebujete vědět o správě sítí]. Vyd. 1. Brno : Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.**
5. **MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. Hacking bez záhad. 1. vyd. Praha : Grada, 2007. 520 s. ISBN 978-80-247-1502-5.**

Vedoucí diplomové práce: **Ing. Jiří Korbel**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce pojednává o problematice Wi-Fi, jejím zabezpečení a možných útocích na bezdrátové počítačové sítě. Díky užití dotazníků a detekční techniky mapuje současnou situaci se zabezpečením Wi-Fi sítí a všechna zjištěná data graficky zobrazuje a vyhodnocuje. Rovněž se zaobírá problematikou přenosu cenných dat prostřednictvím Wi-Fi, přičemž se opírá o platný zákon České republiky.

Klíčová slova: access point, dotazník, internet, Linux, komunikace, stav, útok, zabezpečení, zákon, warchalking, Wi-Fi.

ABSTRACT

This thesis deals with problems of Wi-Fi, its security and possible attacks on wireless computer networks. Thanks to the use of questionnaires and screening techniques the thesis is mapping the current security situation of Wi-Fi networks, and all recorded data are graphically displayed and evaluated. It also deals with security issues of valuable data transfer via Wi-Fi using applicable law of the Czech Republic.

Keywords: access point, attack, communication, state, internet, law, Linux, questionary, security, warchalking, Wi-Fi.

Na tomto místě bych rád poděkoval svému vedoucímu práce, panu inženýru Jiřímu Korbelovi, za ochotný a aktivní přístup k vedení a nápomoci při získávání potřebných vědomostí k vypracování této diplomové práce. Dále bych chtěl poděkovat své rodině a blízkým za podporu nejen při psaní práce, ale i v průběhu celého studia.

Zvláštní poděkování zaslouží spolužák a zejména dobrý přítel Bc. Tomáš Gavenda, který mne svými vědomostmi v průběhu celého pětiletého studia mnohokrát podpořil.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD **11**
I TEORETICKÁ ČÁST **12**
1 WI-FI SÍŤ **13**
1.1 HISTORIE WI-FI 13
1.2 HW HLEDISKO WI-FI 14
1.2.1 AP – Access point 14
1.2.2 Anténa 15
1.2.3 WiFi karta 15
1.2.4 Kabeláž 16
1.3 SW HLEDISKO WI-FI 16
1.3.1 Frekvenční pásmo WiFi 16
1.3.2 IEEE 802.11 17
1.3.3 Připojení klienta k AP 18
1.3.4 Wi-Fi síť bez AP 18
1.4 VÝHODY A NEVÝHODY WI-FI 19
1.5 WI-FI SÍŤ A JEJÍ RUŠENÍ 20
1.5.1 Vzájemné rušení Wi-Fi sítí 20
1.5.2 Rušení Wi-Fi a jiných technologií 22
1.6 BUDOUCNOST WI-FI 22
2 ZABEZPEČENÍ WI-FI SÍTÍ **23**
2.1 ZMĚNA DEFAULTNÍHO NASTAVENÍ SSID 23
2.2 SKRYTÍ SSID 23
2.3 ZMĚNA DEFAULTNÍHO NASTAVENÍ HESLA NA AP 23
2.4 OMEZENÍ PŘÍSTUPU DO AP 24
2.5 OMEZENÍ DOSAHU PŘÍSTUPOVÝCH BODŮ 24
2.6 FILTROVÁNÍ MAC ADRES 24
2.7 MANUÁLNÍ PŘIŘAZOVÁNÍ IP ADRES 25
2.8 AUTENTIZACE A ŠIFROVÁNÍ KOMUNIKACE 25
2.8.1 OKA (Open Key Authentification), SKA (Shared Key Authentification) 25
2.8.2 802.1X 26
2.8.3 WEP (Wired Equivalent Privacy) 27
2.8.4 WPA (Wi-Fi Protected Access) 29
2.8.5 WPA2 30
3 ÚTOKY NA WI-FI SÍTĚ **31**

3.1 DENIAL OF SERVICE (DOS) 31
3.2 CHOP-CHOP ÚTOK 31
3.3 INJEKCE PAKETU 31
3.4 FRAGMENT ÚTOK 32
3.5 DEAUTHENTICATION ATTACK 32
3.6 MAN-IN-THE-MIDDLE ATTACK 32
3.7 PODVRŽENÍ SPOJENÍ 32
3.8 SESSION HIJACK ATTACK 33
3.9 BRUTAL-FORCE ATTACK (ÚTOK HRUBOU SILOU) 33
3.10 FMS ÚTOK 34
3.11 PTW ÚTOK 34
4 CITLIVÁ DATA PŘENÁŠENÁ PŘES INTERNET 35
4.1 UTAJOVANÉ INFORMACE 35
4.1.1 Citace zákona 35
4.1.2 Znaky utajované informace 35
4.1.3 Stupně utajení 36
4.2 KNOW-HOW 37
4.3 OBCHODNÍ TAJEMSTVÍ 37
4.4 OSOBNÍ ÚDAJE 37
5 PRÁVNÍ OMEZENÍ UŽITÍ BEZDRÁTOVÉHO INTERNETU VE FIRMÁCH SBS 39
5.1 INFORMAČNÍ SYSTÉM 39
5.1.1 Citace § 34 39
5.1.2 Výklad § 34 40
5.2 CERTIFIKACE 40
5.2.1 Citace § 46 odst. 1 40
5.2.2 Výklad § 46 odst. 1 41
5.3 POSTOJ NBÚ K PROBLEMATICE WI-FI 41
6 DOTAZNÍK A JEHO TVORBA 42
6.1 ZÁKLADY TVORBY DOTAZNÍKU 42
6.2 STANOVENÍ CÍLE 42
6.3 FORMULACE OTÁZEK 43
6.4 STRUKTURA DOTAZNÍKU 43
6.5 OTESTOVÁNÍ DOTAZNÍKU 43
7 WARCHALKING 45
7.1 DĚLENÍ WARCHALKINGU 45
7.2 WARCHALK MAPA 45
7.3 WARCHALK ZNAČENÍ 46
7.3.1 Open net 46
7.3.2 WEP net 47
7.3.3 Closed net 47
7.4 GOOGLE A WARCHALKING 47
II PRAKTICKÁ ČÁST 49

8 DOTAZNÍK WI-FI ZNALOSTÍ 50
8.1 TVORBA DOTAZNÍKU 50
8.2 ZAMĚŘENÍ DOTAZNÍKU 51
8.3 LOGICKÉ ČLENĚNÍ 51
8.4 DATA ZÍSKANÁ Z DOTAZNÍKU 51
8.4.1 Zkušenost uživatelů 51
8.4.2 Wi-Fi v domácnostech 52
8.4.3 Znalost přístupu do AP 52
8.4.4 Osoba nastavující AP 52
8.4.5 Defaultní nastavení přístupu do AP 52
8.4.6 Použití skrytí SSID 53
8.4.7 Použití filtru MAC 53
8.4.8 Automatické přiřazování IP 53
8.4.9 Druh zabezpečení 53
8.4.10 Nastavení pouze LAN 54
8.4.11 Bezpečnost uložení AP 54
8.4.12 Použití loginu na Wi-Fi 55
8.4.13 Důvěra v bezpečnost Wi-Fi 55
8.4.14 Znalost potenciálního útočníka 56
8.4.15 Setkání s útokem 56
8.4.16 Připojení přes hotspot 56
8.4.17 Použití loginu hotspot 57
8.4.18 Zkušenost s krádeží 57
8.4.19 Pohlaví 57
8.4.20 Věk 58
8.5 VYHODNOCENÍ DOTAZNÍKU 58
8.5.1 Hodnocení surových dat 58
8.5.2 Hodnocení hlubších vztahů 59
9 ZJIŠTĚNÍ REÁLNÉHO STAVU ZABEZPEČENÍ WI-FI DETEKČNÍ TECHNIKOU 61
9.1 SOFTWAROVÁ VÝBAVA 61
9.1.1 Operační systém 61
9.1.2 Software pro monitoring 61
9.2 HARDWAROVÁ VÝBAVA 62
9.2.1 Popis užitého zařízení 62
9.2.2 Wi-Fi síťová karta 62
9.3 MÍSTA MONITORINGU WI-FI SÍTÍ 63
9.3.1 Město Kroměříž 63
9.3.2 Velké náměstí v Kroměříži 63
9.3.3 Sídliště Zachar 64
9.4 POSTUP MONITORINGU WI-FI SÍTÍ 66
9.4.1 Konzole 66
9.4.2 Zjištění jména síťové karty 66
9.4.3 Zapnutí monitorovacího módu 67
9.4.4 Spuštění vlastního monitorování 68
9.4.5 Příklad výsledku vlastního monitorování 68

9.5 VÝSLEDKY MONITORINGU 71
9.5.1 Velké náměstí 71
9.5.2 Sídliště Zachar 74
9.5.3 Srovnání zabezpečení sítí v typově různých lokalitách 77
9.6 SROVNÁNÍ S JINÝMI VÝZKUMY 78
9.6.1 Ernst & Young v Praze a Bratislavě 78
9.6.2 Srovnání s mnou naměřenými daty 79
9.7 HODNOCENÍ ZÍSKANÝCH DAT DÍKY MONITORINGU SÍTÍ 80
10 ZABEZPEČENÍ WI-FI VE FIREMNÍM SEKTORU 82
10.1 VÝBĚR FIREM 82
10.2 RESTAURAČNÍ ZAŘÍZENÍ A KAVÁRNY 82
10.2.1 Wi-Fi průzkum a jeho výsledky 83
10.2.2 Shrnutí, hodnocení 83
10.3 BĚŽNÉ FIRMY 84
10.3.1 Wi-Fi průzkum a jeho výsledky 84
10.3.2 Shrnutí, hodnocení 85
10.4 SPECIÁLNÍ FIRMY 85
10.4.1 Wi-Fi průzkum a jeho výsledky 85
10.4.2 Shrnutí, hodnocení 87
ZÁVĚR 88
ZÁVĚR V ANGLIČTINĚ 89
SEZNAM POUŽITÉ LITERATURY 90
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 92
SEZNAM OBRÁZKŮ 95

ÚVOD

Oblíbenost Wi-Fi sítí v České republice i nadále roste. Z mých předběžných výzkumů vyplynulo, že řada běžných uživatelů používá v domácnosti svůj vlastní Wi-Fi router, taktéž velká spousta providerů používá k poskytování připojení právě technologie Wi-Fi.

O nutnosti zabezpečení takovýchto bezdrátových přenosů toho byly napsány již spousty a většina, byť i méně znalých uživatelů, ví o možnosti zneužití bezdrátového přenosu. Jak palčivou problematikou je ale ve skutečnosti zabezpečení Wi-Fi? Projevuje se i v této problematice naše, pro Českou republiku tolik příznačná, lenost? Ačkoliv víme o možných rizicích spojených s užíváním bezdrátové LAN, spoléháme se raději na štěstí a doufáme, že nás osobně nic zlého nepotká?

Na tyto a další otázky se pokouší odpovědět tato diplomová práce. Cílem praktické části práce je vyhledání Wi-Fi sítí v předem vybrané lokalitě, zjištění jejich skutečného zabezpečení a následné vyhodnocení, stejně tak jako dotazníková forma zjišťující povědomí uživatelů Wi-Fi a skutečné zabezpečení jejich zařízení.

Práce volně navazuje na mou bakalářskou práci, v níž jsem mimo jiné prokázal nedostatky v zabezpečení řady sítí vstupem do zabezpečené sítě a rozšifrováním komunikace v ní. Rovněž z ní čerpá poznatky, které jsou shrnuty zejména v prvních třech kapitolách.

I. TEORETICKÁ ČÁST

1 WI-FI SÍŤ

Slovo Wi-Fi bylo vytvořeno sdružením WECA a pochází z anglického Wireless Fidelity do češtiny přeloženého jako „bezdrátová věrnost“. Ačkoliv se řada uživatelů s tímto pojmem často setkává, ne každý by dokázal přesně zodpovědět otázku, co přesně se pod ním skrývá. Jedná se o bezdrátovou komunikaci v počítačových sítích, tedy technologii, díky níž můžeme pomocí svého zařízení navázat síťové spojení bez nutnosti užití přímého kabelového připojení. [6]

1.1 Historie Wi-Fi

Počátky bezdrátového internetu (Wi-Fi) datujeme do roku 1990, z nějž pochází první oficiální zprávy o počátku práce na něm. O sedm let později vyšla první norma nesoucí označení IEEE 802.11, jež dovolovala zařízením rychlost 1 nebo 2Mbps, což bylo v praxi samozřejmě nedostatečné, a téměř nepoužitelné. Proto, dva roky nato, vznikla další norma označená jako IEEE 802.11b umožňující zařízením pracovat na frekvenci 2,4GHz rychlostí 11Mbps, což již dostačovalo k běžnému užívání a bylo srovnatelné s pomalejšími síťovými kartami. V roce 2003 vyšel nový standard, který uživatelům frekvence 2,4GHz nabídnul rychlost připojení až 54Mbps, s níž se v dnešní době běžně setkáváme. Jako novinku můžeme označit standard vydaný v roce 2009, nesoucí označení IEEE 802.11n, pracující v pásmu 2,4GHz a 5GHz dosahující maximální teoretické rychlosti 600Mbps. Opomenout nelze ani standard 802.11y z roku 2008, pracující v málo užívaném pásmu 3,7GHz s maximální rychlostí 54Mbps a o devět let dříve vydaný standard 802.11a se stejnou přenosovou rychlostí, určený pro zařízení na frekvenci 5GHz. [6]

V původní navrhnuté normě nebylo přesně definováno šifrování dat ani samotný protokol, proto nebyla zaručena vzájemná kompatibilita jednotlivých zařízení od různých výrobců. Tohoto problému se ujalo sdružení WECA (Wireless Ethernet Compatibility Alliance), jehož testy musí projít každé zařízení, jež chce bezdrátový přenos používat. Zařízení vzájemně kompatibilní a tedy splňující testy sdružení WECA jsou označeny logem Wi-Fi. [6]

Obr. 1. Wi-Fi logo.

Na obrázku je logo s barevnými variantami indikujícími standard, dle kterého Wi-Fi zařízení pracuje.

1.2 HW hledisko Wi-Fi

Každá WiFi síť obsahuje určité povinné komponenty, bez kterých by se nedala sestavit. Další komponenty mohou záviset na tom, za jakým účelem danou bezdrátovou síť sestavujeme. Následující kapitola popisuje hlavní povinné komponenty a stručně je charakterizuje. [6]

1.2.1 AP – Access point

Access point představuje stěžejní prvek bezdrátové sítě umožňující vysílat či přijímat data. V praxi je možné se setkat s využitím AP, kdy tento funguje jako spojení klasické LAN díky ethernetovým portům a WLAN za použití antény. Pro použití k pokrytí objektu internetem je třeba přijímat na portu WAN či přijímací anténou u systému point-to-multipoint signál od providera. [6]

Obr. 2. Access point.

V programovém nastavení přístupového bodu se nalézají důležité volby pro konfiguraci WiFi sítě včetně jejího zabezpečení, viditelnosti sítě či volby filtrování MAC adres. [6]

Pro nastavení AP je určeno uživatelské rozhraní. Pro přístup do něj je třeba znát jeho IP adresu, dále uživatelské jméno a heslo. [6]

Defaultní IP adresa přitom bývá nejčastěji 192.168.1.1, defaultní nastavení loginu se daleko častěji liší podle výrobce. Seznam loginů těchto zařízení v závislosti k výrobci je

možné dohledat na internetových stránkách. Příkladem takové stránky je http://www.phenoelit-us.org/dpl/dpl.html, obsahující řádově několik stovek zařízení a jejich defaultních nastavení. [6]

1.2.2 Anténa

Pro účely WiFi se antény dělí na všesměrové a směrové. Všesměrové jsou používány pro pokrytí bytů, domů či jiných objektů. Užití všesměrové antény v domácnosti zvyšuje komfort při používání PC a zejména internetu. K připojení se na internet již není třeba mít stanici (laptop, PDA, mobilní telefon, apod.) propojenou kabelem. Díky WiFi je možné se volně pohybovat v prostoru. Vzdálenost, na kterou je komunikace s AP možná, závisí na typu antény. Pro nejlepší příjem signálu je důležitá její přímá viditelnost. Při přímé viditelnosti se dosah antény pohybuje řádově v desítkách metrů, přičemž tato vzdálenost rapidně klesá s překážkami, které dělí anténu a stanici. [6]

Obr. 3. Všesměrová anténa.

Pravidla přímé viditelnosti platí i u antén směrových. Tyto antény jsou využívány zejména k překonání vzdálenosti od hlavního vysílače k přijímači. Hlavní vysílač bývá většinou majetkem providera, bývá umístěn na nejvyšší budově a pokrývá určitou oblast. Dosah je opět závislý na typu antény, řádově se však pohybuje okolo stovek metrů až několika málo kilometrů. [6]

1.2.3 WiFi karta

Slouží pro připojení počítače či laptopu do WiFi sítě. Je bezdrátovou analogií k síťové kartě, která se používá pro připojení k LAN. V zásadě je ji možné připojit do dvou různých

rozhraní – do PCI u stolního počítače a do PCMCIA u laptopu. V poslední době se rozmohlo i používání USB WiFi karet s integrovanou nebo externí anténou.

Řada jiných zařízení má WiFi modul pevně zabudován již od výrobce. Klasickými zástupci těchto přístrojů jsou PDA, mobilní telefony a VOIP telefony. [6]

Obr. 4. USB Wi-Fi karta.

1.2.4 Kabeláž

Jak je z obrázku č. 2 patrné, pro správnou funkci Wi-Fi pro připojení k internetu je třeba kabelového připojení AP. Ve většině případů je užit kabel pro napájení AP a vstup WAN, tedy vstup internetu do AP. Dále může být užito připojení LAN, tedy kabelového ethernetového propojení AP s PC. To bývá nejčastěji užito pro poskytnutí internetu v rámci provozování stolního počítače, který nebývá vybaven Wi-Fi kartou, což je logické i kvůli jeho značné imobilitě. [1]

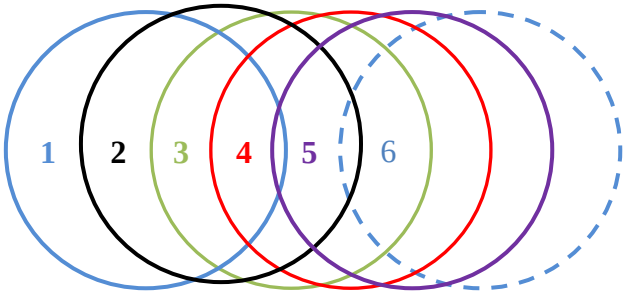
1.3 SW hledisko Wi-Fi

Na Wi-Fi může být nahlíženo také jako na elektromagnetické záření, díky němuž se můžou uživatelé připojovat k počítačové síti. Síla záření je závislá nejen na vysílači – anténě, ale i na prostředí, v němž se uživatel pohybuje. [6]

1.3.1 Frekvenční pásmo WiFi

Zařízení WiFi nejčastěji pracují v bezlicenčním pásmu na frekvenci 2,4GHz a 5GHz. To je sice na jednu stranu výhodné, jelikož provoz bezdrátových sítí je tak zdarma, na druhou stranu je to však jeden z důvodů rušení, protože na frekvenci 2,4GHz pracují nejen další WiFi sítě, ale i další technologie, především mikrovlnné trouby a bluetooth. V rámci WiFi sítí může být vzájemnému rušení částečně předcházeno užitím jednoho ze 13 kanálů. Tyto jsou v rozmezí od 2,412GHz do 2,484GHz. Komunikace na dvou různých kanálech však ještě nezaručuje nulové rušení. Odstup kanálů je totiž 5MHz, ale šířka pásma jednoho

kanálu je celých 22MHz. Z uvedeného vyplývá, že se v praxi neruší jen kanály s rozestupem pěti a to například 1., 6. a 11. [6]



Obr. 5. Překrývání komunikačních kanálů.

1.3.2 IEEE 802.11

U bezdrátových zařízení, kterými se má práce zabývá, se je možno dočíst, že pracují dle standardu IEEE 802.11, což je označení WiFi standardu vyvíjeného pracovní skupinou IEEE. [6]

Označení IEEE je zkratkou pro Institute of Electrical and Elektronics Engineers (česky Institut pro elektrotechnické a elektronické inženýrství), což je nezisková organizace zahrnující mimo jiné i zmíněnou pracovní skupinu standardizační komise. [6]

Označení 802.11 bývá doplněno malým písmenem. V tom případě se jedná o jeden ze standardů, přičemž písmeno označuje jeden ze 6 druhů modulací radiového signálu. V praxi nejužívanější modulace jsou 802.11a, 802.11b a 802.11g, přičemž první jmenovaná pracuje na frekvenci 5GHz, další dvě v pásmu 2,4GHz. [6]

Jak již bylo uvedeno v části s názvem Historie Wi-Fi, prvotní rychlost dle standardu 802.11 byla 1 až 2Mbps. Následoval standard 802.11b dosahující rychlosti až 11Mbps a po něm standard s označením 802.11g dosahující rychlosti 54Mbps. Všechny tyto rychlosti jsou však pouze teoretické. [6]

Hlavní příčinou, proč zařízení nekomunikuje maximální možnou rychlostí, je totiž mechanismus ARS (Automatic Rate Selection). Tento zajišťuje spolehlivost přenosu a

v případě zhoršeného signálu (způsobeného například stíněním, větší vzdáleností komunikujících zařízení, apod.) zvyšuje redundanci (tj. zvyšuje počet bitů) a snižuje rychlost. Rychlost se snižuje ve skocích 54Mbps, 11Mbps, 2Mbps až 1Mpbs.

Další, jistě ne zanedbatelnou příčinou, je i fakt, že zařízení v síti většinou není samo, s přístupovým bodem totiž komunikuje více zařízení, která jsou k němu připojena. Rychlost se tak dělí mezi všechna tato zařízení.

Maximální rychlosti připojení je tedy při běžném užívání Wi-Fi prakticky nemožné dosáhnout. Takových rychlostí by se dosáhlo jen v případě, kdy by bylo naše zařízení jediným zařízením v síti a toto zařízení by bylo v dostatečné blízkosti k AP. [3]

1.3.3 Připojení klienta k AP

Připojení klienta k AP je důležité pro vzájemnou komunikaci. Klasické připojení bez užité autentizační metody je podmíněné pouze přístupem k příslušnému portu AP a vzájemnou kompatibilitou zařízení. [6]

Pro připojení k AP prostřednictvím bezdrátové technologie je v případě užitého zabezpečení podmínka znát tyto přístupové údaje, popřípadě splnit další podmínky definované administrátorem sítě. [6]

V současnosti je téměř absolutní nutností užití autentizačních metod k zabránění přístupu neoprávněných uživatelů k Access Pointu. Dobrým příkladem této autentizační metody je 802.1X, o níž je zmínka v následující kapitole. [6]

Pokud chce zařízení komunikovat, musí zaslat access pointu rámec RTS (Ready To Send). Ostatní body v síti dostávají rámec NAV (Network Allocation Vector), jež je upozorní na komunikující zařízení. Access point pak odpovídá zmíněnému zařízení rámcem CTS (Clear To Send), čímž oznamuje, že je připraveno ke komunikaci se zařízením a že s ním v současnosti nekomunikuje zařízení jiné. Po přenesení dat mezi zařízeními je přenos ukončen rámcem ACK (Acknowledge), čímž potvrzuje příjem dat a ukončuje komunikaci.

1.3.4 Wi-Fi síť bez AP

Ve výčtu základních vlastností bezdrátových sítí nesmí být opomenuta možnost připojení dvou zařízení bez použití Access pointu. Jedná se tedy o přímé spojení dvou zařízení, při němž nedochází ke komunikaci s prostředníkem (AP). Tento způsob spojení bývá

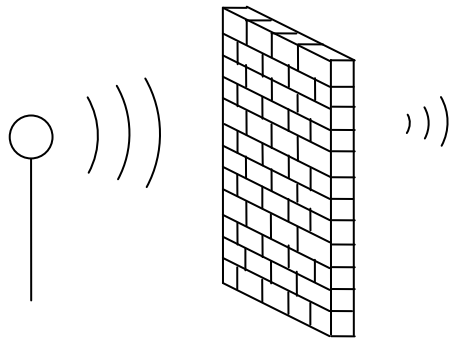
označován jako Ad-hoc. Ad-hoc přináší jednu zásadní nevýhodu, tou je fakt, že ani jedno ze zařízení díky němu nemá přístup na internet prostřednictvím používané bezdrátové síťové karty. Tento druh spojení bývá použit pro přenos dat mezi dvěma zařízeními, popřípadě pro hraní PC her v režimu multiplayer[1].

