Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta

BAKALÁŘSKÁ PRÁCE

Miroslav Přitasil

PROBLEMATIKA ZABEZPEČENÍ BEZDRÁTOVÝCH SÍŤÍ

Vedoucí bakalářské práce: Ing. Michal Šerý

Studijní předmět: MVT/KS

2007

Na tomto místě bych rád poděkoval vedoucímu bakalářské práce Ing. Michalovi Šerému za pomoc a komentáře. Firmě KP NETWORK spol. s r.o. za odbornou konzultaci založenou na dlouholetých zkušenostech.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Českých Budějovicích dne 15.11.2007

Miroslav Přitasil

Obsah:

1 Úvod

S rozvojem IT techniky, masivním nástupem moderních telekomunikačních technologií a jejich cenovou dostupností se tato zařízení stávají samozřejmou součástí našeho všedního života. Tím vzrůstá požadavek a nároky na jejich šířku, kvalitu, bezpečnost a okamžitou dostupnost přenášených dat. Díky tomuto trendu se požadavky na mobilitu spojení stupňují a do praxe vstupují bezdrátové přenosy.

Bezdrátové sítě jsou významnou součástí datových sítí obecně. Jejich přenosové rychlosti se dnes již blíží přenosovým rychlostem sítí LAN. Velkou výhodou je nižší pořizovací náklad v porovnání s kabelovými rozvody. Nezanedbatelnou výhodou bezdrátového přenosu, v porovnání s metalickými sítěmi, jsou především vzdálenosti přenosu dosažitelné touto technologií a možností jejich použití v prostředí, kde není možné instalovat pevný rozvod.

Bezdrátové sítě si však našly své uplatnění i v mnoha jiných oblastech. Jsou to především firemní sítě, kam bezdrátová technologie vnesla jisté pohodlí a komfort práce, domácnosti, kde je použita pro svou snadnou instalaci a cenovou dostupnost, v mobilních telekomunikacích nebo v Čechách hojně používána menšími lokálními poskytovateli internetu ISP (internet service provider).

Na rozdíl od pevných LAN síti zde vzniká problém s ochranou přenášených dat. Je to především proto, že data volně přenášená vzduchem je možné v dosahu sítě odposlechnout nebo jinak zneužít. Sítě bývají často proti těmto jevům nedostatečně zabezpečeny. Instalace v domácnostech jsou prováděny nepříliš zručnými uživateli svépomocí a často zařízení nechávají v režimu továrního nastavení s vypnutými ochrannými prvky. Ani ve firemních

sítích nebývá výjimkou nedostatečné zabezpečení a to především pro podcenění nebezpečí zneužití a nižší znalost dané problematiky lokálními správci sítí.

Problematiky zabezpečení jsou si vědomi i vývojáři přenosových systémů. V současné době je k dispozici několik typů a možností zabezpečení, popsaných v poměrně dobře zpracované a dostupné české i světové literatuře.

2 Princip bezdrátového přenosu

Elektromagnetické pole může ve vodiči indukovat proud a naopak, toho se využívá při bezdrátovém přenosu. Elektromagnetické vlnění mohou pohlcovat molekuly, přijatá energie se bude přeměňovat na teplo (princip mikrovlnné trouby).

2.1 Vznik elektromagnetického záření

Jakýkoli elektrický náboj pohybující se s nenulovým zrychlením vyzařuje elektromagnetické vlnění. Prochází-li vodičem (nebo jiným vodivým předmětem, např. zářičem antény) střídavý elektrický proud, vyzařuje elektromagnetické záření o frekvenci proudu.

Vlastní přenos energie je v případě elektromagnetického záření zajišťován změnami elektromagnetického pole. Přenos energie tedy není zajištěn prostřednictvím pohybujících se elektronů (takové záření se označuje jako záření beta), ale prostřednictvím časových a prostorových změn elektromagnetického pole. Tyto změny spojuje kvantová teorie s fotony, tzn. elektromagnetické záření lze označit za usměrněný pohyb fotonů. Vlnový charakter elektromagnetického záření udává vlnová délka, frekvence a rychlost šíření, tedy fázová rychlost, která je ve vakuu rovna rychlosti světla ve vakuu. Elektromagnetické záření se projevuje jako vlnění se všemi jevy spojenými s vlněním, např. interference vlnění, disperze apod. především pro dlouhé vlnové délky, např. rádiové záření, infračervené záření, světlo a ultrafialové záření. Na elektromagnetické záření se dá nahlížet jako na vlnu nebo proud částic (fotonů).

Zdroj: http://cs.wikipedia.org/wiki/Elektromagnetické_záření

2.2 Rádiové záření (rádiové vlny)

- je částí spektra elektromagnetického záření s vlnovými délkami od 1 milimetru až po tisíce kilometrů. Slouží především ke komunikaci, a to v mnoha různých podobách. Následující tabulka zobrazuje rozdělení rádiových vln na jednotlivá pásma a jejich využití:

Název pásma	Zkratka	Značení ITU	Frekvence Vlnová délka	Příklady využití
			< 3 Hz > 100,000 km	
Extrémně nízká frekvence	ELF	1	3–30 Hz 100,000 km – 10,000 km	Komunikace s ponorkami
Super nízká frekvence	SLF	2	30–300 Hz 10,000 km – 1000 km	Komunikace s ponorkami
Ultra nizká frekvence	ULF	3	300–3000 Hz 1000 km – 100 km	Komunikace v dolech
Velmi nízká frekvence	VLF	4	3–30 kHz 100 km – 10 km	Komunikace s ponorkami, bezdrátové měřiče pulsu
Nízká frekvence	LF	5	30–300 kHz 10 km – 1 km	Navigace, časové signály, AM vysílání (dlouhé vlny)
Střední frekvence	MF	6	300–3000 kHz 1 km – 100 m	AM vysílání (střední vlny)
Vysoká frekvence	HF	7	3–30 MHz 100 m – 10 m	Krátkovlnné vysílání a amatérské rádio
Velmi vysoká frekvence	VHF	8	30–300 MHz 10 m – 1 m	FM rádiové a televizní vysílání
Ultra vysoká frekvence	UHF	9	300–3000 MHz 1 m – 100 mm	Televizní vysílání, mobilní telefony, Wi-Fi, komunikace typu země-vzduch nebo vzduch-vzduch
Super vysoká frekvence	SHF	10	3–30 GHz 100 mm – 10 mm	Mikrovlnná zařízení, Wi-Fi, většina moderních radarů
Extrémně vysoká frekvence	EHF	11	30–300 GHz 10 mm – 1 mm	Radioastronomie, vysokorychlostní mikrovlnný přenos dat
	IR		Více než 300 GHz < 1 mm	Noční vidění - infračervené spektrum

Zdroj: http://cs.wikipedia.org/wiki/rádiové_vlny

2.3 Vliv počasí

Mikrovlnné spoje mohou bez problémů fungovat při dešti, sněžení či mlze. To však neznamená, že na vlivech počasí závislé nejsou. Vzduch, podobně

jako kov při metalických vedeních, není ideálním přenosovým médiem a způsobuje utlumení signálu. Dalším parametrem, který způsobuje tlumení, je počasí. Zvýšená vlhkost, případně déšť zvyšují tlumení. Vliv počasí na míru tlumení je výraznější při vyšších frekvencích nad 10 GHz. S růstem počtu mikrovlnných spojů přibyl i další faktor – interference z jiných spojů. Proto je důležité dodržovat dohodnuté rozdělení frekvencí na národní i mezinárodní úrovni: Pásma 4-6 GHz a 11 GHz jsou vyhrazena pro dálkové mikrovlnné spoje. Pásmo 12 GHz je určeno pro přenos TV signálů do sítí kabelové televize (CATV). 22 GHz mikrovlnné spoje na krátké vzdálenosti. 10 GHz místní distribuce dat. Zbylá pásma slouží pro další uživatele (vláda, policie, soukromý sektor).

3 Bezdrátová technologie a její přehled

Pro bezdrátový přenos dat v dnešní době existuje mnoho technologií. Hlouběji se budu zabývat pouze technologiemi, které se nejvíce používají, tedy ty, které stojí na otevřených standardech.

3.1 Technologie Wi-Fi

3.1.1 Historie

Wi-Fi (Wireless Fidelity) – souhrnný název pro sítě, které jsou založeny na standardu IEEE 802.11, vytvořený společností IEEE (Institute of Electrical and Electronics Engineers). Původně byla technologie Wi-Fi určena pro vnitřní použití a pro mobilitu zařízení v kancelářských prostorách. Pro její cenovou dostupnost a nedostatek jiných vhodných technologií se v našich podmínkách stala jistou náhradou méně dostupných služeb DSL. Technologie Wi-Fi se

přesunula s pomocí externích antén do volného prostoru, kde dokázala vytvořit spoje na vzdálenost několika km.

V roce 1997 byla vydána původní verze standardu 802.11 ("legacy"), která byla označována jako 802.1y. Tento standard specifikoval přenos dat elektromagnetickým vlněním v bezlicenčním pásmu 2,4-2,4835 GHz, nebo v infračerveném pásmu a to rychlostí 1 Mb/s a 2 Mb/s.V roce 2000 masově nastupuje technologie Wi-Fi na standardu IEEE 802.11b pracující taktéž v pásmu 2,4 GHz a na dalších 5 let se stane nejpoužívanějším způsobem připojení k internetu pro domácnosti i firmy.

