Použití analyzátoru paketů bezdrátových sítí Wireshark

Usage of packet wireless network analyzer Wireshark

Bakalářská práce

Ladislav Sirový

Vedoucí bakalářské práce:

Ing. Ladislav Beránek, Csc., MBA.

Jihočeská univerzita v Českých Budějovicích

Pedagogická fakulta

Katedra informatiky

2009

Prohlášení

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

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

V Českých Budějovicích dne

Anotace

Práce se zabývá problematikou analýzy počítačových sítí především s použitím analyzátoru Wireshark. Zaměřena je také na problematiku zabezpečení bezdrátových sítí obecně. V této problematice je zahrnuto praktické testování různých typů zabezpečení a porovnání zabezpečení bezdrátových sítí ve vybraných lokalitách měřením. Práce přináší přehled nejpoužívanějších open-source síťových analyzátorů a jejich porovnání.

Abstract

This paper contains information about performing computer network analysis using Wireshark application and about wireless network security in general. This involves practical testing of various security models and measuring wireless security coverage in specific areas. The general overview of the most widely used open-source network analyzers and their comparsion is also included.

Klíčová slova

Wireshark, analyzátor, bezdrátová síť, paket, analýza, bezpečnost

Keywords

Wireshark, analyzer, wireless network, packet, analysis, security

Poděkování

Úvodem své bakalářské práce bych rád poděkoval svému vedoucímu

Ing. Ladislavu Beránkovi, CSc., MBA.

za cenné rady a pomoc během zpracování bakalářské práce.

Obsah

1 Úvod

Téma této bakalářské práce jsem si zvolil z důvodu osobního zájmu o problematiku bezdrátových sítí a jejich bezpečnost. Dále jsem chtěl rozšířit obecné povědomí o oboru síťové analýzy, problému nezabezpečených sítí a tento druhý jmenovaný fakt i prakticky dokázat. V neposlední řadě nabídnout přehled a srovnání jednotlivých open-source síťových analyzátorů a jejich předností.

2 Cíle práce

Hlavními cíli této bakalářské práce je několik bodů. Jedním z těchto bodů je porovnat programy pro analýzu počítačových sítí. Dalším bodem je ukázka nastavení a praktického použití analyzátoru paketů Wireshark. Následujícím bodem práce je praktické otestování a porovnání druhů zabezpečení bezdrátové sítě v simulovaných podmínkách. Cílem poslední části této bakalářské práce je zjištění a porovnání zabezpečení bezdrátových sítí ve vybraných lokalitách na základě měření.

3 Bezdrátové sítě

Trendem dnešní doby informačních technologií je předání informace mezi počítači. Rychle, spolehlivě a bezpečně. Dnes k tomuto účelu slouží především počítačové sítě. Počínaje lokálními sítěmi uživatelů, přes rozsáhlé sítě měst, až po světovou síť Internet. V současnosti je pro nás ve většině případů nejdůležitější dostupnost připojení k internetu. K

tomuto účelu, tj. spojení koncového uživatele s internetem, slouží lokální počítačové sítě označované jako LAN. Tyto sítě obvykle sdružují několik uživatelů či stanic o malém počtu, řádově desítky, až po velmi rozsáhlé podnikové sítě i o stovkách připojených zařízeních.

Standard	Rok vydání
IEEE 802.11	1997
IEEE 802.11a	1999
IEEE 802.11b	1999
IEEE 802.11g	2003
IEEE 802.11y	2008
IEEE 802.11n	Očekávaný 2009

Tabulka 1: Tabulka standardů

K snazší distribuci lokální sítě bylo v roce 1997 standardizováno bezdrátové připojení standardu IEEE 802.11. Tento standard se dále rozvíjel (Viz Tabulka 1) do současného návrhu IEEE 802.11n, který prochází schvalováním. Nový standard přinese podstatné zvýšení přenosové rychlosti. Stále však tato přenosová rychlost nedosáhne propustnosti dnešních drátových sítí.

Použití bezdrátového připojování zařízení přineslo mnoho výhod (Viz. Tabulka 2), ale zároveň i nevýhod nebo nedostatků proti klasickým počítačovým sítím, využívajícím jako přenosového média kabely.

Výhody	Nevýhody
využití nelicencovaného pásma	zarušení dostupného pásma více vysílači
dostupné zařízení na trhu	vyšší pořizovací náklady oproti drátovým sítím
mobilitu uživatelů v dosahu vysílače	prozatím nižší přenosové rychlosti
snadné vytvoření vetší sítě bez kabelů	potřeba více znalostí na nastavení bezpečného připojení
snadné připojení uživatele	nejistá kvalita spojení (rušení, neprostupnost signálu)

Tabulka 2: Výhody a nevýhody bezdrátových sítí

Bezdrátové řešení přineslo do mnoha oborů a případů použití lokálních sítí značné usnadnění či zjednodušení používání, ale i fyzické instalace sítě jako takové.

S rozšiřováním bezdrátových sítí a se zvyšující se náročností jejich správy se zároveň objevily i složitější problémy. Tyto problémy vyžadují nasazení specializovanějších nástrojů na odhalování problémů sítě. Těmito nástroji jsou síťové analyzátory nebo paketové sniffery.

4 Monitorování a analýza bezdrátových sítí

Bezpečnost a kvalitu počítačových sítí může ovlivňovat mnoho negativních faktorů. Nebezpečné síťové viry, tzv. červi, mohou způsobit únik dat ze sítě či její velké zatížení, které pak vede k nedostupnosti mnoha služeb sítě. Kvalitu služeb může ovlivnit špatné nastavení sítě, porucha aktivních prvků sítě nebo špatně pracující software využívající ke své funkci síť. Nejčastějšími problémy počítačové sítě obvykle bývá:

- malá datová propustnost i časově krátkodobá
- špatná propustnost a stabilita fyzických portů aktivních zařízení
- špatná adresace v síti
- špatné či neúplné nastavení bezpečnostních prvků (data nesměřují jen tam, kam mají)

K odhalování těchto problémů a monitorování sítě slouží paketové či protokolové analyzátory sítí. Monitorování stavu dostupnosti sítě a z ní vycházejících služeb není ovšem žádnou převratnou novinkou posledních let. Na základní analýzu bylo myšleno již na počátku 80. let při realizaci sítě Internet, kdy byly do základního návrhu zakomponovány protokoly umožnující sledovaní sítě. S určitými modifikacemi se tyto protokoly používají dodnes a poskytují nepostradatelný základ pro analýzu sítě.

Sledování (monitorování) sítě lze provádět několika metodami. Tyto metody lze obecně rozdělit z hlediska časové náročnosti na krátkodobé a dlouhodobé sledování. Při krátkodobém sledováním a analýze provozu sítě se správce sítě zajímá o data aktuálně přenášená a přímo je vyhodnocuje. Vyhodnocovanými daty jsou nejčastěji:

- objem aktuálně přenášených dat
- směr toku dat
- vytížení aktivních prvků a jejich správná činnost

Většinou je správce sítě při tomto sledování zaměřen na konkrétní

problém. Dlouhodobé sledování probíhá obvykle v řádech týdnů až měsíců. Během této doby paketové sniffery zachytávají specifická data jako jsou informace o výpadcích a chybách v provozu sítě. Na tyto nestandardní či nežádoucí stavy může být správce sítě upozorněn pomocí alarmů nebo událostí (odeslání e-mailu, přímé zasáhnutí do provozu či nastavení sítě). Výsledky dlouhodobého sledování lze přehledně zobrazovat v grafech. Z těchto výsledků lze zjistit problémová místa sítě a odvodit z nich případná doporučení na zlepšení služeb sítě, např. zvýšení propustnosti linky, rozdělení zátěže na více aktivních zařízení popř. serverů nebo změnit čas zpracování mimo špičkové zatížení sítě operacím pracujícím se sítí, u kterých je tato změna možná.[3][4]

Síťová protokolová analýza je proces k dekódování síťových paketů zachycených při monitorování sítě. Tento proces se nezabývá pouze počítáním prošlých paketů a čtením jejich hlaviček, ale vede k podrobnějšímu zjištění nebo pochopení informací zapouzdřených v paketech. Takto rozbalená (dekódovaná) data jsou obvykle zobrazována v přehledné formě pro snazší orientaci při vlastní analýze a vyhodnocování konkrétních paketů. Tím lze zjistit ARP datagramy vysílané aktivním prvkem se špatným nastavením popř. poruchou, pokusy o napadení či přímo napadení bezdrátových sítí, špatně pracující nebo špatně nastavené tabulky adres, díky nimž se privátní adresy vyskytují ve vnějších síti a v neposlední řadě správnou či nesprávnou funkci zabezpečení sítě. [3]

Spojením monitorování a analýzy sítě lze tedy výše popsaným problémům předcházet , či je úplně odstranit, lze ale i zefektivňovat využívání prostředků a tím i pracovní čas uživatelů.

5 Bezpečnost bezdrátových sítí

Se vznikem bezdrátových sítí samotných zároveň automaticky vznikla i potřeba tyto sítě zabezpečit. V současné době je k dispozici několik různých způsobů, jak toto učinit. I přesto, že možností, jak účinně bezdrátové sítě zabezpečit existují, jsou mnohdy sítě zabezpečeny málo nebo vůbec. Publikací i článků o detailech a principech jednotlivých typů zabezpečení existuje již několik, proto se tato práce bude věnovat pouze aktuálním doporučením a demonstraci útoků na různé typy zabezpečení bezdrátové sítě.

6 Paketový analyzátor Wireshark

6.1 Síťové analyzátory

Programy a aplikace vykonávající síťovou analýzu se nazývají síťové, popř. paketové analyzátory. Tyto programy slouží k dekódování síťového provozu, rozbalování procházejících paketů. Jednoduše umožňují vizualizaci závislostí paketů. Analyzátory pomáhají správcům sítí odhalovat nežádoucí aktivity na sítích a vyhledávat kritická či problematická místa na síti. Pro snazší orientaci v nabídce analyzátorů se také tato práce zabývá porovnáním dostupných síťových analyzátorů.

Wireshark je jeden z nejznámějších síťových protokolových analyzátorů. Je obecně považován za standard v řadě průmyslových odvětví a vzdělávacích institucí.[5]

Zdroje [2] a [6] uvádí, že Wireshark je síťový analyzátor distribuovaný pod open-source licencí GNU/GPL pracující na více než 20 dnes používaných platformách operačních systémů. Dostupný je jak v podobě zkompilovaných balíčků či instalací, tak i v podobě předkompilovaných binárních souborů, nebo v podobě zdrojového kódu. Podporuje provoz síťových karet jak v normálním, tak i promiskuitním módu síťových karet. Umí zachytávat data z různých přenosových médií (Ethernet, Token-Ring, WLAN 802.11 a další). Podporuje práci s více než sedmi sty protokoly a s daty zachycenými více než 25 odlišnými programy.

6.2 Historie

Dle zdrojů [2], [6] a [7] historie Wireshaku začíná v roce 1997, kdy Gerald Combs (tou dobou zaměstnaný u NIS[1]), aby mohl rozšiřovat své znalosti o počítačových sítích, začal vyvíjet program Ethereal, který mu měl pomoci jako nástroj při řešení problémů na síti. V červenci roku 1998 tedy vychází první verze Etherealu (verze 0.2.0). Krátce poté Gilbert Ramirez vidí potenciál Etherealu a přispívá k vývoji disektorů, které jsou jádrem Wiresharku a umožňují dekódovat jednotlivé protokoly a zobrazovat je v čitelné podobě. V říjnu téhož roku hledal Guy Harris

1 Network Integration Service http://www.netisinc.com/

z firmy Network Appliance[2] lepší program než TCPView. Tak začal přispívat na vývoji záplat a disektorů pro Ethereal. Ke konci roku 1998 viděl Richard Sharpe, který se věnoval kurzům TCP/IP problematiky, potenciál těchto kurzů ve spojení s Etherealem a začal se věnovat hledaní protokolů, jež potřeboval, a které by zároveň Ethereal podporoval. Ale jelikož v té době nebylo možné snadno nové protokoly přidat, věnoval se vývoji disektorů a vylepšení Etherealu.

