Datová bezpečnost bezdrátové komunikace v rámci vnitřních podnikových sítí

Data security of wirelles communication in terms of internal company networks

Lubomír Lefler

Bakalářská práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ABSTRAKT

Cílem této práce je poskytnout čtenáři základní informační rámec v oblasti datové bezpečnosti bezdrátových sítí. Práce seznámí čtenáře s bezpečnostními riziky, která hrozí lokálním bezdrátovým sítím. Jsou zde diskutovány možné útoky na počítačovou síť, základní bezpečnostní technologie, princip vrstvené bezpečnosti sítě a v neposlední řadě také principy bezpečnostní politiky organizace z hlediska práce s informacemi. Popsány jsou také možné způsoby útoku na bezdrátovou síť, způsoby jejich odhalení a to jak v případě bezdrátové sítě radiové tak i v případě bezdrátové sítě optické. Poslední část je věnována firewallu a možnostem jeho použití.

Klíčová slova:

Útok, útočník, bezpečnost, firewall, NAT, WLAN, IEEE 802.11, přístupový bod, autentizace, WEP, WPA, VPN, RADIUS

ABSTRACT

The objective of this work is to provide information about data security of wireless networks to lay readers. In this work readers will learn about security risks occuring in local wireless networks. The work discusses possible attacks on computer network, basics of detecting them, and also the principle of security policices in organizations in terms of handling information. The reader will also learn about the possible ways of attack on a wireless network, the ways of detecting them in radio and also optical wireless networks. The last part discusses firewall and possible usses of it.

Keywords:

Attack, attacker, information security, firewall, NAT, WLAN, IEEE 802.11, acces point, authentication, WEP, WPA, VPN, RADIUS

Poděkování

Chtěl bych poděkovat vedoucímu mé bakalářské práce panu Doc.Mgr.Romanu Jaškovi, Ph.D. za cenné připomínky a rady při řešení problémů souvisejících s bakalářskou prací. Rád bych také poděkoval rodičům a všem dalším kteří mě podporovali nejen při psaní této práce ale i po dobu celého studia.

OBSAH

1 ÚVOD

Funkční počítačová síť se v dnešní době stala podmínkou pro každý podnik či instituci ke kvalitní komunikaci. Počítačové sítě dnes zajišťují přenos dat, hlasu, obrazu ale i pracovní údaje z různých zařízení. Bez použití počítačové sítě je dnes práce nepředstavitelná, finančně náročná a neefektivní. Je také třeba počítačovou síť vnímat jako jeden z mnoha nepostradatelných prostředků k dosáhnutí cíle firmy. Proto je nutné zabývat se otázkou zabezpečení sítě podobně, jako je vhodné se zabývat např. ochranou před krádežemi hmotného majetku.

S rozšířením počítačových sítí také vzrůstá i možnost sítě zneužít. Počítačová kriminalita, zneužívání dat, elektronické krádeže a podvody se staly zcela běžnou realitou našeho života. Přitom požadavek na zabezpečení informačních systémů je velmi zanedbávanou oblastí.

Uživatelé počítačové sítě žádají bezchybné zabezpečení ochrany osobních a/nebo obchodních informací. Z tohoto důvodu je nutné kvalitní a funkční zabezpečení bezdrátové sítě. V komunikačních sítích může neoprávněná osoba odposlouchávat datové přenosy, často i zablokovat provoz celé sítě nebo její části. S rostoucím zájmem o bezdrátové sítě dochází k tomu, že i útočníci zaměřují svoji pozornost více tímto směrem a hledají (a mnohdy i nalézají) nové způsoby k překonání bezpečnostních opatření takovýchto sítí.

Realizace skutečně funkčního a kvalitního zabezpečení u bezdrátových sítí je mnohem problematičtější než u běžné sítě využívající metalických vodičů signálu (např. síť typu Ethernet). Proto bez výborné znalosti přidružených problémů a rizik může snadno dojít k překvapivé situaci. Je téměř jisté, že síť která není zajištěna alespoň primárními bezpečnostními prvky, bude napadena během několika hodin od připojení na Internet. I proto je problém zabezpečení sítě důležitý pro integraci do bezpečnostních směrnic organizace.

Běžně se setkávám s názorem, že zabezpečení sítě není prioritním problémem a to zejména, pokud se operuje s daty, které nejsou tak zásadní. Jenže jedním z prvků zabezpečení počítačové sítě je např. i řízení přístupu do sítě. Není v ničím zájmu, aby se k jeho síti připojoval nevyžádaný uživatel.

Všichni administrátoři počítačové sítě by se měli seznámit s pravidly zabezpečení jejich sítě a požadovat jejich integraci do obecných bezpečnostních stanovisek firmy. Tato bakalářská práce by měla posloužit jako průvodce zabezpečením bezdrátových sítí a poskytnout

ucelené informace o tématice bezpečnosti bezdrátových počítačových sítí aplikovaných v malé organizaci.

2 BEZPEČNOST

O datově zabezpečené síti můžeme hovořit, pokud se nám podaří eliminovat všechna zranitelná místa datové sítě. Bezpečnost je jeden z elementárních pojmů v rámci počítačových sítí. Každý provozovatel datové sítě by měl její zabezpečení brát naprosto vážně. Bezpečnost ovšem nezávisí pouze na primárních technických opatřeních, ale i na organizačních a několika dalších potřebných opatřeních. Pokud všechny potřebná opatření spojíme vhodně v jeden celek, můžeme hovořit o kvalitně zabezpečené síti.

Data společnosti jsou majetkem (aktivem) společnosti, mají určitou finanční i nefinanční hodnotu a proto je třeba je chránit. V průzkumu, který byl proveden v období od září 2003 do března 2004 ve Velké Británii bylo zjištěno, že 40% procent všech organizací, které jsou v soukromém vlastnictví, končí svoji existenci do jednoho roku po napadení datového systému těchto společností. 60% abonentů průzkumu pak bylo nuceno ukončit svoji činnost nejpozději do dvou let od napadení systému. Z daného výzkumu také vyplývá, že společnosti, které neměli svůj informační systém vhodně zabezpečený byly postiženy útokem mnohem více než společnosti, které zabezpečení svých dat nepodcenili. Následky útoku (zejména finanční) byly také mnohem menší pro společnosti, jejichž datový systém byl vhodně zabezpečen. Podle úrovně zabezpečení se rozsah následků pohyboval od mírného oslabení pozice firmy na trhu přes legislativní problémy (např. nedostatečné zabezpečení databáze obsahující osobní údaje zákazníků) po úplné zhroucení společnosti. Při zkoumaných útocích byli napadány zejména jedny z těchto citlivých míst organizací:

- zpracování informací (dat)
- vyhodnocování informací (dat)
- přenos informací (dat)
- prezentaci informací (dat) v informačních systémech

Vhodná bezpečnostní úroveň těchto oblastí práce s daty je i znakem důvěryhodnosti pro obchodní partnery organizace, zejména pak pro zákazníky. Každý (i minimální) progres ve zvýšení datové bezpečnosti organizace zvyšuje její stabilitu a koncurenceschopnost.