Vzhledem k tomu, že technologie Wi-Fi byla vyvinuta pouze pro vnitřní využití a její nárůst použití byl velice dynamický a to hlavně pro vnější použití, dostává se v mnoha případech do nečekaných problémů. Na území velkých aglomerací dochází k rušení moha vysílacích bodů, čímž se její spolehlivost snižuje a stává se až nepoužitelnou. Český telekomunikační úřad (ČTÚ) povoluje na této frekvenci vysílat pouze ve třinácti kanálech, které se na vzájem překrývají. Velkým zájmem uživatelů o toto pásmo dochází k vzájemnému překrývání frekvencí vysílání a následnému rušení, kterému se lze jen obtížně vyhnout.

Stoupajícími nároky uživatelů na šířku datového pásma se tento standard stává nevyhovujícím. Proto přichází nástupce této technologie standard IEEE 802.11g. Standard slibuje vyšší přenosové rychlosti, větší objem přenesených dat, ale pracuje ve stejném frekvenčním pásmu jako standard předešlý, tudíž je v našem zarušeném prostředí opět těžko použitelný. Proto pro potřeby trhu a na četné žádosti uživatelů ČTÚ v roce 2004 uvolňuje další pásmo a to 5 GHz (5,1-5,9 GHz). V tuto chvíli ustoupily používané standardy standardu IEEE 802.11a a to hlavně pro vyšší povolené vysílací výkony, větší šířku datového pásma a nezarušené frekvence.

Tím nastoupila druhá generace Wi-Fi. Avšak i ta se stává v současné době nepoužitelnou a to ze stejných důvodů jako předešlá generace. Z bezdrátových sítí se tvoří metropolitní sítě, kde se ISP snaží minimalizovat bezdrátové spoje a jsou nahrazovány spolehlivými metalickými nebo optickými sítěmi.

Zdroj: http://www.security-portal.cz/clanky/wifi-site-a-jejich-slabiny.html

3.1.2 Přehled standardů IEEE 802.11

IEEE 802.11 - Původní standard pro 1 a 2 Mbit/s rychlost s frekvencí 2.4 GHz (1999)
IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, produkty od 2001)
IEEE 802.11b - Vylepšení 802.11 s podporou 5.5 a 11 Mbit/s (1999)
IEEE 802.11c - Bezdrátové přemostění (bridge); obsaženo v IEEE 802.1D standardu (2001)
IEEE 802.11d - Mezinárodní roamingový dodatek (2001)
IEEE 802.11e - Vylepšení QoS, včetně dlouhých (burst) paketů (2005)
IEEE 802.11F - Komunikace mezi bezdrátovými přístupovými body (2003). Stažen v březnu 2006.
IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (zpětně kompatibilní s 802.11b) (2003)
IEEE 802.11h - Správa spektra 802.11a (5 GHz) pro Evropu (2004)
IEEE 802.11i - Vylepšený autentifikační a šifrovací algoritmus (WPA2) (2004)
IEEE 802.11j - Dodatek pro Japonsko; nové frekvenční pásma pro multimedia (2004)
IEEE 802.11k - Vylepšení správy rádio zdrojů pro vysoké frekvence. (Navazuje na IEEE 802.11j)
IEEE 802.11l - (rezervováno a nebude použito)
IEEE 802.11m - Správa standardu: přenosové metody a drobné úpravy.
IEEE 802.11n - Vylepšení pro vyšší datovou propustnost

IEEE 802.11o - (rezervováno a nebude použito)
IEEE 802.11p - Bezdrátový přístup pro pohyblivé prostředí (auta, vlaky, sanitky)
IEEE 802.11q - (rezervováno a nebude použito, aby se nepletlo s 802.1Q)
IEEE 802.11r - Rychlé přesuny mezi přístupovými body (roaming)
IEEE 802.11s – Samostatně se organizující bezdrátové sítě. (ESS Mesh Networking)
IEEE 802.11T - Předpověď bezdrátového výkonu - testovací metody
IEEE 802.11u - Spolupráce se sítěmi mimo 802 standardy (například s mobilními sítěmi)
IEEE 802.11v - Správa bezdrátových sítí (konfigurace klientských zařízení během připojení)
IEEE 802.11w - Chráněné servisní rámce
IEEE 802.11x - (rezervováno a nebude použito)
IEEE 802.11y - Pro běh ve frekvenčním pásmu 3650 - 3700 MHz (veřejné pásmo v USA)

Pojem 802.11x je neformálně používán k označení libovolného 802.11 standardu. (Standard IEEE 802.1X pro řízení přístupu k síti založený na autentifikaci a filtrování portů, běžně nesprávně označován jako 802.11x.)

802.11F a 802.11T jsou samostatné dodatky k IEEE 802.11 standardu označené velkým písmenem.

3.1.3 Jednotlivé standardy

IEEE 802.11 – je původní standard vytvořený v roce 1997, pracoval v pásmu 2,4 GHz a jeho rychlost byla 1 Mb/s a 2 Mb/s.

IEEE 802.11a – tento standard vyšel o 2 roky později oproti původnímu standardu 802.11, tedy v roce 1999, pracuje v pásmu 5 GHz a jeho nejvyšší rychlost dosahuje 55 Mb/s.

IEEE 802.11b – byl stejně jako předchozí standard uveden na trh v roce 1999, ale pracuje jako původní produkt ve stejném pásmu. 2,4 GHz. Jeho nejvyšší přenosová rychlost dosahuje 11Mb/s.

IEEE 802.11c - je Wi-Fi standard pracující s přemosťováním v bezdrátových zařízeních. Jde o hotový produkt doplňující standard IEEE 802.1d. Je doplněný o požadavky na přemosťování Media Access Control (MAC), což je podvrstva linkové vrstvy. Standard IEEE 802.1d upravuje základní LAN standard pro 802.11 rámce.

IEEE 802.11d - je Wi-Fi standard, často nazývaný také jako globální harmonizační standard. Je používaný v zemích, kde nejsou povoleny systémy využívající jiné dodatky k IEEE 802.11 standardu. Liší se v povolených frekvencích, vyzařovacích výkonech a propustnosti signálu. Specifikace eliminuje nutnost vývoje a výroby vybraných produktů pro různé země. Zapnutím podpory pro IEEE 802.11d v přístupovém bodě se začne vysílat do celé sítě (broadcastovat) ISO kód země, ve které se nachází jako součást svých beacon paketů a požadavků na odpověď. Pokud je zapnut, zařízení klienta přizpůsobí své frekvence, vyzařovací výkon a propustnost sítě. Standard je tak vhodný pro systémy, které chtějí poskytovat globální roaming.

IEEE 802.11e - je Wi-Fi doplněk standardu IEEE 802.11 vylepšující takzvanou Media Access Control (MAC) podvrstvu linkové vrstvy rozšířením podpory kvalitu služeb (Quality of Service, QoS). Standard je důležitý pro aplikace citlivé na zpoždění, jako jsou Voice over Wireless IP a proudová multimédia.

IEEE 802.11g – uvedení na trh v roce 2003. Pracuje v pásmu 2,4 GHz a jeho nejvyšší přenosová rychlost je podobně jako u standardu 802.11a až 54 Mb/s. Princip přenosu je stejný jako u 802.11a, pouze pro přenos používá více kanálů (větší přenesená šířka datového pásma).

IEEE 802.11h – inteligentnější standard, vydán v roce 2004. Je doplňujícím standardem IEEE 802.11a a je určen pouze pro evropské podmínky a to především pro vytváření spojů mezi budovami. Řeší problémy rušení signálu s ostatními zařízeními, které pracují na stejné frekvenci principem dynamického výběru kanálu. Využívá pásmo 5 GHz.

IEEE 802.11n – tento standard byl vylepšen o vyšší datovou propustnost. Jeho nejvyšší přenosová rychlost by měla dosahovat až 300 Mb/s (reálná přenosová rychlost pro vnitřní použití je 70 Mb/s) pracuje v pásmech 2,4 GHz a 5 GHz. Tato technologie využívá vylepšeného algoritmu se třemi výstupními anténami.

Zdroj: http://cs.wikipedia.org/wiki/IEEE_802.11

3.2 Bluetooth

Technologie bluetooth slouží k připojení bezdrátových zařízení. Stejně jako technologie Wi-Fi pracuje na frekvenci 2,4 GHz. Rychlost přenosu dat dosahuje 1 Mb/s. Pro nízké přenosové rychlosti a úzké specifikaci využití, je tato technologie vhodná pouze pro vnitřní použití. Je především používána pro datové přenosy na velmi krátké vzdálenosti mezi mobilními zařízeními. Například u mobilních telefonů nebo příslušenství k PC.

V dnešní době není problém zapojení bezdrátové klávesnice, myši či jiné periférie k počítači. U mobilních telefonů se hojně používá pro příjem hovorů nebo přenos datových souborů mezi nimi.

Pro zabezpečení bluetooth komunikace je používán 128 bitový klíč, který se pro bezpečné spojení odvozuje ze dvou shodných PIN kódů vložených v obou koncích chráněného spojení (tzv. párování). Pro šifrování dat je použita celkem slabá šifra.

3.2.1 Slabiny a útoky na bluetooth

V některých „zastaralých“ mobilních telefonech mohou nastat chyby v implementaci bluetooth, což má za následek, že některý z útočníků bez Vašeho vědomí stáhne veškerá uložená data, jako například – kontakty v telefonním seznamu, SMS zprávy, informace a upomínky v kalendáři. Těmto amatérským náhodným útokům se říká Bluesnarfing.