1.4 Výhody a nevýhody Wi-Fi

Základní výhodou WiFi sítí je možnost propojení zařízení bez nutnosti užití metalických nebo optických linek. Jedná se nejen o ekonomicky výhodné řešení. Mnohdy hraje roli i zachování vzhledu místnosti, tedy pokrytí internetem bez nutnosti narušení jejího vzhledu různými kabely apod. Neopomenutelnou výhodou je jistě i poměrně velká rychlost spojení, která při užití vhodné techniky může dosahovat až rychlosti 54MBit a dosah, který se může v praxi pohybovat řádově v několika desítkách metrů. Pro mnoho firem, podniků a restaurací se WiFi stalo nedílnou součástí reklamy a komerce. Nejen řada podnikatelů, ale i jiných subjektů ráda vyhledává takové kavárny a restaurace, kde se mohou volně připojit k internetu. [6]

Oproti tomu hlavní nevýhodou WiFi je nutnost přímé viditelnosti vysílače a přijímače. S překážkami jako jsou zdi, stromy a jiné objekty rapidně klesá vzdálenost, na kterou lze data přenášet. Problémy způsobují i povětrnostní vlivy jako déšť či sněžení. Další ve výčtu problémů je rušení, které je způsobeno dvěma překrytými bezdrátovými sítěmi, či dalšími zařízeními pracujícími na stejné frekvenci. Zde se jedná zejména o pásmo 2,4GHz, jelikož právě to je v současnosti nejvíce používané. V neposlední řadě je značnou nevýhodou bezdrátových sítí nutnost zajištění bezpečnosti přenosu, které při použití kabelu z velké části odpadá. [6]

[1] Režim PC her, jež podporuje účast více hráčů v rámci jedné hry



Obr. 6. Nevýhoda Wi-Fi – špatná prostupnost překážkami.

I přes velké množství nevýhod se WiFi technologie nezadržitelně rozvíjí. Možnost neomezeného pohybu, jednoduchého připojení a relativní spolehlivosti značně převažuje zmíněné nevýhody a i do budoucna nahrává dalšímu rozvoji této oblasti. [6]

1.5 Wi-Fi síť a její rušení

Jak bylo uvedeno v předchozím textu, bezdrátová internetová síť přináší problémy v podobě rušení. Toto může být způsobeno jak přírodními vlivy, tak i vlivy umělými. Tyto uměle, tedy člověkem, vytvořené vlivy rušení vznikají jak v zařízeních primárně určených k jinému účelu, tak i v zařízeních určených k účelu podobnému. [6]

V praxi se často vzájemně ruší dvě sítě, jejichž AP jsou v blízkosti, a tak se vlny prolínají. Takovýchto příkladů je možno v rámci panelového domu najít opravdu spousty, jak dokazuje i výzkum v praktické části mé diplomové práce. [6]

Použití vhodného komunikačního kanálu[2] je jen částečným řešením, které v mnoha ohledech nedostačuje a použití bezdrátového připojení se tak stává nemožným, nebo velice obtížným a vznikají omezení pro užití snížením dosahu sítě nebo její nestabilita. [6]

1.5.1 Vzájemné rušení Wi-Fi sítí

Vzhledem k faktu vzájemného rušení bylo nutno tuto problematiku upravit zákonem, není totiž těžké představit si providery, kteří by se snažili zvyšovat své pokrytí až za hranici

[2] Jež bylo nastíněno v kapitole 1.2.1 Frekvenční pásmo WiFi.

únosnosti a silou svého signálu znemožnili nejen užití Wi-Fi jiným uživatelům, ale i ohrozili zdraví[3] obyvatel na cílovém prostoru.

Rušení cizí sítě je bohužel ovlivněno snahou o co nejlepší pokrytí vlastního prostoru. Vyzařování do prostoru cizího je tak ve velké většině případů více nechtěným a sekundárním důsledkem, nežli schválností nebo snahou o znemožnění komunikace druhému. Jinou kapitolou je pak snaha o znemožnění komunikace cíleným vyzařováním rušícího signálu, kterou se zabývá třetí kapitole této diplomové práce.

Bohužel, nejsou výjimkou vzájemné „boje" providerů, kteří koexistují na jednom území, nejčastěji na městském sídlišti. Tito používají směrové antény pro přenos na velkou vzdálenost a tyto signály se nezřídka kdy kříží. Pak bohužel platí, že „silnější vyhrává", poskytovatelé připojení tak zvyšují výkon svých vysílačů a tím i zvyšují rušení. [6]

I z toho důvodu přešli poskytovatelé připojení zejména na 5GHz frekvenci svých směrových antén, což zlepšilo situaci pro užívání domácích Wi-Fi sítí. Přesto však k rušení dochází a to ne zřídka.

Proto ČTU[4] vydal „všeobecné oprávnění č. VO-R/1208.2005-34 k využívání radiových kmitočtů a k provozování zařízení pro širokopásmový přenos dat na principu rozprostřeného spektra nebo OFDM v pásme 2,4 GHz a 5 GHz" platné od 1. září 2005. V něm definuje povolený vyzářený výkon pro vysílače v jednotlivých pásmech. Pro naše účely důležitější je text, z nějž vyplývá, že vzájemné rušení řeší uživatelé vzájemnou dohodou. V případě neshody se postupuje dle § 100 zákona č. 127/2005 Sb., o elektronických komunikacích. [9]

Z něj je patrné, že pokud je provozováno zařízení rušící zařízení jiné, je provozovatel tohoto zařízení povinen zabránit tomuto rušení. Pokud tak neučiní, rušení odstraňuje provozovatel „rušeného zařízení" na náklady provozovatele rušícího zařízení.

Co si pod tímto představit, není přesně definováno. Bezdrátové sítě Wi-Fi mají zhoršenou prostupnost materiálem, řešením by proto mohlo být zesílení stěny nebo vytvoření jiné překážky mezi rušícím a rušeným zařízením. V praxi je však těžké přestavit si toto řešení,

[3] Škodlivost Wi-Fi na zdraví nebyla nikdy přímo prokázána.

[4] Český telekomunikační úřad.

následkem by bylo zmenšení obývaného prostoru a jeho designová změna, nehledě na složité dokazování a vymáhání financí.

1.5.2 Rušení Wi-Fi a jiných technologií

Dle článku 2 písmene e) všeobecného oprávnění č. VO-R/10/03.2007-4 k využívání radiových kmitočtů a k provozování zařízení krátkého dosahu je technologie Wi-Fi zařazena do kategorie podružných, sekundárních, služeb. Z toho vyplývá, že jejím provozem nesmí vzniknout rušení, které by škodlivě ovlivňovalo stanice přednostních radiokomunikačních služeb. Případné rušení je opět řešeno dohodou mezi účastníky, pokud se nedohodnou, opět se postupuje dle § 100 zákona č. 127/2005 Sb., o elektronických komunikacích. [9]

1.6 Budoucnost Wi-Fi

Hudbou budoucnosti Wi-Fi technologie je nyní standard nesoucí označení IEEE 802.11ac. Ten by měl, dle dosavadních informací, podporovat pásmo 2,4GHz a zároveň pásmo 5GHz, čímž by měl dosáhnout teoretické rychlosti až 1Gbps. Teoreticky by tedy bylo možné, v případě dostatečně rychlé linky, stáhnout 125MB za 1 sekundu, data mající velikost 1GB by tedy uživatel mohl stáhnout za asi 8 sekund. Reálná rychlost zařízení pracujících na tomto standardu však bude menší, jak je vysvětleno výše. Předpokládaná propustnost se odhaduje na asi 40MB/s.

Standard 802.11ac by měl být schválen během roku 2011 a první zařízení pracující na tomto standardu můžeme očekávat během roku 2012. Zprvu se tato zařízení budou samozřejmě objevovat na výstavách a veletrzích, k masivnímu rozšíření by dle odhadů mělo dojít během roku 2013 a 2014. V roce 2015 by měl trh obsahovat miliardu zařízení s tímto standardem.

2 ZABEZPEČENÍ WI-FI SÍTÍ

Pro bezpečný provoz WiFi sítě můžeme použít různých technik zabezpečení, které níže popisuji. Jak bylo předesláno v předchozích textech, nutnost užití těchto technik tkví zejména v permanentní možnosti zneužití získání přístupu či samotných dat uživatelů neoprávněnou osobou. Představa uživatele, že by jeho data přišla do nepovolaných rukou, jistě není nic příjemného. Jejich zneužitím by vznikla újma, jíž by se dalo snadno předejít užitím správných technik. Právě o těchto technikách pojednává následující kapitola. [6]

2.1 Změna defaultního nastavení SSID

SSID představuje název sítě vytvářené AP, který musí znát každá stanice, která se k němu chce připojit. Továrním nastavením přístupového bodu se vytváří síť s SSID, jež je pro průměrně znalého útočníka známé. Zejména v případě skrytí vysílání SSID (viz níže) a v případě většího množství sítí v jednom bodě je vhodné nastavit SSID vlastního AP na nic neříkající hodnotu – ne tedy jméno firmy, jméno či příjmení uživatele. Vhodné je náhodně generované SSID. Možnost generování náhodného SSID bohužel není obvykle implementována do softwarového prostředí AP, proto doporučuji využít programu Hesluj! verze 3.1. V případě malého počtu sítí v dané oblasti u viditelné sítě je však užitnost této techniky mizivá. [6]

2.2 Skrytí SSID

Zde je využito možného nastavení Access pointu, kterým je možno zabránit, v rámci vysílání tzv. betonů (tedy pravidelného vysílání informací AP), zobrazení názvu SSID. Znalost SSID je při tom podmínkou pro připojení kterékoliv stanice k AP. [6]

Zabránění vysílání SSID se nyní jeví jako absolutní řešení zabezpečení bezdrátového síťového provozu. Nutno podotknout, že existují techniky, které i přes tuto ochranu odhalí SSID příslušné sítě. O těchto technikách se pojednává 3. kapitola této diplomové práce. [6]

2.3 Změna defaultního nastavení hesla na AP

Znalost hesla k AP umožňuje útočníkovi přístup do konfiguračního prostředí, kde může napáchat nezměrné škody. Stejně jako SSID i heslo je z továrního nastavení již předdefinované, a pokud jej nezměníme, notně tím snížíme zabezpečení sítě. Při nastavování přístupového hesla je vhodné použít některé bezpečné heslo, tedy dostatečně dlouhé složené z náhodných písmen a číslic. [6]

2.4 Omezení přístupu do AP

Další možnost ztížení přístupu útočníka do konfiguračního prostředí AP využívá zamezení přístupu klientům komunikujícím s AP prostřednictvím bezdrátového spojení. Přístup do AP má tedy pouze klient připojený prostřednictví LAN (drátové spojení s AP). Fyzický přístup k AP je pro běžného útočníka operujícího na dálku nemožný a nemyslitelný, proto máme velkou šanci, že útočník od pokusů o vstoupení do nastavení AP ustoupí. [6]

2.5 Omezení dosahu přístupových bodů

Jednou z dalších technik je snížení a vymezení dosahu přístupového bodu, tedy ztížení přístupu útočníka k bezdrátové síti. Zde platí pravidlo, že by síť neměla přesahovat hranici objektu, tedy měla by být přístupná jen v objektu, nikoliv mimo něj. V praxi se toto zajišťuje vhodným umístěním AP a zvolením síly signálu. V rámci bytů je však docílení této techniky velice složité až nemožné. [6]

2.6 Filtrování MAC adres

MAC adresa představuje adresu jednotlivých stanic (klientů). Při autentizačním procesu se předává mimo jiné i informace o MAC adrese příslušné stanice. V nastavení většiny AP můžou být jednoduše vymezena zařízení, jejichž MAC adresy budou povoleny či zakázány. Filtrování tedy umožňuje mimo jiné nastavit i klienty, kterým je po kontrole správnosti MAC adresy povolen přístup do sítě. Těm, kteří nejsou filtrem vymezeni, AP přístup nepovolí. [6]

Tato technika zabezpečení si získala oblíbenost zejména u domácích uživatelů a menších firem. Nastavení MAC adres všech zařízení v rámci velké sítě a jejich správa je časově velice náročná. [6]

Podobně jako výše zmíněná technika skrytí SSID, i tato by mohla v uživateli vyvolat pocit absolutního bezpečí. I zde však zdání klame, jelikož opět existují postupy vedoucí k získání cizí MAC adresy. Útočník si následně za pomoci příslušných technik nastaví adresu povoleného zařízení. To pak může použít dvěma různými způsoby dle nastavení zabezpečení. První zabezpečení neřeší, zda mají dvě stanice stejnou MAC adresu, přístup do sítě pro zmíněného útočníka proto není problémem. Druhé zabezpečení však zabraňuje užití dvou stejných MAC adres v témže čase. Útočník se tedy musí buďto připojit dříve, než oprávněný uživatel, nebo počkat, až se oprávněný uživatel odpojí. [6]

2.7 Manuální přiřazování IP adres

V rámci provozu sítě může být pro zjednodušení připojování vlastních zařízení užit DHCP (Dynamic Host Configuration Protocol) server. Ten uživateli usnadňuje práci zejména tím, že automaticky přiřazuje IP připojeným stanicím. To však usnadňuje práci i útočníkovi, jelikož znalost IP adresy je jednou z podmínek pro připojení se k AP. Manuální nastavování IP adres je jistě pracnější, ale může útočníkovi ztížit jeho průnik do bezdrátové sítě. [6]

2.8 Autentizace a šifrování komunikace

Následující text pojednává o autentizaci, tedy ověření přístupu a šifrování, tedy pozměnění dat do podoby, která není běžně čitelná.

Z důvodu možnosti připojení se do bezdrátové sítě i na větší vzdálenost vyvstává pro správce sítě problém v rozlišování klientů, u kterých je a u kterých není toto žádoucí. Tuto problematiku zajišťují autentizační mechanismy, které požadují po klientovi prokázání oprávněnosti přístupu. Autentizace je tedy proces, při kterém sdělujeme požadované údaje či informace, kterými se identifikujeme. Tyto mechanismy napomáhají zabránění přístupu nepovolané osoby do chráněné sítě. [2]

2.8.1 OKA (Open Key Authentification), SKA (Shared Key Authentification)

V případě OKA a SKA se jedná o základní a jednoduše překonatelné autentizační mechanismy. Autentizace prostřednictvím OKA je založena na sdělení informací o klientovi a automatickém přidělení autentizace. Existuje zde i kombinace s užitím metody WEP, kdy se klient prokazuje vlastnictvím šifrovacího klíče, který je na obou stranách – vysílací i přijímací – shodný. Sdělené informace nutné pro připojení totiž musí být pro přístupový bod čitelné. Tento klíč by měli mít k dispozici pouze ověření uživatelé. Vlastní průběh pak vypadá následovně. Vysílající strana text zašifruje svým klíčem, šifrovanou zprávu odešle, přijímací strana ji přijme a dekóduje. V případě dekódování shodným klíčem se shoduje získaný kontrolní součet (ICV – Integrity Check Value) se součtem uvedeným ve zprávě. V opačném případě se součet neshoduje a komunikace je blokována, jelikož se komunikující strana správně neautentizovala – neprokázala znalost klíče. Pro výpočet šifrovacího klíče byla nalezena celá řada postupů popsaných v další kapitole mé diplomové práce. [6]

Na první pohled pokročilejším mechanismem autentizace je SKA, u kterého probíhá opravdová autentizace. Samotný autentizační proces je opět založen na shodných šifrovacích klíčích. Tentokrát však při pokusu stanice o připojení se do bezdrátové sítě vyšle AP text, který stanice obdrží, zakóduje svým klíčem a pošle zpět AP. Ta kódovanou zprávu dešifruje a v případě, že se shoduje s původní odeslanou, stanice může nadále, již výhradně šifrovaně, komunikovat v rámci WLAN. Problém je zřetelný v okamžiku, kdy útočník zachytí první nekódovanou zprávu a následnou zašifrovanou odpověď. Snadným výpočtem získá zmíněný klíč. [6]

2.8.2 802.1X

Jako reakce na neefektivní autentizační metody SKA a SKO spatřil v roce 2001 světlo světa protokol 802.1X. Ten je i v současnosti kvalitním nástrojem pro ověření oprávněnosti přístupu klientů do bezdrátové sítě. Princip činnosti protokolu je v tom, že při pokusu o připojení uživatele (suplikanta) se příslušný port zablokuje a požaduje autentizační údaje. Rozpoznání přítomnosti klienta má za úkol přístupový bod, jenž následně klientovi pošle tzv. EAP REQUEST-ID zprávu. Na tu klient odpovídá řádnou EAP RESPONSE-ID obsahující autentizační údaje. EAP RESPONSE-ID je pak serverem převeden do RADIUS ACCESS-REQUEST, jenž je odeslán RADIUS serveru. RADIUS server údaje vyhodnotí a na základě zadaných údajů rozhodne o povolení či nepovolení přístupu. [6]

V případě povolení přístupu vyšle RADIUS server přístupovému serveru zprávu ACCESS_ACCEPT, která obsahuje informaci EAP SUCCESS, jež je následně odeslána klientovi. Po výše popsaném postupu je klient úspěšně autentizován, asociován a je mu tedy povolena komunikace prostřednictvím příslušného portu. [6]

V případě, kdy RADIUS server vyhodnotí klienta nepovolaným komunikace zvoleným portem, odešle přístupovému serveru zprávu ACCESS_DENY obsahující informaci EAP FAILURE. Ta je následně poslána klientovi a další komunikace po portu je mu odepřena. [5] [6]

Ve výše uvedeném textu se objevují pojmy EAP a RADIUS. EAP je v tomto případě protokol pro komunikaci mezi klientem a přístupovým serverem. RADIUS naopak představuje protokol určený k přenosu autentizačních informací mezi přístupovým serverem a RADIUS serverem. RADIUS server má na starosti použití EAPu k ověření

autentizačních údajů a rozhoduje o dalších otázkách připojení, jako například době, po kterou může klient přes daný port komunikovat či rychlosti připojení. [6]

Protokol EAP zajišťuje autentizaci zařízení dle několika režimů různě složitých na zavedení a s různou mírou zabezpečení. Jedním z příkladů je EAP-MD5 (Message Digest 5), který se velice snadno implementuje, ale jeho míra zabezpečení, kterou poskytuje, je velice nízká, jelikož je náchylný na celou řadu útoků a nepodporuje dynamické generování klíčů. Střední hodnotu zabezpečení i míru složitosti implementace má PEAP (Protected EAP). Mezi verze EAPu s nejlepším zabezpečením se řadí TTSL (Tunneled Transport Layer Security), který vyžaduje prokázání se přístupového bodu vůči klientovi za pomoci digitálního certifikátu. Tato verze je velice jednoduchá pro nasazení v praxi. Složitější pro implementaci s prakticky absolutní mírou zabezpečení je verze nesoucí název TSL (Transport Layer Security), jenž vyžaduje vzájemnou identifikaci mezi stanicí a přístupovým bodem (autentizačním serverem) digitálním certifikátem podepsaným certifikační autoritou. Zřídka se také můžeme setkat s verzí LEAP (Lightweight Extensible Authentication Protocol) pracující pouze s Radius serverem od firmy CISCO. [6]

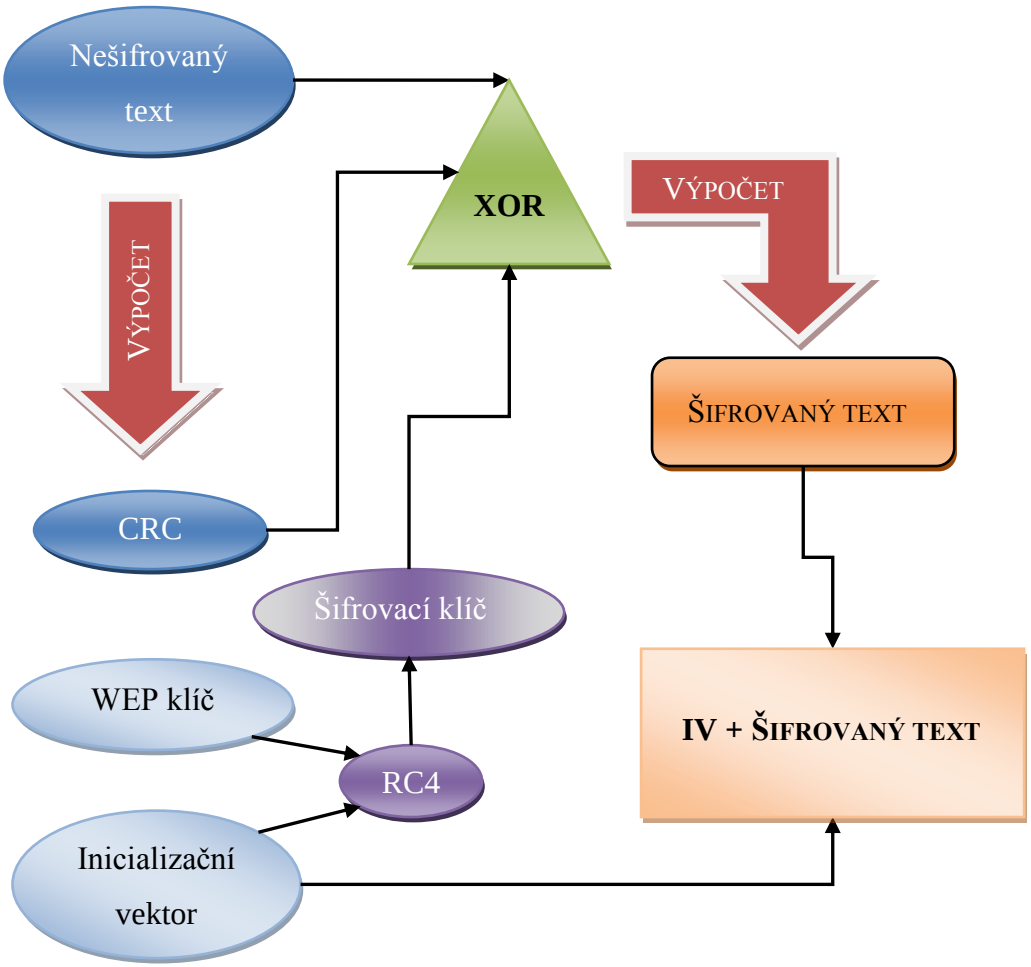
2.8.3 WEP (Wired Equivalent Privacy)

Tento název může být do češtiny přeložen jako „soukromí ekvivalentní drátovým sítím“. Již z názvu je patrné, že vzniklo jako reakce na nutnost zabezpečení bezdrátového provozu. Oproti drátovým sítím mají sítě bezdrátové hlavní nevýhodu – většina útoků je možná bez nutnosti fyzického přístupu k prvkům sítě. [6]

Wired Equivalent Privacy je první a v současnosti stále velice používaný druh zabezpečení. Jeho oblíbenost není jen z důvodu snadného nastavení, ale i kompatibility s řadou starších zařízení. Existuje ve verzi 64bitů, ktera používá 40bitový klíč zřetězený s 24bitovým IV (inicializačním vektorem) a 128bitů s klíčem 104bitovým a stejným počtem IV. K šifrování používá šifru RC4, která se řadí mezi symetrické proudové šifry. Zvolený text či data zpracovává po jednotlivých bitech. Pro kontrolu integrity užívá metody CRC-32. [6]

Šifrování probíhá za použití klíče složeného z uživatelského klíče a inicializačního vektoru. Z textu, který chceme zašifrovat se pomocí CRC-32 spočítá kontrolní součet k ověření integrity zpráv (tzv. Integrity Check Value, který indikuje, zda nebyla data po cestě upravena) a připojí se na konec. Pomocí šifry RC4 spočítáme z IV a UK šifrovací

klíč. Spočítaný ŠK musí mít stejnou velikost jako zpráva s kontrolním součtem. Následuje operace, kdy se mezi ŠK a zprávou proveden logický výhradní součet XOR. Na konec výsledné zprávy je připojen dříve vypočítaný inicializační vektor, nutný k pozdějšímu dešifrování zprávy. [6]



Obr. 7. Princip šifrování WEP.