3 VYMEZENÍ ZÁKLADNÍCH POJMŮ

3.1 Informační datový systém

Takovýto systém sestává z několika základních prvků, jsou to zejména:

- informační technologie
- data
- lidé

3.1.1 Informační technologie

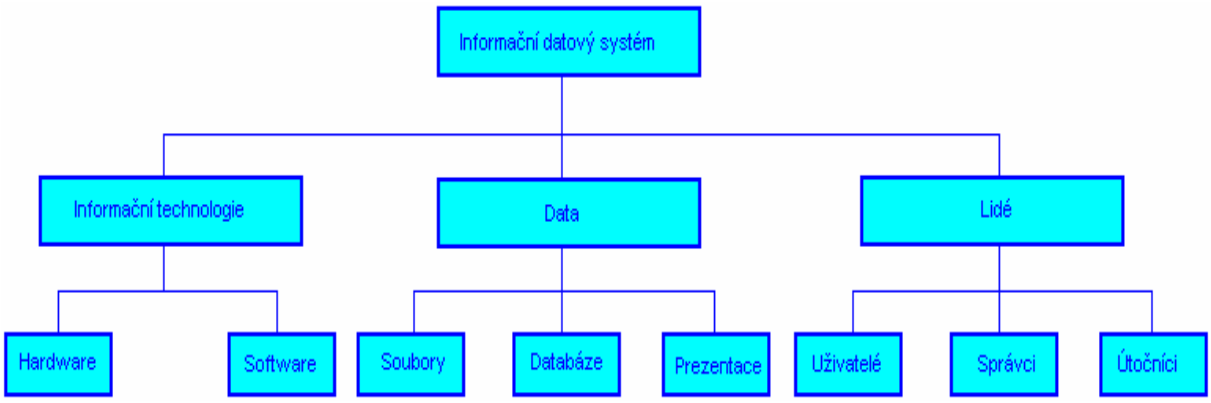
Mají za úkol zpracovávat, ukládat, přenášet a prezentovat data. Informační technologie se obecně dělí na dva sektory. První z nich, Hardware, má za úkol zajišťovat operace s daty na fyzické úrovni na základě instrukcí software (typickým zástupcem hardware je CPU, HDD, RAM, atp.). Dalším sektorem v oblasti informačních technologií je oblast software. Software zajišťuje operace s daty na virtuální úrovni. K tomu využívá služeb hardware (typickým zástupcem software je operační systém, síťový systém, aplikační programové vybavení atp.).

3.1.2 Data

Oblast dat reprezentují informace, zakódované do podoby, se kterou jsou informační technologie schopny pracovat. Patří sem soubory a databáze, vstupní data, výsledná data, prezentace atp.

3.1.3 Lidé

Do této skupiny patří uživatelé, obsluha, správci operačních systémů, sítí a databází, programátoři, útočníci atp.



Obrázek 1: Rozdělení IDS

3.2 Komponenty datového systému (z hlediska jejich aktivity)

3.2.1 Objekty

Jsou v datovém systému pasivními entitami, to znamená, že nejsou schopny podnikat žádné akce. Obsahují nebo přijímají informace nebo přístup pro autorizované subjekty

3.2.2 Subjekty

Subjekty jsou aktivními entitami, to znamená, že mohou v systému podnikat akce. Patří sem uživatelé, procesy, výpočetní systémy, zpracovatelské aplikace, které je třeba autorizovat pro přístup k objektům.

3.3 Klasifikace bezdrátových sítí

Bezdrátové sítě lze klasifikovat dle mnoha kritérií. Kromě kategorií jako dosah, podpora mobility a použitý typ signálu je lze dělit podle topologie na point-to-point nebo point-to-multipoint.

3.3.1 Dosah

Dle dosahu se bezdrátové sítě dělí na:

- bezdrátové osobní sítě *(WPAN, Wireless Personal Network*
- bezdrátové lokální sítě *(WLAN, Wireless Local Area Network)*
- bezdrátové metropolitní sítě *(WMLAN, Wireless Metropolitan Local Area*
- *Network)*

- bezdrátové rozlehlé sítě *(WWAN, Wide Wireless Area Network)*

3.4 Funkční požadavky přístupu k datům

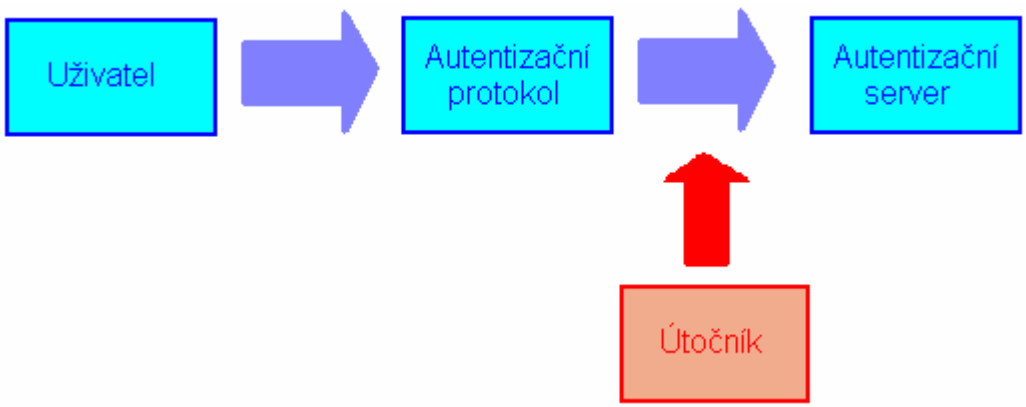
Přístupový kontrolní mechanizmus je klíčovou součástí každé pokročilejší aplikace. Řídí, kteří uživatelé mohou přistupovat k jednotlivým zdrojům, které funkce mohou využívat apod. Měl by ochránit aplikaci před neautorizovaným prohlížením, změnami nebo kopírováním dat. Patří sem:

- Autentizace
- Autorizace
- důvěryhodnost

3.4.1 Autentizace

Autentizace je proces, při kterém se ověřuje, zda je uživatel nebo entita opravdu ten, za koho se vydává, z důvodu udělení/odepření přístupu tomuto subjektu ke zdrojům a objektům v systému.

Samotná autentizace se skládá z několika částí. Zprvu je třeba v systému registrovat nového uživatele, přiřadit mu autentizační informaci a určit jeho práva (registrační část). V druhé části systém žádá od uživatele autentizační informaci. Zadaná data pak systém vyhodnotí v souladu s použitým autentizačním protokolem. Tato část se nazývá Login fáze. Poslední krokem vedoucím k úspěšné autentizaci je rozhodnutí vzdáleného systému, zda je/není uživatel oprávněn působit v sytému a využívat jeho služby.



Obrázek 2: Průběh autentizace

Způsoby získání Autentizační informace

Identitu uživatele je možno získat třemi základními způsoby, na jejichž základě probíhá ověření uživatele v sytému. Z těchto třech způsobů se používá vždy alespoň jeden, ale je možno je kombinovat. Ověření identity probíhá dle zadání těchto údajů:

- ***znalost důležitého údaje*** - jedná se o identifikaci dle znalosti přístupového jména a hesla nebo PINu atp. Jedná se jednoduchý způsob zabezpečení. Slabou složkou tohoto způsobu autentizace jsou samotní držitelé autentizační informace. Přístupová hesla je třeba pečlivě volit, by bylo zamezeno jednoduchému uhádnutí. Heslo by mělo mít minimálně 8 znaků a měly by být kombinována velká/malá písmena a číslice. Heslo by se také mělo pravidleně měnit (alespoň jednou za půl roku) a mělo by být unikátní pro každou službu (např. jiné heslo pro přístup do firemní sítě a jiné pro přístup k e-mailu).