V roce 2006 Gerald Combs změnil zaměstnavatele a chtěl dále pokračovat na vývoji Etherealu. Nepodařilo se mu však vyjednat souhlas na používaní ochranných symbolů Etherealu. Tak založil nový projekt s názvem Wireshark, do kterého přesunul veškerý svůj kód z Etherealu. Nyní k vývoji přispívá přes 600 odborníků a specialistů na počítačové sítě a informační technologie.

6.3 Funkce

Wireshark aktuálně dle [5]poskytuje velmi rozsáhlou sadu funkcí, které zahrnují:

- Hloubkovou inspekci stovek protokolů
- Online zachycování paketů a offline analýzu zachycených dat
- Standardní tří-panelové přehledné grafické rozhraní analyzátoru paketů
- Multiplatformní využití: Windows, Linux, OS X, Solaris,

2 Network Appliance http://www.netapp.com/us/

FreeBSD, NetBSD a mnoho dalších

- Zachycená data lze prohlížet pomocí grafického rozhraní nebo vestavěného příkazového řádku pomocí Tshark utility
- Nejúčinnější zobrazování filtrů v průmyslovém použití
- Bohatou VoIP analýzu
- Čtení a zápis mnoha různých formátů souborů zachytávání: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (komprimovaný i nekomprimovaný), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, a mnoho dalších
- Zachycené soubory komprimované pomocí GZIP lze dekomprimovat za běhu
- Data mohou být zachytávána z Ethernetu, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, a dalších (v závislosti na použité platformě).
- Podpora dešifrování mnoha protokolů, včetně IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP a WPA/WPA2

- Přehledná kolorovatelná pravidla lze uplatnit na seznam zachycených paketů pro rychlou a intuitivní analýzu
- Výstup může být exportován do XML, PostScriptu, CSV nebo prostého textu

7 Příprava porovnání bezdrátových sítí

Cílem této části práce je analyzovat a identifikovat zabezpečení bezdrátových sítí ve vybraných lokalitách. Analýza zabezpečení bude mít pouze informativní charakter, protože vychází z informací vysílaných přístupovým bodem. Metodika porovnání bude volena obdobně, jako již provedené průzkumy uvedené níže, pro možnost porovnání.

7.1 Uskutečněná porovnání

Obdobné analýzy byly provedeny již uplynulých letech. Tyto analýzy zabezpečení bezdrátových sítí byly zaměřeny především na lokality hlavního města Prahy. Jednou z těchto analýz zabezpečení je průzkum firmy Ernst & Young[3]. Jmenovaná firma provádí porovnání bezdrátových sítí pravidelně každý rok již od roku 2004 v oblastech městských částí Praha 1 a Praha 2. Výsledky měření v rámci této práce lze tedy porovnat s výsledky měření v lokalitách hlavního města Prahy. Měření bylo prováděno pomocí směrové antény a programu Kismet. Zároveň byly zapsány údaje o GPS pozici daného měření. Poté byla použitím triangulace a síly signálu vypočtena přibližná poloha přístupového bodu

3 http://www.ey.com/cz/

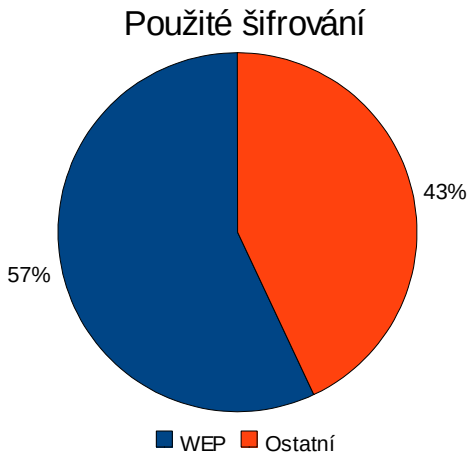
(dále jen AP). Následující výsledky měření z roku 2008 jsou dle [1].

Rok	Počet AP	Meziroční nárůst
2008	3290	97%
2007	1671	91%
2006	876	45%
2005	604	372%
2004	128	

Tabulka 3: Počet AP v jednotlivých letech a meziroční nárůst počtu

Rok	Zabezpečeno	Nezabezpečeno	Meziroční nárůst
2008	73%	27%	9%
2007	64%	36%	12%
2006	52%	48%	8%
2005	44%	56%	11%
2004	33%	67%	

Tabulka 4: Podíl zabezpečených sítí v jednotlivých letech a meziroční nárůst zabezpečených sítí



Graf 3: Podíl typu zabezpečení

Výrobce	Podíl	Výrobce	Podíl
Cisco-Linksys	19%	Apple Computer	2%
D-Link Corporation	15%	Symbol Technologies	2%
ZyGate Communications, Inc.	13%	Planet Technology Corporation	2%
ASUSTek Computer Inc.	11%	Complex, Inc.	2%
Edimax TechnologyCo., Ltd.	5%	Agere Systems	2%
Askey Computer Corp	4%	CC&C Technologies, Inc.	1%
3Com	3%	AboCom	2%
Zyxel Communication	3%	Ostatní	15%
SMC Networks, Inc	2%		

Tabulka 5: Podíl výrobců AP

Další průzkum provedl v březnu 2007 Sebastian Schreiber v rámci IDC Security Roadshow 2007. Toto měření probíhalo v centru Prahy. Pro měření byla použita všesměrová anténa a program NetStumbler. GPS údaje o místě zachycení signálu byly také zaneseny do mapy. Výsledkem měření bylo 847 zachycených přístupových bodů bezdrátových sítí. Z celkového počtu bylo 46,6% nezabezpečeno. [8]

Graf 4: Podíl zabezpečených a nezabezpečených sítí

7.2 Předpoklady

Předpoklady pro měření a analýzu provedené v rámci této práce vycházejí z dostupných zdrojů [1] a [8], které se již problematice věnovaly v jiných lokalitách. Hlavními předpoklady pro porovnání

zabezpečení sítí jsou:

- více než polovina dostupných přístupových bodů bude používat zabezpečení
- více než polovina zabezpečených přístupových bodů bude zabezpečena slabým šifrováním WEP
- největší podíl výrobců přístupových bodů budou mít firmy Cisco a D-Link Corporation

Dalšími předpoklady pro detaily, které nebyly zatím v dostupných zdrojích porovnávány, jsou:

- více než 75 % bezdrátových sítí patřící větším i menším firmám bude zabezpečena – důvodem by měla být vyšší důležitost dat na síti
- v četnosti kanálů frekvenčního pásma budou využity více krajní kanály a střed pásma – snaha o menší zarušení pásma

8 Porovnání síťových analyzátorů

K porovnání bylo zvoleno 5 freewarových paketových analyzátorů či snifferů, které byly nejlépe hodnoceny portálem softpedia.com anebo se umístily v žebříčku „Top 11 Packet Sniffers“ (Nejlepších 11 paketových snifferů) portálu insecure.org, který se věnuje zabezpečení sítí. Výběr byl ovlivněn splněním několika podmínek:

1. open source nebo freeware program

2. umístění v hodnocení portálu insecure.org v Top 11 Packet Sniffers nebo nebo v předních pozicích hodnocení portálu softpedia.com

Jako k dalším parametrům bylo přihlíženo k rozsahu podpory operačních systémů, možnosti ovládaní pomocí grafického rozhraní i příkazového řádku, kompatibilitě zachycených dat s Wiresharkem, dostupnosti zdrojového kódu a k subjektivnímu hodnocení především uživatelského ovládání a komfortu.[19][20][21]

8.1 Porovnání

Testování těchto analyzátorů probíhalo na zařízeních uvedených v tabulce 6.

Počítač	Operační systém	Bezdrátové adaptéry
Dell Studio 1535	Windows Vista Home Premium 32bit Linux BackTrack 4 beta CZ mód 32bit	Dell Wireless 1510 Wireless-N WLAN Mini-Card
		Asus WL-167g
		Edimax EW7318USg
Dell Latitude C500/C600	Linux Kubuntu 8.10 32bit	Asus WL-167g
		Edimax EW7318USg
MacBook Air	Mac OS X Version 10.5.5	AirPort Extreme

Tabulka 6: Zařízení použité při porovnání programů

K testování zachycení byl použit vždy v rámci možností stejný testovací postup. Tato data odpovídají obvyklému nejmožnějšímu použití síťových analyzátorů, které se při zpracování práce podařilo nasimulovat. Ukázka

funkce, použití a ovládaní jednotlivých analyzátorů jsou na tomto vzorku dostatečně patrná. Testování obsahovalo následující operace:

- Připojení k bezdrátové sítí s automatickým přidělováním adresy
- Zkouška odezvy **ping** na server **jcu.cz**
- Příkaz **nslookup jcu.cz**
- Načtení webové stránky **http://www.pf.jcu.cz**
- Načtení webové zabezpečené stránky **https://stag-eb.jcu.cz/apps/stag/zkousky/index**
- Připojeni a odpojeni k FTP serveru **pf.jcu.cz**
- Připojení k e-mail serveru **pf.jcu.cz** pomocí IMAP – nešifrovaně
- Připojení k e-mail serveru **pf.jcu.cz** pomocí IMAP – šifrovaně
- Připojení, testovací konverzace a odpojeni k serveru služby **ICQ**

8.2 Výsledky porovnání

Přehled testovaných analyzátorů a paketových snifferů a jejich vlastností je přehledně zobrazen v Tabulka 7. Programy byly porovnávány především s analyzátorem Wireshark a dále dle výše uvedených podmínek.

Název programu	Windows	Linux	Mac OS	GUI	CML	Zdrojový kód
Wireshark	ano	ano	ano	ano	ano	ano
Tcpdump	ano	ano	ano	**ne**	ano	ano
Ettercap	ano	ano	ano	ano	ano	ano
Ksniffer	**ne**	ano	**ne**	ano	ano	ano
Justniffer	**ne**	ano	ano	**ne**	ano	ano
Cocoa Packet Analyzer	**ne**	**ne**	ano	ano	**ne**	**částečně**

Tabulka 7: Výsledky porovnání - GUI – Grafické rozhraní; CML – Příkazový řádek

8.2.1 Wireshark

Wireshark je jeden z nejrozšířenějších programů pro síťovou analýzu. Tato popularita vychází především z univerzálnosti použití programu, jeho široké podpoře protokolů, přehlednému grafickému rozhraní a dokonalého filtrování paketů,

Klady:

- ✔ přehledné grafické rozhraní
- ✔ podpora stovek protokolů
- ✔ multiplatformní použití
- ✔ nastavení uživatelských pravidel
- ✔ ukládání do mnoha typů formátů
- ✔ široké použití filtrů

- ✔ zachytávání v reálném čase a pozdější analýza těchto dat
- ✔ možnost dešifrování šifrovaných zachytávaných dat

Zápory:

- ✗ Nutnost běhu s administrátorskými právy
- ✗ větší velikost na disku

8.2.2 Tcpdump

Je dalším z velmi silných nástrojů pro síťovou analýzu. Mezi hlavní klady programu patří široká použitelnost na většině operačních systémů, jeho jednoduchost a přenositelnost.

Domovská stránka programu: http://www.tcpdump.org/

Klady:

- ✔ ukládání zachycených dat
- ✔ kompatibilita s Wireshark
- ✔ přenositelnost (není nutná instalace)
- ✔ filtrování zachytávání
- ✔ přes 150 filtrů

Zápory:

- ✗ absence grafického rozhraní

- ✗ pomalý vývoj
- ✗ náročnější nastavení před zachytáváním

8.2.3 Ettercap

Tento program je určen především k zachytávání paketů. Původně byl vyvinut k zachytávání hesel a testování zabezpečení na LAN sítích využívajících přepínané aktivní prvky. Proto má Ettercap implementováno mnoho nástrojů na odhalování hesel a metody na řízení probíhající komunikace.