Vážnější nedostatek v tomto druhu spojení odhalili vědci Avishai Wool a Yaniv Shaked z univerzity v Tel Avivu. Dokázali, že párování lze vynutit kdykoliv. Jedno ze zařízení zašle druhému zprávu, že došlo ke ztrátě klíče. Na základě této chybové zprávy musí párování proběhnout znovu. V praxi to znamená, že pokud dokážete vygenerovat chybovou zprávu o ztrátě klíče, dokážete se spojit s libovolným zařízením.

Dalším problémem jsou některé bluetooth karty v PC, které mají větší náchylnost na útok známým virem Cabir, který se poprvé objevil asi před třemi lety. Scénář útoku byl vyzkoušen na nádraží, kde byla infikována periférie s technologií Bluetooth. Ta poté infikovala další periférie. Složitější bylo přinutit počítače, aby se útočníkovi ohlásily zpátky. I to se posléze podařilo.

Útok byl vyzkoušen italskou laboratoří BlueBag, která byla společně financována firmami Secure Networks a F-Secure.

Zdroj: http://www.dsl.cz/clanky-dsl/clanek-457/Wi-Fi-otevira-dvirka-pro-hackery

Toto nebyl jediný důkaz o citlivosti technologie Bluetooth k útokům hackerů. Před rokem byla prokázána možnost spojení s hands-free systémy v autech používaných k odposlechu hovorů. Za tímto účelem byl napsán software se jménem Car Whisperer, který využíval nedostatečného zabezpečení programů výrobci aut.

K zabránění zneužití přenášených dat nechte raději Vaše bluetooth v mobilním telefonu vypnuté a zapínejte je pouze v době, kdy zařízení využíváte. Vzhledem k tomu, že dosah signálu není velký, čímž se snižuje i pravděpodobnost útoku. Ovšem při použití kvalitní externí antény lze provést útok na Vaše zařízení až na vzdálenost jednoho kilometru.

3.3 Mobilní sítě

3.3.1 Historie

Mobilní sítě a jejich technologie se dělí do několika generací:

1. generace (1G) – analogová generace, která byla určena pro hovorové přenosy. Tato generace nahradila vývojovou generaci radiotelefonů, která nebyla v Evropě v praxi použita. Mezi evropské nejrozšířenější standardy patřil Nordic Mobile Telefone 450 a 900 (označen NMT450 a NMT900), jejichž označení 450 a 900 znamenalo označení kmitočtového pásma ve kterém pracovaly. Tedy 450 MHz a 900 MHz. První mobilní síť v České republice vybudovala na tomto standardu firma Eurotel na počátku 90. let. V první

generaci bylo časem u novějších zařízení umožněno jako nadstandard přijímání a odesílání zpráv SMS (short message service – krátká textová zpráva). Jejich signál se přijímal zpočátku dlouhými vysouvacími anténami, díky nimž se signál zvýšil až na dvojnásobek. S kvalitnějším pokrytím se zkracovaly i antény.

Zabezpečení těchto prvních analogových telefonů nebylo takřka žádné. Hovory bylo možno odposlouchávat vlastní rádio stanicí na uvedeném pásmu. Pro rychlý rozvoj a lepší zabezpečení nastupuje druhá generace (2G).

Standardy a frekvence evropských sítí 1. generace:

Označení standardu:	**Kmitočtové pásmo:**
C-Netz (C-450)	450 Mhz
Comvik	450 Mhz
TACS	900 Mhz
ETACS	900 Mhz
NMT450	450 Mhz
NMT900	900 Mhz
NMT900	900 Mhz
RTMS	450 Mhz

2. generace (2G) – je generace pro Evropu se standardem GSM, která kromě hovorových přenosů umožňuje i přenos dat rychlostí 14,4 kbps. V České republice byla tato síť uvedena do provozu v roce 1996. Pro rychlejší přenos dat se začala používat technologie GPRS (General Packet Radio Services), která pracuje na tzv. „paketovém přenosu dat“.

U GPRS není garantovaná rychlost připojení, díky tomu, že GPRS využívá volného slotu v síti GSM. To znamená že, přednost mají nejprve hovory a následně datové přenosy. Rychlost přenosu se pohybuje maximálně do 160 kbps. Po technologii GPRS přichází datový přenos pomocí technologie EDGE (Enhanced Data Rates for Global Evolution), jak již z názvu vyplývá, zařízení

je konstruováno pro „vylepšenou propustnost a pro globální evoluci“. EDGE pracuje 3x vyšší rychlostí než GPRS a to maximálně 480 kbps.

Slabina v zabezpečení sítí GSM je jednostranná autentizace (autentizován je tedy uživatel, nikoliv síť). V praxi to znamená, že je teoreticky možné vlastní základovou stanicí (BTS) odposlechnout cizí hovor nebo data. Další slabinou je pak malá délka šifrovacího klíče (64bit).

3. generace (3G) – koncem roku 2005 byla u nás spuštěna síť 3. generace, síť UMTS (*Universal Mobile Telecommunications System*). Oproti GSM a GPRS systému přináší UMTS pro uživatele více možností. Síť je například připravena na přenos videohovorů, uživatel může telefonovat a současně využívat datové přenosy. Tato služba nebyla dříve možná, vzhledem k reálné rychlosti, která se pohybovala kolem 2 Mbps (v budoucnu se má pohybovat až kolem 14 Mbps).

Oproti síti GSM zde bylo zabezpečení řešeno celkem kvalitně pomocí mechanismu „výzva-odpověď“. Odpověď vypočte čipová sada SIM pomocí uloženého klíče, který nelze z karty přečíst bez speciálního hardwaru. Tímto řešením a prodloužením šifrovacího klíče byly odstraněny slabiny GSM sítě.

3.4 WiMAX

WiMAX jako jedna z nejmodernějších technologií vyvinutá pro ISP v masovém použití, využívá již vyspělé technologie zabezpečení. Je založeno na autentizaci na bázi veřejného klíče (*PKI, Public-Key Infrastructure*), kdy komunikující strany používají pro vzájemnou autentizaci digitální certifikáty od třetí důvěryhodné strany.

3.4.1 Autentizace a autorizace

WiMAX základnová stanice se autentizuje klientskou stanicí pomocí digitálního certifikátu X.509, který obsahuje MAC adresu zákaznické stanice a veřejný klíč. Tímto certifikátem se identifikuje klientská stanice. Všechny zákaznické stanice mají z výroby instalované páry veřejných/privátních klíčů RSA a instalované certifikáty X.509. Díky těmto certifikátům je velmi těžké zfalšovat identitu klientské stanice Po počáteční autorizaci se musí zákaznická stanice pravidelně reautorizovat při čemž se obnovuj stárnoucí šifrovací klíče, které mají pouze časově omezenou platnost. V rámci (re)autorizace pošle zákaznická stanice žádost *authorization request*, v níž žádá o autorizační klíč (AK) a také o identifikátor bezpečnostní asociace SAID (*Security Association IDentifier*). Žádost obsahuje digitální certifikát stanice a informaci o šifrovacích algoritmech, které stanice podporuje a zároveň identifikátor spojení (*CID, Connection IDentifier*), který základna stanici přidělila v rámci počátečního přidružení. Na základě této žádosti základnová stanice ověří identitu stanice, určí šifrovací algoritmus a protokol, aktivuje AK pro stanici, zašifruje AK veřejným klíčem stanice a pošle zpět v odpovědi *authorization reply*. V té ještě specifikuje životnost klíče a 4bitové pořadové číslo klíče, kterým se rozlišuje mezi generacemi autorizačních klíčů. Další následující generace klíčů AK má takovou životnost, že se jejich platnost překrývá. Je to z důvodu vyloučení přerušení služby během reautorizace.

3.4.2 Slabiny a útoky na WiMAX

Zásadním problémem WiMAXu je jednostranná autentizace ze strany klientské stanice. Naopak základnová stanice klientskou stanicí autorizována není. Tento stav může teoreticky vést k mnoha bezpečnostním problémům. WiMAX sítě jsou proto náchylné k útokům realizovaným prostřednictvím

neautorizovaných základnových stanic, které mohou vystavit uživatele nepříjemným útokům, stejně jako v sítích GSM viz 3.3.

Zdroje:
http://www.dsl.cz/clanek-11/Bude-WiMAX-konkurencí-xDSL%3F-Cast-I
http://www.wimax.cz/index.php?option=com_content&task=view&id=172&Itemid=33

4. Zabezpečení Wi-Fi sítě a její metody

V současné době existuje mnoho způsobů, jak zabezpečit bezdrátovou síť proti vnějšímu napadení. Jedná se o různé druhy jednoduchých metod, které zvládnou prolomit i zkušenější uživatelé, přes různé moderní šifrovací algoritmy, až po specializovaný hardware určený pro zvýšení zabezpečení.

Veškeré screany a testy nastavení byly vyzkoušeny na nejpoužívanějších Access Pointech (AP) v Čechách, vysílajících ve volném pásmu 2,4 GHz Ovislink 1020 a dále pak na operačních systémech Microsoft.

Pro úplnost následujícího textu bych rád popsal průběh připojení klienta k AP. Připojení klienta probíhá ve 2 krocích, autentizace a asociace, pomocí management rámců. Při použití WPA/WPA2 viz 4.1.4 následují po asociaci ještě další kroky používající datové rámce a to především vygenerování šifrovacího klíče.

Access pointy vysílají v pravidelných intervalech zpravidla v desítkách až stovkách ms management beacon, což je rámec prozrazující potencionálním klientům podporované možnosti zabezpečení (např. WPA, WEP atd.), podporované rychlosti, číslo kanálu a může obsahovat i SSID access pointu, jehož znalost musí klient prokázat při asociaci k AP. Klient nemusí pouze pasivně poslouchat beacon rámce, aby se dozvěděl, jaké AP jsou k dispozici a co uvést v association request. Může aktivně poslouchat broadcastem rámec

probe request. Access pointy v dosahu, na takový požadavek odpovídají probe requestem, který obsahuje informace nutné pro asociaci stejně jako beacon.