- ***důkaz vlastnictví*** - historicky nejstarší způsob identifikace. Dříve probíhala na prokázání vlastnictví například pečetě. V dnešní době se používají čipové karty, USB klíče apod. Takto řešená autentizace je uživatelsky velmi příjemná, nevýhodou je velká náchylnost ke ztrátě, tvorbě kopií atp.

- ***důkaz vlastnosti*** - jedná se o identifikaci, při které se zkoumají globálně unikátní znaky (otisky prstů, dynamika stisku klávesy, dynamika podpisu, vodivost kůže, struktura oční rohovky). Tento způsob identifikace se vyznačuje vysokou mírou spolehlivosti. Nevýhodou jsou vysoké pořizovací náklady.

3.4.2 Autorizace

Při autorizaci se ověřuje, zda má uživatel dostatečná oprávnění pro přístup k určitému souboru či pro provedené určité akce. Tato kontrola se provádí na základě členství uživatele v různých uživatelských skupinách, přístupových seznamech apod. Neboli se předpokládá předchozí úspěšná autentizace, na jejíž spolehlivosti je autorizace plně závislá. Tato činnost musí předcházet všem aktivitám subjektu v systému a musí zajistit vhodnou ochranu dat a služeb v síti.

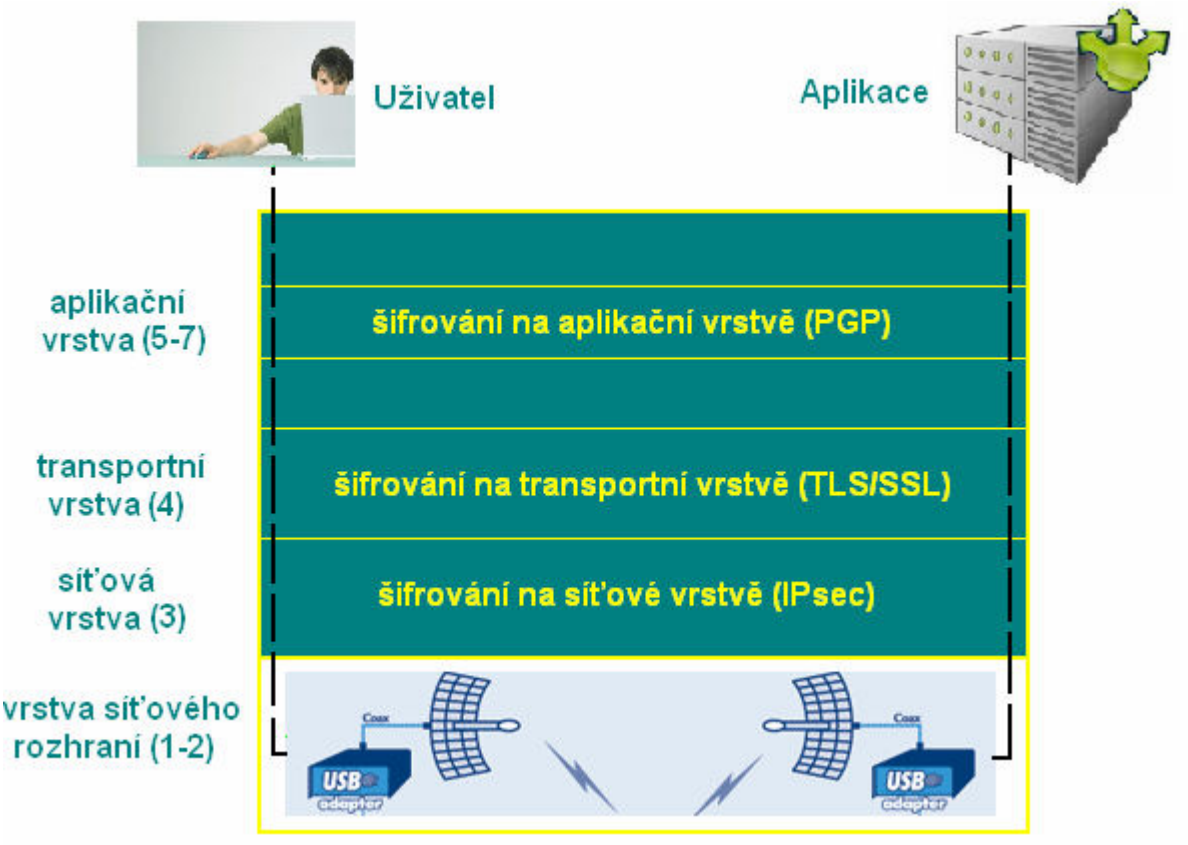
3.5 Digitální podpisy a certifikáty

Digitální podpis je činnost, mající za cíl zajištění integrity dat a jejich nepopiratelnosti. Je to tedy oficiální potvrzení skutečného autora dokumentu, cehož lze dosáhnout více způsoby. Zákony platné v České republice předpokládají použití metody asymetrického šifrování. Pokud chceme vytvořit digitální podpis určitého dokumentu, musíme definovat je hash. Hash je speciální algorytmus, který aplikujeme na podepisovaná data v numerické podobě a výstupu funkce hash získáme číslo o přesně dané délce. Toto číslo nepopiratelně reprezentuje vstupní (podepisovaná) data - vznikne otisk souboru. Hash je poté zašifrován pomocí soukromého klíče podepisující osoby a tím nám vzniká digitální podpis. Tento podpis se potom může přidat k podepisovanému dokumentu, nebo může být zpracován jako samostaný soubor. K digitálnímu podpisu se často také přidává digitální certifikát. Ten může příjemci zprávy pomoci k dalšímu ověření digitálního podpisu.

Digitální certifikát se zkládá ze dvou částí: první je veřejný klíč a druhou jsou pak osobní data držitele certifikátu. Pro důvěryhodné vyznění certifikátu je použita hierarchická autorita (Public Key Infrastructure) a kvalitu certifikátů ověřuje certifikační úřad (certification authority). PKI používá vždy právě dva klíče, jeden pro zašifrování a druhý pro dešifrování. CA pak samotný certifikát vygeneruje a opatří ho digitálním podpisem.

3.6 Šifrování

Slovem šifra nebo šifrování můžeme označit kryptografický algoritmus, který převádí čitelnou zprávu na její nečitelnou podobu, neboli šifrovanou zprávu. Známe dva základní způsoby šifrování: symetrické (používá se pouze soukromý klíč) a asymetrické (za použití soukromého i veřejného klíče)



Obrázek 3: Šifrování na různých vrstvách

3.6.1 Symetrické šifrování

při tomto způsobu šifrování se používá soukromého klíče, který znají obě komunikující strany. Tento klíč se používá jak pro šifrování tak i pro dešifrování. Tohoto způsobu šifrování lze využít při autentizaci i přenosu dat. Slabou stránkou tohoto způsobu šifrování je nutnost distribuce klíče všem, kdo ho potřebují. Při distribuci je ovšem třeba ochránit samotný klíč. Proto je nutné soukromý klíč často měnit.

Obrázek 4: Symetrické šifrování

Příklady šifrování symetrickou šifrou

- DES (Data Encryption Standard, 1977) - klíč o délce 56 bitů se použije na šifrování clusteru o délce 64 bitů (každý osmý bit se použije jako paritní). Tato šifra byla prolomena roku 1997

- AES (Advanced Encryption Standard, 2000) - klíč dlouhý 128, 192 nebo 256 bitů se aplikuje na clustery o délce 128, 192, 256 bitů. Jedná se o pokročilou šifrovací metodu, která byla vyvinuta na žádost Ministerstva obchodu USA. Tato šifra je přímým nástupcem DES.