Domovská stránka programu: http://ettercap.sourceforge.net/

Klady:

- ✔ široké použití pro zachytávání (sniffing)
- ✔ možnost testování zabezpečení a hesel
- ✔ rozbor šifrovaných protokolů
- ✔ filtrování zachytávaného obsahu
- ✔ podpora mnoha OS
- ✔ vytváření rozšíření

Zápory:

- ✗ menší spektrum analyzovatelných protokolů
- ✗ složitější grafické rozhraní

- ✗ odlišná koncepce ovládání
- ✗ slabší podpora bezdrátových sítí

8.2.4 Ksniffer

Ksniffer je síťový sniffer určený pro operační systém Linux používající grafické prostředí KDE.

Domovská stránka programu: http://ksniffer.sourceforge.net/

Klady:

- ✔ vhodný pro méně náročné použití
- ✔ grafické rozhraní určené přímo pro KDE
- ✔ jednoduché ovládání
- ✔ kompatibilita s Wireshark

Zápory:

- ✗ málo podporovaných protokolů
- ✗ pouze pro Linux
- ✗ slabší podpora bezdrátových sítí

8.2.5 Justniffer

Justniffer je TCP paketový sniffer. Umožňuje zachytávání TCP/IP paketů a jejich sestavování do přehledného toku dat.

Domovská stránka programu: http://sourceforge.net/projects/justniffer/

Klady:

- ✔ jednoduchost používání
- ✔ kompatibilita s Wireshark
- ✔ specializovaný na TCP/IP pakety

Zápory:

- ✗ zachytává pouze TCP pakety
- ✗ málo podporovaných protokolů
- ✗ absence grafického rozhraní
- ✗ pomalý vývoj

8.2.6 Cocoa Packet Analyzer

Tento síťový paketový analyzátor paketový sniffer je vyvíjený nativně pro MAC OS X. Obsahuje podporu pro nejpoužívanější typy sítí a protokolů. Umožňuje ukládat zachycená data ve standardním PCAP formátu.

Domovská stránka programu: http://www.tastycocoabytes.com/cpa/

Klady:

- ✔ přímo pro MAC OS
- ✔ velmi intenzivní vývoj

- ✔ přehledné ovládání
- ✔ kompatibilita s Wireshark
- ✔ možnost použití vlastních rozšíření

Zápory:

- ✗ nedostupnost kódu
- ✗ méně podporovaných protokolů

8.2.7 Závěr porovnání

Z tabulky 7 je patrné, že nejlepšími programy vycházejí Wireshark a Ettercap. Při porovnání těchto dvou programů se jeví jako lepší nástroj na analýzu bezdrátových sítí Wireshark. Program Ettercap je od svého původu více zaměřen na problematiku bezpečnosti dat na sítí, než problematiku provozu sítě celkově. Proto jako nejlepším open-source univerzálním řešením pro analýzu sítí vychází program Wireshark.

9 Použití programu Wireshark

Základním prvkem pro sledování a následnou analýzu datového provozu bezdrátové sítě je správné nastavení bezdrátové síťové karty (adaptéru). Pro to, aby bylo možné sledovat většinu požadovaných aktivit, je nutné mít kartu, či adaptér přepnut do tzv. monitor módu (označován i jako RFMON[4]). Karta se v tomto módu chová velmi obdobně jako klasická síťová karta v promiskuitním režimu, ale promiskuitní režim to přímo není, ačkoliv tak často bývá uváděno. Monitor mód karty umožňuje pasivní sledovaní a pouhé příjímání bezdrátového provozu bez nutnosti se k síti přímo připojit. Proto může karta zachytávat většinu bezdrátové komunikace standardu IEEE 802.11, která probíhá v jejím dosahu. Promiskuitní mód bezdrátové karty umožňuje jen zachytávání paketů, které nejsou hlavičkou paketu určeny pro tuto kartu. K tomu je ovšem nutné připojení ke konkretní bezdrátové síti. [22]

Proto je velmi důležitá volba správného adaptéru, který podporuje přepnutí. Originální bezdrátový adaptér v notebooku Dell Studio 1535, který byl pro zpracování této práce použit, Dell Wireless 1510 Wireless-N WLAN Mini-Card, přepnutí do výše uvedeného režimu neumožňuje. Respektive teoretické fungování karty v monitor módu je možné u všech karet, ale bohužel v drtivé většině nejsou ke kartám ovladače, které by je do daného režimu přepnuly. Původně byla pro výběr bezdrátové karty zvažována výměna integrovaného adaptéru v notebooku. Bohužel tento

4 RFMON (Radio Frequency Monitoring)

notebook má pro interní bezdrátové karty pouze slot Mini PCI-Express, a to navíc v poloviční velikosti karty. Výběr možných adaptérů byl tedy zúžen na karty připojitelné pomocí USB nebo slotu ExpressCard. Mezi těmito rozhraními se jevilo jako lepší USB, díky své univerzálnosti použití i na ostatních počítačích. Na trhu je nabídka Wi-Fi USB adaptérů poměrně široká, ovšem, jak již bylo zmíněno výše, většinu nelze přepnout do požadovaného režimu. Proto byl výběr možných karet omezen pouze na karty uváděné v [23] a splňující výše uvedené podmínky. Díky možnosti připojení externí antény pomocí reversního SMA konektoru a příznivé ceně (cca 500,-Kč) byl vybrán bezdrátový USB adaptér Edimax EW-7318USg. Jako operační systém pro demonstraci nastavení a zachytávání byl zvolen Linux distribuce BackTrack 4 beta CZ mód 32bit, ve kterém je velmi dobrá podpora ovladačů výše zmiňovaného adaptéru Edimax.

9.1 Nastavení bezdrátového zařízení

Nastavení adaptéru Edimax EW7318USg v operačním systému Linux distribuce BackTrack 4 beta CZ mód 32bit lze provést následujícím způsobem:

Nejprve příkazem **`iwconfig`** zjistíme název a parametry bezdrátových adaptérů.

```
root@bt:~# iwconfig
lo    no wireless extensions.
eth0  no wireless extensions.
wmaster0    no wireless extensions.
```

```
wlan0      IEEE 802.11bg  ESSID:""
           Mode:Managed Frequency:2.412 GHz  Access
Point: Not-Associated
           Tx-Power=0 dBm
           Retry min limit:7 RTS thr:off Fragment
thr=2352 B
           Encryption key:off
           Power Management:off
           Link Quality:0 Signal level:0 Noise level:0
           Rx invalid nwid:0 Rx invalid crypt:0 Rx
invalid frag:0
           Tx excessive retries:0 Invalid misc:0 Missed
beacon:0
```

Z výpisu příkazu je viditelné, že na použitém počítači se nachází pouze jedno bezdrátové zařízení s názvem **`wlan0`**.

Pomocí volání příkazu **`iwconfig`** s parametry **`wlan0 mode Monitor`** přepneme rozhraní **wlan0** do požadovaného monitor módu. Po opětovném volaní **`iwconfig`** vidíme, že rozhraní **wlan0** je úspěšně přepnuto.

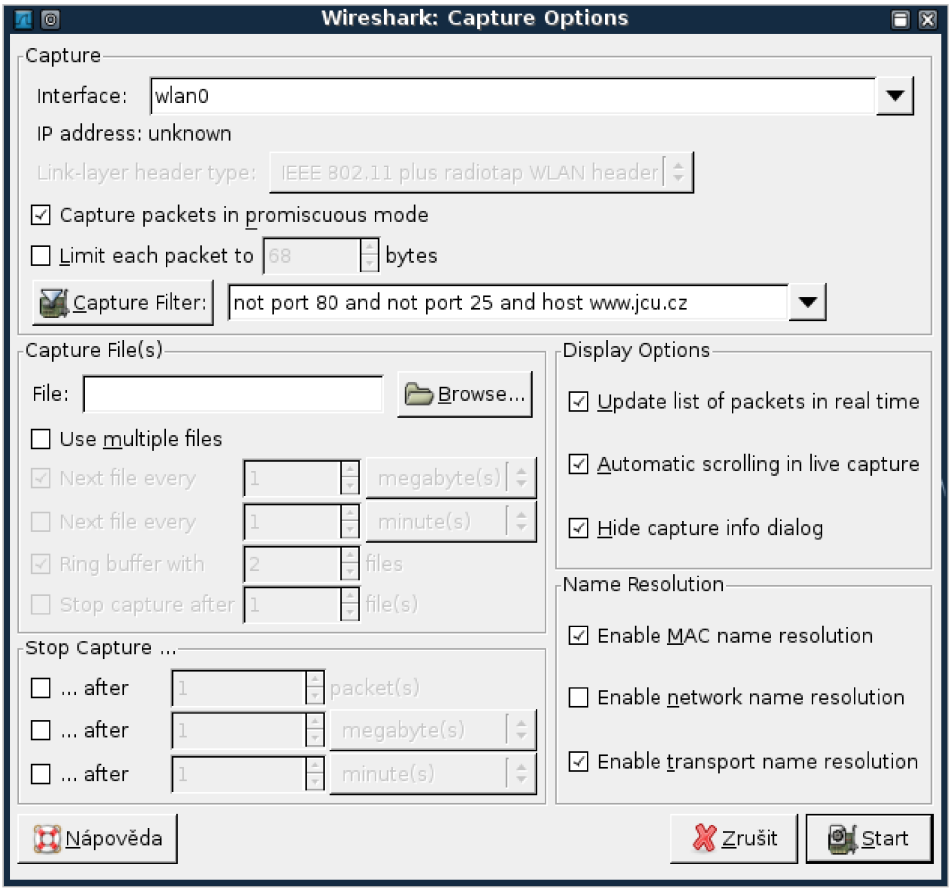
```
root@bt:~# iwconfig wlan0 mode Monitor
root@bt:~# iwconfig wlan0
wlan0      IEEE 802.11bg  Mode:Monitor  Frequency:2.412
GHz  Tx-Power=0 dBm
           Retry min limit:7 RTS thr:off Fragment
thr=2352 B
           Encryption key:off
           Power Management:off
           Link Quality:0  Signal level:0  Noise level:0
           Rx invalid nwid:0  Rx invalid crypt:0  Rx
invalid frag:0
           Tx excessive retries:0  Invalid misc:0 Missed
beacon:0
```

Před spuštěním zachytávaní je obvykle vhodnější ještě nastavit kanál, (frekvenci) na kterém bude bezdrátový adaptér pracovat. Tím docílíme

menšího počtu zachycených nežádoucích paketů z jiných sítí na jiném kanálu. Toto omezení ovšem není úplně jisté, protože odstup jednotlivých kanálů mezi sebou je relativně malý a při různých odrazech signálu může docházet k jejich prolínání. Nastavení provedeme příkazem **`iwconfig wlan0 channel`** a číslo požadovaného kanálu. V našem případě tedy **`iwconfig wlan0 channel 2`**. V případě, že nevíme, na kterém kanálu pracuje bezdrátová síť, jež chceme sledovat, musíme použít skript, který nám bude průběžně měnit nastavení kanálu bezdrátového adaptéru. Skript na tzv. „channel hopping“ lze nalézt na http://802.11ninja.net/code/chanhop.sh. Případně lze použít jinou aplikaci, např. Kismet. Ta nám zobrazí, na kterém kanále požadovaná síť pracuje.

Dalším příkazem **`ifconfig wlan0 up`** rozhraní **wlan0** aktivujeme a můžeme začít zachytávání paketů na tomto rozhraní.

Pomocí zástupce nebo příkazu **`wireshark`** spustíme aplikaci Wireshark. Před spuštěním samotného zachytávání je vhodné nastavit filtr pro zachytávání. Tento filtr nám umožní zachytávat pouze ty pakety, jež potřebujeme. Funkci je výhodné použít především v oblastech s velmi hustým bezdrátovým provozem. Při absenci filtru pro zachytávání by mohl objem zachycených dat prudce stoupat, což v mnoha ohledech není žádoucí.