Zdroj: https://dip.felk.cvut.cz/ browse/pdfcache/kolarj6_2007bach.pdf

4.1 Zabezpečení sítě z WF strany

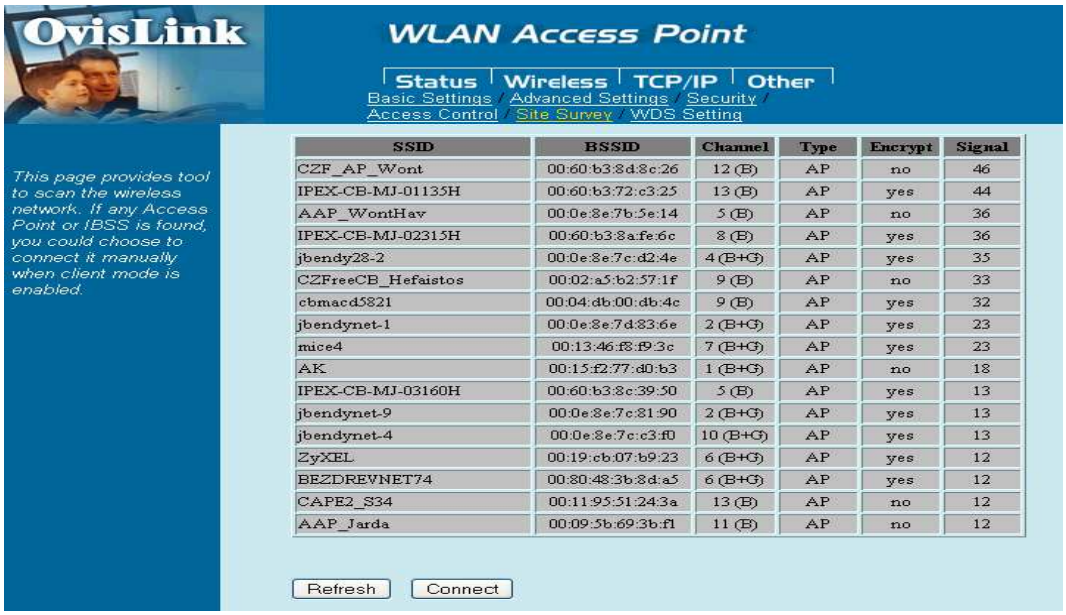
4.1.1 Skrytí SSID (Service Set Identifier)

Jedná se o textový identifikátor bezdrátové sítě, díky němu se připojuje klient do každé bezdrátové sítě (Wi-Fi). Přístupový bod ve výchozím nastavení pravidelně vysílá své SSID a tím ohlašuje svoji přítomnost, viz Obr.1.

Tímto se ohlašují i útočníkovi, který vůbec nemusí hledat přístupové body. Ty se mu totiž nabízí samy. Nabízí mu své SSID, které stačí k připojení do sítě, bez použití zabezpečení. Vysílací AP lze však nakonfigurovat tak, aby své SSID nevysílal. Skrytí SSID umožňují všechny hardwarové Access Pointy .

Zablokování vysílání SSID sice porušuje standard, ale je nejjednodušším zabezpečením bezdrátové sítě pomocí jejího zdánlivého skrytí. Princip spočívá v tom, že klientská síť se nezobrazí v seznamu dostupných bezdrátových sítí. Obr.1, protože klienti nepřijímají vysílané informace o SSID. Při připojování klienta k přípojnému bodu je SSID přenášen v otevřené podobě a lze ho tak snadno zachytit. K zachytávání SSID při asociaci klienta s přípojným bodem se používá i provokací, kdy útočník do bezdrátové sítě vysílá rámce, které přinutí klienty, aby se opět asociovali.

Zdroj:http://www.owebu.cz/wifi/vypis.php?clanek=1067



Obr.1 Dostupné SSID

Útok

Jestliže Access Point nebude vysílat své SSID, nebude ani odpovídat na probe rámce. Proto musí klient SSID znát. Probe rámec je rámec vysílaný klientem při hledání přístupového bodu. Obsahuje informaci o SSID a o podporovaných rámcích. Po připojení klienta k Access Pointu posílá v otevřené podobě SSID v asociačním rámci. Útočník tedy může počkat, až se některý klient pokusí o připojení k Access Pointu a tím SSID odposlechnout. SSID umí zjistit ze zachycených rámců program Kismet. Je to univerzální nástroj, který vyhledává a odposlouchává bezdrátové sítě. Nové spojení a vyslání probe rámce lze vynutit restartem jednoho z asociovaných klientů a to buď hardwarově, nebo softwarově na dálku.

Shrnutí

Pokud není připojen klient do sítě, nemůže útočník zjistit ani SSID. V případě připojení klienta do sítě, útočník nemá problém s odhalením SSID. V některých případech ale tato metoda může pomoci i celkovému zabezpečení sítě a to například v domácích sítích nebo. v sítích, které se využívají jen výjimečně.

4.1.2 WEP (Wired Equivalent Privacy)

Zabezpečení pomocí SSID viz 3.1.1 a MAC a 3.2.1 je nedostačující, proto byl v roce 1999 u zařízení splňující standard 802.11b vypracován nový šifrovací protokol. Ten je založen na šifrovacím algoritmu RC4 (technologie RC4 od laboratoře RCA) s tajným statickým klíčem o velikosti 40 nebo 104 bitů kombinovaným s 24 bitovým inicializačním vektorem IV. Algoritmus RC4 generuje náhodnou posloupnost, která se pomocí operace XOR slučuje s daty. Pro ověření správnosti používá metodu CRC-32 kontrolního součtu. Nový šifrovací algoritmus měl zamezit odposlechu síťového provozu. (Wired Equivalent Privacy = bezpečný jako kabel).

WEP zajišťuje šifrování rámců na druhé síťové vrstvě. Šifruje tedy veškeré rámce (blok binárních dat), které vedou od klienta k AP a ne pouze vybrané služby. Pokud je však AP připojen do Internetu, tak mezi AP a internetovým serverem šifrování neprobíhá.

Odesílatel i příjemce musí mít stejný klíč používaný k šifrování/dešifrování komunikace. Pro vyšší bezpečnost je nutné klíč průběžně obměňovat. To ale WEP ani RC4 sám o sobě nijak neřeší. Jediný možný způsob změny je opětovné nahrazení stávajícího klíče v konfiguraci adaptéru. To u distribuce

klíčů může znamenat bezpečností riziko, protože případný útočník může nový klíč při předání získat.

Šifra RC4 byla použita zejména proto, že ji lze snadno implementovat do hardwaru bezdrátových adaptérů a díky tomu nemá aktivování šifrování téměř žádný vliv na výkon počítače.

Někteří výrobci chrání přístup ke klíči ve speciální paměti síťové karty (NVRAM), kde změny nelze provést bez znalosti hesla. Bohužel tímto způsobem nepostupují všichni. Klíč může být uložen např. v registrech a to v otevřené podobě.

Zdroj: http://www.security-portal.cz/clanky/wifi-site-a-jejich-slabiny.html

Shrnutí

Autentizace:

Nevýhodou je jednostranná autentizace. Uživatel nemá jistotu, že se připojuje k autorizovanému přístupovému bodu (prostor pro falešné AP). Klíč podporuje jen autentizaci zařízení, nikoli uživatele, krádež zařízení znamená krádež klíče (po zlomení klíče je třeba provést přenastavení všech zařízení). Autentizace sdíleným klíčem zvyšuje možnost odchycení a zlomení klíče (výzva i odpověď mezi klientem a AP se posílají v otevřené formě) nulová autentizace je paradoxně z hlediska bezpečnosti u WEP lepší variantou.

Šifrování:

Jak již bylo řečeno slabinou je stejný klíč na všech zařízeních v téže síti (sdílený klíč). Tento statický a krátký klíč – IV (Initialization Vector) o 24 bitech se sice mění s každým paketem, ale v reálném čase se opakuje (slabý šifrovací mechanismus RC4).

Ve velkých sítích nastává nemalý problém s distribucí klíčů. Manuální distribuce a změny WEP klíčů v rozsáhlých sítích jsou velice obtížné jelikož WEP nepodporuje automatickou změnu klíčů.