Bohužel, je třeba říci, že WEP je dnes dosti neúčinný druh zabezpečení právě díky výše zmíněné šifře RC4. Tu vytvořil již v roce 1987 světoznámý kryptolog Ron Rivest a v současnosti je jedna z nejpoužívanějších šifer zejména díky její rychlosti zpracování dat (je asi 10x rychlejší než DES). RC4 je považována za bezpečnou šifru, ale ve WEPu je implementována zcela špatně. Díky omezenému množství IV není dodržena unikátnost WEP klíče, díky tomu je snadné pomocí programů k tomu určených po zachycení určitého množství dat spočítat hodnotu samotného klíče. [6]

Další slabinou WEP je užití CRC-32 z hlediska zabezpečení integrity dat. CRC-32 sice funguje spolehlivě, přesto jsou techniky, kterými mohou být data upravena tak, aby se kontrolní součet nezměnil. [6]

V neposlední řadě je třeba zmínit jeden z hlavních nedostatků WEP a tedy to, že WEP key je pro všechny uživatele stejný, a jelikož řada útoků může vycházet zevnitř sítě, tedy přímo od uživatele připojeného do sítě, s přímou znalostí klíče nemá tento problém dešifrovat obsah všech ostatních uživatelů. Z principu zabezpečení v případě užití statických klíčů by měl vycházet fakt, že by žádný z uživatelů neměl znát klíč, který používá k šifrování. Měl by jej znát pouze samotný správce sítě. [6]

WEP je nejstarší druh zabezpečení a v současnosti značně neúčinný, proto je takřka nutností přejít na novější technologie jako WPA, nebo WPA2. Přesto je i v současnosti značné procento bezdrátových sítí chráněno právě tímto zabezpečením, což je nejspíše způsobeno nedostatečnou osvětou uživatelů. [6]

2.8.4 WPA (Wi-Fi Protected Access)

WPA (česky Wi-Fi chráněný přístup) vychází z WEPu, ale odstraňuje jeho hlavní nedostatek – statické klíče. Je mezikrokem mezi WEPem a novým WPA2 (normy 802.11i). Wifi Protected Access vznikl v roce 2002 jako reakce na nedostatečné zabezpečení Wired Equivalent Privacy. V současnosti se používá zejména z důvodu zpětné kompatibility s WEPem, hardwarové nenáročnosti a zároveň dopředné kompatibility s WPA2. [6]

Stejně jako předchozí WEP i WPA používá k šifrování proudovou symetrickou šifru RC4. Rozdílně však používá 128bitový klíč a 48bitový IV. Původní nedostatek v podobě statických klíčů WPA vyřešilo implementací protokolu TKIP (Temporal Key Integrity Protocol). Ten v sobě slučuje spolu s funkcí dynamického generování klíčů i kontrolu integrity dat (MIC) a číslování jednotlivých paketů, čímž brání útočníkovi v útoku opakováním. TKIP mění klíč pro každý odeslaný paket, proto je nemožné odposlechnout dostatek paketů se stejným šifrovacím klíčem k rozluštění samotného klíče. [6]

MIC (Message Integrity Code) je hashovací funkce z dílny Nielse Fergusona, která využívá dvojnásobné délky inicializačního vektoru, než starší WEP. Dále přidává ke každému rámci digitální podpis, jenž se vypočítá z datové části rámce, zdrojové a cílové

MAC adresy, pořadového čísla paketu a náhodné hodnoty. Při kolizi MIC zjistí zařízení, že se jedná o útok a proběhne automatická výměna původních klíčů za nové. [6]

V případě nemožnosti užití autentizační metody 802.1X zejména z důvodu absence RADIUS serveru se využívá WPA-PSK, tedy Pre-Shared Key. TKIP se pak vypočítává na základě znalosti tzv. Master Key, který musí být předem nastavena ve všech zařízeních, které chtějí v rámci sítě komunikovat. [6]

2.8.5 WPA2

WPA2 je dodnes nejlepší formou zabezpečení bezdrátových sítí. Rozdílem oproti předchozím technikám zabezpečení je u WPA2 využití blokové šifry AES. Přesto ponechává možnost využívání TKIP pro zpětnou kompatibilitu s WPA. [6]

AES (Advanced Encryption Standard) se řadí mezi blokové šifry, data šifruje symetrickým klíčem po blocích o velikosti 128 bitů. Využívá velmi rychlého a hardwarově nenáročného algoritmu Rijndael pojmenovaného podle jeho tvůrců Vincenta Rijmena a Joana Daemena. AES v implementaci do WPA2 pracuje v čítačovém režimu s protokolem CCMP (Counter-mode CBC Message Authentication Code Protocol), který zajišťuje autentizaci a integritu dat. CCMP obsahuje algoritmus MIC známý z WPA TKIP. [6]

Autentizace je u WPA2 zajištěna stejně jako u WPA, tedy PSK, nebo 802.1x. Navíc má možnost roamingu zajištěnou pomocí pre-authentication, tedy autentizace k AP, které není v dosahu autentifikujícího se klienta pomocí AP, u kterého je klient již autentifikován. Zrychluje se tak přechod mezi body bez výpadků v připojení. [6]

Stejně jako u WPA i WPA2 má možnost využití jak 802.1X, tak PSK. Je jen na uživateli, jak s tímto naloží, ovšem i zde platí u 802.1X nutnost existence RADIUS serveru, tudíž existuje předpoklad, že jej bude využito spíše v podnikových a větších sítích, PSK pak ve středních a malých sítích. [6]

3 ÚTOKY NA WI-FI SÍTĚ

V pořadí třetí kapitola pojednává o některých útocích na zabezpečení Wi-Fi se snahou popsat podrobněji způsoby a principy jednotlivých postupů. Některé z těchto útoků vedou pouze ke znemožnění komunikace, jiné jsou schopny získat data a pomocí některých může útočník získat přístup do chráněné sítě. [6]

V celé práci včetně následujícího výčtu není vzpomenuta tématika útoků spojených se sociálním inženýrstvím. Tyto útoky spadají spíše do oblasti psychologie. Přesto jsou to útoky jedny z nejkvalitnějších a nejjednodušších. Relativně snadným zmanipulováním, popřípadě oklamáním, může útočník od samotných uživatelů získat většinu důležitých informací včetně MAC adres jednotlivých zařízení a šifrovacích klíčů. [6]

Pokud se ovšem útočník rozhodne využít některou z technik získání přístupu díky chybám v zabezpečení, s velkou pravděpodobností použije některou z níže uvedených technik. [6]

3.1 Denial of Service (DoS)

Jedná se o škodlivý útok založený na vysílání velkého množství zbytečných zpráv AP či samotným klientům. Má za úkol znemožnit komunikaci mezi zařízeními i přístupu na internet, což může zejména v prostředí firem způsobit nezměrné škody. [6]

Někdy se do tohoto útoku nesprávně řadí i cílené rušení komunikace prostřednictvím antén a obdobných zařízení pracujících na stejné frekvenci jako rušená síť. [6]

3.2 Chop-Chop útok

CRC32 i s jejími nedostatky nabízí jednoduchou možnost zneužití. Výpočet integrity není zcela dokonalý, existují totiž postupy, kterými můžeme data poupravit bez změny ICV. Pokud jsou takto upravená data poslána přístupovému bodu, tento je díky správnému kontrolnímu součtu neodmítne, ale po přečtení vrátí šifrovanou chybovou hlášku v podobě ICMP paketu. Nešifrované znění této hlášky může být snadno předvídáno. [6]

3.3 Injekce paketu

Po odposlechu (sniffingu) nešifrovaného textu a jeho šifrované podoby je vypočtena šifrovací sekvence, jíž je následně zašifrován vlastní text, který bude přijímacím zařízením úspěšně dešifrován v (útočníkem) vytvořenou zprávu. Tento útok je pomyslným můstkem pro využití dalších útoků, jejichž výčet následuje níže. [6]

3.4 Fragment útok

Tento útok je založený na principu fragmentace. Útočníkovi stačí znalost jedné dvojice (IV a keystreamu). Využitím Injection packet attacku jednotlivé fragmenty zašifrujeme touto dvojicí a odešleme AP. Výsledkem složení jednotlivých fragmentů bude v tomto případě broadcast paket. AP jej zašifruje vlastní dvojicí a odešle jako jeden rámec. Tento je zachycen útočníkem a ten, díky znalosti obsahu, může za pomoci XORu a opakováním této metody zjistit hodnotu dalších dvojic. [4] [6]

Vychází z nedostatku ve standardu 802.11, jímž je málo možností výsledků při náhodném generování inicializačních vektorů. Inicializační vektor má délku 3 byty, možných kombinací je tedy 2^{24} (16777216). [6]

3.5 Deauthentication Attack

Útočník se vydává za zvolenou stanici a vysílá pokyny k deautentifikaci daného zařízení. Tím přeruší komunikaci s AP a stanice musí znovu projít autentifikačním procesem, což prodlužuje dobu, po kterou není schopna komunikovat. Deautentifikačních pokynů je možno odeslat pomocí příslušných programů prakticky neomezeně, proto je tato metoda velice škodlivá. [6]

3.6 Man-in-the-Middle Attack

Mezi AP a klienta se zařadí útočník, který filtruje veškerou komunikaci, může ji ovlivňovat a řídit. Obě strany přitom žijí v domnění, že komunikují přímo spolu navzájem. Mimo to umožňuje útočníkovi posílat deautentizační rámce, čímž docílí opakovaného odpojení klienta od AP. [6]

3.7 Podvržení spojení

Útočník vytvoří vlastní přístupový bod (může využít i stejné SSID pro zvýšení pravděpodobnosti oklamání), na který se budou klienti pokoušet připojit. V případě přihlašování se přes šifrovanou stránku uloženou na AP má útočník práci ještě více ulehčenou. Oběť zadá své obvyklé přihlašovací údaje, jejichž výstup však nejde k originálnímu AP, ale k útočníkovu. Tyto údaje si útočník jednoduše zaznamená pro vlastní připojení k opravdovému AP. [6]

Další možností tohoto útoku je poskytnutí připojení klientům přes náš přístupový bod s jediným povoleným portem 80. Veškerá následná komunikace včetně zadávání přihlašovacích údajů nejen do emailových schránek, ale i do internetového bankovnictví atp. probíhá nešifrovaně, jelikož port zabezpečující bezpečnou komunikaci SSL (Secure Socket Layer s označením 443) není povolen. [6]

Možnost využití výše popsané metody útoku vychází z nedokonalosti WEPu, kdy přístupový bod sice ověřuje identitu zařízení připojujících se k němu, ale sám neposkytuje ověření identity sebe sama. [6]

3.8 Session Hijack Attack

Útočník sniffingem získá pakety komunikujícího klienta a přístupového bodu. Díky získanému obsahu paketů (při užitém šifrování se využívá útoků určených k dešifrování) může přijmout identitu komunikující stanice, aniž by AP poznalo jakoukoliv změnu. Všechna data jsou tedy posílána na obě stanice současně a stejně i zpracovávána. To může způsobit nestabilitu spojení, proto je vhodné počkat, až stanice přestane komunikovat, popřípadě ji násilně (např. DoS útokem) v komunikaci zabránit. Tento útok je vhodné použít zejména při útoku na sítě s vypnutým DHCP serverem a nastaveným filtrováním MAC adres. [6]

3.9 Brutal-Force Attack (Útok hrubou silou)

Jde o analogii ke slovníkovému útoku, kdy se testováním různých hodnot šifrovacího klíče snaží útočník o jeho uhádnutí. V praxi je v dnešní době tato metoda prakticky nepoužitelná, jelikož úspěšné odhalení WEP klíče s délkou 40 bitů může trvat i několik hodin (v závislosti na síle použitého klíče). U klíče s délkou 104 bitů tato doba narůstá řádově do dnů. V případě užití dynamických klíčů je metoda zcela neúčinná.[5] [6]

V praxi se dá proti tomuto útoku úspěšně bránit omezením počtu autentizací za časový úsek. Při nasazení tohoto opatření však musí být hodnota nastavena tak, aby neomezovala oprávněné klienty zejména v prostředí více rušeném, kde není spolehlivé připojení. Velké

[5] Názor autora.

časové prodlevy mezi jednotlivými autentizacemi také mohou nahrávat výše popsanému deautentifikačnímu útoku. [6]

3.10 FMS útok

Útok vedoucí ke zjištění hodnoty WEP klíče. Podmínkou pro úspěšné provedení tohoto útoku je získání velkého množství dat, což je ovšem u sítí s velkým provozem otázka řádově desítek minut. Pokud provoz není dostatečný, útočník může využít techniky zachycení paketu se známým obsahem, který následně několikrát pošle do sítě. Od AP přicházejí odpovědi užívající postupně všechny náhodné inicializační vektory, které útočník zachytává. [6]

Problematika znalosti paketu není nikterak složitá, jelikož útočníkovi postačuje jen částečná znalost a útok je principielně možný zejména díky tomu, že každý IP a ARP paket začíná hodnotou OxAA. [6]

3.11 PTW útok

Útok využívající 16B keystream, jenž získává ze zachycených ARP rámců. Vychází z útoku FMS. Velkou výhodou tohoto typu útoku je jeho nízká náročnost na množství zachycených dat. Udává se, že pro získání 104 bitového WEP klíče postačuje asi 85000 zachycených keystreamů. V tomto případě je pravděpodobnost úspěšného získání klíče okolo 95%. [6]

V případě užití tohoto útoku na WEP klíč délky 40 bitů se nutné množství zachycených dat rapidně snižuje. Výzkumem nutného množství zachycených dat se zabývá praktická část mé bakalářské práce, uvedené v literárních zdrojích. [6]

4 CITLIVÁ DATA PŘENÁŠENÁ PŘES INTERNET

Z dosavadní práce je zřejmé, že Wi-Fi nemusí být vnímána jako nejbezpečnější způsob přenosu dat. V některých speciálních případech se jedná o přenos skutečně důležitých dat, jejichž únik by mohl způsobit nezměrné škody. Ošetřuje toto nějaký zákon? Kde je zakotveno omezení používání Wi-Fi?

Primárním důvodem zabezpečení internetového přenosu, v našem případě zejména prostřednictvím Wi-Fi, je možný přenos citlivých dat, které jsou pro uživatele cenné. Čtvrtá kapitola mé diplomové práce se tedy zabývá některými možnými druhy dat, jejichž znalost nepovolanou osobou by mohla způsobit újmu komunikujícímu subjektu.

4.1 Utajované informace

Jelikož se tato práce přímo nezabývá otázkou utajovaných informací, jsou zde pouze nastíněny vybrané základní principy. Pochopením komplexní problematiky se zabývají práce jiné.

4.1.1 Citace zákona

Dle zákona §č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti se rozumí

a) utajovanou informací informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací (§ 139),

b) zájmem České republiky zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob. [7]

4.1.2 Znaky utajované informace

a) Utajování

Informace podléhá speciálnímu režimu zacházení, který zamezuje, aby se k informaci dostala nepovolaná osoba a to jak náhodou, tak i cíleným chováním, tedy prolomením ochrany utajení. Stejně tak je všeobecná snaha zajistit, aby nemohla být informace

upravena nebo zničena, popřípadě nahrazena informací jinou. Způsob utajení by však neměl znemožnit či nad míru ztížit přístup oprávněných osob k těmto informacím.

b) Újma

Dle §3 zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti rozumíme

Újmou zájmu České republiky se pro účely tohoto zákona rozumí poškození nebo ohrožení zájmu České republiky. Podle závažnosti poškození nebo ohrožení zájmu České republiky se újma člení na mimořádně vážnou újmu, vážnou újmu a prostou újmu. [7]

Jak již bylo řečeno, zneužití utajované informace cizí osobou by způsobila újmu subjektu. Z tohoto faktu vychází nutnost utajení. Tato újma může mít buď finanční, materiální, újma na zdraví, životě či majetku a újma, která se nedá jednoznačně finančně vyčíslit.

c) Sankce

Porušení zákona o utajovaných informacích vede k sankci. Fyzické osoby se tak musí chovat tak, aby daný zákon neporušily. Sankce má formu finanční, majetkovou nebo sankci dle trestního zákona[6].

4.1.3 Stupně utajení

Dle závažnosti a důležitosti informací jsou tyto rozděleny do čtyř stupňů. Následuje výčet a to od nejpřísněji utajovaných po nejméně utajované.

a) **Přísně tajné**, mají nejvyšší stupeň utajení. Vyzrazení takovéto informace neoprávněné osobě nebo její zneužití může způsobit zájmům ČR mimořádně vážnou újmu.

b) Jako „**tajné**“ označujeme ty informace, které mají druhý nejvyšší stupeň utajení. Vyzrazení takovéto informace neoprávněné osobě nebo její zneužití může způsobit zájmům ČR vážnou újmu.

[6] Zák. č. 40/2009 Sb.

c) **Důvěrné** informace mají třetí nejvyšší stupeň utajení a jejich vyzrazení neoprávněné osobě nebo zneužití informace může způsobit zájmům ČR prostou újmu.

d) **Vyhrazené** mají nejnižší stupeň důležitosti, přesto splňují veškeré znaky utajovaných informací. Vyzrazení vyhrazené informace neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy ČR. Nedochází tedy k újmě ani k hrozbě újmy.

4.2 Know-how

Informace v podobě poznatků, které ve většině případů vlastní právnické osoby, popřípadě podnikající fyzické osoby. Jde o informace týkající se zejména výrobních postupů, složení výrobků nebo návodů na výrobu, které vlastníkovi dávají konkurenční výhodu a jejichž prozrazení, popřípadě zneužití, by způsobilo vlastníkovi buď přímé, nebo nepřímé škody.

Otázka ochrany know-how bývá často zakotvena i v pracovní smlouvě mezi zaměstnancem a zaměstnavatelem, kde se zaměstnanec zavazuje k udržení výrobních a jiných firemních tajemství, přičemž těchto informací nabude v souvislosti s vykonávanou profesí. Vyzrazení takového tajemství bývá podmíněno sankcí, se kterou zaměstnanec svým podpisem souhlasí.

4.3 Obchodní tajemství

Jako obchodní tajemství označujeme ty informace, které jsou spjaté s podnikem a nejsou běžně přístupné. Tyto informace bývají utajeny, jejich vyzrazení by způsobilo podniku přímé či nepřímé finanční škody.

Stejně jako know-how, i otázka ochrany obchodního tajemství bývá jedním z předmětů pracovní smlouvy, zaměstnanec se tedy zavazuje k udržení tohoto tajemství a bere na sebe zodpovědnost. Při porušení tajemství bude sankcionován ve smlouvě definovaným způsobem.

4.4 Osobní údaje

Další z možných informací přenášených prostřednictvím bezdrátové sítě jsou osobní údaje. Cílem mé práce není vzdělávání čtenářů ohledně poskytování osobních údajů po internetu, co je však obecně známo, tento problém je aktuální a spousta uživatelů bezmyšlenkovitě

své údaje poskytne. Špatně zabezpečená Wi-Fi síť umožní takto neznalým uživatelům internetu šíření svých osobních údajů nejen směrem, kterým plánovali, ale i směrem k útočníkovi.

Co si však představit pod pojmem „osobní údaje“?

Pro účely Zák. č. 101/2000 Sb., o ochraně osobních údajů se dle §4 rozumí

a) osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,

b) citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů. [8]

5 PRÁVNÍ OMEZENÍ UŽITÍ BEZDRÁTOVÉHO INTERNETU VE FIRMÁCH SBS

Wi-Fi je jistě přínosná technologie, která v řadě případů usnadňuje práci. Jak je to ale s užitím Wi-Fi ve speciálních případech? Tato kapitola obsahuje omezení pro užití bezdrátového internetu ve specializovaných odvětvích, která pracují s citlivými informacemi, jejichž povaha a charakter jsou definovány ve čtvrté kapitole mé diplomové práce.

Faktem je, že firmy průmyslu komerční bezpečnosti, a tedy i firmy soukromých bezpečnostních služeb, nakládají s citlivými daty, jejichž zneužití by způsobilo újmu. Mezi tato data patří i výše zmíněné utajované informace, jimž se věnuje zákon. V rámci zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti je upraven i způsob přenosu takovýchto informací, jenž je dle § 5 tohoto zákona označen jako jeden z „druhů zajištění ochrany utajovaných informací“. Zákonné úpravy zaměřující se na samotný přenos utajovaných informací se nalézají v Hlavě VI s názvem Bezpečnost informačních a komunikačních systémů. Tímto vzniká pro firmy SBS omezení v užívání přenosových zařízení.

5.1 Informační systém

Na následujících řádcích je rozebrán § 34, jenž definuje pojem Informační systém a je stěžejní pro problematiku přenosu Utajovaných informací.

5.1.1 Citace § 34

(1) Informačním systémem nakládajícím s utajovanými informacemi se pro účely tohoto zákona rozumí jeden nebo více počítačů, jejich programové vybavení, k tomu patřící periferní zařízení, správa tohoto informačního systému a k tomuto systému se vztahující procesy nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací (dále jen "informační systém").

(2) Informační systém musí být certifikován Úřadem [§ 46 odst. 1 písm. b)] a písemně schválen do provozu odpovědnou osobou.

(3) Nakládat s utajovanou informací lze pouze v informačním systému splňujícím podmínky podle odstavce 2.

(4) Schválení informačního systému do provozu podle odstavce 2 musí odpovědná

osoba písemně oznámit Úřadu do 30 dnů od tohoto schválení.

(5) Prováděcí právní předpis stanoví

a) požadavky na informační systém a podmínky jeho bezpečného provozování v závislosti na stupni utajení utajovaných informací, s nimiž nakládá, a na bezpečnostním provozním módu a

b) obsah bezpečnostní dokumentace informačního systému. [7]

5.1.2 Výklad § 34

První odstavec tohoto paragrafu začleňuje Wi-Fi, tedy prostředek určený pro přenos, do pojmu „Informační systém“. V paragrafu se lze dále dočíst, že tento informační systém musí být řádně certifikován, což upravuje § 46, jímž se zabývá následující podkapitola.

Mimo jiné hovoří paragraf o tom, že certifikovaný Informační systém musí navíc schválit odpovědná osoba, která toto musí oznámit Úřadu[7] do 30 dní. S utajovanou informací lze nakládat jen v informačním systému splňujícím podmínky zákona č. 412/2005 Sb. V souvislosti s Informačním systémem vzniká podmínka existence „prováděcího předpisu“.

5.2 Certifikace

Jak nastínila předchozí podkapitola, k přenosu Utajovaných informací musí být Informační systém řádně certifikován. Certifikací celého Informačního systému se věnuje § 46. Pro naše účely je důležitý především první odstavec.

5.2.1 Citace § 46 odst. 1

(1) Certifikace je postup, jímž Úřad

a) ověřuje způsobilost technického prostředku k ochraně utajovaných informací,

b) ověřuje způsobilost informačního systému k nakládání s utajovanými informacemi,

[7] Národnímu bezpečnostnímu úřadu.

c) ověřuje způsobilost kryptografického prostředku k ochraně utajovaných informací,

d) ověřuje způsobilost kryptografického pracoviště pro vykonávání činností podle § 37 odst.6, nebo

e) ověřuje způsobilost stínící komory k ochraně utajovaných informací. [7]

5.2.2 Výklad § 46 odst. 1

Pro účely této diplomové práce je stěžejní písmeno b) prvního odstavce. Dle něj musí být každé přenosové zařízení nakládající s utajovanými informacemi schváleno Národním bezpečnostním úřadem.

5.3 Postoj NBÚ k problematice Wi-Fi

Pro zjištění skutečného vztahu Wi-Fi k možnosti přenosu utajovaných informací byl mnou v rámci této práce osloven p. RNDr. Pavel Adler z odboru Informačních technologií Národního bezpečnostního úřadu.

Postoj NBÚ k Wi-Fi je jednoznačný. Pokud technologie vyzařuje data do předem přesně nedefinovatelného prostoru, musí být data šifrována, přičemž samotná šifra, jíž využívá W-Fi, by nestačila svojí silou.

Každé zařízení sloužící k přenosu utajovaných informací musí projít certifikačním procesem dle § 46 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Dle informací p. RNDr. Pavla Adlera neexistuje v podmínkách ČR žádné certifikované přenosové zařízení Wi-Fi určené pro tyto účely, rovněž v zahraničí o ničem podobném neslyšel. Na NBÚ neexistuje, ani neexistoval požadavek na certifikaci podobného zařízení.

6 DOTAZNÍK A JEHO TVORBA

Pro účely výzkumu této diplomové práce bylo užito dotazníku, zaměřeného především na znalost uživatelů. Dotazník může tazateli poskytnout cenné údaje a informace, ne však v případě, kdy je sestaven špatně. Existují zásady, jichž by se měl tazatel držet, aby zvýšil užitnou hodnotu svého dotazníku a čeho by se naopak měl vyvarovat, aby svůj dotazník neodsoudil již v začátku k záhubě. V následujícím textu jsou shrnuty základy tvorby dotazníku a další otázky s tím spojené.

6.1 Základy tvorby dotazníku

Dotazník by měl upoutat pozornost a neodradit respondenta. Zdroj pro tvorbu dotazníku uvádí 6 bodů, jichž se má tvůrce držet. Jsou jimi:

- srozumitelnost,
- přehlednost a snadná orientace,
- jednoduchost vyplňování,
- jazyková korektnost,
- typografická úprava,
- grafická úprava.

6.2 Stanovení cíle

Před začátkem vytváření dotazníku je nutné stanovit si cíl, jenž má tento naplnit. Otázky pak musí směřovat k dosažení zvoleného cíle tak, aby průzkum splnil očekávání. Délka dotazníku by se měla pohybovat mezi 40 a 50 otázkami a doba jeho vyplnění by neměla přesáhnout 20 minut.

Dnešní uživatelé internetu jsou bohužel deformováni roky testování a nepříjemných otázek hraničících s problematikou hoaxů, proto jen malé množství z nich je jim ochotno věnovat tolik času. Hraniční hodnota počtu otázek se tedy udává jako 20 a doba vyplňování by neměla přesáhnout 10 minut.