Ilustrace 1: Nastavení zachytávání

9.2 Filtry

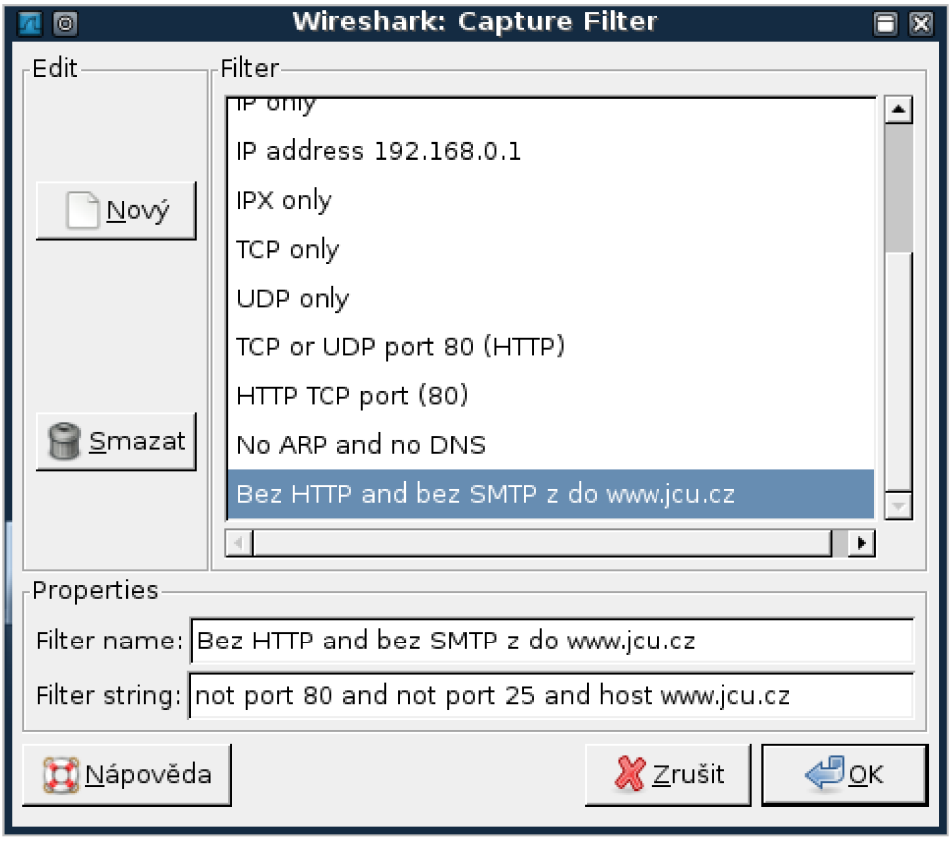
Jednou z hlavních předností analyzátoru paketů Wireshark jsou jeho rozsáhlé možnosti filtrování. Data lze filtrovat na dvou různých úrovních:

1. Filtr při zachytávání – Aplikace zaznamenává pouze ty pakety, které splňují podmínky vstupního filtru. Pakety filtrem

nepropuštěné nejsou žádným způsobem uloženy pro další zpracování. Použití filtru je využitelné při nasazení, kdy víme, na kterém protokolu či vrstvě se pracuje nebo víme, kde se nachází cíl analýzy, potažmo problém. Tento typ filtrování přináší hlavní výhodu ve velikosti a obsáhlosti souboru se zachycenými daty.

2. Zobrazovací filtry umožňují přehledné procházení a oddělování již zachycených dat. Pomocí těchto filtrů se o žádné pakety při zachytávání nepřichází. Tento typ filtrování pouze skrývá pakety, které neprojdou podmínkou filtru. Výhodou je, že se při zachytávání nepřichází o žádná data, která by se mohla postupem času ukázat jako potřebná.

Obě metody lze velmi účinně kombinovat. Ovšem před nastavením filtru pro zachytávaní se doporučuje dobré uvážení. Z vlastní zkušenosti lze doporučit filtrování při zaznamenávaní paketů pouze v oblasti s velkým bezdrátovým provozem, či filtrování sítí, které nejsou pro další analýzu důležité.



Ilustrace 2: Nastavení filtru pro zachytávání

Parametry filtrování lze snadno definovat pomocí operátorů a logických výrazů.

Zkratka	Znak	Význam anglicky	Význam česky
eq	==	equal	rovno
ne	!=	not equal	není rovno
gt	>	greater than	větší než
lt	<	less than	menší než
ge	>=	greater than or equal	větší nebo rovno
le	<=	less than or equal	menší nebo rovno

Tabulka 8: Seznam možných operátorů

Zkratka	Znak	Význam
and	&&	logický AND
or	||	logický OR
not	!	logický NOT

Tabulka 9: Seznam možných logických výrazů

Jak u logických výrazů tak i u operátorů lze používat v definici filtrování zkratku i zástupný znak. Jak by mohl vypadat filtr pro zachytávání a pro zobrazení je možné vidět níže.

Filtr pro zachytávání

```
not port 80 and not port 25 and host www.jcu.cz
```

Při nastavení filtru nebude Wireshark zachytávat veškerou http komunikaci používající port 80 a zároveň žádnou SMTP komunikaci procházející portem 25 z nebo do domény www.jcu.cz

Zobrazovací filtr

```
wlan.fc.protected == 1
```

Tento zobrazovací filtr vyloučí ze zobrazování všechny pakety používající šifrování.

Po nastavení vhodného filtru lze tedy zahájit zachytávání dat. Po ukončení zachytávání, nebo i při jeho běhu, je možné data dál detailně filtrovat. A to pomocí již výše zmíněných zobrazovacích filtrů. Několik takovýchto filtrů je uvedeno v další části práce.[24]

9.2.1 Zobrazovací filtry rozlišující zabezpečení sítě

Pomocí následujících filtrů lze rozlišit dostupné bezdrátové sítě dle zabezpečení.

Nezabezpečená síť

wlan_mgt.fixed.capabilities.privacy == 0

WEP

(wlan_mgt.fixed.capabilities.privacy == 1) &&

(wlan_mgt.tag.number == 0)

WPA

wlan_mgt.tag.interpretation == "# of unicast cipher suites: 1"

WPA2

(wlan_mgt.tag.interpretation == "# of unicast cipher suites: 2") or
(wlan_mgt.tag.interpretation == "# of unicast cipher suites: 3")

9.2.2 Zobrazovací filtry pro řídící rámce bezdrátové sítě

Tyto rámce slouží k řízení provozu bezdrátové sítě, k získání informace o dostupných bezdrátových sítích a podobně.[25]

Management rámce

Management rámce umožňují povolení či odmítnutí připojení klienta k sítí nebo udržování spojení. Pomocí těchto rámců lze identifikovat i pokusy o napadení bezdrátové sítě.

Association Request	*wlan.fc.type_subtype == 0*
Association Response	*wlan.fc.type_subtype == 1*
Probe Request	*wlan.fc.type_subtype == 4*
Probe Response	*wlan.fc.type_subtype == 5*
Beacon	*wlan.fc.type_subtype == 8*
Authentication	*wlan.fc.type_subtype == 11*

Deauthentication	*wlan.fc.type_subtype == 12*

Ovládací rámce

Ovládací rámce pomáhají při předávání údajů mezi stanicemi a pomáhají omezit kolize.

Request to Send (RTS)	*wlan.fc.type_subtype == 0x1b*
Clear to Send (CTS)	*wlan.fc.type_subtype == 0x1c*
Acknowledgement (ACK)	*wlan.fc.type_subtype == 0x1d*

9.2.3 Zobrazení dat

Pomocí filtrů lze zobrazit i požadované údaje v komunikaci. Např. lze velmi účinně sledovat zabezpečení dat procházejících sítí či stanice, kam tato data směřují. Filtry vybraná data lze velmi snadno analyzovat, z analýzy vyvodit závěry a případná opatření.

Protokol HTTP

Pokud stránka nepoužívá šifrování přenášených dat, lze tato na síti velice snadno sledovat. Obzvláště citlivá data jsou informace o přihlášení, především uživatelské jméno a heslo, které lze po zachycení neoprávněnou osobou zneužít.

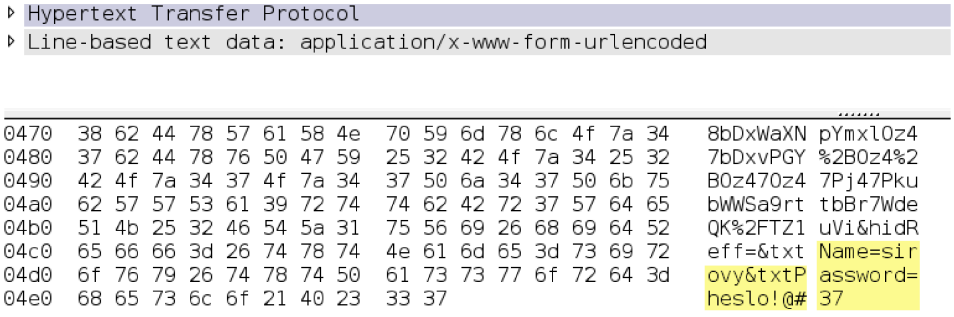
Pomocí jednoduchého filtru lze zobrazit komunikaci přicházející od uživatele, jenž se přihlašuje:

http and ip.src == IP adresa klienta

případně

http and eth.src == MAC adresa klienta

Jak může vypadat uživatelské jméno a heslo zachycené při přihlašování na webovou stránku založenou na technologii ASP, lze vidět na obrázku níže.



Ilustrace 3: Zachycený paket s uživatelským jménem a heslem v prostém textu

Protokol FTP

Obdobně jako u výše zmíněného protokolu http, u protokolu FTP určeného pro přenášení souborů, prochází diskrétní údaje sítí v textové podobě a lze je odchytit a zneužít.

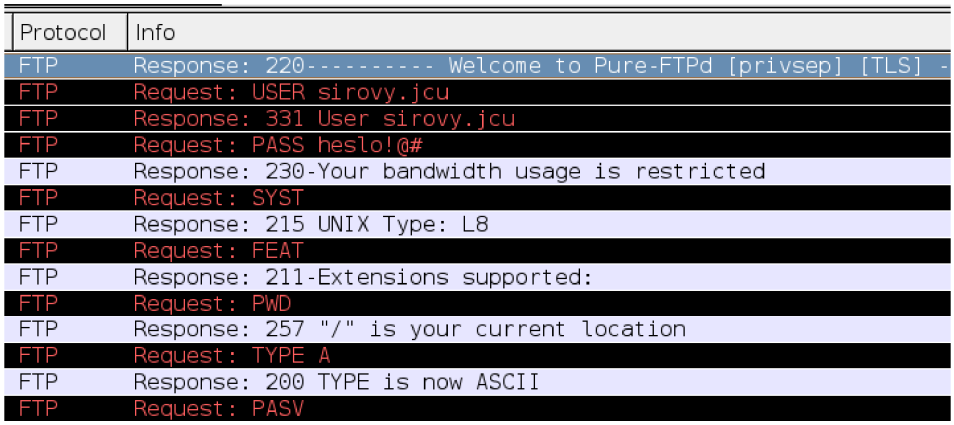
Filtrování lze provést stejně jednoduše jako u protokolu http a zobrazit soukromé údaje přihlašujícího se uživatele pomocí následujících filtrů:

ftp and ip.src == IP adresa klienta

případně

ftp and eth.src == MAC adresa klienta

Na ilustraci č. 4 je vidět proces přihlášení k FTP serveru a výměna údajů mezi klientem a serverem včetně nešifrovaných soukromých údajů.