Zdroj: http://www.lupa.cz/clanky/bezpecnost-wifi-zalezi-jen-na-vas/

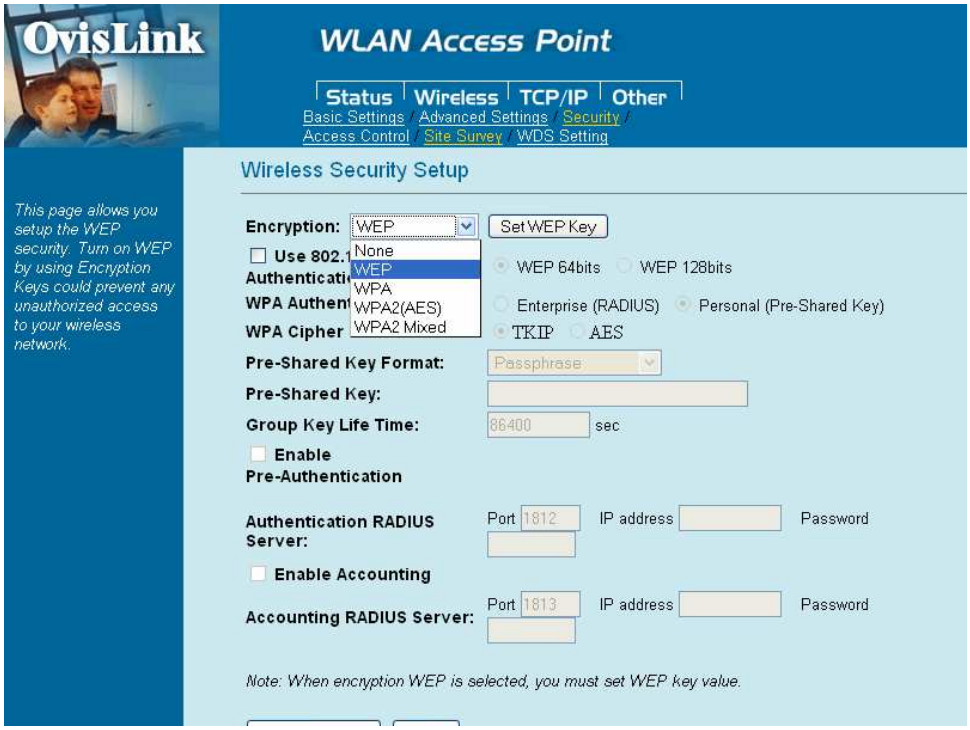
Největší problém standardu WEP tedy tkví ve způsobu distribuce klíče. Dalším problémem je také jeho délka. WEP definuje délku klíče pouze 40 bitů. Někteří výrobci sice začali používat vlastní šifry o délce 128 nebo 256 bitů, ale to může způsobit nekompatibilitu výrobků od různých výrobců.

Zdroj: http://bezdratovesite.wz.cz/#_Toc170470628

Slabiny a útoky na WEP

Standard WEP je pro kvalitní zabezpečení sítě nedostačující. Je to způsobeno zranitelností šifrovacího algoritmu RC4, který se stal díky délce klíče a kolizím v síti snadno rozluštitelným pomocí dostupných odposlouchávacích zařízení.

V dnešní době se nedoporučuje toto zabezpečení ani pro domácí potřeby. K prolamování tohoto typu zabezpečení již existuje velké množství programů a to jak v prostředí Linuxu, tak i Microsoft Windows. Pokud se někdo rozhodne napadnout síť zabezpečenou pouze přes WEP, je jen otázkou několika hodin než se mu to podaří. S odstupem času je možné WEP chápat jako narychlo implementovanou metodu šifrování, která měla alespoň částečně řešit otázku bezpečnosti a to i přes to, že se už od září 1995 ví o zranitelnosti RC4.



Obr.2 Nastavení standardu zabezpečení

Jak vůbec tedy funguje autentizace?

Nejdříve klient pošle Access Pointu požadavek na připojení, následně pošle Access Point výzvu o délce 128 bitů zpět klientovi. Tuto výzvu klient zašifruje WEP klíčem a zvoleným IV a pošle Access Pointu. V posledním kroku Access Point provede stejné šifrování a s přijatou zprávou výsledek porovná.

Autentizace 802.1x

Ověřování 802.1x je standard IEEE pro ověřený přístup ke kabelovým sítím Ethernet a bezdrátovým sítím 802.11. Standard ověřování IEEE 802.1X podporuje centralizovanou identifikaci uživatelů, ověřování, dynamickou správu klíčů a účtování. 802.1X zvyšuje zabezpečení tím, že povoluje ověření mezi počítačem a sítí, generuje podle uživatele nebo relace klíč, který slouží

k šifrování dat v bezdrátových připojeních a umožňuje dynamickou výměnu klíčů. Ověřování 802.1x je doporučeno použít při každém připojení k bezdrátové síti 802.11. Připojíme-li se k bezdrátové síti s ověřováním 802.11 a nepovolí se ověřování 802.1x, budou odesílaná data vystavena vyššímu nebezpečí útoků, například analýze provozu sítě v režimu offline a změnám paketů a dat (bit flip) uživateli se zlými úmysly.

Zdroj: http://technet2.microsoft.com/WindowsServer/cs/Library/ff7c2ac9-5db3- 4b71-a31b-9604dce0b2171029.mspx?mfr=true

Protokol 802.1x ve spojení s protokolem EAP (Extensible Authentication Protocol) umožňuje bezpečnou výměnu dat mezi klientem a domovským radius serverem přes přístupové body nebo switche a ostatní radius servery sítě. EAP protokol zajistí přenos přihlašovacích údajů až na domácí radius server, který autentizuje uživatele. O výsledku je informován přístupový prvek, který poté uživatele vpustí do sítě nebo naopak zamítne přístup. Jakýkoliv radius server nebo přístupový bod předávající požadavek dál, viděl klientovo uživatelské heslo.

Důležitou vlastností EAP ve spojení s radius infrastrukturou je ustavení bezpečného (šifrovaného) kanálu mezi klientem a cílovým radius serverem. Je proto vyloučeno, aby jakýkoliv radius server nebo přístupový bod, který předává požadavek dál, „viděl“ uživatelské heslo.

Radius server

(Remote Authentication Dial In User Service) je určen k ověřování identity uživatelů, dále provádí autorizaci uživatelů a accounting na základě informací z přístupového bodu Obr. 2. S radius serverem nekomunikuje přímo uživatel, ale pouze přístupové body. Radius server může také fungovat jako proxy server - v tom případě neověřuje identitu uživatelů, ale pouze přeposílá požadavky na jiné radius servery.

Klíče:

Klíč je sdílený, proto není problém, aby uživatel data přenášená ostatními uživateli odposlouchával. Pokud ale například z důvodu krádeže zařízení nebo ukončení pracovního vztahu chceme zabránit přístupu do sítě, nastává problém. Nezbývá nic jiného, než manuálně nastavit veškeré klíče znovu.

4.1.3 WEP2

K vytvoření druhé verze WEPu vedla snaha odstranit chyby verze původní – rozšířením inicializačního vektoru IV a zesílení 128 bitového šifrování. I tak původní mezery tohoto zabezpečení zůstaly a útočníkovi zabere jen o něco více času, aby tuto šifru prolomil. WEP2 byl použit zpravidla na zařízeních, která hardwarově nestačila na novější šifrování WPA.

4.1.4 WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access (Wi-Fi chráněný přístup) vznikl jako produkt na základě neuspokojivé situace v oblasti bezpečnosti Wi-Fi vyvolaný negativními reakcemi uživatelů na WEP a WEP2. Z těchto důvodů byla v dubnu roku 2003 vytvořena skupina, která měla za úkol předložit kvalitnější způsob zabezpečení.

V červnu následujícího roku bylo přijato nové řešení v podobě šifrování WPA. Stejně jako u WEP je použit šifrovací algoritmus RC4, ale se 128 bitovým klíčem a 48 bitovým inicializačním vektorem.

Další podstatná změna spočívala v klíči. Není zde již používán statický klíč, jak tomu bylo v případě WEP, ale klíč dočasný, který se pravidelně obměňuje - technologie TKIP – TKIP (Temporal Key Integrity Protocol), kde se mění klíč dynamicky, díky metodě MIC (Message-Integrity Cheb). Je zde použitý nový algoritmus označovaný jako Michael, který pomocí výpočetních možností existujících bezdrátových zařízení vypočítá osmibajtový kontrolní součet MIC (Message Integrity Code). Kontrolní součet MIC je umístěn mezi datovou částí rámce IEEE 802.11 a čtyřbajtovou hodnotou ICV (Integrity Check Value). TKIP prodlužuje délku zprávy zašifrované pomocí WEP o 12 bajtů. 4 bajty pro rozšířenou informaci a 8 bajtů pro kód integrity zprávy (MIC). Kód MIC se používá k zajištění integrity dat. Ke každému rámci přidává digitální podpis, čímž zamezuje útoku typu man-in-the-midle. Digitální podpis se automaticky vypočítává na základě datové části rámce, zdrojové a cílové MAC adresy, pořadového čísla paketu a náhodné hodnoty. Tyto hodnoty se zabudují do datové části rámce a následně je celý rámec zašifrován.

Pole kontrolního součtu MIC je šifrováno společně s daty rámce a hodnotou ICV. Metoda Michael také pomáhá zajistit ochranu proti přehrání. K zamezení útoků pomocí přehrání slouží nový čítač rámců v rámci IEEE 802.11. WPA také nabízí více možností, jak zabezpečit síť pomocí PSK (Pre-Shared Key) v případě stejných přístupových hesel všech uživatelů. Tento způsob se používá převážně v domácnostech.

Dalším způsobem jak zabezpečit síť je způsob použití Radius autentizačního serveru, který zasílá každému uživateli jiný přístupový klíč.

Zabezpečení WPA je těžko prolomitelné a často se používá v podnikových sítích.

Zdroj:http://www.ics.muni.cz/zpravodaj/articles/538.html

Shrnutí

Zvětšení celkové velikosti klíče, snížení počtu zasílaných paketů s podobnými klíči a ověření integrity vede k celkově dostačujícímu zabezpečení přenosu a stává se těžko prolomitelným.

WPA představuje podmnožinu prvků 802.11i. Byly zvoleny takové prvky, které nevyžadovaly změny hardwaru, takže modernizace všech zařízení šla provést pouze aktualizací firmwaru.

Standard WPA je dopředně slučitelný s 802.11i, ale ještě nezahrnuje takové prvky, jako jsou bezpečné předávání stanice mezi přístupovými body na základě předběžné autentizace, bezpečné deautentizace a odpojení. Dále pak rozšířený protokol pro šifrování na bázi AES.