I dobře vytvořený dotazník postrádá smysl, pokud jsou jeho otázky špatně či nesrozumitelně položeny.

6.3 Formulace otázek

Ačkoliv dotazník není tvořen pouze otázkami a odpověďmi, jsou tyto pro náš účel nejdůležitější. Proto jim je třeba věnovat zvýšenou pozornost a dbát na následující:

- jednoznačnost vět,
- srozumitelnost – nepoužívat cizí a odborné výrazy, nebo tyto řádně objasnit,
- stručnost vět,
- validnost – otázky směřovat k hlavnímu téma dotazníku,
- vyhnout se užívání sugestivních otázek, tj. otázek, směřujících respondenta ke konkrétní odpovědi.

6.4 Struktura dotazníku

Řazení otázek má svá zvláštní pravidla, jejichž dodržování redukuje počet respondentů, kteří v průběhu vyplňování toto ukončí, protože jim přijde dotazník příliš složitý, nudný nebo zbytečný. Osvědčilo se tedy začít otázkami zajímavými, za ně zařadit otázky složitější, vyžadující pozornost a soustředění a vše zakončit otázkami jednoduchými.

Každý dotazník by měl mít úvod, v němž tazatel respondenta seznamuje se svou prací. Tento by neměl být příliš dlouhý, popřípadě by v něm měly být zvýrazněny stěžejní informace. Zpravidla platí, že respondent přejde rovnou k testu, aby splnil svou „povinnost“ a zabralo mu to co nejméně času. V dotazníku by nemělo chybět:

- oslovení respondenta a žádost o vyplnění dotazníku,
- představení cílů a významu dotazníku a vysvětlení jeho smyslu,
- sdělení stručných pokynů pro vyplnění,
- zmínka o přibližné délce vyplňování a počtu otázek,
- poděkování za vyplnění.

6.5 Otestování dotazníku

Před vypuštěním dotazníku do světa by měl být tento řádně otestován a měly by být eliminovány jeho případné nedokonalosti. Testování nemůže spočívat pouze v rukou tazatele, jelikož tento je zainteresován. Je tedy vhodné vyzkoušet dotazník na cvičné

skupině respondentů a využít zpětné vazby, která poskytne cenné informace pro změnu a dotvoření konečné podoby. [10]

7 WARCHALKING

Slovo Warchalking označuje způsob detekce sítí, který byl užit v praktické části této diplomové práce. Tato činnost bývá často označován jako Wardriving a Warwalking. Obě výše zmíněné metody jsou podskupinou Warchalkingu, který bývá často chybně chápán jako něco nezákonného či škodlivého a uživatelé, kteří tyto metody provozují, jsou obvykle nesprávně bráni jako kriminálníci.

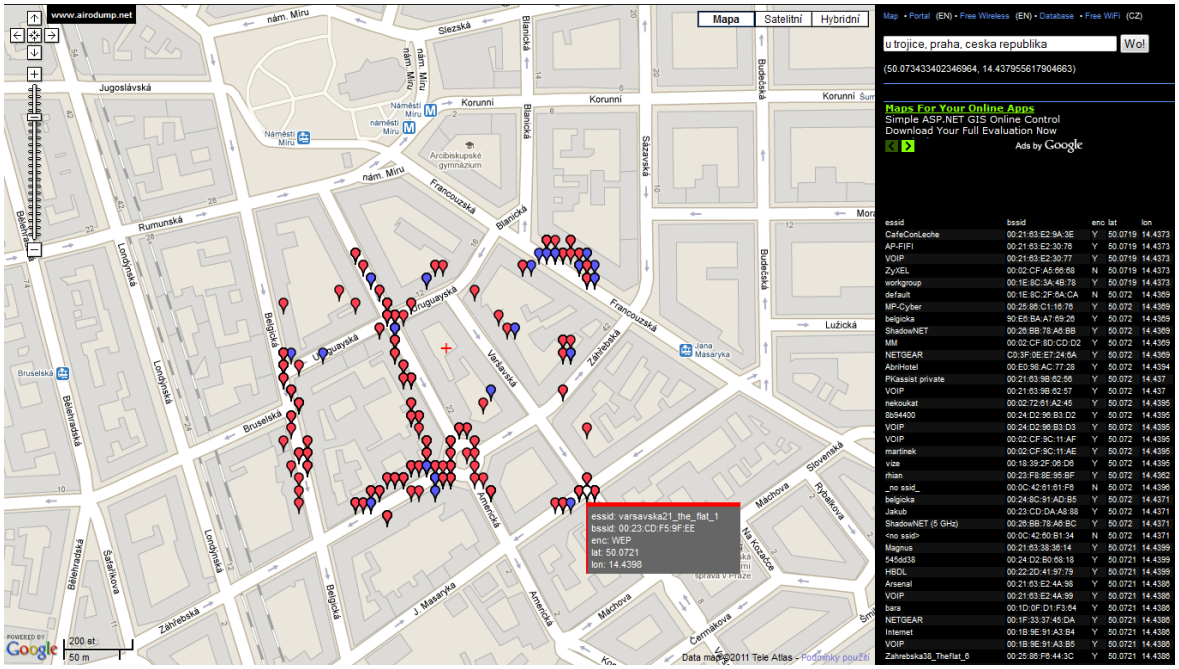
Ve skutečnosti jde pouze o jediné – zjištění bezdrátových sítí, jejich zabezpečení, popřípadě i jejich zmapování. Tyto informace mohou sloužit uživatelům, kteří následně mohou využít možnosti připojení se k internetu zdarma. Ani jedna z výše popsaných metod přitom neslouží k získání přístupu do zabezpečené sítě, je tedy pouze na administrátorovi, jak si vlastní síť zabezpečí a tím zamezí možnosti přístupu cizím osobám.

7.1 Dělení Warchalkingu

Při detekci sítí pro účely této diplomové práce bylo použito Wardrivingu (detekce sítí při jízdě autem) a Warwalkingu (též známého jako „Warjogging“, tedy detekce „za chůze“). Samozřejmě jsou známy i další druhy detekce, jako například Warboating (detekce při plavbě na lodi), Warflying (detekce při letu letadlem), Wartraming (detekce při jízdě tramvají) a další.

7.2 Warchalk mapa

Postup užití pro detekci ne zcela naplnil pojem „Warchalking“. Tento je charakteristický přesným zjištěním umístění přístupového bodu a následným zveřejněním této informace pro potřeby široké veřejnosti. Warchalkeři tak vytváří jakousi mapu, na níž je možné vysledovat sítě s bezplatným přístupem na internet, popřípadě sítě se slabým zabezpečením WEP. Mapa je veřejně přístupná na adrese http://map.airodump.net/.



Obr. 8. Warchalk mapa.

Jak je na obrázku patrné, Warchalking ukládá do databáze přesné GPS souřadnice jednotlivých AP, jejich MAC adresu, ESSID a BSSID. K vlastnímu zobrazení pak používá červených značek pro zabezpečení WEP a modrých značek, které představují sítě otevřené. Warchalking využívá aplikace Google Maps, v jejímž prostředí pracuje.

7.3 Warchalk značení

Warchalkeři se nedělí o zjištěná data pouze prostřednictvím internetu a Warchalk map. Na místech, kde detekují sítě, zanechávají i speciální značky. Ten, kdo se ve značení vyzná, pak jednoduše zjistí, jaká síť je v dosahu a zda se k ní může jednoduše připojit. Značky kreslí Walchakeři fixami či spreji na chodníky nebo zdi. Tato značení mají i tu výhodu, že jsou mezinárodní, jednoduše je tak může využít osoba, která je někde na dovolené, apod.

7.3.1 Open net

Toto značení charakterizuje síť, která je otevřená. Nemá tedy žádné zabezpečení, k přístupu do ní není třeba znát žádná hesla, je tedy veřejná (často hotspoty). K SSID se přidává i informace o rychlosti připojení v síti.

Obr. 9. Open net

7.3.2 WEP net

Toto označení reprezentuje síť se zabezpečením WEP. K přístupu do sítě je tedy potřeba jednoduchý WEP klíč, který je snadno zjistitelný. Opět je zde uvedeno a rovněž i rychlost sítě.

Obr. 10. WEP net.

7.3.3 Closed net

Poslední značení patří síti uzavřené, tj. se zabezpečením WPA, nebo WPA2. V tomto případě se uvádí pouze SSID. [11]

Obr. 11. Closed net.

7.4 Google a Warchalking

Že se nejedná o nic ilegálního, dokazuje i fakt, že Warchalking využívá i tak obrovská společnost, jakou je Google. Jeho spolupráce s Walcharkery nezůstala pouze u poskytnutí Google maps ke zobrazení Warchalk informací.

Jelikož hlavním cílem Googlu je shromažďování veškerých informací a jejich prezentace široké veřejnosti, nemohl opomenout i na mapování Wi-Fi sítí. Proč? Možná jste se někdy ptali, jak je možné, že Google určí Vaši polohu i v případě, že Váš přístroj není vybaven GPS, nebo toto zařízení nemáte aktivováno. Odpovědí je právě geolokace pomocí Wi-Fi sítí, kterou tato firma prováděla zároveň s fotografováním ulic měst a vytvářením podkladů pro známé Street view.[8]

[8] Aplikace Street view rozšiřuje možnosti zobrazení map tím, že nabízí uživateli možnost 3D pohledu. Uživatel se tak může procházet po mapě a jsou mu poskytovány autentické 360° snímky těchto míst.

Obr. 12. Automobil Streetview.

Pakliže se nyní připojíte přes některou ze zmapovaných sítí, Google tak může jednoduše díky jedinečné MAC adrese AP určit Vaši polohu. Jelikož se ale sítě neustále mění, zanikají a nově vznikají, Google přišel na způsob, jak svou databázi zachovat aktuální. Při připojení na Google si totiž tento vyhledávač vyžádá informace od Vašeho počítače o tom, které bezdrátové sítě má v dosahu. Toto nejen že zvětšuje a zanechává aktuální databázi Wi-Fi sítí, ale i napomáhá určení Vaší přesné polohy průnikem jednotlivých sítí. [12]

II. PRAKTICKÁ ČÁST

8 DOTAZNÍK WI-FI ZNALOSTÍ

Šestá kapitola této diplomové práce se zaměřuje na dotazník, který sloužil k získání důležitých informací o reálném stavu zabezpečení Wi-Fi v domácnostech. Mnou vypracovaný dotazník je přílohou diplomové práce a je umístěn na konci této práce. Osmá kapitola se zabývá vypracováním tohoto dotazníku, prezentací zjištěných dat, zhodnocení těchto dat a vyvozením závěru.

8.1 Tvorba dotazníku

Při vypracování dotazníku bylo dbáno zejména na dodržení základních principů pro tvorbu dotazníku uvedených v teoretické části této diplomové práce se snahou, aby dotazník případného respondenta zaujal a aby byl pro něj srozumitelný. Vzhledem k obtížnosti některých otázek byla vytvořena legenda, která vysvětluje otázky v dotazníku a napomáhá tak odpovědím nejvíce odpovídajícím realitě. Otázky v dotazníku byly díky tomu položeny jednoduchou formou, ačkoliv se jedná o specifické, neřku-li odborné téma.

Dotazník byl sestaven tak, aby na sebe otázky co možná nejvíce navazovaly. Při sestavování otázek byl dbán důraz na správnou gramatiku. Pro přehlednost bylo užito zvýraznění důležitého textu tučným písmem.

Motivací pro mé respondenty byla zejména naše osobní známost; ačkoliv dotazník byl otevřen široké veřejnosti, velké procento respondentů pocházelo z mého blízkého okolí. Dalším motivačním faktorem byl počet otázek, který skončil na čísle 20. Průměrný čas pro vyplnění dotazníku tak nepřesáhnul hranici 5 minut, čímž byla alespoň z části eliminována nevůle současných uživatelů internetu trávit svůj volný čas podobným způsobem.

Pro potřeby užitého dotazníku byla použita aplikace Microsoft Word. V nabídce po stisknutí tlačítka „Office“ a vybráním možnosti „Možnosti aplikace Word“ a následným zaškrtnutím „Zobrazit na pásu panel Vývojář“ byla zpřístupněna karta „Vývojář“. Tato karta nabízí funkci „Nástroje starší verze“ obsahující i „Zaškrtávací políčko (ovládací prvek ActiveX), jež bylo užito pro značení odpovědí.

Po sestavení a umístění otázek byl dokument uzamknut, čímž bylo docíleno nejen zamezení úprav dotazníku respondentem, ale i samotné aktivace zaškrtávacích polí, a tedy správné funkce dotazníku.

8.2 Zaměření dotazníku

Otázky byly vytvořeny s cílem ověřit znalosti respondentů se zaměřením na jejich vlastní domáckou síť. Rovněž byly testovány jejich znalosti o jejím zabezpečení. Při té příležitosti byl dotazník rozšířen i za hranice původního zadání a díky jeho otázkám byly zjišťovány i způsoby zabezpečení Wi-Fi v domácnostech, zejména u uživatelů, kteří dané problematice rozumí.

8.3 Logické členění

Dotazník je logicky rozdělen na část předmluvy, dotazníkovou část, tedy samotné otázky a část legendy, která pomáhá respondentům v zodpovězení některých problematičtějších otázek.

K vytvoření dotazníku bylo záměrně užito prostředí Word, pro účely mého průzkumu bylo důležité co nejlepší pochopení otázek respondenty, a tedy získání údajů co nejvíce odpovídajících skutečnosti. Z tohoto hlediska bylo nevhodné užití elektronických dotazníků, u nichž není možnost užití legendy sloužící k osvětě respondentů a zvýšení fundovanosti odpovědí.

8.4 Data získaná z dotazníku

Tato podkapitola shrnuje surová data získaná z dotazníku. Obsahuje tedy výčet všech otázek a následných procentuálních odpovědí a počtu jednotlivých respondentů.

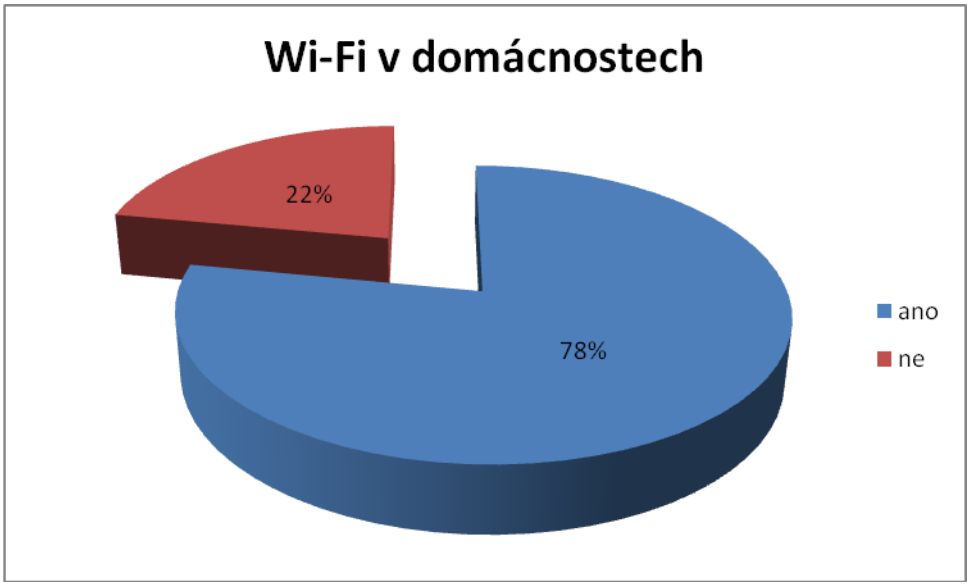
Otázka číslo 2 rozděluje uživatele do dvou, pro můj výzkum hlavních, skupin dle používání/nepoužívání Wi-Fi sítě v domácnosti. Na otázky 3 až 12 byli dotazování pouze ti uživatelé, kteří v domácnosti Wi-Fi síť používají. Počet respondentů odpovídajících na tyto otázky je tedy nižší. Oproti celkovému počtu 241 respondentů zodpovídalo tyto otázky 188 respondentů.

8.4.1 Zkušenost uživatelů

- 7% (17 respondentů) – nezkušený
- 29% (71 respondentů) – málo zkušený
- 53% (127 respondentů) – středně zkušený
- 11% (26 respondentů) – velmi zkušený

8.4.2 Wi-Fi v domácnostech

- 78% (188 respondentů) – ano
- 22% (53 respondentů) – ne



Obr. 13. Graf Wi-Fi v domácnostech.

8.4.3 Znalost přístupu do AP

- 70% (132 respondentů) – ano
- 30% (56 respondentů) – ne

8.4.4 Osoba nastavující AP

- 50% (94 respondentů) – nastavuje zkušenější uživatel
- 47% (88 respondentů) – nastavuje sám/sama
- 2% (4 respondenti) – nevím
- 1% (2 respondenti) – nikdo

8.4.5 Defaultní nastavení přístupu do AP

- 11% (20 respondentů) – ano
- 16% (30 respondentů) – spíše ano

- 25% (47 respondentů) – nevím
- 6% (12 respondentů) – spíše ne
- 42% (79 respondentů) – ne

8.4.6 Použití skrytí SSID

- 15% (28 respondentů) – ano
- 6% (11 respondentů) – spíše ano
- 45% (85 respondentů) – nevím
- 5% (10 respondentů) – spíše ne
- 29% (40 respondentů) – ne

8.4.7 Použití filtru MAC

- 19% (35 respondentů) – ano
- 5% (9 respondentů) – spíše ano
- 42% (80 respondentů) – nevím
- 6% (12 respondentů) – spíše ne
- 28% (52 respondentů) – ne

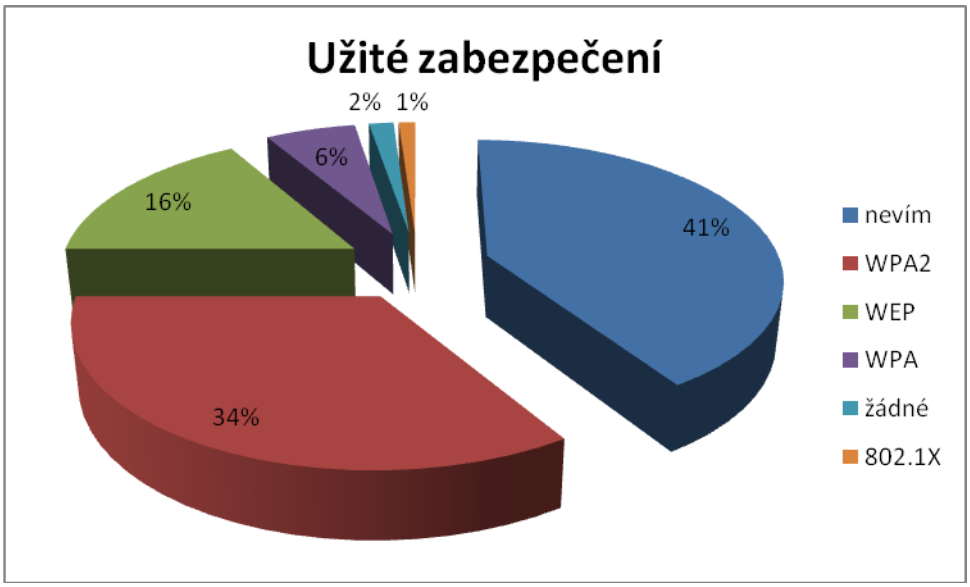
8.4.8 Automatické přiřazování IP

- 40% (76 respondentů) – ano
- 8% (14 respondentů) – spíše ano
- 27% (51 respondentů) – nevím
- 7% (13 respondentů) – spíše ne
- 18% (34 respondentů) – ne

8.4.9 Druh zabezpečení

- 41% (77 respondentů) – nevím

- 34% (64 respondentů) – WPA2
- 16% (31 respondentů) – WEP
- 6% (11 respondentů) - WPA
- 2% (3 respondenti) – žádné
- 1% (2 respondenti) - 802.1x



Obr. 14. Graf užitého zabezpečení v domácnostech

8.4.10 Nastavení pouze LAN

- 26% (49 respondentů) – ano
- 8% (14 respondentů) – spíše ano
- 22% (42 respondentů) – nevím
- 6% (12 respondentů) – spíše ne
- 38% (71 respondentů) – ne

8.4.11 Bezpečnost uložení AP

- 65% (123 respondentů) – ano
- 11% (20 respondentů) – spíše ano
- 8% (14 respondentů) – nevím

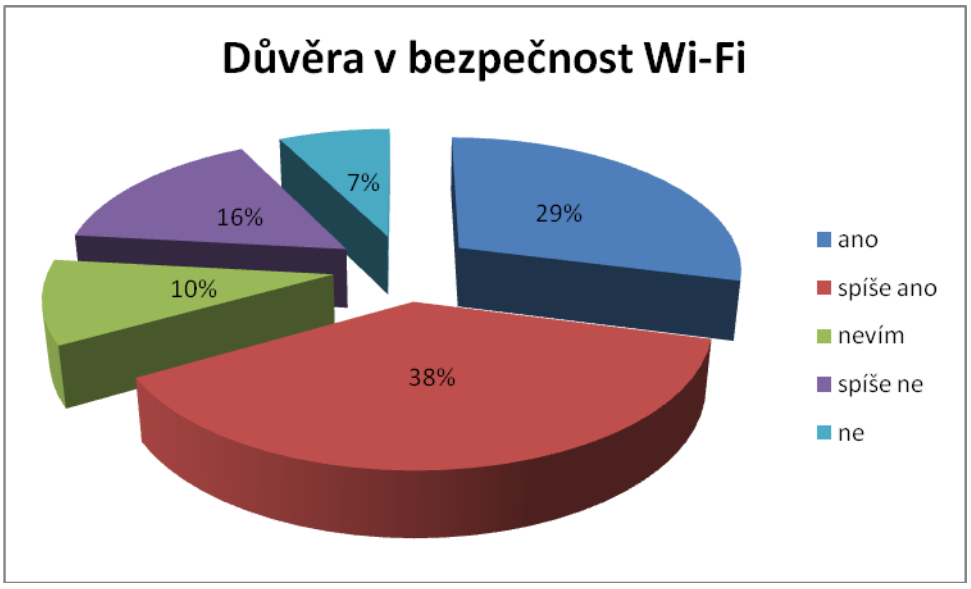
- 5% (10 respondentů) – spíše ne
- 11% (21 respondentů) – ne

8.4.12 Použití loginu na Wi-Fi

- 73% (176 respondentů) – ano
- 3% (6 respondentů) – spíše ano
- 3% (8 respondentů) – nevím
- 6% (15 respondentů) – spíše ne
- 15% (36 respondentů) – ne

8.4.13 Důvěra v bezpečnost Wi-Fi

- 29% (70 respondentů) – ano
- 38% (91 respondentů) – spíše ano
- 10% (24 respondentů) – nevím
- 16% (38 respondentů) – spíše ne
- 7% (18 respondentů) – ne



Obr. 15. Graf důvěry respondentů v bezpečnost Wi-Fi

8.4.14 Znalost potenciálního útočníka

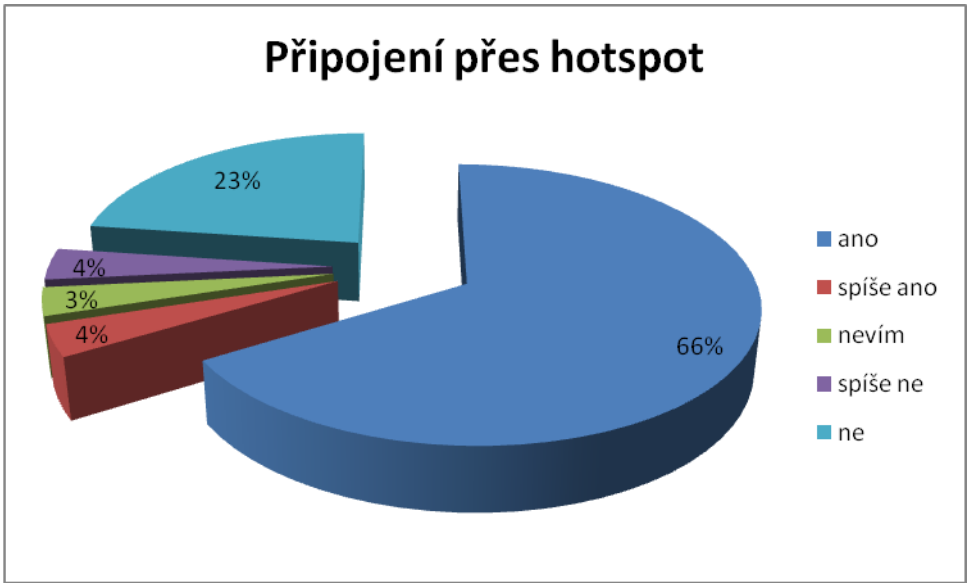
- 32% (77 respondentů) – ano
- 9% (23 respondentů) – spíše ano
- 12% (28 respondentů) – nevím
- 13% (32 respondentů) – spíše ne
- 34% (81 respondentů) – ne

8.4.15 Setkání s útokem

- 19% (46 respondentů) – ano
- 4% (8 respondentů) – spíše ano
- 8% (20 respondentů) – nevím
- 13% (32 respondentů) – spíše ne
- 56% (135 respondentů) – ne

8.4.16 Připojení přes hotspot

- 66% (160 respondentů) – ano
- 4% (9 respondentů) – spíše ano
- 3% (8 respondentů) – nevím
- 4% (9 respondentů) – spíše ne
- 23% (55 respondentů) – ne



Obr. 16. Graf připojení přes hotspot

8.4.17 Použití loginu hotspot

- 49% (118 respondentů) – ano
- 7% (16 respondentů) – spíše ano
- 4% (10 respondentů) – nevím
- 7% (17 respondentů) – spíše ne
- 33% (80 respondentů) – ne

8.4.18 Zkušenost s krádeží

- 23% (55 respondentů) – ano
- 4% (9 respondentů) – spíše ano
- 16% (39 respondentů) – nevím
- 9% (21 respondentů) – spíše ne
- 48% (117 respondentů) – ne

8.4.19 Pohlaví

- 56% (136 respondentů) – muž

- 44% (105 respondentů) – žena

8.4.20 Věk

- 65% (157 respondentů) – 13 až 25 let
- 23% (56 respondentů) – 26 až 40 let
- 7% (17 respondentů) – 41 až 55 let
- 5% (11 respondentů) – 56 a více let

8.5 Vyhodnocení dotazníku

Celkový počet respondentů dosáhl čísla 241 a tento počet, dle mého názoru, představuje dobrý vzorek pro získání zajímavých informací. Dotazník byl šířen zejména mezi mými přáteli a známými, tedy mezi vrstevníky. Věk respondentů se tak logicky pohybuje zejména v rozmezí od 13 do 25 let a od 26 let do 41 let. V relativní rovnováze zůstalo i pohlaví respondentů, téměř stejným dílem odpovídali muži i ženy.