Protocol	Info
FTP	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] -
FTP	Request: USER sirovy.jcu
FTP	Response: 331 User sirovy.jcu
FTP	Request: PASS heslo!@#
FTP	Response: 230-Your bandwidth usage is restricted
FTP	Request: SYST
FTP	Response: 215 UNIX Type: L8
FTP	Request: FEAT
FTP	Response: 211-Extensions supported:
FTP	Request: PWD
FTP	Response: 257 "/" is your current location
FTP	Request: TYPE A
FTP	Response: 200 TYPE is now ASCII
FTP	Request: PASV

Ilustrace 4: Komunikace při přihlašování na FTP server - uživatelské jméno a heslo v prostém textu

Další protokoly

Obdobně jako výše uvedené protokoly lze sledovat desítky dalších nešifrovaných přenosů soukromých údajů. Z nejznámějších např. chatovací protokol ICQ, poštovní protokoly IMAP, POP3, SMTP a další. Uklidněním pro uživatele je, že většina zmíněných protokolů dostala zabezpečenou alternativu, či možnost použití šifrování. Ovšem problémem je podpora tohoto zabezpečení ze strany serverů, která nebývá pravidlem. Dalším omezením je nutnost výše zmíněné zabezpečení zapnout nebo použít na straně klienta. Používání šifrovaného přenosu bývá u mnoha aplikací a webových stránek ve výchozím nastavení vypnuté.

V kombinaci s nezabezpečenou či slabě zabezpečenou bezdrátovou sítí se

toto nepoužívání šifrovaných přenosů stává velkou a nebezpečnou „trhlinou“ v zabezpečení soukromí uživatelů.

10 Testování zabezpečení bezdrátové sítě

Pro demonstraci různých typů zabezpečení byl vytvořen testovací vysílač (Access point), dále jen AP, který byl postupně nastaven na různé druhy šifrování a metody zabezpečení. K testování sloužilo jako AP zařízení OvisLink AirLive WL-5460AP. K simulaci útočníka byl použit notebook Dell Studio 1535 s operačním systémem Linux distribuce BackTrack 4 beta CZ mód 32bit s USB WiFi adaptérem Edimax EW7318USg s originální všesměrovou anténou. Klienty AP (případné oběti útoku) simulovala zařízení notebook Dell Latitude C500/C600 s operačním systémem Linux distribuce Kubuntu 8.10 32bit s USB adaptérem Asus WL-167g s integrovanou anténou, HP Compaq nx6125 s operačním systémem Windows XP 32bit SP3 s integrovaným bezdrátovým adaptérem Broadcom b/g a mobilní telefon Nokia E71 s integrovaným bezdrátovým adaptérem. U jednotlivých testů jsou uvedeny softwarové nástroje či aplikace, které byly při útoku použity. Postup testování vychází z návodů uvedených v literatuře.

10.1 WEP

První šifrování implementované přímo ve standardu IEEE 802.11. Dnes slouží jako velmi slabé zabezpečení proti útoku na bezdrátovou síť. Šifrování lze velmi snadno prolomit. [11]

Testováváno

➔ útok na 64 bitové WEP šifrování s aktivním klientem útokem hrubou silou a s injekcí paketů.

PROLOMENO

➔ útok na 128bitové WEP šifrování s aktivním klientem útokem hrubou silou a s injekcí paketů.

PROLOMENO

Použité nástroje: balík Aircrack-ng

Vyhodnocení:

Proti prolomení WEP zabezpečení není prakticky obrany a prolomit lze jakkoliv silný klíč. [18]

10.2 WPA, WPA2

Zabezpečení typu WPA je částečnou implementací standardu IEEE 802.11i z roku 2004. Mělo za úkol nahradit již v tehdejší době nedostačující šifrování WEP. [9][10]

Jedním ze zlepšení je zdokonalené šifrování dat prostřednictvím kódování klíčů a přidáním funkce kontroly bezpečnosti. Druhým zlepšením je autentizace uživatele, která obvykle v systému WEP chybí. Obdobně jako WPA i Wi-Fi Protected Access 2 (WPA 2) zajišťuje, že bezdrátové sítě jsou používány pouze oprávněnými uživateli. Certifikované produkty

WPA2 jsou založené na standardu IEEE 802.11i. WPA 2 se od WPA odlišuje tím, že využívá pokročilý standard šifrování AES (Advanced Encryption Standard), který poskytuje silnější šifrování požadované některými uživateli z řad velkých firem a státních institucí. [1]

Testováno

zabezpečení typu WPA-PSK následujícími útoky:

➔ útok slovníkového typu na klíč

PROLOMENO

➔ Útok zachycením handshake a následným porovnáním kontrolních součtů (hashů)

PROLOMENO

Testováno

zabezpečení typu WPA2-PSK následujícími útoky:

- ➔ útok slovníkového typu na klíč - slabý klíč

PROLOMENO

- ➔ útok slovníkového typu na klíč - silný klíč

NEPROLOMENO

Použité nástroje: Wireshark, balík Aircrack-ng, Cowpatty, genpmk

Vyhodnocení:

Proti slovníkovému útoku se lze účinně bránit volbou silného klíče. Proti útoku se zachyceným handshake jako takovému není příliš účinná obrana. Řešením je použitím nestandardního SSID a velmi silného klíče. Pro obecné zvýšení odolnosti zabezpečení proti útoku je použití šifrování AES či použití autorizačního serveru Radius a certifikátů. [14][15][16] [17][18]

10.3 Skryté SSID

Mnoho správců přístupových bodů považuje za zabezpečení nebo zvýšení zabezpečení zakázaní vysílaní SSID informace. Toto je jen velmi slabá ochrana před napadením sítě, především je-li na sítí připojen klient a probíhá na síti komunikace. Tento způsob ochrany sítě lze považovat spíše za drobnou komplikaci pro útočníka než za zabezpečení.

Testováno

➔ připojení k jinak nezabezpečenému AP se skrytým SSID názvem


PROLOMENO

Použité nástroje: Wireshark, Kismet

Vyhodnocení:

V kombinaci s jiným zabezpečením, ať výše či níže uvedeným, lze uvažovat, že určitým způsobem bude útočníkovi ztížen útok. Jako samostatná metoda tato funkce ve smyslu zabezpečení bezdrátové sítě selhává.[18]

10.4 Filtrování MAC adres na AP

Nastavení filtrování dle MAC adres přináší obdobně jako výše uvedené skrytí SSID informace falešný pocit zabezpečení. Navzdory tomu, že MAC adresa síťové karty nebo bezdrátového adaptéru by měla být jedinečná, není za pomoci jednoduchých nástrojů problém pro útočníka tuto adresu změnit či podvrhnout. Útočník musí ovšem znát MAC adresu autorizovaného klienta, kterou poté podvrhne AP jako svojí.

Testováno

➔ připojení k jinak nezabezpečenému AP s nastavením autorizovaných MAC adres a aktivním klientem.

PROLOMENO

Použité nástroje: Wireshark, Kismet, Airodump-ng

Vyhodnocení:

Zabezpečení AP pouze seznamem MAC adres, které mohou k tomuto AP přistupovat, lze považovat za velmi slabé. Použití daného způsobu obrany před napadením sítě lze uvažovat pouze v kombinaci s dalšími prvky zabezpečení. Ovšem ne pouze s výše uvedeným skrytím SSID informace.[18]

10.5 Shrnutí

Jako nejúčinnější ochranu před napadením a zneužitím bezdrátových sítí lze tedy považovat použití WPA2. Pro domácí či kancelářské použití s autentizací pomocí PSK a šifrováním AES-CCMP. Za předpokladu dobře zvoleného silného klíče, který nebude prolomen slovníkovým útokem nebo útokem „hrubé síly“. Pro podniky pak použití autentizace dle standardu IEEE 802.1x a šifrování opět AES-CCMP. Pro zajištění co nejvyšší bezpečnosti používat pro datový provoz na bezdrátové sítí šifrovaný tunel.

11 Porovnání zabezpečení bezdrátových sítí

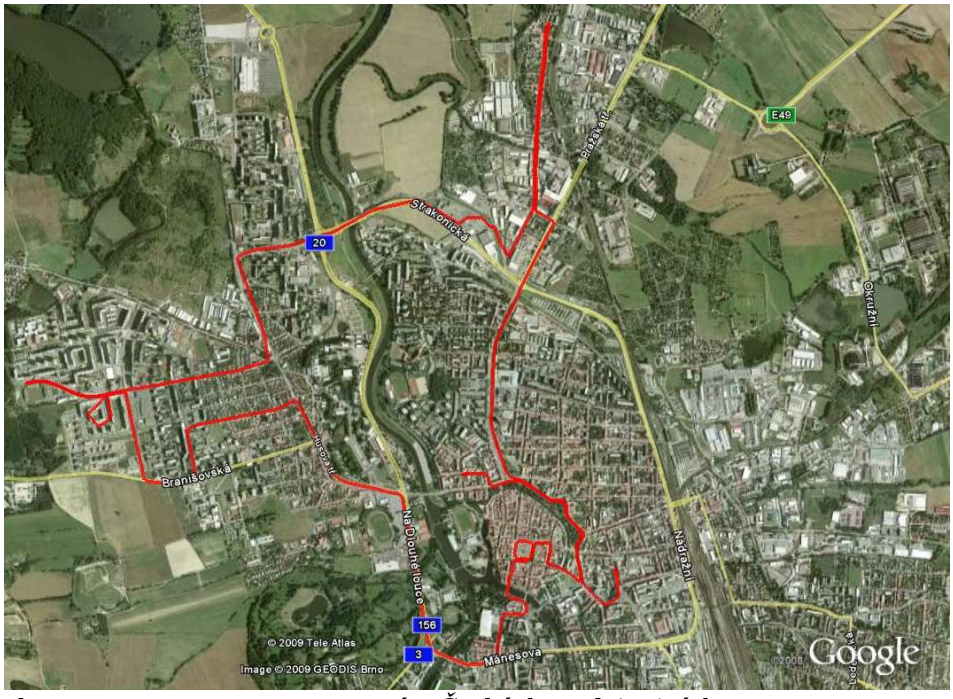
V následující části se práce zabývá praktickým porovnáním zabezpečení bezdrátových sítí. Lokality pro měření byly vybrány s ohledem na umístění univerzity a mé bydliště. Lokalitou pro první měření bylo zvoleno krajské město Jihočeského kraje České Budějovice[5] (dále jen: ČB). Toto město má dle [26] k roku 2001 necelých 100 000 obyvatel. Lokalitou druhého měření bylo zvoleno okresní město Český Krumlov[6] (dále jen: ČK) vzdálený cca 25km jižně od Českých Budějovic. Počet obyvatel ČK je dle [26] k roku 2001 14 443. V ČK bylo měření zaměřeno také na průmyslovou zónu Tovární ulice, kde sídlí všechny velké firmy z ČK. Měření v obou zmíněných lokalitách bylo provedeno v březnu 2009 a bylo zaměřeno na bezlicenční frekvenční pásmo 2,4GHz.

11.1 Postup

Měření probíhalo pomocí osobního automobilu projíždějícího lokalitami rychlostí do 50 km/h s umístěnou všesměrovou anténou na střeše vozidla a vnitřní všesměrovou anténou integrovanou v bezdrátovém adaptéru umístěném v interiéru vozidla v blízkosti čelního skla. V případě upřesňujícího měření v průmyslové zóně ČK byla použita panelová anténa zaměřená na objekty budov jednotlivých firem. Ke zpracování dat z antén byly použity bezdrátové adaptéry Asus WL-167g a Edimax

5 http://www.c-budejovice.cz
6 http://www.ckrumlov.info

EW7318USg. Oba adaptéry byly připojeny do notebooku Dell Studio 1535. Jako softwarové vybavení bylo použito v operačním systému Windows Vista Home Premium 32bit program Inssider, dále pomocí virtualizace byl použit operační systém Linux BackTrack 4 beta CZ mód 32bit s programy Kismet a Wireshark. Při zachytávání byla zároveň zaznamenávána GPS data s informacemi o trase. Tato data byla poté zobrazena pomocí aplikace Google Earth.