Blokové šifrovací algoritmy jako DES a AES pracují ve dvou režimech: ECB (Electronic Code Book) nebo CBC (Cipher Block Chaining). Formát ECB je slabší, protože stejný blok dat zašifruje vždy právě do jednoho bloku šifrovaného textu. Z tohoto důvodu je vhodnější použít formát CBC (používá se například u IEEE 802.11i). CBC používá inicializační vektor IV. IV je posloupností náhodně generovaných bitů, který se užijí jako vstup šifry spolu s daty. IV není tajný, ale nesmí být předvídatelný.

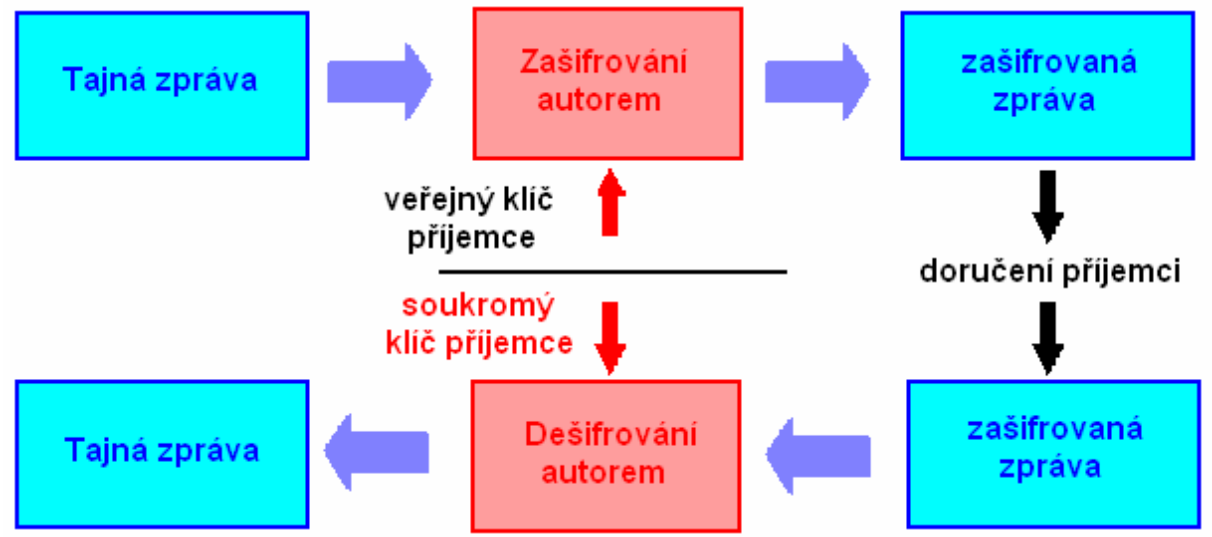
3.6.2 Asymetrické šifrování

Tento způsob šifrování používá osobního i veřejného klíče. S jejich pomocí probíhá šifrování asymetricky. Oba typy klíče, veřejný i osobní, tvoří unikátní pár. Klíč veřejný je volně dostupný komukoliv, kdežto klíč osobní je přísně osobní. Za pomocí veřejného klíče dojde k zašifrování dat, s osobním klíčem můžeme zprávu dešifrovat.Asymetrické šifrování se tedy nedá použít při autentizaci původce zprávy. Výhodou je, že každé dvě stanice mohou komunikovat bez předcházejícího předávání klíčů a to v jakémkoliv pořadí.

Příklady šifrování asymetrickou šifrou

- Diffie - Hellman (D-H, 1976) - první algoritmus, který používal veřejný klíč, distribuce klíčů probíhala bezpečně, proto se stal na dlouhou dobu velmi používaným

- RSA (autoři Rivest, Shamir, Aleman, 1977) - tento algoritmus pracuje na principu, že spolehlivost šifry závisí na délce použitého klíče. RSA se používá v širokém spektru aplikací (elektronická pošta, digitální podpis, při budování VPN).



Obrázek 5: Asymetrické šifrování

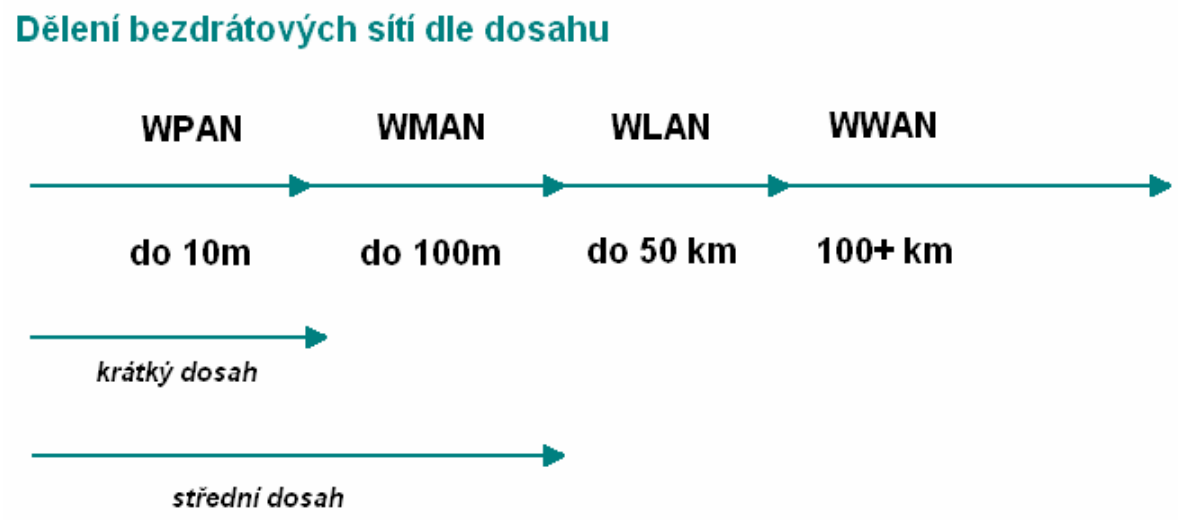
4 KLASIFIKACE BEZDRÁTOVÝCH SÍTÍ

Bezdrátové sítě lze dnes klasifikovat dle mnoha různých kritérií. Kromě dosahu, mobility a typu signálu můžeme tyto sítě dělit na podle topologie na point-to-point (zejména optické sítě) a point-to-multipoint (radiové sítě), případně podle typu určení na vnitřní (infračervené, radiové WLAN) a venkovní.

4.1 Dělení dle dosahu

Dle dosahu se bezdrátové sítě dělí na:

- bezdrátové sítě osobní *(WPAN, Wireless Personal Area Network)*
- bezdrátové lokální sítě *(WLAN, Wireless Local Area Network)*
- bezdrátové metropolitní sítě *(WPAN, Wireless Metropolitan Area Network)*
- bezdrátové rozlehlé sítě *(WWAN, Wireless Wide Area Network)*



Obrázek 6: Dosah bezdrátových rádiových sítí

4.2 Dělení dle mobility

Není pravda, že každé bezdrátové zařízení je mobilní. Mobilní bezdrátové zařízení je tedy takové, které umožní kontrolovatelný pohyb uživatele v rámci sítě v a v rámci jiných sítí. Pevné bezdrátové zařízení umožní mobilitu jen v rámci dané sítě a s každou další už není schopno pracovat. Skutečně funkční mobilní připojení je problematické zejména kvůli nut-

nosti zajistit správné směrovaní paketu na síťové vrstvě. Je tedy nutné znát lokalitu, kde se uživatel v rámci sítě vyskytuje.