Nové bezpečnostní mechanismy musely odstranit zásadní nedostatky protokolu WEP. Prakticky nulovou autentizaci a velmi slabé šifrování statickým klíčem. WPA nabízí různé režimy autentizace pro různá prostředí. V podnikovém prostředí předpokládá využití centralizovaného autentizačního serveru, který je zodpovědný za distribuci klíčů.

Zdroj: http://bezdratovesite.wz.cz/#_Toc170470628

4.1.5 WPA2

O dva roky později v roce 2004, vznikl WPA2 u kterého byl použit protokol CCMP (Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol), který využil principu silného šifrování AES (Advanced Encryption Standard), jenž dynamicky mění 128 bitový klíč.

Šifrování, které vymyslela americká vláda, je od 13. března 2006 povinné pro všechna nová zařízení, která mají certifikaci Wi-Fi.. S pokračujícím vývojem standardu IEEE 802.11i , který používá k zašifrování - algoritmus AES, bylo také vyvinuto úsilí do AES integrovat WPA . WPA2 přináší kvalitnější šifrování, které má však vyšší hardwarové nároky.

Zdroj: http://www.owebu.cz/wifi/vypis.php?clanek=1067

WPA2 je navržen tak, aby byl zpětně kompatibilní s původním standardem WPA, a proto podporuje také TKIP, AES, WPA, WPA-PSK a 802.1x autentizované WPA sítě.

Zdroj:http://notebook.cz/clanky/tiskova-zprava/2005/050621-ASUS-WL-520G-Deluxe/

Certifikace WLAN produktů pro WPA2 je rozdělena do dvou kategorií, podobně jako tomu bylo v případě WPA a to pro podnikové a pro osobní sítě. Zatímco v prvním případě půjde o kompletní podporu WPA2, včetně 802.1x a PSK pro podnikovou infrastrukturu, v druhém případě jsou požadavky na zabezpečení menší, takže není potřeba 802.1x a zůstane pouze PSK.

Zdroj: http://telnet.cz/content.php?con_id=570

Tato nová architektura pro bezdrátové sítě nese označení RSN (Robust Security Network) a používá autentizaci 802.1x, silnou distribuci klíčů a další nové mechanismy k zajištění integrity a soukromí.

I když architektura RSN je složitější, nabízí bezpečná a variabilní řešení pro bezdrátovou komunikaci. Ve většině případech akceptuje RSN pouze zařízení s podporou RSN, nicméně IEEE 802.11i definuje také architekturu TSN (Transitional Security Network), do které lze zahrnout jak systémy RSN, tak systémy WEP. Toto řešení umožní uživatelům včas aktualizovat své zařízení.

Sestavení bezpečného komunikačního kontextu se skládá ze čtyř fázi:

- odsouhlasení bezpečnostních zásad
- autentizace 802.1x
- odvozování a distribuce klíče
- utajení a integrita dat RSN

Shrnutí

I když od vydání WPA/WPA2 byla odhalena celá řada méně důležitých slabých míst, žádná z nich nejsou příliš nebezpečná, za předpokladu dodržování poměrně jednoduchých bezpečnostních opatření.

Standard IEEE 802.11i přinesl takové základní změny jako jsou oddělování autentizace uživatele od vynucování integrity a soukromí zprávy. Tím poskytuje stabilní a škálovatelnou bezpečnostní architekturu vhodnou nejen pro domácí sítě, ale i pro velké podnikové systémy.

Slabiny a útoky na WPA2

Nejzranitelnějším místem WPA2 je útok na klíč PSK WPA/WPA2. PSK poskytuje alternativu ke generování 802.1x PMK pomocí autentizačního serveru. Jedná se o řetězec s 256 bity nebo heslo skládající se z 8 až 63 znaků, které slouží pro generování řetězce pomocí známého algoritmu. Všechny informace, které slouží k výpočtu jeho hodnoty, se přenáší jako nešifrovaný text. Může být předmětem, slovníkových útoků.

Rozdíly mezi WPA a WPA2

Uzamykající protokol CCMP umožňuje přidávat do WPA2 ad-hoc. Toto má nahradit také dlouhodobý TKIP.

Jednoduché přestavení od WEP na WPA nebo WPA2 není u každého zařízení možné. Zčásti je hardware příliš pomalý na emulování uzamykajícího SW AES. Zjednat nápravu můžete potom jen novým terminálem se speciálním hardwarem pro AES.

WPA2 a WPA může spolu komunikovat, pokud WPA2 podporuje AccessPoint. Standard WPA2 se používá dodnes a bývá považován za nejlepší standardní zabezpečení.

4.1.6 Topologie sítě

Jak již bylo zmíněno, správná topologie sítě má důležitý vliv na náhodné, hlavně amatérské, útoky. Příčinou může být špatné použití vysílacích antén nebo špatný návrh použité technologie.

Již při plánování výstavby bezdrátové sítě je dobré se zamyslet, kde všude budeme potřebovat signál a použít takový typ antény, která pokud je to možné,

pokryje signálem jen námi využívaný prostor. Téměř vždy je tento požadavek v praxi nesplnitelný a zároveň s požadovaným prostorem pokryjeme signálem i prostor nežádoucí. Proto je vhodné nevyužitý prostor alespoň minimalizovat – použitím sektorové nebo směrové antény.

Všeobecně používané pravidlo je, snažit se nepoužívat sektorové antény, pokud to není nezbytně nutné a totéž platí i pro topologii při všesměrovém vysílání. Potenciální útočník musí před zahájením útoku vyhledat a vystihnout vyzařovací úhel antén a pro Point to Point spoje používat zásadně úzce směrové antény.

Tohoto sytému využívá jedna z největších českých firem dodávající Point to Point spoje v bezlicencovaném pásmu 10 GHz - Alcoma. Tato technologie je hojně používána statní správou, např. pro kamerové městské systémy, či propojení budov městské správy. Používané antény mají nejčastěji vyzařovací úhel 0,9´. Nevyužívají žádné jiné techniky zabezpečení, pouze úzce směrový vyzařovací úhel a kompatibilitu zařízení vlastní značky a typové řady. Pro útočníka je velmi těžké až nemožné v praxi trasu spoje vystihnout.

Této technologie využívají i jiná bezdrátová pojítka, např. úzké infa spoje, v praxi téměř neprolomitelné. Pokud by útočník chtěl tento spoj prolomit, musel by své zařízení umístit přesně do směru aktivního spoje, čímž by celou komunikaci přerušil. ¨

Zdroj: http://www.xmaestro.com/view.php?cisloclanku=2006100024

4.2 Zabezpečení sítě z ethernetové strany

4.2.1 Filtrace MAC adres

MAC adresa (media access control) je fyzická a jedinečná adresa pro každé síťové zařízení nebo aktivní prvek Má jedinečné číslo, které je udáno výrobcem – nemůžeme tedy toto číslo (skládající se z devíti písmen a číslic) měnit. Je to z důvodu bezpečnosti a přístupového práva při připojování.

MAC adresu lze zjistit kliknutím na nabídku START -> SPUSTIT a do příkazového řádku napíšeme příkaz „cmd“. Dále napíšeme příkaz, který nám ukáže veškeré parametry síťového adaptéru včetně MAC adresy.

4.2.2 MAC Access List

Většina Access Pointů má ve standardním vybavení funkci “MAC access“ list. Tato funkce umožňuje Access Pointu si pamatovat MAC adresu připojovaného klienta. Pokud jí však nezná, klient se nebude moci připojit.

Obr. 3 MAC Access list

4.2.3 Filtrace pomocí firewallu

Z předchozího MAC Access Listu víme, že Access point si pamatuje adresu připojovaného klienta a neznámého neregistrovaného klienta neautorizuje, ale již nedokáže dát dohromady určitou IP adresu s příslušnou MAC adresou. Tato funkce je potřebná například pro statistiku, sledování počtu přenesených dat nebo shaping (omezení rychlosti některým uživatelům). Problém s přiřazováním adres lze vyřešit přidáním firewallu. Tato metoda je oblíbená hlavně u veřejných hotspotů, kde firewall dle přiřazené IP adresy a MAC adresy vyhodnotí identitu uživatele. Pokud je uživatel neznámý, je přesměrován na DashBoard, tedy speciální stránku např. s informacemi o poskytovateli služby. Po přihlášení známé IP a MAC adresy, firewall změní pravidla a uživatel je připojen k síti.

4.2.4 Útok

Fyzicky většinou nelze změnit MAC adresu zařízení. I přesto je však útok triviální vzhledem k tomu, že není problém MAC adresu změnit v operačním systému. Například u nejpoužívanějšího operačního systému Windows XP, pokud nelze provést změnu v konfiguraci síťového adaptéru, jde MAC adresa změnit úpravou jediného záznamu v registru.