Ilustrace 5: Mapa trasy měření v Českých Budějovicích

Trasa měření v ČB vedla centrem i okrajovými částmi a několika sídlišti. Přesná trasa měření v ČB je viditelná na ilustraci 5. Trasa měření v ČK

vedla převážně centrem, okrajovými částmi a několika sídlišti. Do trasy byla zahrnuta i průmyslová zóna v Tovární ulici. Přesná trasa měření v ČK je viditelná na ilustraci 6. Detailnější obrázky map obou tras je možné nalézt v přílohách 1 a 2.

Ilustrace 6: Mapa trasy měření v Českém Krumlově

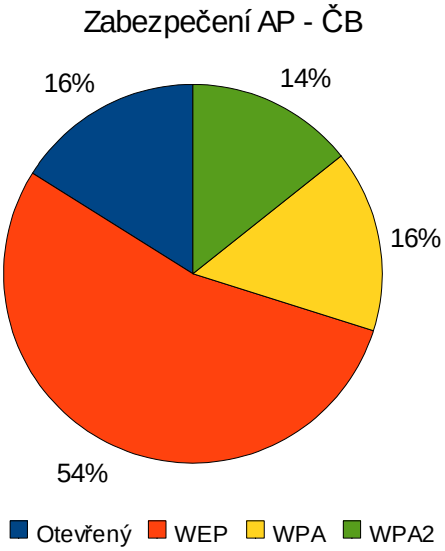
11.2 Zpracovaní získaných dat

Naměřená data byla postupně zpracována do tabulek pomocí tabulkového procesoru a pomocí filtrů byly získány detailní informace o zaznamenaných bezdrátových sítích. Tyto informace byly rozděleny podle posuzovaných kritérií a následně porovnány s výsledky měření na druhé trase a s výsledky měření uváděnými výše. Informace o zastoupení výrobců AP byly zjištěny podle jedinečné adresy vysílače BSSID. Tato adresa byla porovnána s databází[7] výrobců zařízení. Do hodnocení bylo pro možnost porovnání s předchozím měřením zahrnuto prvních 17 výrobců, kteří měli největší zastoupení po sečtení všech adres.

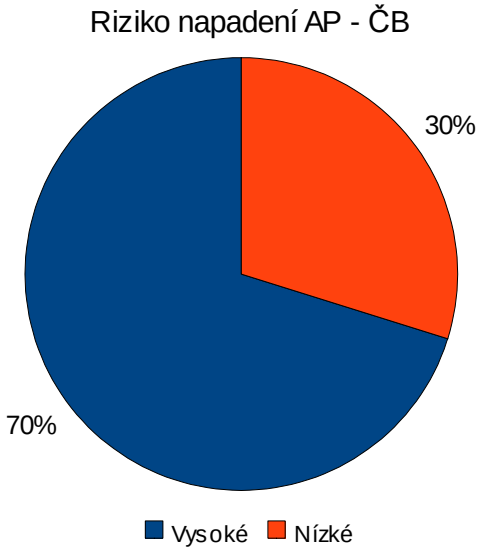
11.3 Vyhodnocení

Celkově během měření v lokalitě Českých Budějovic bylo zaznamenáno 727 jedinečných bezdrátových sítí. Z toho 117 (16 %) z nich nepoužívalo žádné zabezpečení zjistitelné tímto měřením. Celkem 393 (54 %)sítí používalo již zastaralé zabezpečení technologií WEP. Lepší zabezpečení typu WPA bylo použito u 113 (16 %). U celkem 104 (14 %) zaznamenaných sítí bylo použito zabezpečení typu WPA2. Sečteme-li nezabezpečené sítě a sítě používající slabé WEP zabezpečení vychází orientační údaj o počtu sítí s vysokým rizikem napadení. V případě Českých Budějovic je až 70 % naměřených sítí potenciálně velmi snadno napadnutelných.

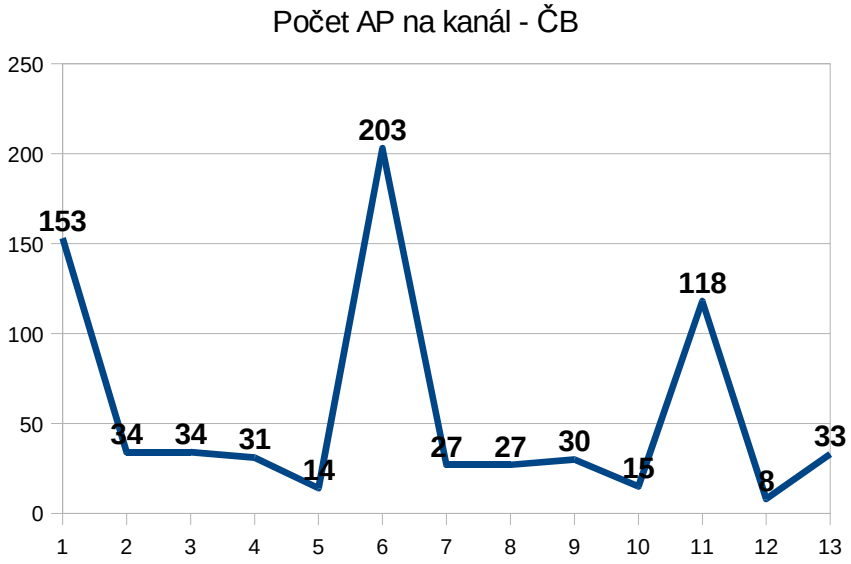
7 http://standards.ieee.org/regauth/oui/oui.txt



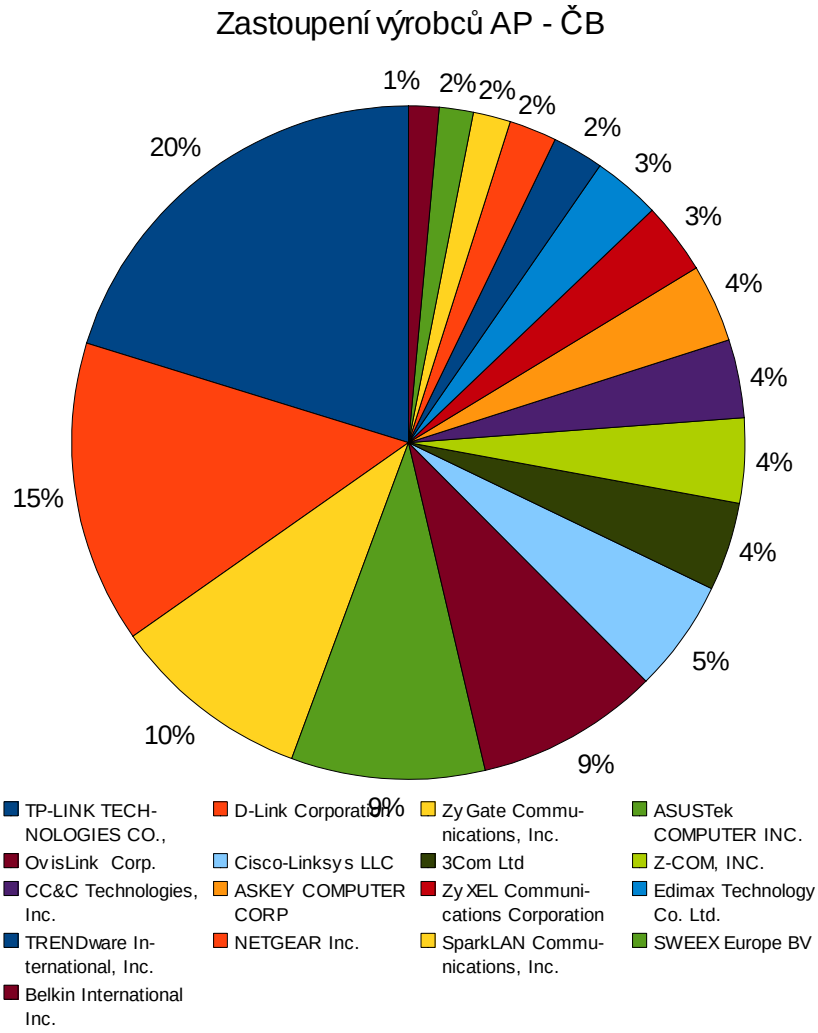
Graf 5: Podíl typu zabezpečení AP v Českých Budějovicích



Graf 6: Podíl rizika napadení AP v Českých Budějovicích



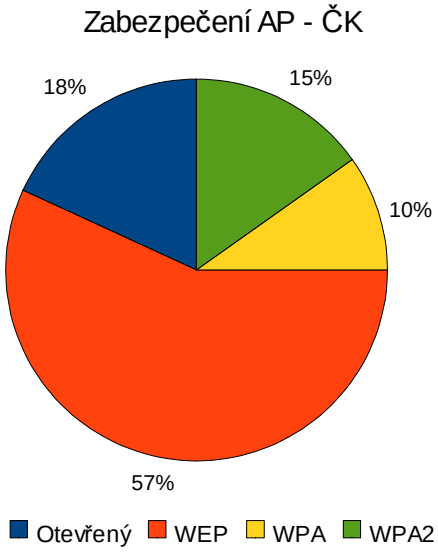
Graf 7: Počet AP na kanál pásma v Českých Budějovicích



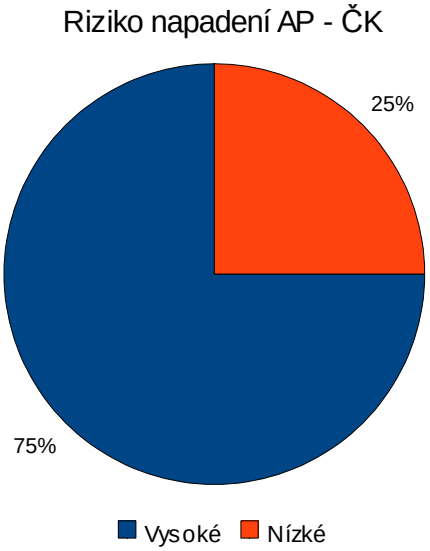
Graf 8: Podíl výrobců AP v Českých Budějovicích

Během měření v lokalitě Českého Krumlova bylo zaznamenáno celkem 336 jedinečných bezdrátových sítí. Z toho 61 (18 %) z nich nepoužívalo

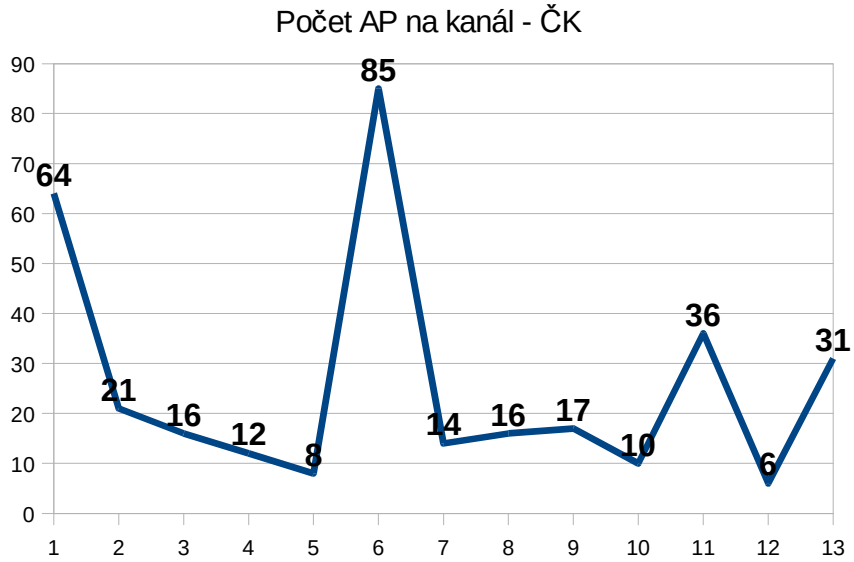
žádné zabezpečení zjistitelné tímto měřením. Celkem 191 (57 %)sítí používalo již zastaralé zabezpečení technologií WEP. Lepší zabezpečení typu WPA bylo použito u 33 (10 %) sítí. U celkem 51 (15 %) zaznamenaných sítí bylo použito zabezpečení typu WPA2. Po sečtení nezabezpečených sítí a sítí používající slabé WEP zabezpečení lze získat orientační údaj o počtu sítí s vysokým rizikem napadení bezdrátové sítě. V případě Českého Krumlova je až 75 % naměřených sítí potenciálně velmi snadno napadnutelných.