4.3 Dělení dle typu signálu

Dle typu signálu lze sítě dělit do dvou kategorií:

- rádiové
- optické

Radiové sítě jsou co do použití nejčastější. Jsou vhodné zejména pro domácí a podnikové užití i širokopásmový přístup k internetu. Rádiové sítě se velmi liší svým dosahem – čím vyšší kmitočet, tím nižší dosah. Signál o nízkém kmitočtu se šíří povrchovou vlnou – kopíruje povrch země. Signál o kmitočtu 1 Ghz a výše se šíří jako přímá vlna a je omezen geometrickým horizontem, proto je jeho dosah zpravidla omezen přímou viditelností.

Optické bezdrátové sítě nabízejí střední dosah přenosu (x100 m) a vysokou přenosovou rychlost. Nasazení optické bezdrátové technologie je vhodné například při nutnosti spojit dvě budovy jedné společnosti (podmínka pro aplikaci je přímá viditelnost mezi těmito budovami).

4.4 Rádiové sítě

Vzhledem k tomu, že cílem této práce je objasnit problematiku zabezpečení, nikoliv problematiku rádiové komunikace, zmíním se o fyzikálních a technologických principech bezdrátové komunikace jen všeobecně.

4.4.1 Výkon rádiových systémů

Vyšší výkon znamená větší dosah sítě, ale také větší možnosti pro narušitele. Možnost připojení z větší vzdálenosti, větší možnost při použití útoku DoS a větší naději na úspěch útoku Man In The Midle na fyzické vrstvě.

4.4.2 Antény

Antény jsou významným prvkem bezdrátové sítě a hrají také významnou úlohu při jejich zabezpečení. Dvě hlavní vlastnosti, které charakterizují anténu jsou tyto:

- **zisk** – zesílení výkonu měřené v dBi, dB vztažené k imaginárnímu izotropickému vysílači, který září ve všech směrech
- **šířka paprsku** – beamwidth – popisuje zónu pokrytí anténou a bývá zpravidla trojrozměrný (horizontální i vertikální)

Antény se dělí dle typu vyzařovací charakteristiky na několik základních typů:

- **všesměrové –** (tzv. pruty) – vyzařují v okruhu 360 °. Umísťují se na stožáru, sloupu, stropě, vysílají v horizontální rovině
- **částečně směrové** – (patche, panelové, sektorové, Yagi) – vyzařovací charakteristika 60-120 °.
- **vysoce směrové** – parabolické, mřížkové (tzv. síta), vyzařovací charakteristika je v jednotkách stupňů vertikálně i horizontálně.

Umístění a správný výběr antén pomáhá vymezit jinak neurčité hranice bezdrátové sítě. Zatímco při návrhu sítě je vhodné použít směrové antény, například pro penetrační test je ideální použít antény sektorové nebo všesměrové. Ovšem všesměrová anténa s vysokým výkonem je omezena ve vertikálním směru, může tedy nastat problém např. při jejím použití v budovách s více patry.

4.4.3 Kabeláž a konektory

Kabely patří mezi hlavní strůjce ztrát v bezdrátových sítích, proto vždy volíme kabeláž s co nejmenším útlumem. Je nutné, aby kabely měli stejnou impedanci (zpravidla 50 Ω) jako všechny ostatní prvky v síti.

Pro WLAN je maximálně důležitý silný a jasný signál a dobrá citlivost přijímače. Z provozního i bezpečnostního mohou nehodné kabely znamenat ztrátu signálu, a tím otevřít cestu útokům Man In The Midle na fyzické vrstvě.

4.4.4 Kmitočtové pásmo

Bezdrátové sítě potřebují ke své činnosti kmitočtové pásmo, které je buď volné (bezlicenční) nebo pásmo, které vyžaduje licenci. Provoz rádiových sítí sleduje autorita Regulátora. Jeho kontrolní orgány mají za úkol kontrolovat provoz licencovaných i bezlicenčních pásem.

4.4.5 Porovnání bezdrátových sítí a technologií

Bezdrátové sítě se značně liší svoji povahou. Každá ze sítí, zejména pokud je dělíme dle dosahu, má svá specifika. Různé vlastnosti také mají sítě užité pro datovou komunikaci a jinak se tváří sítě pro hlasový přenos. Tyto sítě se také liší objektem provozovatele (osoby zodpovědné za zabezpečení): u mobilních sítí je vnitřní zabezpečení mimo dosah působnosti uživatele ovšem v sítích WPAN a WLAN je bezpečnost komunikace plně v režii vlastníka, provozovatele a uživatele v jedné osobě.

Tabulka 1: Porovnání bezdrátových technologií

technologie	spektrum	fyzická vrstva	maximální kapacita	dosah	rušení	bezpečnost
malé (osobní) sítě WPAN						
802.15.3a	7,5 Ghz	110-480 Mbit/s	10m	ne	vysoká	
bezdrátové sítě LAN (WLAN)						
80211b	2,4Ghz	DSSS	11Mbit/s	100+ m	ano	třeba WPA/802.11 i
80211g	2,4Ghz	OFDM/DSSS	54Mbit/s	100 m	ano	třeba WPA/802.11 i
bezdrátové MAN (WMAN)						
IEEE802.16 WiMAX	2-11 Ghz licenční /bezlicenční	TDMA, QPSK, 16QAM, 64QAM	75Mbit/s	50 Km	omezené	vysoká
802.16e (mobilní + fixní podpora)	2-6 Ghz		30 Mbit/s	x1 Km		
Bezdrátový mobilní přístup						
802.20 MBWA	1,9 Ghz		384kbit/s	x1 Km		

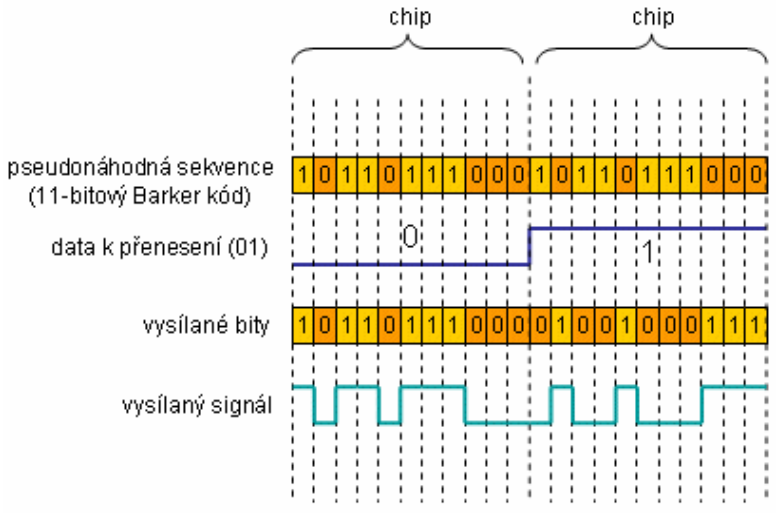
Mobilní sítě (WWAN)						
2,5 G: EDGE	1,9 Ghz		384 kbit/s	do 7 km		
3 G: UMTS	1,92 - 1,98 Ghz a 2,11 - 2,17 Ghz, 2x5 kanálů	DSSS s QSPK	2 Mbit/s (s HSPDA 10 Mbit/s)	do 7 km	omeze-né	vysoká
3 G: cdma 2000	480, 800, 900, 1700, 1800, 1900, 2100 Mhz		max 2,4 Mbit/s	x1 Km		