Úprava systémového registru:

Na většině karet lze, jak je výše uvedeno, změnit MAC adresa přímo přes uživatelské rozhraní Windows. To provedeme následovně:

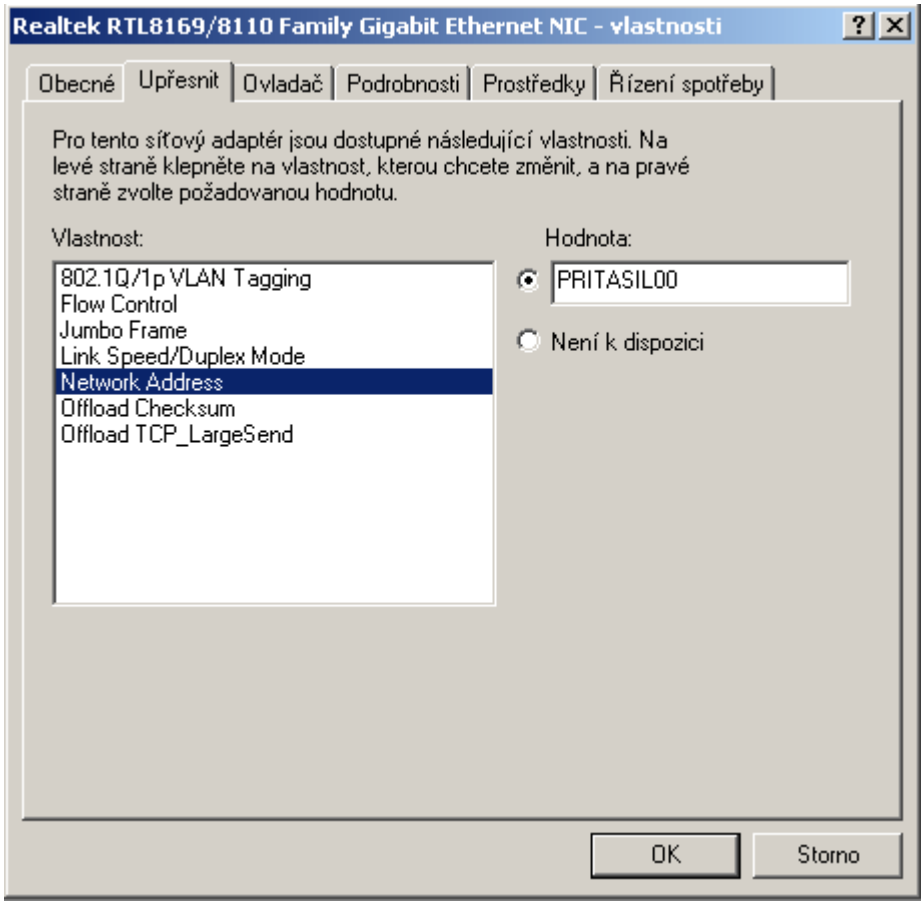
V nabídce Start \ Nastavení \ Ovládací panely otevřeme položku Systém, kde přejdeme na Hardware \ Správce zařízení \ Síťové adaptéry. Zde vybereme požadovanou síťovou kartu, kde chceme změnit MAC adresu. Klikneme na ni pravým tlačítkem myši, dáme volbu Vlastnosti a přejdeme na záložku Upřesnit.

Zde nalezneme vlastnost, podle které můžeme MAC adresu změnit. Vlastnost se liší podle zařízení.

Vlastnosti:

- **Místně spravovaná adresa** - Intelovský integrovaný síťový čip
- **Network Adress** - nForce integrovaný síťový čip
- **Síťová adresa** - 3Com PCI síťová karta
- **MAC adress** – VPN např. Hamatchi (virtuální privátní síť)

Zde zadáme jakoukoliv MAC adresu ve formátu deseti znaků – XXXXXXXXXX (bez pomlček). Tuto změnu si můžeme prohlédnout v nabídce Start \ Spustit, příkazem „cmd“ a v následujícím příkazovým řádku příkazem ipconfig/all.



Obr 4. Změna MAC adresy

Pokud Vaše síťové zařízení neumožňuje změnu síťové MAC adresy, lze ji změnit pomocí zmiňované úpravy registrů (jen pro Win 9x, ME, 2k, XP a server 2k3). Před úpravou registrů se doporučuje je zálohovat.

Pomocí příkazu regedit editujeme systémové registry a vyhledáme klíč [HKEY_LOCAL_MACHINESystemCurrentControlSetServicesClassNet]. Nalezneme zde podklíče 0000, 0001 … atd. podle instalovaných síťových adaptérů vybereme MAC adresu, kterou chceme změnit. Název adaptéru, tak jak jej vidíme po editaci příkazem winipcfg, najdeme u položky "DriverDesc". V podklíči (např. 0001, 0002…) musíme vytvořit novou textovou hodnotu, kterou si pojmenujeme "networkaddress". Do údaje Hodnota zadáme novou MAC adresu, např. podle obrázku, změníme na PRITASIL00.

Jsou další a další způsoby jak lze změnit MAC adresu v registrech. Tento postup mám vyzkoušený, funguje bez problému.

VPN (Virval Private Network)

Možná se zdá, že virtuální privátní síť nemá nic společného s bezpečností bezdrátových sítí, ale pomocí VPN můžeme dosáhnout minimálně zabezpečení WPA.

VPN (virtual private network) je prostředek pro propojení několika počítačů na různých místech internetu do jediné virtuální počítačové sítě. I když počítače mohou být v naprosto fyzicky nezávislých sítích na různých místech světa, prostřednictvím virtuální privátní sítě mezi sebou mohou komunikovat, jako by byly na jediném síťovém segmentu.

Prostřednictvím VPN lze zajistit například připojení firemních notebooků kdekoliv na internetu do firemního intranetu (vnitřní firemní sítě). K propojení je třeba VPN server, který má přístup na internet i intranet (může sloužit pouze

pro jednoho klienta, nebo sloužit jako hub a přijímat spojení od více klientů) a VPN klient, který se přes internet připojí k serveru a prostřednictvím něj pak do intranetu. VPN server pak plní v podstatě funkci síťové brány. VPN používá jeden z největších poskytovatelů datových služeb v České Republice O2, CDMA.

Zdroj: http://cs.wikipedia.org/wiki/Virtualní_privátní_síť

VNP lze tedy chápat jako bezpečné (autentizované a šifrované) a přitom pro uživatele zcela transparentní spojení mezi dvěma či více sítěmi, přičemž pro spojení mezi uživatelem a požadovanou destinací je použita veřejná síť - nejčastěji internet.

Mezi hlavní výhody použití VPN patří rozšíření hranic působnosti bez nutnosti budovat další síťovou infrastrukturu. To přináší značné úspory proti budování vlastních WAN sítí, možnost být stále v kontaktu s daty v lokální síti a v neposlední řadě rovněž rozšiřitelnost - možnost růstu úměrně potřebám uživatelů.

Zdroj: http://home.zcu.cz/~ondrous/

VPN používá dva šifrovací klíče vějný klič a soukromý klíč. Veřejný klíč, jak již z názvu vyplývá, je dostupný každé stanici a tedy každý může pomocí tohoto klíče zašifrovat data, která ovšem dokáže dešifrovat opět pouze majitel soukromého klíče.

Soukromý klíč je určen pouze pro jedno jediné zařízení k dešifrování zaslaných dat. Klíč si ovšem může kdokoliv vygenerovat, proto je potřeba ještě třetí strana, která je důvěryhodná, tzv. certifikační autorita. Certifikační autorita

ověří, zda jsou v certifikátu odpovídají údaje a zda tomuto certifikátu udělí elektronický podpis. Z tohoto vyplývá, že je vše postaveno na soukromém klíči. Kdo jej získá, bez problému může vytvářet libovolný certifikát. Certifikáty mají platnost jen po určitou dobu. Kontrolu platnosti certifikátu klienta provádí takzvaný CRL, který se na server nakopíruje. Vše je založeno na standardu X.509, stejně jako zabezpečení WiMAXu viz 2.3.1.

VPN sítě jsou založeny na protokolu IPSec, který se musí nakonfigurovat v jádře OS. Nejedná se o jednoduchou záležitost a mohou nastat později další problémy s kompatibilitou. IPSec mimo jiné si nedokáže poradit s překládáním NAT adres (Network Address Translation). Pomocí programu OpenVPN se tyto problémy řeší jednodušeji.

OpenVPN

OpenVPN je open-source program (volně šiřitelný s možností zásahu do zdrojového kódu). Je pro všechny operační systémy, dokonce i pro Windows. Využívá protokol TCP/IP případně UDP Princip spočívá v tom, že OpenVPN obdrží paket, naváže UDP spojení (případně se pokusí navázat) na SSL/TLS komunikaci a ověří certifikáty druhé strany oproti certifikátu zvolené certifikační autority. Pomocí SSL/TLS se dohodnou obě strany na šifrách a klíčích, které se použijí k zabezpečení přenášených dat. Server OpenVPN pošle konfigurační volby klientovy například klientovo IP adresu.

OpenVPN má i některé nevýhody, například větší zátěž systému pakety jsou baleny do UDP nebo TCP. Při stahování velkých souborů přes OpenVPN je tento proces o něco pomalejší, než u přímého stahování bez OpenVPN.

5 Předpokládaný vývoj

Klíčovou roli bude pravděpodobně i nadále hrát samotné chování uživatelů, neboť podle průzkumu Wi-Fi Aliance, asociace pro propagaci a certifikaci Wi-Fi sdružující přední výrobce bezdrátových technologií považuje 44 % uživatelů konfiguraci zabezpečení WLAN za středně až velmi obtížnou. Proto se v krátkodobém horizontu jeví jako perspektivní program Wi-Fi Protected Setup (WPS), kdy směrovač poskytne klientům šifrovací klíče pro WPA/WPA2 na základě stisknutí „jediného knoflíku“ nebo zadáním PIN (ten je generovaný softwarově a zobrazovaný na monitoru nebo předprogramovaný v klientském zařízení a vytištěný na přiložené kartě či nálepce).

Nejjednodušší varianta WPS je užití šifrovacího klíče, který je buď vygenerovaný, nebo předprogramovaný a zároveň je součástí uživatelského balíčku (podobně jako PIN u SIM karty).