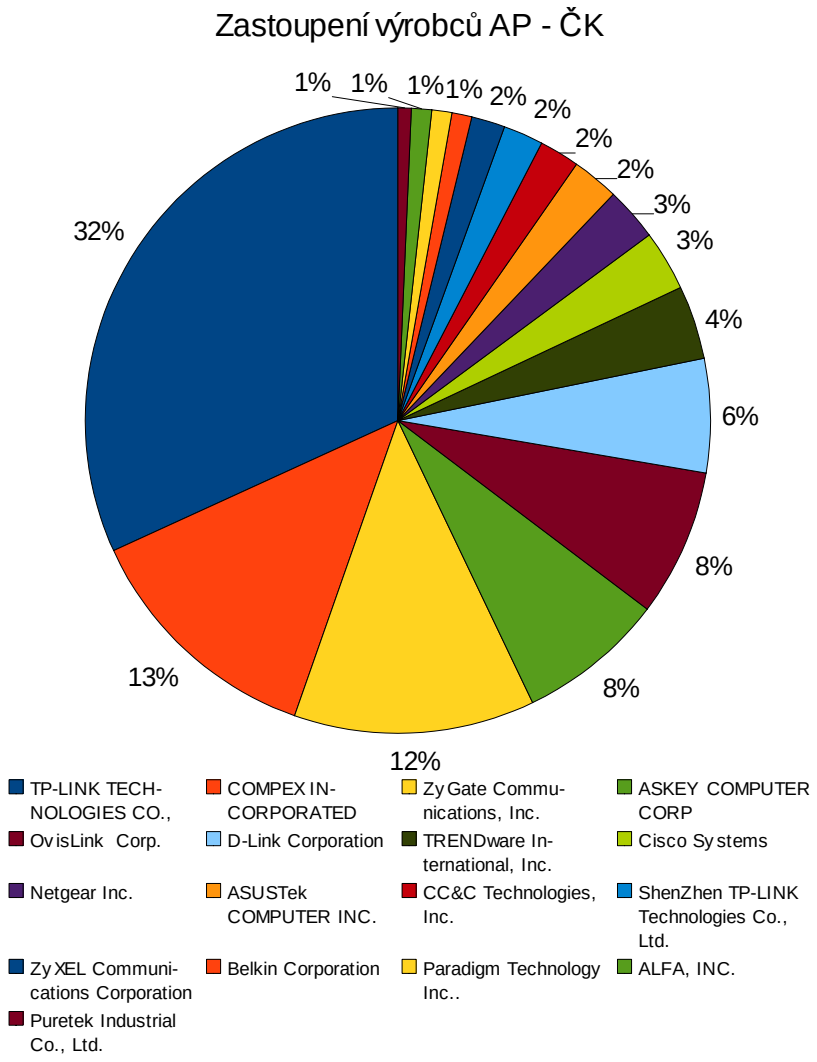
Graf 9: Podíl typu zabezpečení AP v Českém Krumlově



Graf 10: Podíl rizika napadení AP v Českém Krumlově



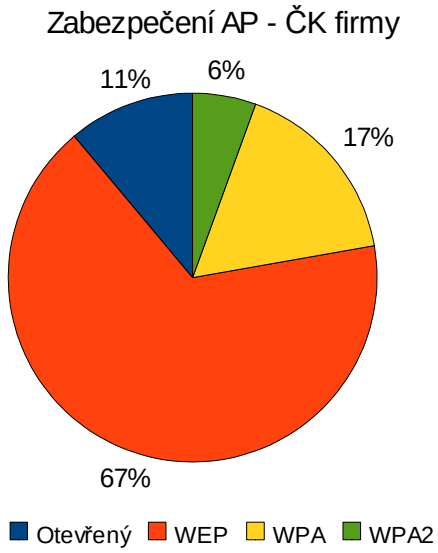
Graf 11: Počet AP na kanál pásma v Českém Krumlově



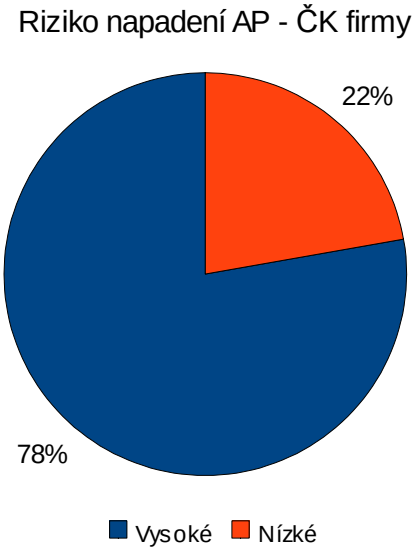
Graf 12: Podíl výrobců AP v Českém Krumlově

V Českém Krumlově byla část měření zaměřena také na zabezpečení firemních bezdrátových sítí. Výsledkem tohoto měření je zjištění, že

z celkových 18 jedinečných bezdrátových sítí nepoužívají žádné tímto měřením zjistitelné zabezpečení pouze 2 (11 %) sítě. Ovšem 12 (67 %) bezdrátových sítí používá slabé zabezpečení typu WEP. Zabezpečení pomocí WPA používají 3 (17 %) zachycené sítě. Překvapivě pouze 1 (6 %) síť používá silné zabezpečení typu WPA2. Vysoké riziko teoretického napadení sítě připadá na 78 % sítí.

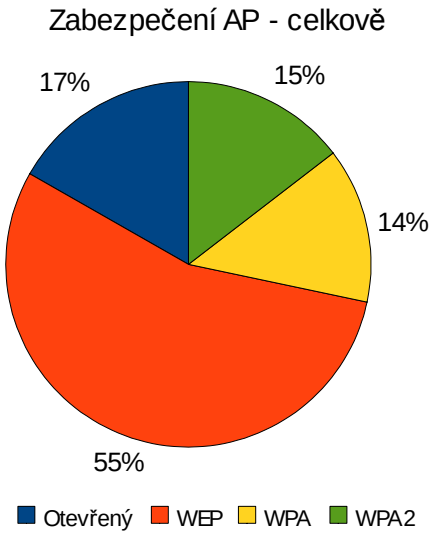


Graf 13: Podíl typu zabezpečení AP firem v Českém Krumlově

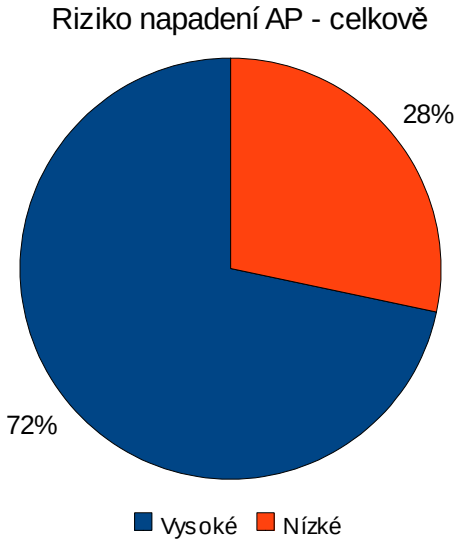


Graf 14: Podíl rizika napadení AP firem v Českém Krumlově

Celkem tedy bylo tedy během všech měření zaznamenáno 1063 jedinečných bezdrátových sítí. Z celkového počtu jich nepoužívalo 178 (17 %) žádné zabezpečení. Celkem 584 (55 %) stanic používalo slabé zabezpečení WEP. Celkem 146 (14 %) sítí používalo jako zabezpečení WPA. Nejmodernější technologií zabezpečení bezdrátových sítí WPA2 používalo pouze 155 (15 %) sítí. Při sečtení sítí používajících jako zabezpečení WEP a sítí nepoužívajících žádné zabezpečení vychází hrozivé číslo 762 (72 %) potenciálně velmi snadno napadnutelných bezdrátových sítí.



Graf 15: Podíl typu zabezpečení AP celkově



Graf 16: Podíl rizika napadení AP celkově

11.4 Závěr porovnání

Vyhodnocením měření byla většina předpokladů potvrzena. Předpoklad, že více než polovina přístupových bodů bude používat zabezpečení se potvrdil. Celkově využívá zabezpečení 83 % zachycených bezdrátových sítí. Tento předpoklad se potvrdil i pro jednotlivé lokality měření. V lokalitě ČB používá zabezpečení 84 % a v lokalitě ČK 82 %. Ze srovnání s měřením z roku 2008 uvedeným ve teoretické části této problematiky vyplývá, že z provedeného měření je o 10 % více sítí zabezpečeno. Toto zvýšení lze zdůvodnit meziročním nárůstem zabezpečených sítí či větším výskytem veřejných bezdrátových sítí v měřených lokalitách Prahy.

Dalším potvrzeným předpokladem je to, že u více než poloviny zabezpečených sítí bude používáno slabé zabezpečení typu WEP. Tento předpoklad byl potvrzen výsledky pro celkové měření 66 %. Pro jednotlivé lokality byly zjištěny tyto výsledky. V lokalitě ČB byl tento předpoklad potvrzen zjištěním 64 % sítí a v lokalitě ČK až 69 % sítí. Celková naměřená hodnota je o 9 % vyšší oproti měření uvedené v úvodu do problematik. Jednoznačně zdůvodnit toto rozšířenější použití zabezpečení typu WEP nelze. Lze spekulovat o používaní většího počtu modernějších zařízení podporující novější zabezpečení v lokalitách Prahy.

Předpoklad o podílu výrobců se potvrdil jen z části. Společnost D-Link je druhou nejčetnější značkou s 15 % z počtu AP v lokalitě ČB. V lokalitě

ČK je až šestou nejčetnější s 6 % z počtu AP. Firma Cisco je v lokalitě ČB šestá nejčetnější firma s 5 % z počtu AP, a v lokalitě ČK je až osmá se 3 % z počtu AP. Největší zastoupení v obou lokalitách má firma TP-LINK TECHNOLOGIES CO., LTD. V lokalitě ČB tuto firmu zastupuje celých 20 % z celkového počtu AP a v lokalitě ČK až 32 % z celkového počtu AP.

Dalším předpokladem který se potvrdil, je očekávané zabezpečení firemních bezdrátových sítí. Tento předpoklad se sice potvrdil z pohledu jakéhokoli zabezpečení, a to 89 % z celkového počtu firemních bezdrátových sítí, ale překvapivě ze 75 % z počtu zabezpečených firemních sítí k zabezpečení používá slabé zabezpečení WEP. Lze ale předpokládat, že tyto sítě používají šifrování na přenášených datech, či šifrování pomocí VPN tunelu.

Posledním očekávaným předpokladem je rozložení počtu bezdrátových sítí po frekvenčním pásmu. Jak je jednoznačně z výše uvedených grafů patrné, tento předpoklad se potvrdil. Zajímavé je rozložení počtu bezdrátových prvků ke konci pásma. Konkrétněji tedy mezi 11. a 13. kanálem. Dle [27] se v USA a Kanadě používá pouze 11 kanálů. To vede k určité nekompatibilitě ze strany klientských zařízení. Proto někteří správci přístupových bodů nastavují maximálně 11. kanál. Případně některé AP vůbec možnost vysílat na vyšším kanálu než jedenáctém nepodporují. Proto jsou na grafu číslo 11 viditelné dva horní okraje frekvenčního pásma v podobě počtu AP.