4.4.6 Bezpečnost rádiových sítí

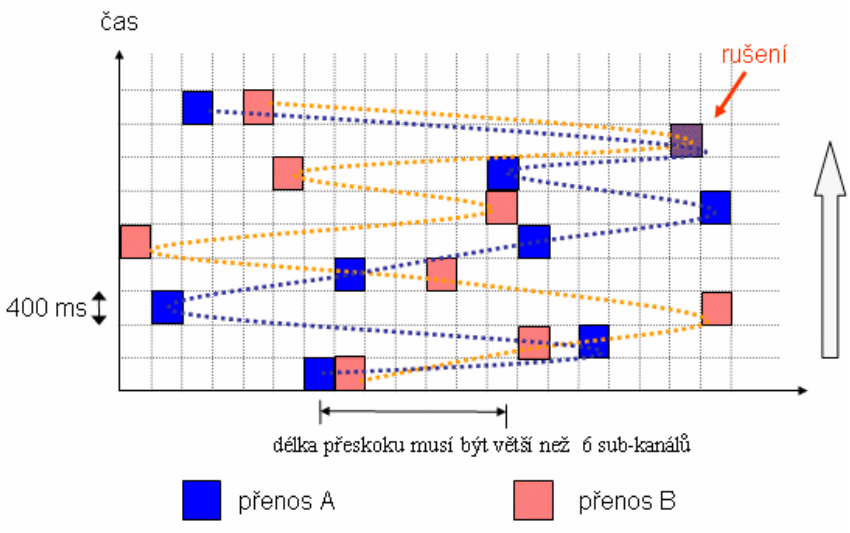
Je realitou, že rádiová komunikace prostřednictvím WLAN je velmi náchylná k odposlechu a může být snadno zachytitelná (náhodně nebo úmyslně) i do vzdálenosti několika kilometrů. Na této charakteristice nelze nic měnit, ale cílem je nedat útočníkovi šanci jakkoliv zachycená data využít, ani připojit se do dané sítě jako oprávněný uživatel.

Ve WLAN se na fyzické vrstvě nejprve použila přenosová technologie rozprostřeného pásma ve dvou typech:

- FHSS – (Frequency Hopping Spread Spektrum) – Vysílá jeden nebo více paketů pojednom kmitočtu (pásmo obsahuje 79 podkanálů), pak přeskočí na jiný kmitočet a vysílá dál. Rušení se tak minimalizuje jen na dobu, po kterou se vysílá na jednom kmitočtu. Změna kmitočtu probíhá minimálně 2,5 za sekundu, takže je málo pravděpodobná kolize. Navíc jen oprávněný příjemce zná posloupnost přeskoků kmitočtů.
- DSSS – (Direkt Sequence Spread Spektrum) – vysílač přemění tok dat na tok symbolů, kde každý symbol představuje skupinu jednoho nebo více bitů. Za použití metody QPSK vysílač moduluje nebo násobí každý symbol pseudonáhodnou sekvencí šumu – výsledkem je tzv. čip. Na generování čipu je se používá 11-bitový Barkerův kód.



Obrázek 7: Princip FHSS



Obrázek 8: Princip DSSS

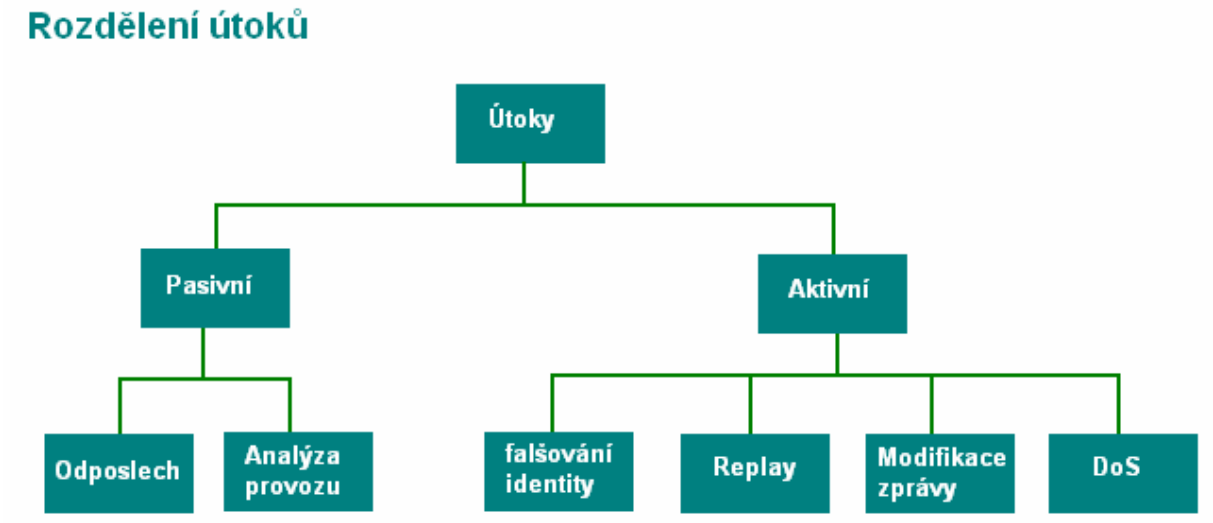
Metoda rozprostřeného spektra je schopna odolat odposlechu, ovšem pouze za předpokladu, že čipový kód nebo kontinuita přeskoků není útočníkovi známa. Tyto parametry jsou však zveřejněny v normě 802.11 pro WLAN a jsou tedy všeobecně známé.

Pro dosažení vyšší rychlosti se používá ortogonální multiplex s kmitočtovým dělením – **OFDM**, při kterém se data rozdělí na několik paralelních toků bitů. Každý tok je pak modulován jinou nosnou. Způsobem vysílání se OFDM brání zkreslení při přenosu signálu různými cestami, protože každý přenášený symbol trvá dílčí nosné déle, takže vyloučí nepříznivý dopad zpoždění signálu delší cestou.

Výhledově se také uvažuje o aplikaci metody **UWB** (Ultrawideband). Jako první se normalizuje její použití v malých sítích. UWB se dá použít pouze na krátkou vzdálenost. Nejedná se o technologii novou, pro vojenské účely se používá již třicet let. UWB rozkládá signál c rámci velmi širokého spektra, tak aby výkon v každém pásmu byl pod úrovní možného rušení jiných úzkopásmových zařízení. Proto je UWB nenáchylná na rušení, neboť systém vykazuje rovnoměrně rozprostřený výkona v celé šíři spektra. Úzkopásmové přijímače nejsou zpravidla schopny rozlišit UWB od šumu.