8.5.1 Hodnocení surových dat

Dotazník vyplňovali převážně středně a málo zkušení uživatelé v oblasti informačních technologií. Více než tři čtvrtiny z mých respondentů užívá Wi-Fi po bytě, i toto ukazuje na důležitost diplomové práce a podstatu osvěty uživatelů, kteří o tak rozšířené technologii, jakou Wi-Fi je, vědí velmi málo.

Vcelku pozitivním výsledkem dopadly odpovědi na otázku, zda umí uživatelé vstoupit do nastavení AP. Téměř tři čtvrtiny z nich toto ovládají. Asi polovina odpovědí na otázku defaultního nastavení access pointu napovídá skutečnosti, že uživatelé často login nemění. Vystavují se tak značnému riziku znemožnění komunikace, nebo dokonce zničení hardwaru.

Bezpečnost sítě byla zvýšena skrytím SSID v asi třetině případů. Dle odhadů ze získaných odpovědí tak asi dvě třetiny uživatelů nepoužívá skrytí SSID. Téměř stejná situace je i u využití filtru MAC adres, který je jen o něco málo užívanější. Automatické přiřazování IP adres pomocí DHCP serveru využívají asi tři pětiny uživatelů, čímž tito mírně snižují její bezpečnost.

Dle výzkumu převažuje v nastavení sítí zabezpečení prostřednictvím WPA2, jež užívají asi dvě třetiny respondentů. Asi čtvrtina používá zastaralé zabezpečení WEP a asi desetina nepoužívá zabezpečení žádné. Relativně často je užito zabezpečení WPA, naproti tomu jen ve dvou případech je užito 802.1x.

Podle předpokladů odpověděla asi tři čtvrtina uživatelů kladně na otázku, zda je jejich AP bezpečně uložen a tím chráněn proti LAN připojení cizího PC. Oproti tomu větší polovina respondentů uvedla, že má povolenu správu AP i přes Wi-Fi.

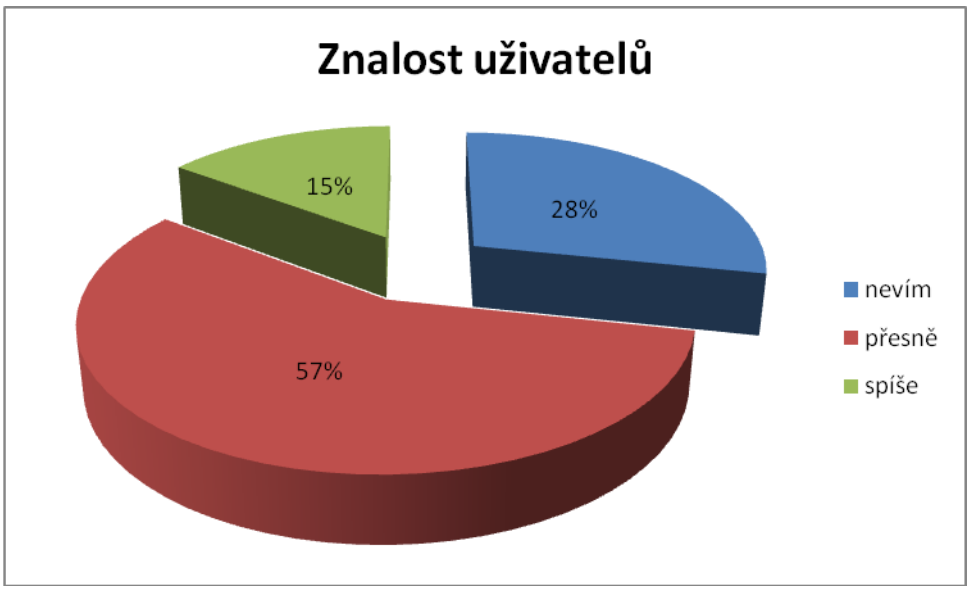
Asi tři čtvrtě uživatelů se, dle mého výzkumu, připojuje přes Wi-Fi na své osobní stránky a další místa chráněná loginem. Přitom necelá čtvrtina všech respondentů si je jistá, že se nikdy nepřipojila přes rizikový hotspot. Alarmující je fakt, že 49% respondentů ví jistě, že se přes hotspot připojilo a použilo svůj login.

Dle mého výzkumu zná asi třetina respondentů člověka, který by byl schopný číst nechráněná data posílaná přes Wi-Fi nebo se dokonce vlámat do jejího šifrování. Necelá pětina respondentů odpověděla, že se setkala s útokem na Wi-Fi síť a asi čtvrtina se setkala s případem, kdy byl login nebo osobní data odcizena.

Neznalost uživatelů podtrhuje fakt, že celé dvě třetiny z nich věří v bezpečnost Wi-Fi sítí a neobává se přes ni komunikovat.

8.5.2 Hodnocení hlubších vztahů

Znalost uživatelů ohledně jejich konkrétní sítě byla testována zejména v otázkách, na něž se odpovídalo možnostmi „ano“, „spíše ano“, „nevím“, „spíše ne“, „ne“. Z 6 otázek a celkového počtu 1128 možných odpovědí bylo 319 krát užito odpovědi „nevím“, 167 krát odpovědí typu „spíše“ a v 642 případech respondent znal odpověď.



Obr. 17. Graf znalosti uživatelů.

Ze všech 241 respondentů pouze 5 uvedlo ve svých odpovědích, že má prakticky dokonale zabezpečenou síť. Jejich Wi-Fi síť je chráněna pomocí WPA2, užívá filtr MAC adres, má vyplou funkci DHCP serveru a do nastavení jejich AP, který je bezpečně uložen proti připojení nepovolané osoby, může uživatel vstoupit jen přes LAN. Tři z nich ještě navíc používají skrytí SSID, přičemž dva se považují za velmi zkušeného uživatele a jeden za středně zkušeného.

Z 26 velmi zkušených uživatelů celkem 17 užívá WPA2. Po rozdělení odpovědi „nevím“ v poměru odpovídajícímu získaným informacím, z 88 nezkušených a málo zkušených uživatelů používá WPA2 asi jedenáct uživatelů. Z toho vyplývá, že uživatelé, kteří dané problematice rozumí, si více uvědomují rizikovost bezdrátového přenosu, a proto i více dbají na samotné zabezpečení.

9 ZJIŠTĚNÍ REÁLNÉHO STAVU ZABEZPEČENÍ WI-FI DETEKČNÍ TECHNIKOU

Devátá kapitole je zaměřena na zjištění reálného stavu zabezpečení sítí v dané reprezentativní oblasti pomocí speciálního diagnostického softwaru a běžného hardwaru. Předešlá kapitola byla zaměřena na zjištění reálné situace ze znalostí uživatelů, v této kapitole je zjišťován reálný stav prostřednictvím monitorovací techniky.

Pro vlastní monitoring sítí v dosahu bylo užito speciálního softwaru, díky němuž bylo možno zobrazit i sítě, jež nevysílaly své SSID. Pomocí obyčejného softwaru, například toho, v systému Windows defaultně implementovaného, by tyto skryté sítě nebyly možny zobrazit.

9.1 Softwarová výbava

Pro monitoring zabezpečení Wi-Fi sítí byl po zkušenostech zvolen operační systém Linux. V minulosti, při snaze o monitoring sítí a penetrační testy prostřednictvím různých verzí systému Windows (včetně Windows 7 – 64bit), nebyly výsledky a zejména uživatelská přívětivost se systémem Linux ani v nejmenším srovnatelná.

Speciální softwarová výbava spolu s Kubuntu zajistila nejen výše zmiňovanou výhodu zobrazení sítí se skrytou SSID, ale i možnost monitorovat provoz na sítích a tedy zjistit, kolik dat bylo v síti přeneseno.

9.1.1 Operační systém

Pro vlastní diagnostiku byl zvolen operační systém Linux postavený na jádře 2.6.32-30. Byla užita uživatelsky přívětivá distribuce Kubuntu verze 10.04.2, jež je odnoží klasického Ubuntu s využitím pracovního prostředí KDE (K Desktop Environment) verze 4.

9.1.2 Software pro monitoring

K samotnému monitoringu sítí byl použit software Airmon-ng a Airodump-ng. První zmiňovaný byl využit ke zjištění informací o bezdrátové síťové kartě, zejména pro zjištění přiřazení „aliasu“, tedy dočasného jména Wi-Fi karty dále potřebného pro samotný monitoring. Díky Airodump-ng byly zachycena pakety v dosahu zařízení, čímž bylo možno detekovat aktuálně vysílající Wi-Fi sítě v dané oblasti.

9.2 Hardwarová výbava

Ke zjištění výskytu Wi-Fi sítí a jejich zabezpečení nebylo třeba využít žádný speciální hardware, postačil kvalitní přenosný počítač. Nutno podotknout, že veškeré programy mají opravdu nízké hardwarové požadavky a bylo možno s nimi úspěšně pracovat i na zařízeních řádově několikrát méně výkonných, než bylo použito.

9.2.1 Popis užitého zařízení

Diagnostika zabezpečení Wi-Fi sítí v dané oblasti byla prováděna na laptopu firmy Sony Vaio s označením VPCEB1S1E/WI. Tento je osazen dvoujádrovým procesorem značky Intel typu Core i5 s označením M430 pracujícím na frekvenci 2,27 GHz s podporou technologie Intel Hyper-Threading a mezipamětí 3MB, pamětí DDR3 SDRAM o velikosti 4GB na frekvenci 1066MHz. Grafické zobrazení zajišťuje grafická karta ATI Mobility Radeon HD 5650 s pamětí 1024MB.

Obr. 18. Laptop použitý k detekci.

9.2.2 Wi-Fi síťová karta

Pro vlastní výzkum stěžejní byla Wi-Fi síťová karta s označením Atheros AR9285 Wireless Network Adapter. Tato je schopna pracovat v pásmech 802.11 b/g/n rychlostí až 150Mbps na frekvenci 2,4GHz. Tato karta je z mých zkušeností velmi citlivá, ke zmíněné diagnostice typu zabezpečení Wi-Fi sítí proto nebylo třeba žádné externí bezdrátové síťové karty, ačkoliv pomocí dalšího speciálního HW, zejména díky kvalitní anténě, by se zvýšil rozsah zkoumané oblasti. Pro náš výzkum však toto nebylo stěžejní.

9.3 Místa monitoringu Wi-Fi sítí

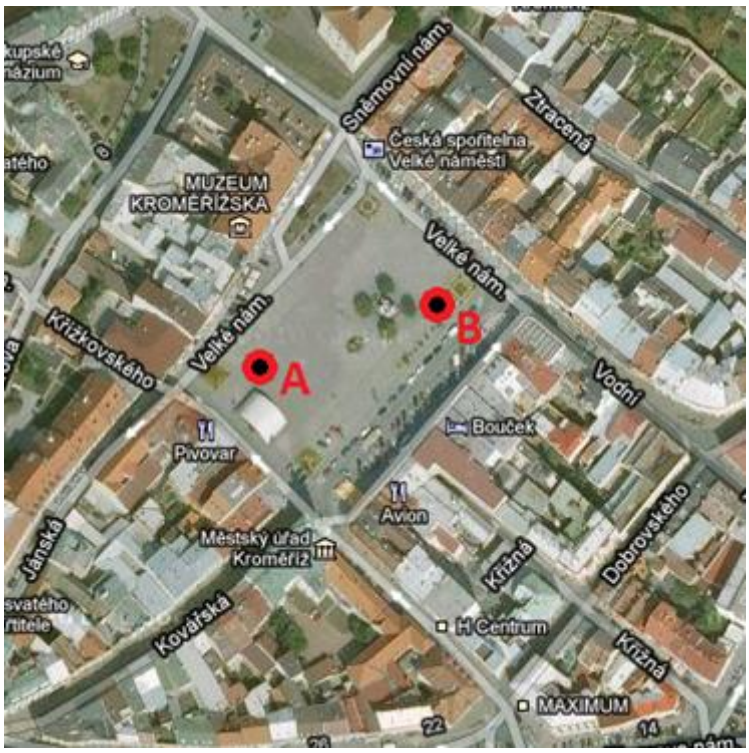
Pro získání většího množství dat z měření a zajímavějších výstupů byla detekce prováděna ve dvou odlišných oblastech. Tou první bylo Velké náměstí v Kroměříži, které v měření reprezentovalo klasickou kulturní zónu s převahou restauračních a jim podobných zařízení a s předpokladem výskytu několika hotspotů. Jako protipól náměstí, tedy kulturní zóny, byla vybrána zóna obytná, přesněji sídliště Zachar, v němž byl předpoklad výskytu převážně domácích Wi-Fi sítí. Toto sídliště bylo vybráno v Kroměříži jako nejvhodnější i s přihlédnutím k faktu, že je zde mnoho bytových zástav na malém prostoru.

9.3.1 Město Kroměříž

Město Kroměříž bylo vybráno hned z několika důvodů. Toto město je reprezentativní a tedy vhodné pro můj výzkum. Je střední velikosti, má asi 30 tisíc obyvatel, rovněž jsou zde zastoupeny kulturní i obytné zóny, jež byly dále podstatné pro vyváženost výsledků měření. Místa měření tak byla vybrána s přihlédnutím k jejich vhodnosti pro test.

9.3.2 Velké náměstí v Kroměříži

Pro monitoring sítí na Velkém náměstí byly vybrány dvě lokace označené na obrázku písmeny A a B. Obě tato místa byla strategicky určena, jsou v blízkosti restauračních zařízení a hotelů, je zde dobrá viditelnost a tedy dobrý předpoklad pro šíření elektromagnetických vln. Pro toto měření bylo užito metody Warwalkingu někdy rovněž označovaného jako Warjogging.



Obr. 19. Lokace pro detekci - náměstí

9.3.3 Sídliště Zachar

Sídliště Zachar bylo vybráno, jelikož je v něm velká hustota bytů na malém prostoru. Panelové domy na druhou stranu velmi dobře stíní Wi-Fi, což bylo negativní stránkou mého výběru. Díky velkému množství bytů byl i předpoklad velkého počtu bezdrátových připojení, a tedy dobré podmínky pro získání užitečných údajů.

V předpokládaném dosahu níže označených míst, na nichž byla detekce prováděna, se nalézá 10 obytných domů s celkem 26 vchody a 415 byty. Provedenou detekcí je možné odhalit sítě v přízemí domů a prvním patře.[9] Pro toto měření bylo užito metody Wardrivingu.

[9] Při použití obvyklého access pointu a antény.

Obr. 20. Lokace pro detekci - sídliště

Destinace měření byly strategicky vybrány tak, aby byla pokryta co největší plocha v prostoru a aby bylo naopak zamezeno detekci nežádoucích sítí pocházejících z domů mimo cílovou oblast.

9.4 Postup monitoringu Wi-Fi sítí

Veškerá práce se odehrávala v dříve zmíněném operačním systému za užití výše zmíněného software. Práce s Linuxem, v našem případě s Kubuntu, je v řadě případů velmi podobná práci ve Windows[10].

9.4.1 Konzole

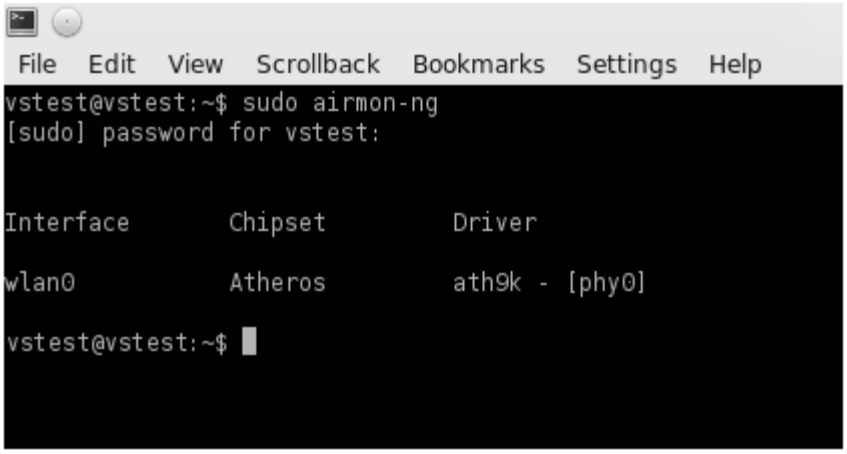
Složitější programy jsou v Linuxu v mnoha případech spouštěny a dále ovládány prostřednictvím Konzole, což je alternativa k příkazovému řádku[11] ve Windows. V konzoli je vždy příkazový řádek započat „vstest@vstest : ~ $“, což není nic jiného, než jméno uživatele. Do konzole se zadávají příkazy, vše se potvrzuje klasickým Enterem.

9.4.2 Zjištění jména síťové karty

Pro práci s bezdrátovou síťovou kartou musí být nejdříve zjištěno její jméno, které je třeba zadávat v dalších krocích v příkazech do konzole. K tomuto zjištění byl použit program Airmon-ng, který zobrazil Wi-Fi síťovou kartu. Program Airmon-ng je snadno spuštěn napsáním jeho názvu do konzole.

[10] Záměrně neupřesňuji verzi Windows, pro některé méně zkušené uživatele by mohlo být Kubuntu lehce zaměnitelné za některou z variant Windows, zejména v případě, že se nesetkali se všemi jeho verzemi.

[11] Oproti příkazovému řádku však nabízí spoustu dalších možností, jako je přímý přístup k aplikacím a jejich snadná instalace, apod.



Obr. 21. Spuštění Airmon-ng.

Z obrázku je zřejmá přítomnost slůvka „sudo“ před samotným „airmon-ng“. Ke spuštění některého softwaru a využívání jeho funkcí je třeba přístup správce. „Sudo“ před spouštěným programem vyvolává autentifikační požadavek, zadáním hesla správce pak můžeme používat program bez omezení.

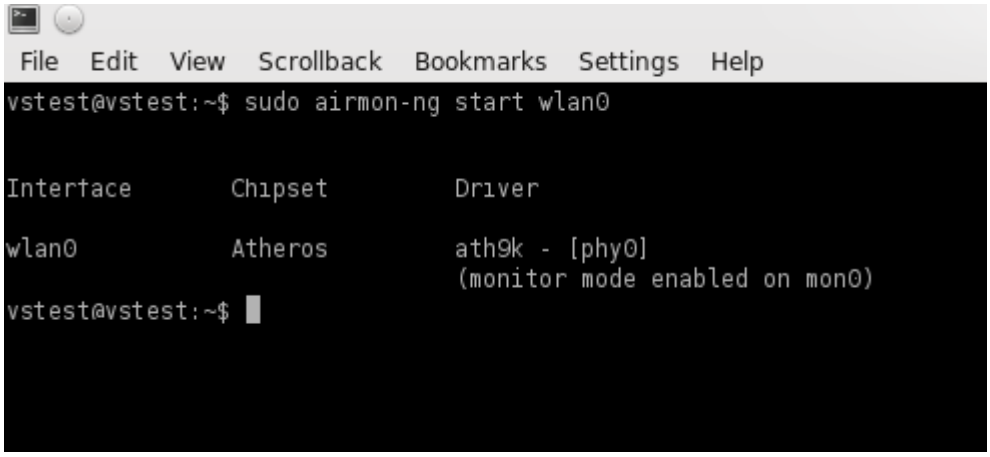
Po zadání výše uvedeného bylo možno z výstupní obrazovky (obr. 22) odečíst název bezdrátové síťové karty „wlan0“, což bylo potřebné pro zapnutí monitorovacího módu.

9.4.3 Zapnutí monitorovacího módu

Monitor mód bývá označován jako pasivní skenovací technika. Běžný mód Wi-Fi karty umožňuje připojení a komunikaci v rámci jedné sítě, v níž je uživatel připojen, což může být využito při sledování síťového provozu této sítě.

Pro náš výzkum bylo však nutné sledovat veškerý síťový provoz v dosahu Wi-Fi, k čemuž byl využit právě monitorovací mód. Přechod do monitorovacího módu bývá v prostředí Windows hlavním problémem, vinu přitom přisuzuji špatným ovladačům pro síťové karty. Tyto, dle mého názoru, ve většině případů nepodporují monitorovací mód, se získáním vhodných ovladačů pak bývá nadměrná práce. Tomuto problému se dá snadno vyhnout použitím v systému Linux, jenž je oproti Windows otevřenější a uživatele zbytečně neomezuje.

Ke spuštění monitorovacího módu bylo opět využito programu Airmon-ng, v němž byl zadán příkaz „sudo airmon-ng start wlan0“. Příkaz „start“ značí spuštění módu, „wlan0“ je dříve zjištěný název bezdrátové síťové karty, na které se monitorování spouští.



Obr. 22. Oznámení o zapnutí monitorování.

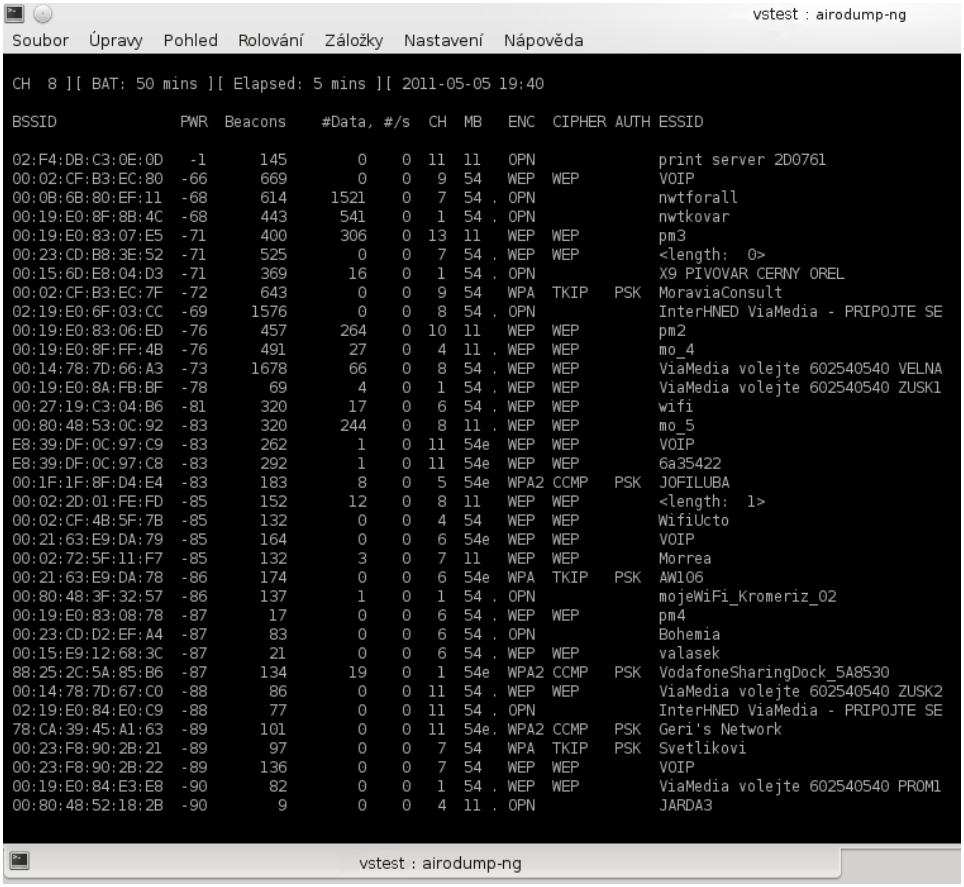
Program vrátil výstupní informaci, přičemž důležitý je zejména řádek „monitor mode enabled on mon0“. Ten říká, že byl monitorovací mód úspěšně spuštěn a že alias, tedy dočasný název síťové karty pro účely monitorování, byl nastaven na „mon0“.