Vyšší stupeň zabezpečení WPS využívá tokeny nebo bezkontaktní karty. Přiblížení karty nebo tokenu k bezdrátovému zařízení iniciuje výměnu klíčů.

Nejvyšším stupněm zabezpečení je využití USB paměti flash, jejímž prostřednictvím se manuálně přenesou potřebné informace do všech klientských zařízení v síti.

V blízké budoucnosti (pravděpodobně v druhé polovině roku 2008) můžeme rovněž očekávat definitivní schválení dlouho očekávaného standardu IEEE 802.11n, který sám o sobě z hlediska bezpečnosti nic nového nepřináší, naopak díky vyšší přenosové rychlosti de facto umožní ještě rychlejší proražení WEP zabezpečení, např. pomocí aktivních „útočných“ ARP (Address Resolution Protocol) paketů.

Na straně výrobců lze ve střednědobém horizontu předpokládat, že se zvyšováním výpočetního výkonu hardware bude narůstat podíl šifry Serpent,

která šifruje data 3X za sebou 256bitovou šifrou, jež je v současnosti kryptology hodnocena jako nejbezpečnější bloková šifra (ačkoliv předpokládaná životnost dnes nejrozšířenější šifry je 20 až 30 let).

Zdroje:

http://gumysh.freeweb7.com/docs/AES/Pages/Page04.html

http://www.lupa.cz/clanky/bezpecnost-wifi-zalezi-jen-na-vas/

http://www.isvs.cz/bezpecnost/jak-zabezpecit-wifi.html

6 Závěr

S odkazem na předchozí text je třeba zhodnotit celou problematiku a poukázat na jednotlivé výhody a nevýhody výše popsaných metod zabezpečení ve vztahu k jejich typovému použití.

Je samozřejmostí, že jiný typ zabezpečení bude vyhovovat domácí síti, oproti poskytovateli datových služeb.

6.1 Domácí síť

Zabezpečení domácí sítě by mělo být naprosto samozřejmé. Bohužel je limitováno několika faktory. Cenovou dostupností vybraného řešení s ohledem na důležitost zabezpečovaných dat, znalostmi a schopnostmi uživatele.

Z mých vlastních zkušeností není příliš velká znalost a ochota uživatele věnovat se zabezpečení vlastní sítě.

Pro zabezpečení domácí sítě vznikla metoda WPA2, která je pro uživatele, bez dalších nákladů snadno použitelná. Tento standard dnes musí splňovat každé prodávané zařízení.

6.2 Firemní síť

Dá se předpokládat, že ve firemní síti jsou poskytována strategická data potřebná pro fungování podniku. Především těmto aspektům by se mělo podřídit zabezpečení celé sítě, zvláště bezdrátové části, která představuje jednu z největších slabin..

Pokud se i přesto firma rozhodne zavést bezdrátovou síť, je třeba celou akci dobře naplánovat. Stanovit a sepsat bezpečnostní pravidla pro bezpečné používání celého sytému. Eliminovat možnost vynesení a následného zneužití

bezpečnostních hesel. Mít jasná pravidla pro případ krádeže některého z mobilních zařízení připojovaných do sítě.. Použít co možná nejvíce výše popsaných bezpečnostních prvků a to i pokud je firemní síť zabezpečena po ethernetové části. Tím se zamezí zbytečným útokům a vytěžování serverů požadavky útočníků.

Dále je třeba zhodnotit použití sítě, zda je určena pouze pro vnitřní prostory, nebo pokud má sloužit i pro připojení firemních prostorů přístupných veřejnosti. Pro tento druhý případ je kromě robustního zabezpečení bezdrátové části dobré použít například VPN. Ostatní přístupy odfiltrovat pomocí kvalitního firewallu.

Vyvarovat se připojování životně důležitých částí sítě jako jsou například servery přes bezdrátovou část. Dávat pozor na vystavení neautorizovaných přístupových bodů.

6.3 Síť poskytovatele připojení k Internetu (ISP)

Vzhledem k předpokládanému velkému množství připojených klientů (v řádu stovek až tisíců) a plošnému pokrytí velké časti území v síti poskytovatele internetového připojení je třeba přihlédnout k vyšší pravděpodobnosti napadení. Ze své vlastní zkušenosti vím, že drtivá většina sítí ISP z reklamních důvodů nepoužívá skryté SSID a usnadňuje útočníkovi lokalizaci vhodných přístupových bodů.

Na rozdíl od firemní sítě, nebo domácí sítě, ve stejné míře hrozí útok z vnitřní strany sítě od uživatele jako z vnější strany od útočníka. Dokonce se stává jistou prestižní záležitostí prolomit zabezpečení těchto poskytovatelů a dokázat tím slabinu provozované sítě. Dále je třeba brát v úvahu různorodost uživatelů sítě a to od firemních zákazníků, pro které je datová komunikace a přenášení privátních strategických dat životně důležité, až po domácí

uživatele využívající připojení pro zábavu a volný čas spojené s větším rizikem virové nákazy. Nemalým problémem je umístění samotného zařízení uživatele. Většinou se jedná o veřejně přístupná místa (půdy, strojovny výtahů, chodby), kde může dojít k snadnému odcizení nebo přímému kontaktu se zařízením. Tím vzniká riziko přímého útoku na přístupová hesla spojené se zneužitím šifrovacích klíčů.

Z těchto důvodů se ISP stává asi nejrizikovější skupinou ze tří porovnávaných sítí. Proto bych doporučoval kombinaci různých druhů zabezpečení. Od triviálních, přes mechanické až po robustní softwarovou šifrovací ochranu. Vše je podmíněno cenou navrženého řešení, v počtech uživatelů jakými tyto sítě disponují a výběrem řešení podle typu uživatele tak, aby navrhované řešení bylo co neefektivnější. Proto je třeba naplno využít standardních zabezpečovacích systémů s důrazem na jejich snadnou konfiguraci a funkčnost.

Z praxe mohu doporučit následujících několik pravidel, které se mi osobně osvědčily a eliminovaly úspěšné útoky na mou síť. Základem je zamezení krádeže a přímého kontaktu nepovolaných osob s aktivními prvky sítě (klientské zařízení, vysílací body). Konfigurační prostředí všech aktivních prvků v síti chránit přístupovými hesly. Dbát na správné zacházení s těmito údaji. Dále bych doporučoval nepoužívat v síti DHCP servery, ale přidělovat každému uživateli sítě vlastní IP adresu manuálně. Každou IP adresu párovat s MAC adresou zařízení. Pokud je to možné rozdělit síť pomocí WLAN do menších segmentů (ideální případ - každý uživatel vlastní WLAN). Použít alespoň zabezpečení WPA lépe WPA2.

Anotace

Práce popisuje problematiku zabezpečení bezdrátového přenosu dat u jednotlivých bezdrátových technologií. Podrobně se zabývá standardy 802.11x, různými druhy zabezpečení technologií vycházejících z těchto standardů a možnými útoky na ně. Dále se zabývá související problematikou s ochranou hesel a citlivých údajů, důležitých pro správu sítě. V práci je několik příkladů zabezpečení konkrétní typové sítě.

Klíčová slova: bezdrátová síť, zabezpečení sítě, Wi-Fi, WEP, WPA, WiMAX, MAC

Annotation

This diploma thesis describes the secure wireless data transfer mediated by various technologies. A special attention is given to standards 802.11x, different kinds of technologies protection originating of the standards and to possible attacts targeted against them. Moreover, it deals with the problems related to password and sensitive data protection which are important to the network administration. The thesis gives also some examples of particular network type securing.

Keywords: wireless connection, network protection, Wi-Fi, WEP, WPA, WiMAX, MAC

Seznam použité literatury

Většina použité literatury byla uveřejněna v elektronické podobě na internetu. Citace byly volně reprodukovány.

[1] http://cs.wikipedia.org/wiki/Elektromagnetické_záření

[2] http://cs.wikipedia.org/wiki/rádiové_vlny

[3] http://www.security-portal.cz/clanky/wifi-site-a-jejich-slabiny.html

[4] http://cs.wikipedia.org/wiki/IEEE_802.11

[5] http://www.dsl.cz/clanky-dsl/clanek-457/Wi-Fi-otevira-dvirka-pro hackery

[6] http://www.dsl.cz/clanek-11/Bude-WiMAX-konkurencí-xDSL%3F-Cast-I

[7] http://www.wimax.cz/index.php?option=com_content&task=view&id=172 &Itemid=33

[8] https://dip.felk.cvut.cz/ browse/pdfcache/kolarj6_2007bach.pdf

[9] http://www.owebu.cz/wifi/vypis.php?clanek=1067

[10] http://www.security-portal.cz/clanky/wifi-site-a-jejich-slabiny.html

[11] http://www.lupa.cz/clanky/bezpecnost-wifi-zalezi-jen-na-vas/

[12] http://bezdratovesite.wz.cz/#_Toc170470628

[13]http://technet2.microsoft.com/WindowsServer/cs/Library/ff7c2ac9-5db3-4b71-a31b-9604dce0b2171029.mspx?mfr=true

[14] http://www.ics.muni.cz/zpravodaj/articles/538.html

[15] http://www.owebu.cz/wifi/vypis.php?clanek=1067

[16] http://telnet.cz/content.php?con_id=570

[17] http://www.xmaestro.com/view.php?cisloclanku=2006100024

[18] http://cs.wikipedia.org/wiki/Virtualní_privátní_síť

[19] http://home.zcu.cz/~ondrous/