12 Závěr

Práce nakonec splnila všechny předem stanovené cíle.

Mnoho předpokladů práce bylo potvrzeno, ale nastaly i nepředpokládané komplikace. První skutečností je, že po zadání práce byla vydána publikace v českém jazyce (Viz [2]), která kompletně mapuje použití a teorii paketového analyzátoru sítí Wireshark. Nicméně ani tento fakt nedegradoval v práci popsané rady a doporučení pro praktické použití Wiresharku. Výše popsaný návod může sloužit jako úvod do problematiky používání tohoto analyzátoru. Komplikací spíše technického směru byla výroba držáku všesměrové antény na automobil, která nakonec dopadla úspěšně.

Práce byla také rozšířena o porovnání dostupných síťových analyzátorů. Výsledek daného porovnání, jak je již uvedeno výše, potvrdil široké možnosti použití a očekávanou kvalitu programu Wireshark. V porovnání lze však najít i jiné velmi kvalitní nástroje pro specifické použití při síťové analýze. Testování odolnosti zabezpečení bezdrátové sítě proti napadení v simulovaných testovacích podmínkách přineslo poměrně překvapivá zjištění o tom, jak snadno lze různé ochrany prolomit. Testování také přineslo celkový souhrn informací o možnosti prolomení zabezpečení bezdrátových sítí a údaje, jak tomuto prolomeni předcházet. Porovnání zabezpečených bezdrátových sítí ve vybraných lokalitách také splnilo většinu očekávaných předpokladů. Je však nutno podotknout, že porovnávání zabezpečení bezdrátových sítí na základě odezvy s

informací od AP dané sítě nemusí být úplně přesné. Existují metody, které provoz dat na sítí dělají bezpečnější a tímto způsobem měření nejsou zjistitelné. Především jimi jsou již zmiňované VPN tunely a jiné druhy šifrování přenosu. Ovšem i tak má většina takto zjištěných informací velkou informativní hodnotu o nízkém zabezpečení bezdrátových sítí v porovnávaných lokalitách. Osobně jsem předpokládal, že počet zabezpečených sítí nebo sítí používající silnější zabezpečení bude mnohem více. Výše uvedené výsledky jsou podle mého názoru až alarmující.

Seznam použité literatury

[1] Ernst & Young. *Průzkum bezpečnosti bezdrátových sítí v Praze a Bratislavě 2008*. [s.l.] : [s.n.], 2008. 22 s.

[2] OREBAUGH, Ramirez, et al. *Wireshark a Ethereal : Kompletní průvodce analýzou a diagnostikou sítí*. 2008. vyd. [s.l.] : Computer press, 2008. 448 s.

[3] *Connect! : Není datům v síti těsno?*. 2004- , roč. 2005, č. 11- . CZ : 2005- . ISSN 1211-3085.

[4] *Analýza sítě* [online]. [2008] [cit. 2009-03-02]. Dostupný z WWW: <http://www.computerhelp.cz/sluzby/analyza/default.asp>.

[5] *Wireshark:About* [online]. [2008] [cit. 2008-11-20]. Dostupný z WWW: <http://www.wireshark.org/about.html>.

[6] Chapter 1. Introduction [online]. c2004-2008 [cit. 2009-03-02]. Dostupný z WWW: <http://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html>.

[7] *1.5. A brief history of Ethereal* [online]. c2004-2005 [cit. 2009-03-02]. Dostupný z WWW: <http://www.ethereal.com/docs/eug_html_chunked/ChIntroHistory.html>.

[8] LODL , Jan. Víte, kdo vidí vaše soubory? Hacker testoval bezpečnost Wi-Fi sítí. *Idnes.cz* [online]. 2007 [cit. 2009-02-15]. Dostupný z WWW: <http://technet.idnes.cz/vite-kdo-vidi-vase-soubory-hacker-testoval-bezpecnost-wi-fi-siti-pxu-/sw_internet.asp?c=A070307_163712_bezpecnost_lhc>.

[9] *WPA2* [online]. 2008 [cit. 2009-03-15]. Dostupný z WWW: <http://wiki.airdump.cz/WPA2>.

[10] *Wireless Protected Access* [online]. 2008 [cit. 2009-03-15]. Dostupný z WWW: <http://wiki.airdump.cz/WPA>.

[11] *Wired Equivalent Privacy* [online]. 2008 [cit. 2009-03-15]. Dostupný z WWW: <http://wiki.airdump.cz/WEP>.

[12] STRAND, Lars. *802.1X Port-Based Authentication HOWTO* [online]. 2004 [cit. 2009-03-08]. Dostupný z WWW: <http://tldp.org/HOWTO/html_single/8021X-HOWTO/>.

[13] PUŽMANOVÁ , Rita. *WLAN konečně bezpečné* [online]. 2004 [cit. 2009-03-08]. Dostupný z WWW: <http://www.lupa.cz/clanky/wlan-konecne-bezpecne/>.

[14] *Prolomení WPA zabezpečení* [online]. [2008] [cit. 2009-03-02]. Dostupný z WWW:

<http://airdump.cz/crack-wpa-zabezpeceni/>.

[15] *TKIPtun-ng - První implementace útoku na WPA-TKIP šifrování* [online]. [2008] [cit. 2009-03-02]. Dostupný z WWW: <http://airdump.cz/tkiptun-ng-prvni-implementace-utoku-na-wpa-tkip/>.

[16] *Alternativa coWPAtty Plus a genPMK Plus - návod* [online]. [2008] [cit. 2009-03-02]. Dostupný z WWW: <http://airdump.cz/alternativa-cowpatty-plus-genpmk-plus-navod/>.

[17] *WiFi Crack WPA Handshake* [online]. [2008] [cit. 2009-03-02]. Dostupný z WWW: <http://airdump.cz/wifi-crack-wpa-handshake/>.

[18] *Hacking WiFi sítí* [online]. 2008 [cit. 2009-02-15]. Dostupný z WWW: <http://wiki.airdump.cz/Hacking_WiFi_sítí>.

[19] *Top 11 Packet Sniffers* [online]. [2006] [cit. 2008-11-11]. Dostupný z WWW: <http://sectools.org/sniffers.html>.

[20] *Selecting a protocol analyzer* [online]. 10/08/01 [cit. 2008-12-08]. Dostupný z WWW: <http://www.networkworld.com/columnists/2001/1008helpdesk.html>.

[21] *Networking* [online]. c2001-2009 [cit. 2008-12-10]. Dostupný z WWW: <http://linux.softpedia.com/get/System/Networking/>.

[22] KALEEM, Zaib . *RFMON at WLAN* [online]. c2008 [cit. 2009-03-02]. Dostupný z WWW: <http://www.wlanbook.com/rfmon-monitor-mode/>.

[23] *Co umí vaše WiFi karta* [online]. [2008] [cit. 2009-03-02]. Dostupný z WWW: <http://airdump.cz/wifi-sniffing-monitor-mode/>.

[24] *Sniffing hesel LAN a WLAN sítě* [online]. [2008] [cit. 2009-03-02]. Dostupný z WWW: <http://airdump.cz/sniffing-hesel-lan-a-wlan-site/>.

[25] *How 802.11 Wireless Works* [online]. March 28, 2003 [cit. 2009-03-15]. Dostupný z WWW: <http://technet.microsoft.com/en-us/library/cc757419.aspx>.

[26] *Úvodní stránka, krajská reprezentace České Budějovice Český statistický úřad - ČESKÉ BUDĚJOVICE* [online]. c2009 [cit. 2009-03-14]. Dostupný z WWW: <http://www.czso.cz/xc/edicniplan.nsf/o/13-3104-04--2__obyvatelstvo>.

[27] GRYGAREK. *Rádiové sítě IEEE 802.11 (WiFi)* [online]. 2004 [cit. 2009-03-15]. Dostupný z WWW: <http://www.cs.vsb.cz/grygarek/LAN/lect/WiFi.pdf>.

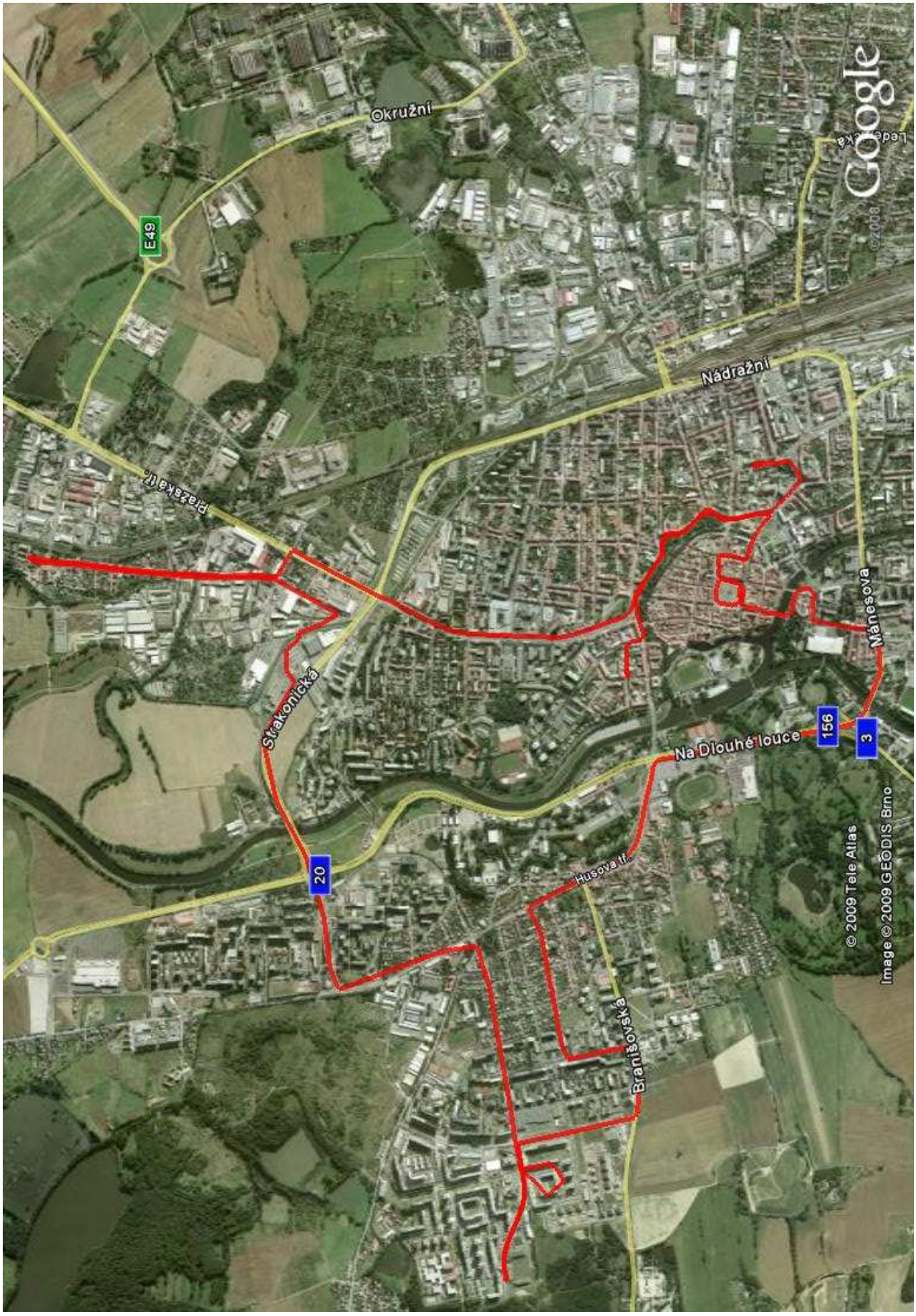
Seznam ilustrací

Seznam tabulek

Seznam grafů

Seznam příloh

Příloha 2 - Mapa trasy měření lokality Český Krumlov



Příloha 2 - Mapa trasy měření lokality Český Krumlov