9.4.4 Spuštění vlastního monitorování

Po nastavení karty do monitorovacího módu bylo možno začít sledovat a zaznamenávat síťový provoz v dosahu. K tomu bylo využito programu Airodump-ng, který byl opět vyvolán příkazem v konzoli. V příkazu bylo taktéž definováno, kterým zařízením má být monitorování prováděno, což bylo zjištěno v předchozím bodě. Zvolený příkaz tedy byl „sudo airodump-ng mon0“.

9.4.5 Příklad výsledku vlastního monitorování

Výsledek monitorování bezdrátových sítí je zobrazen na obrázku č. 24. První sloupec reprezentuje jedinečný identifikátor sítě BSSID, který je důležitý zejména v případě rozlišení dvou sítí, které mají stejná jména.



Obr. 23. Výstupní data programu Airodump-ng.

Těmito „jmény“ je myšleno ESSID, což je název sítě, který je zobrazen počítači při obvyklé snaze o nalezení sítě a následnému připojení. Na následujícím obrázku je pak zobrazení ESSID v prostředí Windows.

Obr. 24. ESSID v prostředí Windows 7.

Jak je vidět, prostředí Windows tedy defaultně nenabízí zobrazení BSSID, v případě stejného ESSID tedy není možné rozeznat dva různé access pointy. Obrázek č. 24 pak obsahuje dvě sítě se stejným jménem (ESSID), jimiž je InterHNED ViaMedia – Pripojte se. Díky BSSID je možno spolehlivě říci, že se jedná o dva různé AP.

Nejdůležitějším sloupcem je pro účely této práce ten označený jako ENC, tedy z anglického „encryption“ neboli šifrování. Zkratka OPN označuje otevřenou síť, WEP síť se zabezpečením WEP, WPA zabezpečení WPA a WPA2 zabezpečení WPA2. V případě, kdy není šifrování sítě zobrazeno, nedokázalo zařízení zabezpečení rozpoznat.

Za zmínku ve sloupci ESSID stojí hodnota <length: #>. Tuto síť by nebylo možno zobrazit obvyklým způsobem, má totiž zabezpečení skrytím SSID (přesněji ESSID). Číslo místo „#“ označuje, v případě hodnoty větší než 1, skutečnou délku ESSID. V případě sítě s názvem „Network“ a skrytí jejího ESSID by tedy bylo detekováno <lenght: 7>. U sítě, jejíž ESSID je zobrazeno jako <length: 0> nebo <length: 1> nebylo možno zjistit skutečnou délku ESSID. Vzhledem k tomu, že ESSID je pouze informativního charakteru, jeho znalost není pro výzkum, potažmo ani pro útok na takovouto síť, podstatné. V těchto případech se totiž používá jedinečný identifikátor BSSID.

Pro útočníka je důležitý i sloupec s názvem „PWR“, který určuje sílu signálu a pomáhá mu tak zjistit polohu access pointu. Nejdůležitější je však sloupec s označením „#Data“, který udává množství přenesených dat a tedy aktivitu na síti.

9.5 Výsledky monitoringu

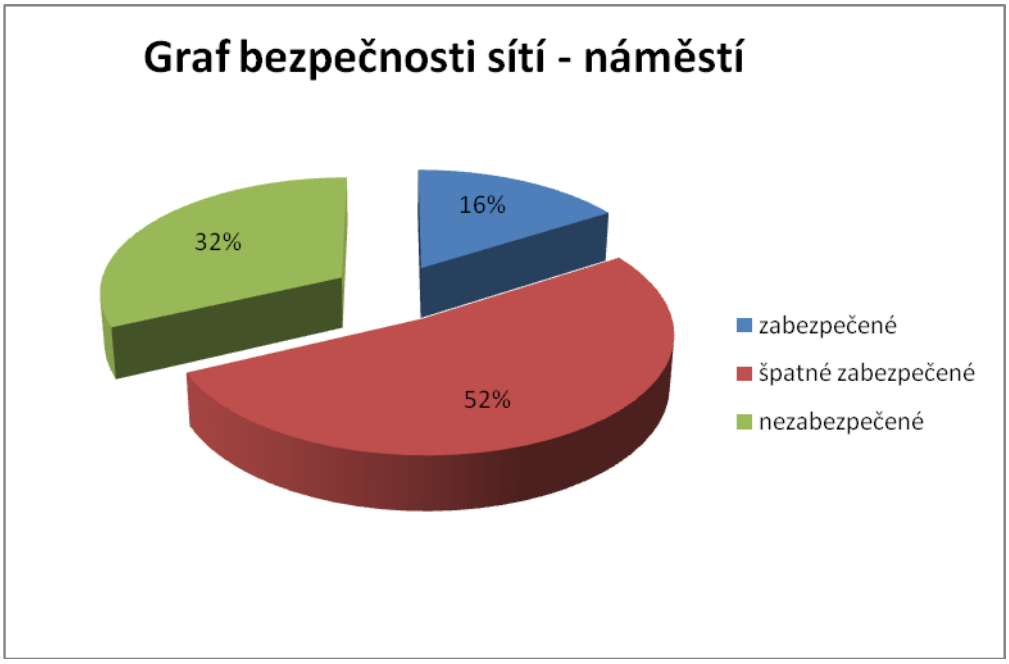
Na následujících řádcích jsou shrnuty výsledky monitorování a s nimi související grafy, které lépe pomáhají zvýraznit získaná data.

9.5.1 Velké náměstí

Na náměstí bylo detekováno celkem 50 Wi-Fi sítí s unikátní BSSID. Dle předpokladů zde byla řada otevřených sítí, jejichž výskyt je třetinový a jsou nejvíce zastoupeny hned po zabezpečení WEP, které využívá více než polovina místních sítí. Zabezpečení WPA bylo užito v 6 procentech případů a zabezpečení WPA2 bylo zjištěno u 10% sítí.

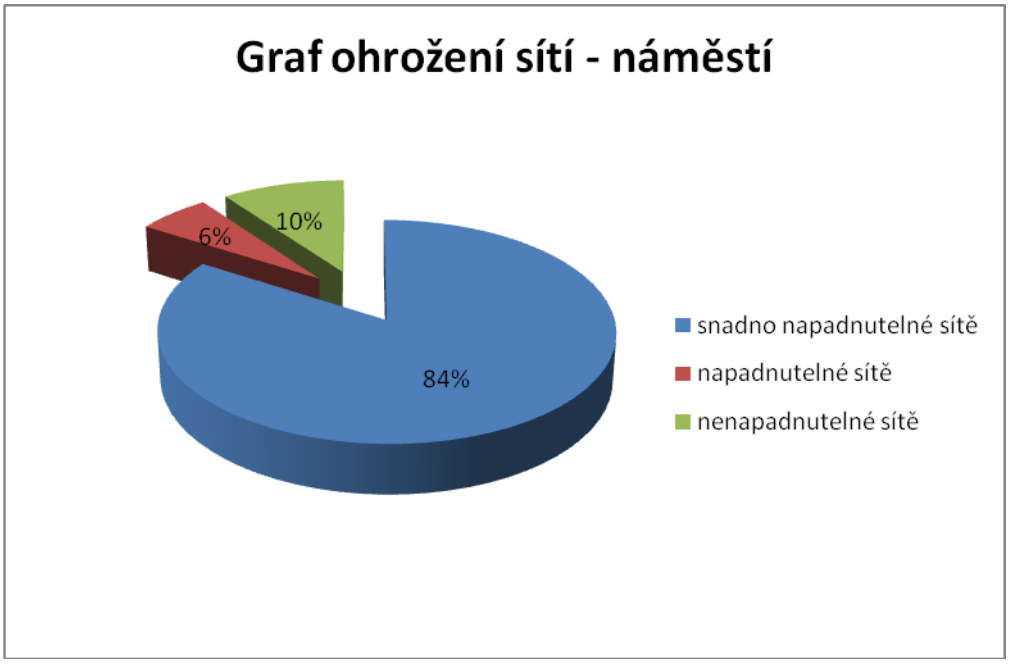
Obr. 25. Graf rozložení zabezpečení – náměstí.

Z výše uvedeného grafu tak zle jednoduše vyhodnotit kvalitu zabezpečení sítí na Velkém náměstí v Kroměříži. Jako „zabezpečené sítě“, jež tvoří 16% všech místních sítí, jsou zde označeny ty, které jsou zabezpečeny prostřednictvím WEP2. „Špatně zabezpečené“ sítě pak zahrnují zabezpečení WPA a vyskytují se zde z 52%. Jako „nezabezpečené sítě“ jsou zde sítě otevřené a sítě WEP, jež případnému útočníkovi kladou buď žádné, nebo jednoduše překonatelné překážky.



Obr. 26. Graf bezpečnosti sítí – náměstí.

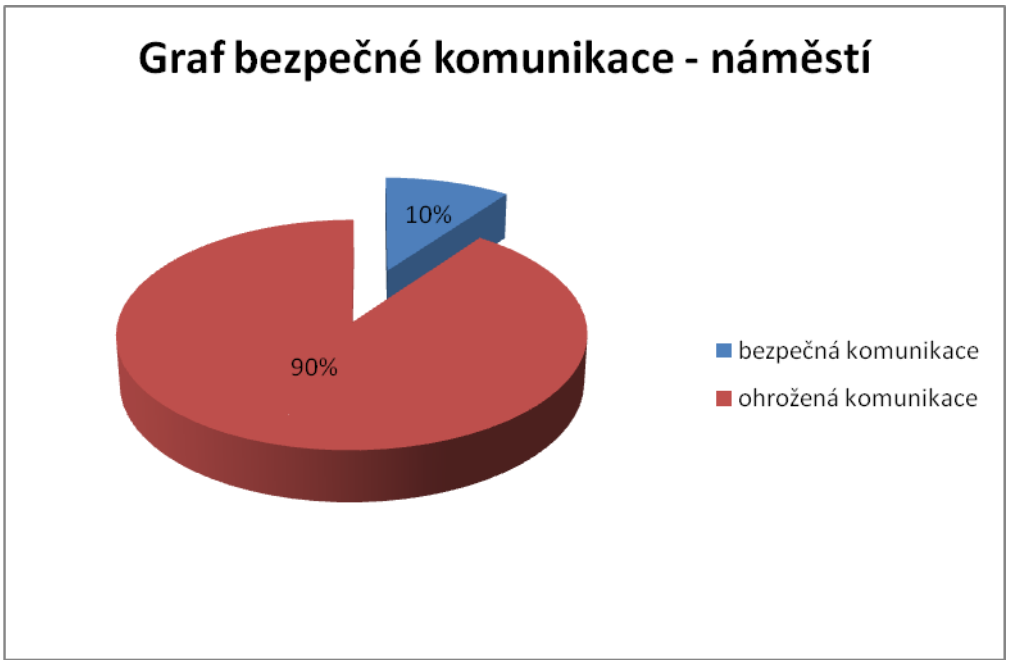
Snadno napadnutelné sítě tedy tvoří celkem 84% všech sítí, 6% je napadnutelných a 10% je nenapadnutelných.



Obr. 27. Graf ohrožení sítí – náměstí.

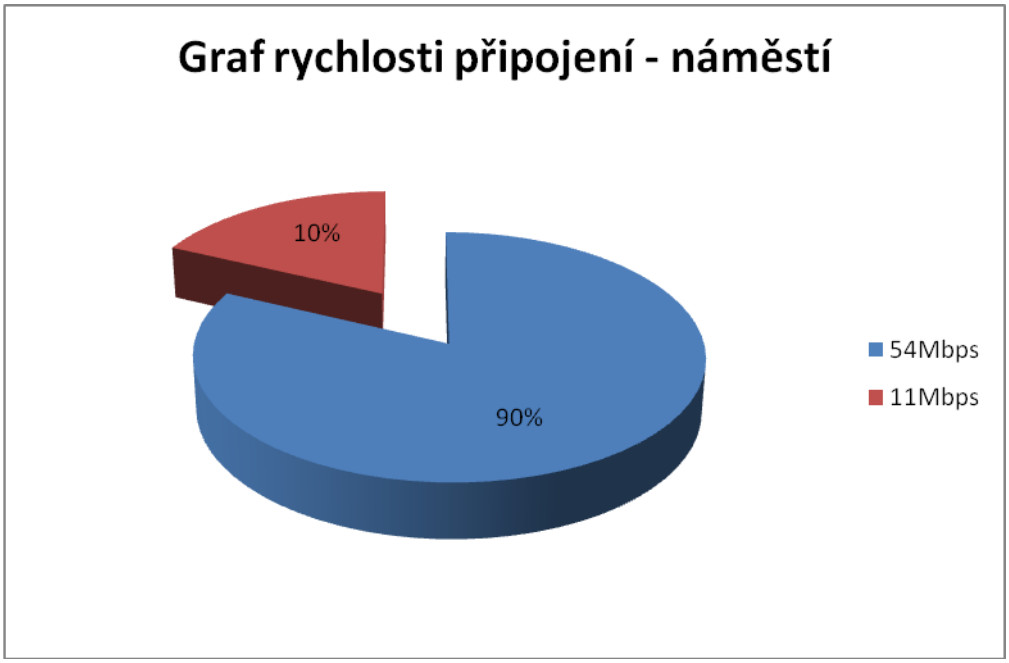
Celkový pohled na zabezpečení bezdrátových sítí v oblasti Velkého náměstí může být shrnut do následujícího grafu, který reprezentuje bezpečnost komunikace v rámci těchto sítí. Graf bezpečné komunikace je založen na předchozích textech, z nichž vyplývá, že jedinou bezpečnou komunikací v rámci Wi-Fi je ta, probíhající mezi zařízeními užívajícími

WPA2. Veškerá ostatní komunikace lze v zásadě jednoduše odposlouchávat a získaná data zneužít ve vlastní prospěch útočníka.



Obr. 28. Graf bezpečné komunikace – náměstí.

Rychlost komunikace v síti přehledně shrnuje následující graf. Na náměstí převažuje rychlost 54Mbps, jež byla zjištěna u 90% sítí. Pouhá desetina sítí užívala rychlost 11Mpbs.



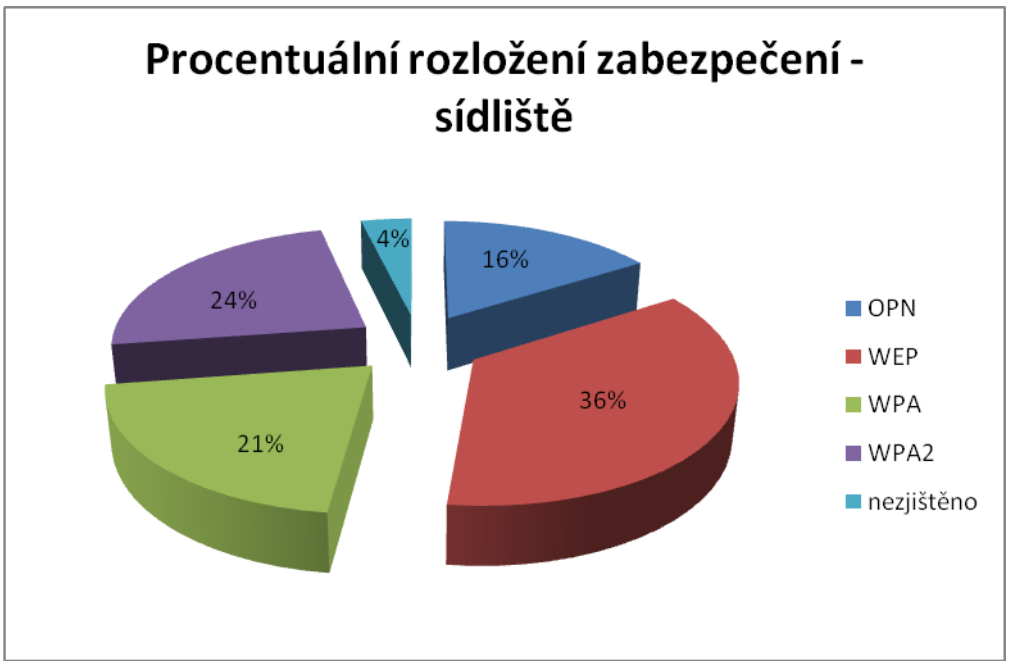
Obr. 29. Graf rychlosti připojení – náměstí.

Ze získaných hodnot lze mimo jiné vyčíst i použití zabezpečení „Skrytí SSID“. V případě Velkého náměsti v Kroměříži byly detekovány dvě sítě užívající toto zabezpečení, přičemž

ani u jedné z nich nebylo možno zjistit délku jména. Obě tyto sítě bohužel užívají zabepečení WEP, proto jsou potenciálně nechráněny a aplikované zabezpečení pomocí skrytí ESSID tedy postrádá smysl.

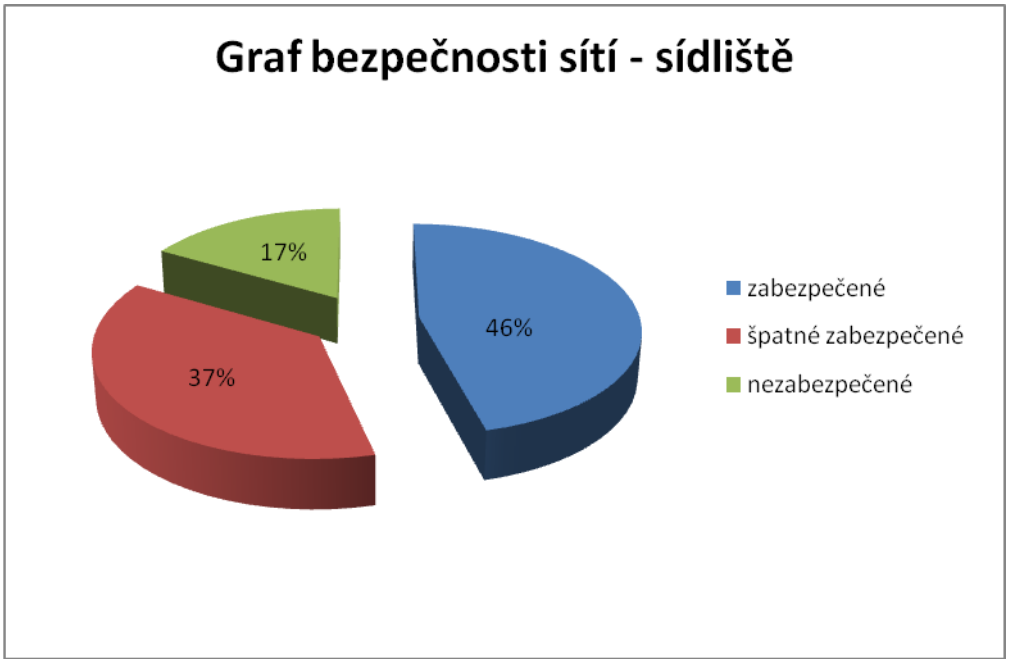
9.5.2 Sídliště Zachar

Detekce sítí na sídlišti Zachar rovněž splnilo má očekávání. Celkem zde bylo zjištěno 106 sítí s unikátní BSSID. 16% z těchto sítí bylo veřejně přístupných, u více než třetiny sítí bylo zjištěno zabezpečení WEP. Byla zjištěna i vysoká procenta zabezpečení prostřednictvím WPA, které činilo 21% a WPA2 se 24%. U 4% sítí nebylo možno zjistit druh zabezpečení.



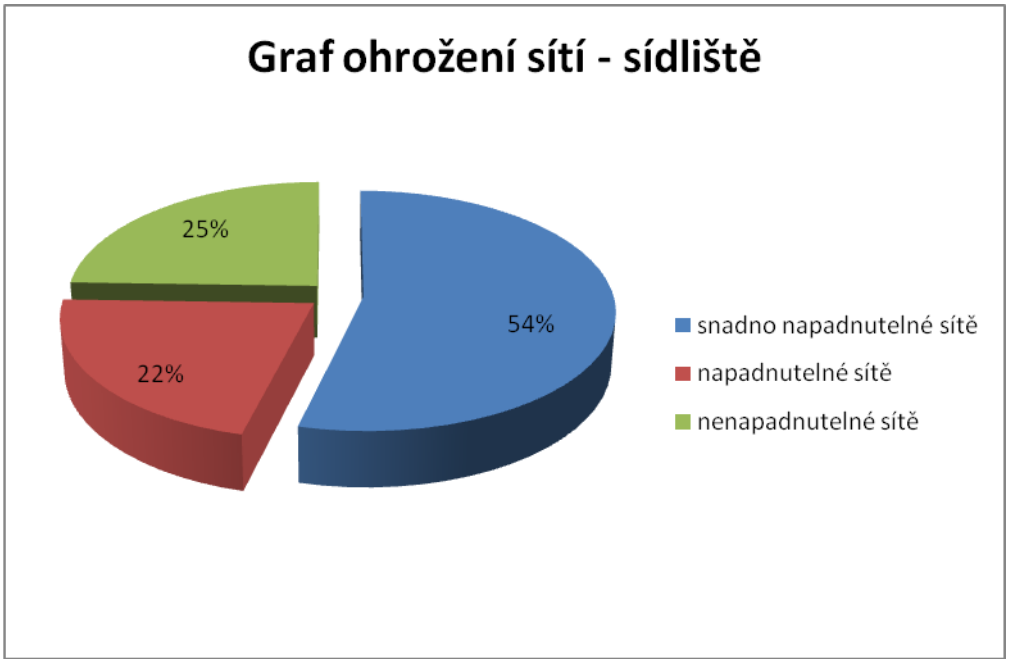
Obr. 30. Graf procentuálního rozložení zabezpečení – sídliště.

Následující graf tedy zobrazuje celkovou bezpečnost sítí na sídlišti. Byl sestaven ze zjištěných zabezpečení sítí, při jeho sestavování tedy byly vynechány sítě s nedefinovaným zabezpečením. Z výsledků vyplývá, že 46% sítí, tedy téměř polovina, je zabezpečeno kvalitnějším zabezpečením (WPA2 nebo WPA), 37%, a tedy více než třetina, je zabezpečena špatně (WEP) a 17% sítí není zabezpečeno vůbec.



Obr. 31. Graf bezpečnosti sítí – sídliště.

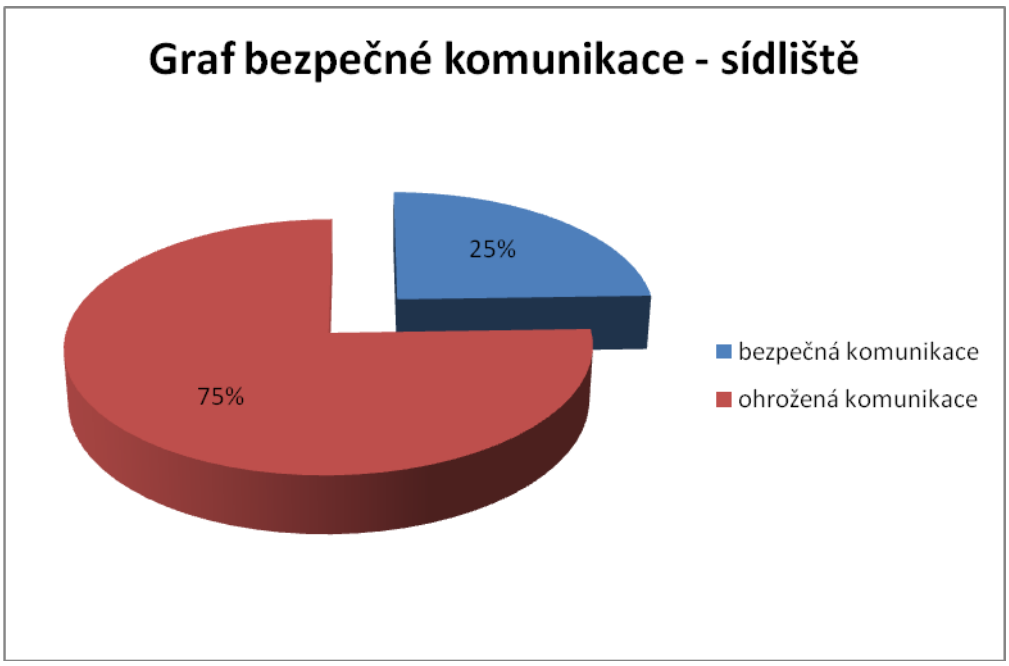
„Graf ohrožení sítí - sídliště“ nám dále zobrazuje snadno napadnutelné sítě, do nichž jsou zařazeny sítě OPN nebo WEP, jež se vyskytovaly ve čtyřiapadesáti procentech případů, sítě napadnutelné, používající zabezpečení WPA a použité ve 22% případů a sítě nenapadnutelné se zabezpečením WPA2 užité ve čtvrtině případů.