5 CÍLE ÚTOKU

Cílem útoku se může stát každá část informačního systému společnosti. Která z nich se stane skutečným cílem útoku pak závisí zejména na charakteru činnosti společnosti, na topologii použité sítě, na úrovni zabezpečení. Obecně se dá říci, že cílem útoku se stává každý objekt, který je nositelem informace (tedy soubor, databáze, atp.) nebo subjekt, který může být zneužit k následnému napadení objektu (například vymezení určité části broadband připojení pro útočníkovy účely). Cíle útoku mohou být náhodné nebo soustavné (záměrné). Útoky se také dělí na aktivní a pasivní. Mezi pasivní útoky patří odposlech a analýza provozu, mezi aktivní metody útoku pak patří falšování identity, opakování, modifikace zprávy a odmítnutí služby (DoS).



Obrázek 9: Dělení útoků

5.1 Náhodné cíle

Útok vedený na náhodný cíl bývá často co do intezity méně nebezpečný než útok vedený na cíl záměrný. Útočník podnikající takovýto typ útoku je zpravidla motivován jiným než finančním způsobem a jeho útok není soustavný a zpravidla ani moc cílevědomý. Nebezpečnost takového útoku spočívá zejména v jeho společenské nebezpečnosti. Útočníka napadajícího náhodné cíle bychom mohli přirovnat k výtržníkovi, který bloumajíc nočním městem bez vetšího rozmyslu likviduje vše co mu přijde pod ruku. Takovéto útoky podnikají zejména společensky málo vyspělí lidé a děti (teenageři), kteří pouze používají programy a scripty, které napsal zkušenější útočník. Také podle toho se takovýmto útočníkům

říká script-kids. Script-kids jsou nováčci a zpravidla ani netuší co dělají. Nevědí, jakého exploitu využívají a bezpečnostní komunita bývá dobře seznámena s jejich technikami. Takovýto útočníci se zpravidla zastaví na obvodových ochranných prvcích sítě a dále už neproniknou. Ovšem i přes svoji nevědomost mohou výjímečně proniknout za obvodovou ochranu sítě a tam způsobit nemalé škody.

5.2 Soustavné (záměrné) cíle

Pokud se datová síť použitá v organizaci stane soustavným cílem útočníka, nastávají této organizaci horké chvilky. Útočník, který napadá záměrný cíl bývá zpravidla finančně motivován a dostatečně vzdělán v oboru informačních technologií, sociálního inženýrství a dalších věd. Hacker má velice konkrétní představu o tom jak a proč cíl napadne. Má dostatečné technologické zázemí a umí s ním výborně operovat. Faktory, které ze sítě dělají sít rizikovou jsou následující:

- firma operuje s daty, které by mohly být lukrativní pro jiný subjekt
- firma působí ve vysoce konkurenčním prostředí
- firma má vysoký majetek
- firma se účastní soudního procesu a je držitelem důležitých informací
- firma se účastní vývoje a výzkumu
- další

5.3 Průběh záměrného útoku

Obecně se dá říci, že je vcelku jedno, zda hacker útočí na malou podnikovou síť nebo na síť domácí. Vždy podniká několik základních kroků. Patří sem tyto činnosti:

- operativní obhlídka terénu
- sledování chování subjektů a objektů v síti
- syntéza získaných údajů
- zajištění přístupu do sítě
- zneužití služeb a práce s informacemi
- vytvoření zadních vrátek do systému a zničení stop

5.3.1 Operativní obhlídka terénu

Operativní obhlídka terénu spočívá v pečlivém průzkum všech hlavních vlastností napadené sítě. Ze zjištěných informací se pak útočník pokusí sestavit podrobnou mapu vlastností sítě. V této části útoku hacker používá nenásilné metody, které mohou být dlouho neodhaleny. Prověrka sítě jde do nejmenších detailů. Průzkumník mapuje poměr signál/šum (SNR, Signal To Noise Ratio) v celé zóně pokrytí a běžně používá průběžné ověřování komunikace s AP nebo branami prostřednictvím ICMP nebo Ping. Důležitý je také údaj o ztrátovosti paketů a zpoždění. Útočník zpravidla používá běžně dostupná zařízení, která ovšem musí splňovat určité požadavky, zejména citlivosti v dBm, čipových sad, konektorů a kabeláže, externích antén, případně výdrže baterie apod. U sítí standardu 802.11 hackera zajímají zejména tyto vlastnosti sítě.:

- SSID sítě
- Doménový název a IP DNS serverů cílové sítě
- Způsob kontroly (monitoringu) sítě
- Které veřejné IP jsou volně dostupné z internetu
- Typ PC na kterých běží kritické služby – zejména hardware a operační software
- Zda je v síti použit firewall a jaký je jeho typ
- Zda je v síti aplikován detekční systém IDS
- Hierarchické uspořádání uživatelů a skupin uživatelů – jejich práva v síti.
- Fyzické umístění systému (zejména AP) v objektu
- Který provider zajišťuje připojení k internetu
- Jiné

5.3.2 Sledování chování subjektů a objektů v síti

V této fázi získává hacker konkrétní představu o vlastnostech sítě, zejména pak o použitém síťovém systému, kvalitě administrátorů apod. Útočník se nyní začíná zabývat dlouhodobějším sledováním sítě. Jedním z cílů jeho pozorování je zjištění vlastností prevenčního systému IPS (intrusion prevention systém). Začíná se také zabývat vyhledáváním slabých míst systému.

5.3.3 Syntéza získaných údajů

Při syntéze získaných údajů se hacker zaměří na široké spektrum informací o použitelných uživatelských účtech a pracovních prostředí. Rozdíl proti sledování spočívá v tom, že hacker již začíná s kontaktáží dané sítě a z tohoto důvodu již dochází k přímému spojení mezi ním a cílovou bezdrátovou sítí. I tato část má za úkol zjistit některé informace o síti. Tyto informace mohou být pro všechny typy systémů stejné, často se ovšem diametrálně liší v závislosti na síťovém systému (Windows, Linux, Novell, apod.) a proto hacker musí umět flexibilně reagovat na specifika daného typu sítě. Mezi další zjišťované položky patří:

- síťové položky
- uživatelé a uživatelské skupiny
- použité aplikace a služby
- způsob správy zařízení

5.3.4 Zajištění přístupu do sítě

Jedním z cílů útočníkova snažení je získání přístupu do sítě, převzetí kontroly nad systémem, ale častěji se hacker bude snažit získat přístup pouze k jednotlivým serverům a klientským stanicím. Tato činnost je doprovázena invazivními metodami a hacker útočí na jednu z těchto složek informačního systému:

- operační a síťový systém
- použité aplikace
- využívání nesprávné konfigurace
- využití skriptů

Útočník má na výběr z několika způsobů, jak se dostane do sítě:

- **automatizovaný útok –** hacker si vybere určitou část systému a vyhledává napadnutelná místa ve vybrané skupině veřejných IP adres. Takovýto útok se zpravidla zaměřuje na jeden typ konkrétní služby – například webové služby, které využívají portu 80. Tento útok probíhá do jisté míry automaticky dle předem určených skriptů a pravidel.

- **cílený útok –** útočník se zaměří na konkrétní síť a ví co zde chce udělat. Jedná se o velmi nebezpečný typ útoku, tento útok může být motivován například politicky nebo sociálně.