Obr. 32. Graf ohrožení sítí – síliště.

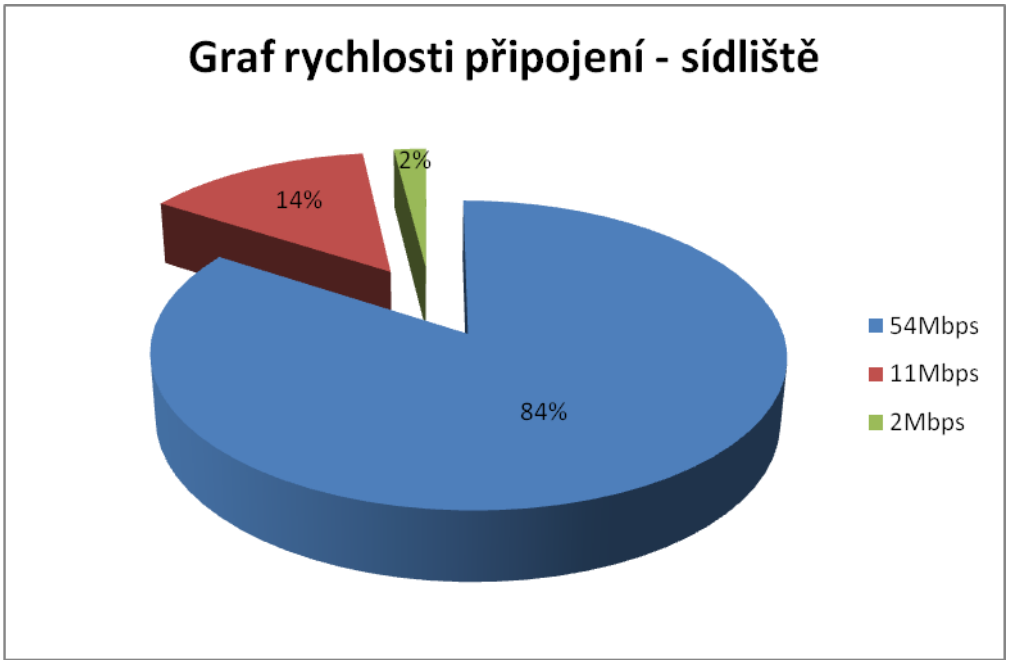
Následující graf zobrazuje bezpečnost komunikace probíhající na sídlišti Zachar. Jak je z něj patrné, pouze čtvrtina uživatelů Wi-Fi zde bezpečně komunikuje díky užívání WPA2,

nemusí tak mít obavy o svá soukromá data. Zbylých 75% uživatelů užívá nedostatečně zabezpečenou komunikaci, do níž řadíme OPN sítě, WEP a WPA sítě. Data těchto uživatelů jsou tedy v ohrožení.



Obr. 33. Graf bezpečné komunikace – sídliště.

Následuje „Graf rychlosti připojení - sídliště“, který charakterizuje rozložení rychlosti zabezpečení. Zde zcela převažuje s 84% rychlost 54Mbps, za ní se 14% sekunduje rychlost 11Mbps a jen ve 2% případů byla zjištěna rychlost 2Mbps.

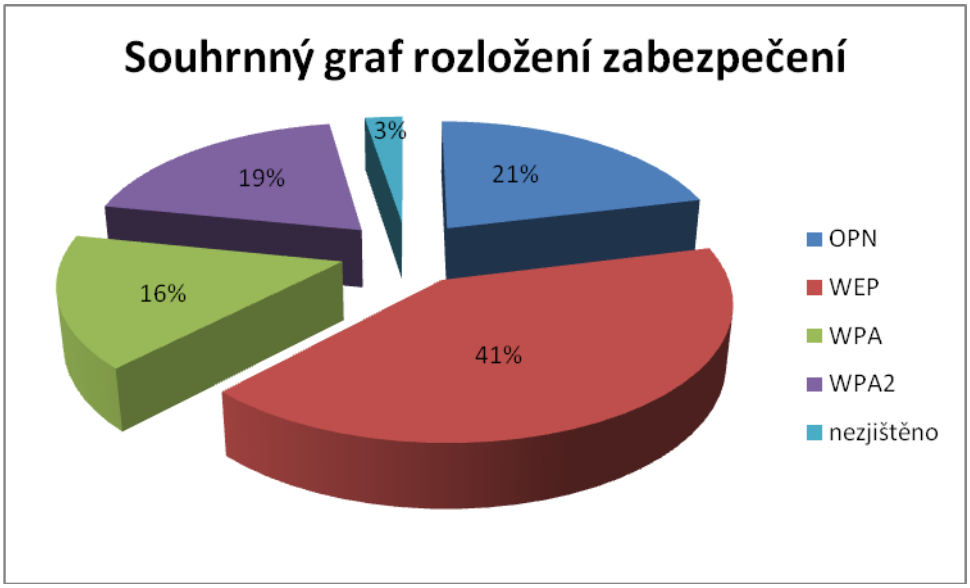


Obr. 34. Graf rychlosti připojení – sídliště.

Za povšimnutí stojí i oblíbenost použití zabezpečení „skrytí SSID“, které bylo odhaleno u 14 sítí z celkového počtu 106, což je téměř 15% celkově nalezených sítí.

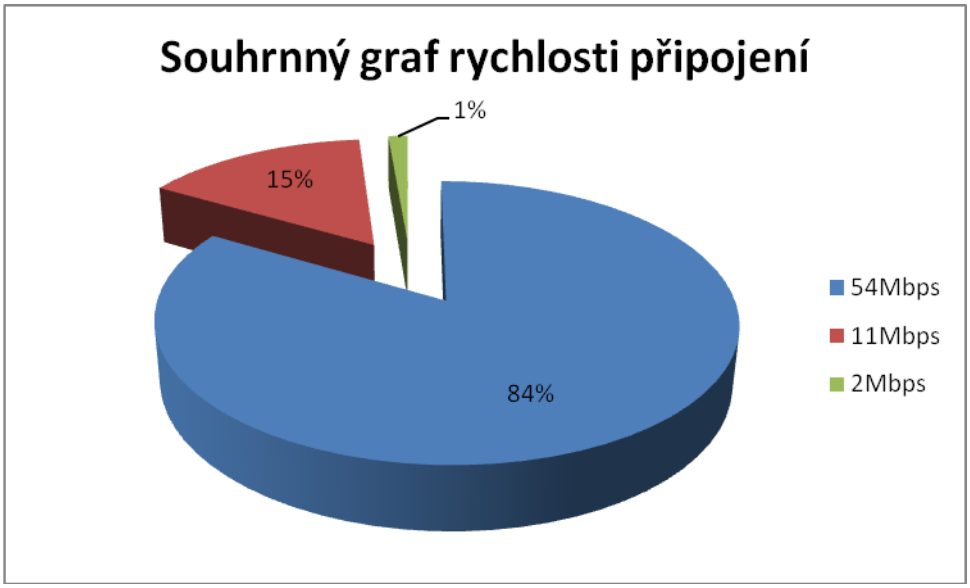
9.5.3 Srovnání zabezpečení sítí v typově různých lokalitách

Zabezpečení sítí vychází z potřeb, jež jsou charakteristické pro dané podmínky a prostředí. Celkové rozložení zabezpečení sítí charakterizuje následující graf, který slučuje data z obou prostředí a vytváří tedy jakýsi obrázek průměrného prostředí města.



Obr. 35. Souhrnný graf rozložení zabezpečení.

Jak ukazuje následující graf, na průměrném kroměřížském prostředí převažuje u Wi-Fi sítí rychlost 54Mbps. Jen v malém procentu případů se můžeme setkat s rychlostí 11Mbps, rychlost 2Mbps je zcela výjimečná a byla zaznamenána pouze v 1% případů.



Obr. 36. Souhrnný graf rychlosti připojení.

9.6 Srovnání s jinými výzkumy

Zajímavé je jistě i srovnání s jinými výzkumy, které byly provedeny odbornými pracovníky. Tato testování jsou velmi prestižní a napomáhají k rozvoji IT zabezpečení, často jsou také užívány pro potřeby marketingu. Z výzkumů byl vybrán ten, jenž je dosti aktuální, byl vydán 10. března 2011 a navíc byl proveden v České republice, což napomohlo prestižnosti srovnání průzkumů.

9.6.1 Ernst & Young v Praze a Bratislavě

Dle tohoto výzkumu je podíl pražských uživatelů používajících zabezpečení Wi-Fi 63%, 37% tedy užívá sítí bez zabezpečení. V Bratislavě je zabezpečeno 51% sítí, téměř polovina sítí není zabezpečena. 39% pražských přístupových bodů bylo nastaveno na rychlost vyšší než 11Mbps. V Bratislavě bylo detekováno 59% sítí s rychlostí vyšší než 11Mbps.

ERNST & YOUNG

Obr. 37. Logo společnosti Ernst & Young.

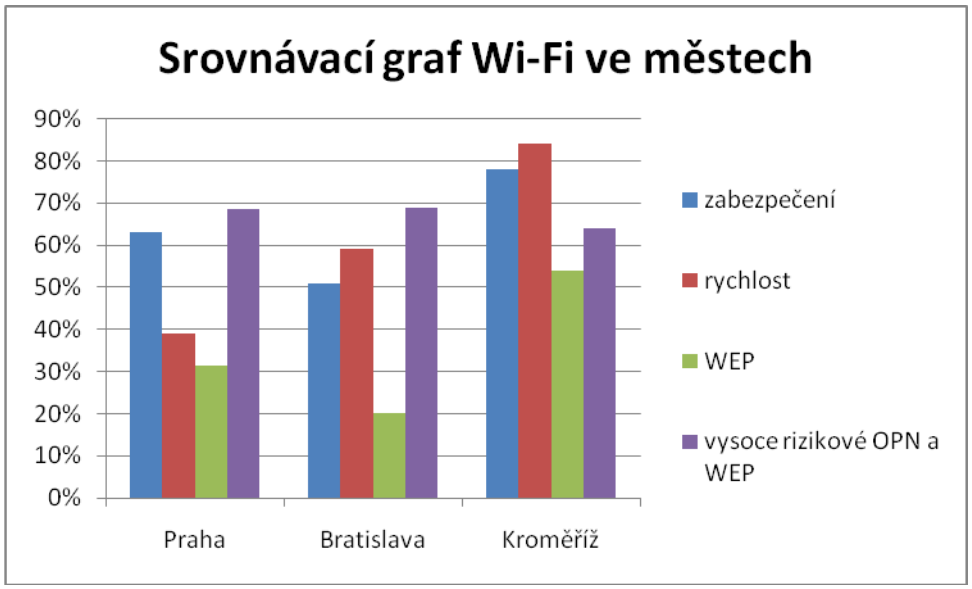
Poměr zabezpečených sítí k nezabezpečeným v Praze vychází asi na 2 ku 1 (63% zabezpečených, 37% nezabezpečených), v Bratislavě je tento poměr 1 ku 1, přesněji 51% a 49%. Samotný druh zabezpečení pak vyznívá nejlépe pro šifrování WEP, které je v Praze zastoupeno v 50% případů, ostatní typy šifrování tak byly zastoupeny rovněž v polovině případů. Bratislava používá WEP u 40% sítí.

Celkově tedy z průzkumu vyplývá, že je v Praze 37% otevřených sítí, 31,5% používá šifrování WEP, šifrování WPA a WPA2 je pak zastoupeno ve zbylých případech, tedy v asi 31,5%.

Bratislavský průzkum detekoval neuvěřitelných 49% otevřených sítí, 20% všech sítí je zabezpečeno šifrováním WEP a asi 31% sítí užívá zabezpečení WPA nebo WPA2. [13]

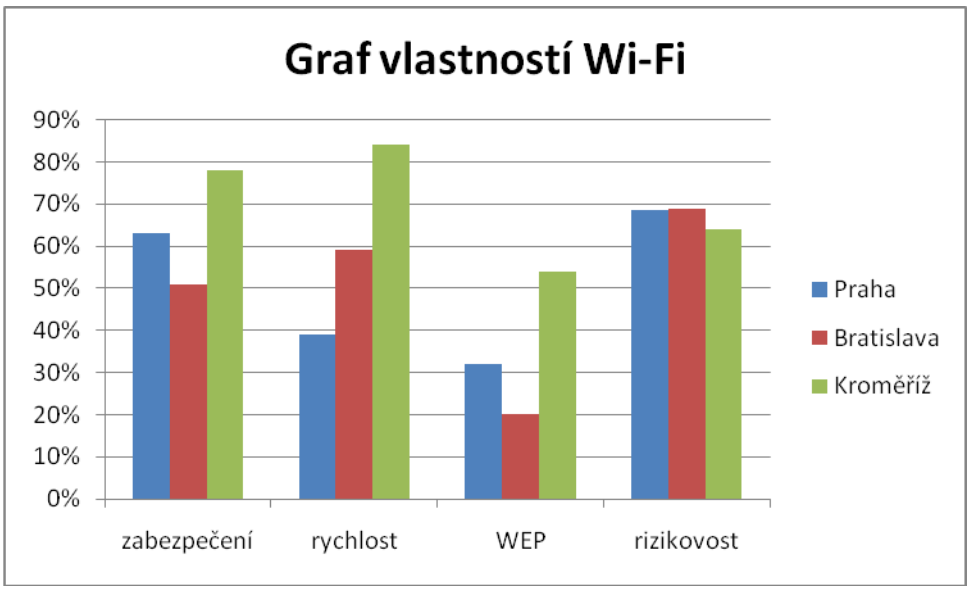
9.6.2 Srovnání s mnou naměřenými daty

Oproti výzkumu Ernst & Young bylo mým průzkumem detekováno vyšší procento zabezpečených sítí. Tyto tvořily 78% sítí, E&Y detekoval pouze 63% v Praze a pouhých 51% v Bratislavě. Naprosto jiným výsledkem dopadl test detekce rychlosti připojení, v němž byla mým testem prokázána existence 84% sítí s rychlostí vyšší než 11Mbps.



Obr. 38. Srovnávací graf Wi-Fi ve městech.

Naproti tomu E&Y uvádí pouhých 39% v Praze a mému průzkumu více se blížících 59% v Bratislavě. Můj výzkum zjistil u zabezpečených sítí použití šifrování WEP v 54% případů, E&Y detekoval v Praze 31,5% a v Bratislavě pouze 20%.



Obr. 39. Graf srovnání vlastností Wi-Fi ve městech.

Jako vysoce rizikové byly označeny sítě s buď žádným zabezpečením, nebo s šifrováním WEP, ostatní byly označeny jako relativně bezpečné. V tomto srovnání se mé hodnoty dostaly do vzácné shody s hodnotami testu E&Y. Vysoce rizikových sítí bylo nalezeno v Kroměříži 64%, v Praze 68,5% a v Bratislavě 69%.

9.7 Hodnocení získaných dat díky monitoringu sítí

Získaná data pro mne nebyla prakticky žádným překvapením. Ukázalo se, že lidé obecně spíše podceňují význam bezpečnosti dat a zvolené zabezpečení bezdrátových sítí neřeší. Toto je klasickým úkazem lidské populace, je zřejmé, že dokud se tito uživatelé nesetkají s útočníkem a jejich data nebudou zneužita, jejich přístup se jen těžko změní.

Grafy v předchozí podkapitole přehledně charakterizují rozložení zabezpečení Wi-Fi, a to ať už v kulturní zóně charakterizované náměstím, tak v zóně obytné, již charakterizuje sídliště. V obou lokacích se na nejvyšším místě pomyslného žebříčku umístilo zcela nedostatečné zabezpečení WEP, další získaná data se již výrazně odlišují. Náměstí pokrývá řada zcela nezabezpečených sítí, což potvrzuje existenci nezabezpečených hotspotů. Naopak oblast sídliště je charakteristická výskytem alespoň několika znalých uživatelů, kteří svou síť zabezpečili silným WPA2 nebo alespoň WPA.

Naprosto běžnou se stala rychlost 54Mpbs, která byla použita ve velké většině případů. Vyšší rychlosti nebyly zaznamenány, relativně často byly objeveny sítě s rychlostí 11Mbps, další rychlosti se vyskytovaly jen v zanedbatelném množství případů.

Srovnání s výzkumem Ernst & Young ukázalo rozdílné výsledky. Kroměřížský výzkum přitom vyzněl lépe, v porovnání s výzkumy v Praze a Bratislavě předčily kroměřížské domácnosti tato dvě velká města ve všech ohledech, tj. v zabezpečení komunikace i její rychlosti. Velké procento zabezpečených sítí však bylo v Kroměříži šifrováno prostřednictvím WEP, oproti tomu pokud byly sítě ve dvou větších městech zabezpečeny, byly tyto zabezpečeny kvalitněji. Poslední srovnání bylo zaměřeno na rizikovost sítí, toto srovnání vyznělo pro všechna města téměř stejně.

10 ZABEZPEČENÍ WI-FI VE FIREMNÍM SEKTORU

Ke zjištění zabezpečení ve firmách bylo přistoupeno, na rozdíl od dotazníkového průzkumu v domácnostech, formou diskuze se zástupci firem. Celkem bylo mnou navštíveno asi 30 firem, ne každá však byla ochotná se mnou komunikovat. Mnou vybraný počet 18 firem byl nakonec úspěšně dotázán, což mi pomohlo v dokončení mého průzkumu.

Jelikož není pro účely mé práce nutné uvádět jména firem, byly tyto označeny obecně. V některých případech by totiž mohly být ukázány konkrétní firmy ve špatném světle, čemuž bylo obecným označením úspěšně předejito.

10.1 Výběr firem

Firmy byly zvoleny cíleně tak, aby jejich zaměření co nejlépe pokrylo celé spektrum účelu užití Wi-Fi sítě.

Typy firem:

- restaurační zařízení a kavárny,
- běžné firmy,
- speciální firmy.

Rovněž bylo k výběru firem použito kritérium jejich velikosti. Pro účel této diplomové práce obecně označuji firmy prvního a druhého typu jako malé a velké. Od těchto dvou typů firem jsem oslovil 3 malé a 3 velké firmy.

10.2 Restaurační zařízení a kavárny

Kritérium velikosti firem bylo, oproti ostatním dvěma typům, posuzováno dle počtu hostů. Jako malá restaurační zařízení byla označena ta, jejichž maximální kapacita hostů nepřesahuje 50 osob, přičemž byly do počtu zahrnuty i „zahrádky“ před restauračními zařízeními. Označení „velké“ si vysloužily ty zařízení, jejichž maximální kapacita hostů přesahuje číslo 50 osob.

10.2.1 Wi-Fi průzkum a jeho výsledky

Restaurace č. 1 – malá

Jednalo se o restaurační zařízení cílené především na hosty, požívající alkohol. Toto zařízení nenabízelo hostům Wi-Fi síť a nepoužívalo ji ani pro žádné další účely.

Restaurace č. 2 – malá

Toto restaurační zařízení bylo zaměřeno jak na večerní posezení, tak i na poskytování jídla. Zařízení umožňovalo hostům využívat službu Wi-Fi a tuto službu nemělo zabezpečeno žádným způsobem.

Kavárna – malá

Tato kavárna slouží ke krátkému posezení menších skupin osob a nabízí především kávy, čaje a sladkosti. Mimo jiné poskytuje návštěvníkům připojení k internetu prostřednictvím nechráněné sítě Wi-Fi.

Restaurace č. 3 – velká

Restaurace zaměřená převážně na poskytování levných obědů, s otvírací dobou od 11 do 15 hodin a to od pondělí do pátku, nenabídla připojení k internetu.

Restaurace č. 4 – velká

Kvalitní a notně drahá restaurace se všeobecným zaměřením navíc poskytující připojení k internetu chráněné pomocí 128bitového WEPu. WEP klíč poskytuje obsluha na vyžádání.

Restaurace č. 5 – velká

Obvyklá restaurace s 24 hodinovým provozem nabízející veškerý sortiment. Zároveň poskytuje Wi-Fi připojení se zabezpečením WPA. Klíč k připojení opět poskytuje obsluha na vyžádání.

10.2.2 Shrnutí, hodnocení

Dle předpokladů nabízela restaurační zařízení a kavárny ve většině případů připojení k internetu, z celkem šesti vybraných zařízení jen 2 internet zákazníkům neposkytovaly. Další dvě internetová připojení prostřednictvím Wi-Fi poskytovaly, toto však nebylo

zabezpečeno žádným způsobem. Poslední dvě používaly zabezpečené připojení. V prvním případě šlo o zabezpečení prostřednictvím WEPu a využívajícím jeho delší 128bitovou variantu s klíčem o délce 104bitů. Poslední, nejlépe zabezpečené připojení, používalo WPA a bylo pro mne příjemným překvapením.

Ačkoliv některá zařízení internet skutečně poskytovala a dokonce na něj aplikovala i některý druh zabezpečení, v praxi je toto zbytečné zejména z důvodu snadného zjištění klíče díky poskytování personálem. Vyplývá z toho jednoduchá skutečnost – k internetu v tomto prostředí je lépe se nepřipojovat.

10.3 Běžné firmy

Tímto pojmem byly označeny firmy, které nakládají s běžnými daty a jejichž činnost nemusí být nijak speciálně upravena. Jedná se tedy o skutečně běžné firmy, jichž je na trhu práce, oproti mým druhým dvěma typům firem, největší procento.

10.3.1 Wi-Fi průzkum a jeho výsledky

Firma č. 1 – malá

Firma nabízející tiskařské práce. Z praktických důvodů zde používají Wi-Fi internet společně s internetem po LAN. Bezdrátový internet je zabezpečen pomocí WEPu s vysvětlením, že se majitel, který Wi-Fi nastavoval, obával nekompatibility se staršími zařízeními. Poslední Wi-Fi nastavení proběhlo před asi 6 roky, od té doby se nic nezměnilo.

Firma č. 2 – malá

Firma zabývající se vytvářením nového softwaru. Bezdrátový internet je zde všudypřítomný, přičemž jeho nastavení provedl jeden ze zaměstnanců. Wi-Fi tak používá zabezpečení WPA2.

Firma č. 3 – malá

Cestovní kancelář používající Wi-Fi připojení z důvodu striktního používání notebooků, tedy přenosných počítačů. Wi-Fi není zabezpečeno žádným způsobem, osoba, která Wi-Fi síť instalovala, věnovala čas pouze základnímu nastavení. AP je tedy v defaultním stavu.

Firma č. 4 – velká

Tato firma spravuje telefonní spojení. Sama Wi-Fi síť nevyužívá, používá totiž USB modemy využívající 3G síť. Používá tedy „konkurenční techniku“ k Wi-Fi sítím.

Firma č. 5 – velká

Jedná se o školu, která studentům nabízí bezdrátový internet s kvalitním zabezpečením WPA – EAP – MSCHAP v2. Login je uživateli přidělen po registraci, která je podmíněna zadáním vlastních přístupových údajů užívaných v rámci této školy. Na nastavení bezdrátové sítě pracuje vlastní správce sítě.

Firma č. 6 – velká

Firma se zabývá prodejem zemědělských strojů, v objektu firmy je jak hlavní sídlo, v němž je umístěno administrativní oddělení, tak i prostory pro opravu strojů. Wi-Fi je zde použito pouze v prezentační a jednací místnosti, kde probíhají obchodní schůze. Zabezpečení užité v rámci této sítě, je WPA2. AP nastavuje externí správce sítě a v pravidelných intervalech mění hesla, jež jsou běžně přístupná obchodním partnerům.

10.3.2 Shrnutí, hodnocení

Zde je třeba upozornit na rozdíl mezi velkými a malými firmami. Velké firmy mívají většinou své vlastní správce sítě, nastavení takovýchto Wi-Fi sítí tak bývá v pořádku a není třeba se obávat úniku dat. Naopak malé firmy si v lepším případě najímají externí správce sítě, v tom horším se pokouší o nastavení samy a toto pak nedopadá nejlépe, jak ukazuje i můj průzkum. Jako specifický příklad byla použita firma č. 2, která svým zaměřením vybočuje z obvyklého standardu, jsou v ní totiž IT odborníci.

10.4 Speciální firmy

Do speciálních firem byly zařazeny především firmy SBS, jelikož tyto přenášejí důležité informace, jež je třeba chránit. Ve dvou případech byly osloveny státní subjekty.

10.4.1 Wi-Fi průzkum a jeho výsledky

Firma SBS č. 1

Jednatel této firmy se nechal slyšet, že Wi-Fi technologii nevěří. Dle jeho slov „kabel je kabel“. Zákon, který by se vztahoval k použití bezdrátového internetu tak nikdy nestudoval, nebylo to třeba.

Firma SBS č. 2

Tato firma se zabývá montážemi bezpečnostních systémů. V jejím sídle bezdrátový internet nevyužívá, v případě montáže technologií zákazníkům dodržuje striktně pokyny projektanta, přičemž s využitím Wi-Fi se za dobu své existence nesetkali.

Firma SBS č. 3

Firma provozující PCO a poskytující kompletní sortiment bezpečnostních služeb. Wi-Fi technologie se zde používala především dříve, nyní je pouze v místnosti s PCO, kde umožňuje osobě obsluhující pult přístup na internet. V případě instalací je u firmy docela běžné používání IP kamer s technologií Wi-Fi, při němž nekladou žádné nároky na zabezpečení vzhledem k přenášeným datům, jimiž jsou obrázky, které už samy o sobě jsou ve formátu, který není zobrazitelný obvyklým softwarem. Většinou se navíc jedná o obrázky, které nejsou cenné, například několikahodinové záběry na chráněný pozemek, apod.

Firma SBS č. 4

Zástupce této firmy nechtěl o této problematice jednat, prý je to jejich tajemství. Firma nemá oprávnění pro nakládání s utajovanými informacemi, přesto zachází s citlivými údaji svých zákazníků. Ze zajímavosti byla následně provedena detekce sítě prostřednictvím detekční metody popsané v kapitole č. 9 této diplomové práce. Bylo zjištěno, že firma ve svém objektu používá nedokonalé zabezpečení WPA.

Obvodní oddělení PČR

Jako skutečně velký subjekt má PČR své vlastní správce sítě. S jedním z nich byla sjednána schůzka, na níž objasnil situaci s Wi-Fi u PČR. Dle jeho slov má PČR vlastní předpisy, jimiž se při sestavování sítě musí řídit. Díky těmto předpisům Wi-Fi v praxi nepoužívají, jediné využití, o kterém osobně věděl, je v některých policejních autech, která si díky internetu stahují data, která jsou sama o sobě šifrovaná. O přesném zabezpečení nevěděl, jeho předpokladem je ovšem WPA2 s radius serverem.

Štáb AČR

Komunikace s pracovníkem na štábu Armády České republiky vedla ke zjištění místního stavu s Wi-Fi sítěmi. Tyto se zde striktně nepoužívají, vzhledem k faktu, že většina zaměstnanců pracuje s utajovanými informacemi. Z toho plynou velká omezení, ne

všechny počítače mají totiž přístup na internet. K tomu je vždy na určitou skupinu vyhrazen jeden počítač, u kterého se pak uživatelé střídají v případě nutnosti užití internetu.

10.4.2 Shrnutí, hodnocení

Jak je možno vysledovat, Wi-Fi je jednoduše technologie, jíž subjekty zacházející s důležitými daty nevěří, a proto ji nepoužívají. Předchází tak nebezpečí úniku informací a rovněž snižují množství problémů spojených s rušením a tedy špatným přenosem dat.

Jedna z firem (firma SBS č. 4) používá nedokonalé zabezpečení, data jejích zákazníků jsou tak v permanentním ohrožení, což je mnou hodnoceno velmi negativně. Ani zabezpečení Wi-Fi u firmy SBS č. 3 by se neobešlo bez výhrad. Zde není problémem ani tak způsob zabezpečení, spíše možnost zneužití komunikace obsluhy s možnými zloději. Spolupráce by mohla vypadat tak, že v případě výjezdu na některé místo obsluha PPC ví, že další pracovníky na výjezd firma nemá, což oznámí prostřednictvím internetu zlodějům a tito mohou bez obav vyloupit objekt jiný.

ZÁVĚR

V teoretické části mé diplomové práce je přehledně shrnuta problematika Wi-Fi sítí, jejího zabezpečení a možných útoků na ně. Práce je dále zaměřena na výčet možných citlivých dat, jež jsou přes internet posílána a jsou zde rozebrány i právní podmínky pro užití Wi-Fi ve firmách SBS. Závěr teoretické části patří principu tvorby dotazníku, jež byl využit v části praktické a objasňuje pojem Warchalking, kterýmžto byl proveden praktický výzkum.

Odpovědi na nejdůležitější otázky, jimž byla má práce věnována, poskytuje část praktická. Dotazník Wi-Fi znalostí dokázal neznalost uživatelů Wi-Fi sítí a zároveň nedokonalost jejich zabezpečení domácího bezdrátového internetu. To potvrdila i měření detekční technikou, která odhalila velké procento špatně zabezpečených sítí jak v kulturní zóně, tak i v zóně obytné.

Zabezpečení bezdrátového internetu v podmínkách firemního sektoru odpovídá ve většině případů druhu zaměření firem a jejich velikostí. Často zde rozhoduje i faktor existence vlastního, popřípadě využití externího, správce sítě.

Diplomová práce naplnila má očekávání a ověřila skutečný stav zabezpečení Wi-Fi sítí v dané oblasti. Podala řadu zajímavých odpovědí na důležité bezpečnostní otázky a nastínila možnou nápravu neuspokojivého aktuálního stavu.

ZÁVĚR V ANGLIČTINĚ

In the theoretical part of my thesis I clearly summarized the issue of Wi-Fi networks, its security and possible attacks on them. I also focused on possible sensitive data that is sent over the Internet. In the thesis I have analyzed the legal conditions for the use of Wi-Fi by SBS companies. Conclusion the theoretical part is the principle of creating a questionnaire that was used in the practice and clarifies the koncept of Warchalking, which was used during practical research.

Answers to all important questions, which my work was devoted to, are mentioned in the practical part. The questionnaire about Wi-Fi knowledge proved the ignorance of the Wi-Fi networks users and it also proved the imperfection of their home wireless internet security. This was confirmed by measuring detection technique, which revealed a large percentage of poorly secured networks both in the cultural area, and in a residential zone.

Security of wireless Internet in terms of the corporate sector in most cases corresponds to the type of focus of companies and their size. What often matters is whether companies use their own or an external, network administrator.

The diploma thesis met my expectations and verified actual security status of Wi-Fi networks in the area. It gave us many interesting answers to important safety issues and outlined possible remedy of the current unsatisfactory situation.

SEZNAM POUŽITÉ LITERATURY

[1] MA, Jianfeng. *Security access in wireless local area networks : from architeckutre and protocols to realization.* Beijing : Higher Education Press, 2009, 431 s. ISBN 978-3-642-00941-9.

[2] LUDVÍK, Miroslav; ŠTĚDROŇ, Bohumír. *Teorie bezpečnosti počítačových sítí*. 1. vyd. Kralice na Hané : Computer Media, 2008. 98 s. ISBN 978-80-86686-35-6.

[3] GORANSSON, Paul; GREENLAW, Raymond. *Security roaming in 802.11 networks [online]*. Oxford : Newnes, [cit. 2011-01-19]. 343 s. Dostupné z WWW: [http://www.sciencedirect.com/science/book/9780750682114]. ISBN 9780750682114.

[4] SOSINSKY, Barrie. *Mistrovství - počítačové sítě : [vše, co potřebujete vědět o správě sítí].* Vyd. 1. Brno : Computer Press, 2010. 840 s. ISBN 978-80251-3363-7.

[5] MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. *Hacking bez záhad.* 1. vyd. Praha : Grada, 2007. 520 s. ISBN 978-80-247-1502-5.

[6] SVOBODA, Petr. *Techniky průniku do bezdrátových počítačových sítí.*. [s.l.], 2009. 57 s. Bakalářská práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky.

[7] Česká republika. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. In *Sbírka zákonů*. 2005, 143, s. 72.

[8] Česká republika. Zák. č. 101/2000 Sb., o ochraně osobních údajů. In *Sbírka zákonů*. 2000, 32, s. 64.

[9] Česká republika. Zákon č. 127/2005 Sb., o elektronických komunikacích. In *Sbírka zákonů*. 2005, 43, s. 1330-1408..

[10] *Dotazník-online* [online]. 2007 [cit. 2011-05-23]. Jak na dotazník. Dostupné z WWW: <http://www.dotaznik-online.cz/zaklady-dotazniku.htm>.

[11] *Guide-to-Symbols* [online]. 2011 [cit. 2011-05-23]. Warchalking. Dostupné z WWW: <http://www.guide-to-symbols.com/_images_pub2/warchalking.png>.

[12] *Živě.cz* [online]. 2010 [cit. 2011-05-23]. Živě.cz. Dostupné z WWW: <http://www.zive.cz/clanky/pravda-o-googlu-skutecne-kradl-cisla-kreditnich-karet/sc-3-a-152347/default.aspx>.

[13] *Ernst & Young* [online]. 2011-03-10 [cit. 2011-05-23]. Quality In Everything We Do. Dostupné z WWW: <http://www.ey.com/CZ/cs/Newsroom/News-releases/2011_Pocet-wifi-pripojeni>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard.
AMD	Advanced Micro Devices.
AP	Access Point.
ARP	Adress Resolution Protocol.
CCMP	Counter mode – CBC Message Authenication Protocol.
CRC-32	Cyclic Redundancy Check.
DDR2	Double Data Rate 2.
DES	Data Encryption Standard.
DHCP	Dynamic Host Configuration Protocol.
DoS	Denial of Service.
EAP	Extensible Authentication Protocol.
EAP-MD5	Extensible Authentication Protocol – Message Digest 5.
FMS	Fluhrer, Mantin, Shamir.
FTP	File Transport Protocol.
FTPS	FTP over SSL.
GHz	Gigahertz.
ICMP	Internet Control Message Protocol.
ICV	Integrity Check Value.
IEEE	Institute of Electrical and Electronics Engineers.
IV	Initialization Vector.
IP	Internet Protocol.
KDE	K Desktop Environment.
LAN	Local Area Network.
LEAP	Lightweight Extensible Authentication Protocol.

OKA	Open Key Authentication.
MAC	Message Authentication Code.
MHz	Megahertz.
MIC	Message Integrity Check.
PC	Personal Computer.
PCI	Peripheral Component Interconnect.
PCMCIA	Personal Computer Memory Card International Association.
PDA	Personal Digital Assistant.
PEAP	Protected Extensible Authentication Protocol.
PKB	Průmysl Komerční Bezpečnosti.
PSK	Pre-Shared Key.
PTW	Pyshkin, Tews, Weinmann.
RC4	Ron's Code No. 4.
OS	Operační Systém.
SKA	Shared Key Authentication.
SSID	Service Set Identifier.
SSL	Secure Sockets Layer.
ŠK	Šifrovací Klíč.
TKIP	Temporal Key Integrity Protocol.
TSL	Transport Security Layer.
TTSL	Tunneled Transport Security Layer.
UK	User Key.
USB	Universal Serial Bus.
VoIP	Voice over Internet Protocol.
WAN	Wide Area Network
WEP	Wired Equivalent Privacy.

WiFi	Wireless Fidelity.
Wi-Fi	Wireless Fidelity.
WLAN	Wireless Local Area Network.
WPA	WiFi Protected Access.
WPA-PSK	WiFi Protected Access – Pre-Shared Key.
WPA2	WiFi Protected Access 2.
XOR	Exclusive OR.

SEZNAM OBRÁZKŮ

Obr. 1. Wi-Fi logo. 13
Obr. 2. Access point. 14
Obr. 3. Všesměrová anténa. 15
Obr. 4. USB Wi-Fi karta. 16
Obr. 5. Překrývání komunikačních kanálů. 17
Obr. 6. Nevýhoda Wi-Fi – špatná prostupnost překážkami. 20
Obr. 7. Princip šifrování WEP. 28
Obr. 8. Warchalk mapa. 46
Obr. 9. Open net 46
Obr. 10. WEP net. 47
Obr. 11. Closed net. 47
Obr. 12. Automobil Streetview. 48
Obr. 13. Graf Wi-Fi v domácnostech. 52
Obr. 14. Graf užitého zabezpečení v domácnostech 54
Obr. 15. Graf důvěry respondentů v bezpečnost Wi-Fi 55
Obr. 16. Graf připojení přes hotspot 57
Obr. 17. Graf znalosti uživatelů. 60
Obr. 18. Laptop použitý k detekci. 62
Obr. 19. Lokace pro detekci - náměstí 64
Obr. 20. Lokace pro detekci - sídliště 65
Obr. 21. Spuštění Airmon-ng. 67
Obr. 22. Oznámení o zapnutí monitorování. 68
Obr. 23. Výstupní data programu Airodump-ng. 69
Obr. 24. ESSID v prostředí Windows 7. 70
Obr. 25. Graf rozložení zabezpečení – náměstí. 71
Obr. 26. Graf bezpečnosti sítí – náměstí. 72
Obr. 27. Graf ohrožení sítí – náměstí. 72
Obr. 28. Graf bezpečné komunikace – náměstí. 73
Obr. 29. Graf rychlosti připojení – náměstí. 73
Obr. 30. Graf procentuálního rozložení zabezpečení – sídliště. 74
Obr. 31. Graf bezpečnosti sítí – sídliště. 75
Obr. 32. Graf ohrožení sítí – síliště. 75

Obr. 33. Graf bezpečné komunikace – sídliště. 76
Obr. 34. Graf rychlosti připojení – sídliště. 76
Obr. 35. Souhrnný graf rozložení zabezpečení. 77
Obr. 36. Souhrnný graf rychlosti připojení. 78
Obr. 37. Logo společnosti Ernst & Young. 78
Obr. 38. Srovnávací graf Wi-Fi ve městech. 79
Obr. 39. Graf srovnání vlastností Wi-Fi ve městech. 80

PŘÍLOHA P I: WI-FI DOTAZNÍK S LEGENDOU

Vážený čtenáři,

oslovil jsem Vás za účelem vyplnění mého dotazníku, jenž mi má poskytnout podpůrné informace pro vypracování některých bodů zadání praktické části mé diplomové práce na téma Zjištění reálného stavu Wi-Fi přenosů v dané oblasti.

Při vypracování dotazníku byl kladen důraz na stručnost a jednoznačnost otázek a odpovědí, konečný počet otázek je tedy 20, a proto by Vám vyplnění dotazníku nemělo zabrat příliš mnoho času.

Ačkoliv jsem dbal na jednoduchost otázek s přihlédnutím k možné neznalosti respondentů, v případě nejasností přidávám k samotnému dotazníku i dokument s legendou, jenž by měl důkladněji vysvětlit složitější body v něm obsažené, a v případě nejasné odpovědi na otázku by měla legenda pomoci jejímu zodpovězení. Legenda je zařazena za samotné otázky, je tedy umístěna od strany číslo 6 do strany číslo 9.

Druhá otázka je označena jako „dělící“ a rozděluje uživatele na ty, kteří Wi-Fi internet doma používají a ty, kteří jej nepoužívají. V případě odpovědi „ne“ na tuto otázku prosím pokračujte k otázce č. 12.

Vyplněný dotazník prosím zašlete v příloze na e-mailovou adresu VS.dotaznik@gmail.com. Před odesláním prosím zkontrolujte, že je u každé otázky zaškrtnuta pouze jedna odpověď a nezapomeňte uložit změny.

Děkuji za Vaši ochotu a čas, každý vyplněný dotazník je pro mne velmi hodnotný. Věřím, že mi Vaše spolupráce pomůže k úspěšnému složení státní zkoušky.

Bc. Petr Svoboda

Otázky

1. V oblasti IT se považujete za

- ☐ nezkušeného uživatele
- ☐ málo zkušeného uživatele
- ☐ středně zkušeného uživatele
- ☐ velmi zkušeného uživatele

2. Připojujete se v domácnosti k internetu prostřednictvím Wi-Fi?

- ☐ ano
- ☐ ne
- ☐ nevím

V PŘÍPADĚ ZODPOVĚZENÍ „NE“ NA OTÁZKU Č. 2 POKRAČUJTE PROSÍM OTÁZKOU Č. 12.

3. Umíte vstoupit do uživatelského rozhraní Vašeho AP?

- ☐ ano
- ☐ ne

4. Správu a zabezpečení Vaší Wi-Fi sítě

- ☐ provádíte sám/sama
- ☐ provádí zkušenější uživatel

5. Máte defaultní (původní) nastavení přístupu na Váš access point?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

6. Používáte skrytí SSID?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

7. Používáte filtr MAC adres?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

8. Máte nastaveno automatické přiřazování IP adres?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

9. Který z následujících druhů zabezpečení používáte?

- ☐ žádné
- ☐ WEP
- ☐ WPA
- ☐ WPA 2
- ☐ autentifikace 802.1x
- ☐ nevím

10. Máte povolenu správu AP pouze počítači připojenému přes LAN?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

11. Máte svůj AP bezpečně uložen a zabezpečen proti LAN připojení cizího PC?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

12. Připojujete se prostřednictvím Wi-Fi sítě na svůj e-mail, IM, FTP, apod.?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

13. Věříte v bezpečnost svých dat při připojení k internetu přes Wi-Fi?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

14. Znáte někoho, kdo umí získat login (přístup) do Wi-Fi sítě bez účasti administrátora sítě?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

15. Setkali jste se někdy s útokem na Wi-Fi síť?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

16. Připojil/a jste se někdy přes hotspot?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

17. Připojil jste se někdy přes hotspot na svůj e-mail, IM, FTP, apod.?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

18. Byl Vám nebo někomu ve Vašem okolí ukradnut přístup na e-mail, IM, FTP, apod.?

- ☐ ano
- ☐ spíše ano
- ☐ nevím
- ☐ spíše ne
- ☐ ne

19. Jste

- ☐ muž
- ☐ žena

20. Váš věk je

- ☐ méně než 13 let
- ☐ 13 až 25 let
- ☐ 26 až 40 let
- ☐ 41 až 55 let
- ☐ 56 a více let

Závěrem bych Vám chtěl ještě jednou poděkovat za vyplnění dotazníku.

Bc. Petr Svoboda

Legenda k dotazníku

Tato legenda slouží k objasnění a vysvětlení některých složitějších otázek v dotazníku. Pakliže některé otázce z dotazníku nerozumíte, po přečtení příslušné legendy k této otázce byste jí již měli porozumět. Není tedy třeba, abyste četli celou legendu, stačí pouze ty otázky, jimž plně nerozumíte.

1. V oblasti IT se považujete za

Pod písmeny zkratky IT se skrývá pojem informační technologie. Tento pojem můžeme jednoduše vysvětlit jako znalost počítačů (ať už stolních, tak přenosných), práci s programy a vše, co se počítačové techniky týká.

2. Připojujete se v domácnosti k internetu prostřednictvím Wi-Fi?

Pojmem Wi-Fi je myšlena bezdrátová technologie pro přístup do sítě Internet. Otázka je zaměřena na používání AP (access point) s anténou (obr. 1), vysílající v domácnosti elektromagnetické vlnění, díky němuž můžete, v dnešní době především prostřednictvím notebooků nebo mobilních telefonů, přistupovat do sítě Internet bez nutnosti kabelového připojení LAN. Pro bližší představu přikládám obrázek AP s anténou.

Obr. 1 - AP (access point) s anténou.

3. Umíte vstoupit do uživatelského rozhraní Vašeho AP?

Pojem AP (access point) je vysvětlen v otázce č. 4. Uživatelské rozhraní AP (obr. 2) zpřístupňuje uživateli nastavení tohoto zařízení a to nejen nastavení připojení k Internetu, ale i možnost zabezpečení jeho sítě a další. Obvykle se do něj přistupuje přes Webový prohlížeč (Internet Explorer, Mozilla Firefox a jiné).

Obr. 2 - Uživatelské rozhraní AP.

5. Máte defaultní (původní) nastavení přístupu na Váš access point?

Prostřednictvím uživatelského rozhraní (viz. legenda k otázce č. 5) můžete přistoupit k nastavení AP (viz. legenda k otázce č. 4). K samotnému přístupu do AP je však potřeba znalosti loginu (jména a hesla a znalosti IP adresy (adresa zadávaná do webového prohlížeče). AP má již z výroby nastaveny původní (defaultní) hodnoty pro vstup do uživatelského rozhraní.

6. Používáte skrytí SSID?

Skrytí SSID je jedním z možných zabezpečení Vaší bezdrátové sítě. SSID je název sítě, tedy jméno, které může být viditelné nebo skryté. To se zobrazuje při vyhledávání sítí v dosahu běžnými zařízeními (notebook, mobilní telefon, atp.). Otázka je tedy zaměřena na to, zda se jméno Vaší sítě zobrazuje, či nikoliv.

7. Používáte filtr MAC adres?

Filtr MAC adres je jedním z možných zabezpečení Vaší bezdrátové sítě. Každé zařízení, které se chce připojit na internet prostřednictvím Vaší sítě, má vlastní adresu.

V uživatelském rozhraní AP (viz. legenda k otázce č. 5) může být nastaveno filtrování MAC adres a tedy povolení připojení jen některým vybraným zařízením.

8. Máte nastaveno automatické přiřazování IP adres?

Manuální přiřazování IP adres (tedy adres nutných pro připojení do sítě) ztěžuje případný útok na Vaši síť. AP (viz. legenda k otázce č. 4) může uživateli přiřadit IP adresu buď samo, nebo si ji musí uživatel při přihlášení nastavit vlastnoručně a opakovaně (pozor, některé programy pro připojení k internetu si pamatují první volbu nastavení IP, proto stačí jedno úspěšné zadání, o vyplnění v následujících připojeních se stará již zmíněný program).

9. Který z následujících druhů zabezpečení používáte?

Přenosy po Vaší Wi-Fi síti mohou být zabezpečeny pomocí některých druhů zabezpečení. Zvolte prosím možnost, která odpovídá Vašim znalostem ohledně Vaší sítě.

10. Máte povolenu správu AP pouze počítači připojenému přes LAN?

V uživatelském rozhraní (viz. legenda k otázce č. 5) je možno nastavit povolení k přístupu do tohoto rozhraní pouze prostřednictvím LAN, tedy přímého kabelového připojení. Jednoduše řečeno, toto nastavení zamezuje správě Vašeho AP (viz. legenda k otázce č. 4) prostřednictvím přístrojů (notebooky, mobilní telefony, atp.) připojených přes Wi-Fi.

11. Máte svůj AP bezpečně uložen a zabezpečen proti LAN připojení cizího PC?

Tato otázka je úzce spjata s otázkou č. 16. Táže se na umístění Vašeho AP (viz. legenda k otázce č. 4) v domácnosti a jeho zabezpečení proti LAN připojení, tedy přímého kabelového připojení osob, které by k němu neměly mít přístup.

12. Připojujete se prostřednictvím Wi-Fi sítě na svůj e-mail, IM, FTP, apod.?

Otázka je zaměřena na samotný přístup na zaheslované internetové stránky a užívání programů komunikujících s internetem prostřednictvím loginu (uživatelské jméno a heslo) v době, kdy jste přihlášeni do sítě Wi-Fi.

14. Znáte někoho, kdo umí získat login (přístup) do Wi-Fi sítě bez účasti administrátora sítě?

Existují způsoby, jak se nepovolaná osoba může vlámat do Wi-Fi sítě, ve většině případů zejména díky nedokonalému zabezpečení. K takovému útoku je však třeba určitých pokročilých znalostí.

15. Setkali jste se někdy s útokem na Wi-Fi síť?

Útokem na Wi-Fi síť je myšleno prolomení zabezpečení Vaší Wi-Fi sítě a tedy neoprávněný přístup do ní, popřípadě znemožnění fungování sítě či získání osobních údajů napadením Vaší Wi-Fi sítě, nebo jakýkoliv pokus o výše popsané.

16. Připojil/a jste se někdy přes hotspot?

Místa s připojením hotspot jsou nejčastěji restaurace, kavárny, vzdělávací centra, apod. Tato místa nabízejí připojení k Wi-Fi zdarma a často jsou brány jakou doplňkové služby jednotlivých zařízení. K jejich užívání, tedy k přístupu na internet, většinou není třeba znalosti žádných hesel, popřípadě je heslo „veřejné“, obsluha těchto zařízení Vám je poskytne.

17. Připojil jste se někdy přes hotspot na svůj e-mail, IM, FTP, apod.?

Kombinace dvou předchozích otázek (viz. legenda k otázce č. 14 a viz. legenda k otázce č. 18).

18. Byl Vám nebo někomu ve Vašem okolí ukradnut přístup na e-mail, IM, FTP, apod.?

Otázka je zaměřena na zjištění, zda Vám nebo někomu ve Vašem okolí nebyl odcizen přístup k zaheslovaným internetovým stránkám či k programům komunikujících s internetem prostřednictvím loginu (uživatelské jméno a heslo). V praxi se setkáváme zejména s nemožností přístupu na místa, kam jsme se dříve běžně přihlašovali, popřípadě zjištění vstupu na tato místa nepovolanou osobou a změna (úprava, smazání) Vašich dat.