- **útoky na operační systém –** nevhodně nastavený operační systém je přímo lákadlem pro útočníky. Zpravidla je nutné OS nastavit na jiné hodnoty než defaultní a pokud se tak nestane bývá velice lehko napadnutelný (samozřejmě záleží na typu operačního sytému). Obecně se dá říci, že čím více je operační systém využíván v síťovém provozu, tím více má aktivovaných portů a tím více vrátek je otevřeno útočníkovi.
- **útoky na použité aplikace –** jedná se o využití bezpečnostních děr v konkrétních aplikacích. Obecně se dá říci že každá aplikace, která se při použití připojuje k síti, obsahuje nějakou bezpečnostní díru. Této díry může hacker využít k přístupu do systému. Z tohoto důvodu je nutné, definovat jaké programy mohou uživatelé sítě na svém PC používat a které jsou k použití nevhodné.
- **využití nesprávné konfigurace –** každou část systému (použitý hardware i software) je nutné vhodně nakonfigurovat. Například nový acces point má IP adresu a heslo udávané výrobcem a informovaný hacker tuto IP zpravidla zná. Proto je nutné tytoúdaje nastavit na hodnoty nové. Ztížíme tak hackerovi jeho práci.
- **skriptové útoky -** skriptovými útoky bývají napadeny operační systémy Linux a Unix. Tyto systémy mají už od výroby v mnoho zbytečných skriptů a Plutonů. Pokud tyto skripty a Plutony zůstanou aktivované nebo bez kontroly, stávají se pomocníkem při útoku.

5.3.5 Rozšíření oprávnění

V tuto chvíli již útočník pronikl do naší sítě. S největší pravděpodobností získal přístup k účtu nějakého zaměstnance, který měl slabé heslo nebo s ním špatně nakládal. Takovýto uživatel má ale slabá oprávnění, proto si útočník musí svá oprávnění rozšířit. Může si je rozšířit těmito způsoby:

- prolomení hesla vhodně aplikovaným programu
- hledání nešifrovaných hesel
- využití nějakého exploitu
- zneužití vztahů důvěry mezi napadeným systémem a dalšími systémy v síti
- zneužití chybných nastavení účtu

5.4 Technologické postupy útoků na síť

Následující stať popisuje některé základní technologické postupu, které může hacker použít při útoku na síť. Způsobů útoků je samozřejmě mnohem více, ale myslím si že níže vy-

jmenované se používají nejčastěji. Je také nutné si uvědomit, že hacker při útoku na síť používá více technologií.

5.4.1 Falešná zařízení

Pro bezpečnost sítě jsou z hlediska bezpečnosti nežádoucí falešná zařízení. Takováto zařízení mohou reprezentovat AP nebo i klientské stanice. Falešným zařízením se rozumí takové, které není autorizováno organizací. Mnoho falešných AP je umísťováno zaměstnanci, kteří si tak zajišťují větší svobodu pohybu po pracovišti. Tyto neautorizované AP bývají zpravidla nezabezpečené, proto mohou být snadnou kořistí útočníka. Speciální nebezpečné jsou malé AP, protože generují malý provoz (max.2-3 stanice) a nejsou v rámci infrastrukturní sítě lehce zachytitelné. Takovéto AP taky zpravidla nekomunikuje s jiným AP.

5.4.2 WEP Cracking

Jak již bylo řečeno, šifrovací algoritmus v sobě obsahuje mnoho závažných slabin. Tyto slabiny byli obecně popsány a jsou tedy útočníkům dobře známy.

- Útočník může znovu vysílat odposlechnuté rámce a navíc může v zachycených datových rámcích bez znalosti šifrovacího klíče invertovat některé bity a díky linearitě kontrolního součtu (CRC-32) použitého pro ICV upravit odpovídajícím způsobem i kontrolní součet tak, aby byl upravený rámec ostatními uzly akceptován. Toho lze využít k zahlcení sítě nebo některých uzlů, nebo lze úpravou cílových adres přesměrovat zašifrovaná data na útočníkův počítač, kam už budou doručena v otevřeném tvaru.

- Zná-li útočník obsah určitého datového rámce, může vypočítat klíčovou sekvenci pro daný tajný klíč a použitou hodnotu IV a se znalosti této klíčové sekvence dešifrovat všechny rámce zašifrované stejnou kombinací klíče a IV. IV může nabývat pouze 2^{24} různých hodnot, a proto je prakticky proveditelné, aby útočník mající přístup k otevřenému textu některých rámců zjistil hodnoty všech klíčových sekvencí a byl tak schopen dešifrovat veškerou komunikaci šifrovanou za použití daného tajného klíče. Navíc už se znalostí jediné klíčové sekvence je možné vysílat falešné šifrované rámce.

- Slabina v inicializaci PRNG v RC4 umožňuje pro určité tzv. slabé hodnoty IV útočníkovi odvodit ze znalosti prvního bajtu výstupu PRNG, který je zároveň pou-

žit jako první bajt klíčové sekvence, částečnou informaci o jednom bajtu tajného klíče. První bajt klíčové sekvence lze určit ze znalosti prvního bajtu dat, a tuto datovou hodnotu je prakticky vždy možné odhadnout. Útočník, který zachytí dostatečné množství rámců se slabým IV, pak může vypočítat tajný klíč. Známých slabých hodnot IV je cca 3000 pro 40bitové klíče resp. Cca 9000 pro 104bitové klíče.

Prolomení klíče je velmi oblíbenou metodou útočníků. K spolehlivému rozluštění je třeba komunikovat 5 – 10 miliónů paketů. Po celou dobu útoku narušitel spoléhá, že WEP klíč zůstane zachován. Při luštění WEP klíče útočník zpravidla používá freeware tool, jako jsou AirSnort nebo WEPCrack. Obrana proti WEP crackingu může být následující: použít další šifrování a autentizační mechanismy, například pomocí VPN a 802.1x

5.4.3 MAC attack

Zjištění MAC adresy pro připojení k AP probíhá podobně, jako se zjišťuje WEP klíč. Pokud není v síti WEP aktivováno, stačí narušiteli pouze odposlouchávat komunikaci mezi klientem a AP a posléze vyhledat hlavičku MAC a přečíst si ji. V případě, že je WEP aktivován, je nutné nejdříve prolomit WEP. V takovémto případě mu postačí i offline analýza zachycených dat. MAC útokům lze předcházet použitím autentizačních mechanismů jako 802.1x a zabezpečení na bázi VPN.

5.4.4 Útok typu Man-in-the-midle

Útok typu man in the midle je charakteristický tím, že útočník vstoupí mezi přístupový bod a klienta a přeruší mezi nimi komunikaci. Útočník zachytává a čte data přenášená mezi AP a klientem během asociačního procesu. Získané informace jsou následující:

- IP adresy obou zařízení
- Asociační ID klienta
- SSID AP

S těmito informacemi může být útočník schopen vytvořit podvržený přístupový bod blíže uživateli (na jiném kanálu) a změnit připojení uživatele na tento podvržený přístupový bod. Data, která takto přijal zaznamenává a také posílá na skutečný AP, takže se klient i originální AP domnívají že spolu komunikují. Útoky tohoto typu patří mezi technicky náročnější, i tak k nim ale zájemci najdou mnoho pomůcek na Internetu a nelze je šmahem

odsoudit jako předem vyloučené. Použití VPN a autentizačních mechanismů 802.1x jim může pomoci zabránit. Rovněž se vyplatí mít podrobnou radiovou mapu sítě a občas projít a zkontrolovat ručně, zda někde nevysílá nějaký přístupový bod, který nemáte v plánu a který by mohl být tím podvrženým přístupovým bodem.

5.4.5 Denial of Service

Denial of services (DoS, odepření služeb) není útok v pravém slova smyslu. Jedná se o činnost, při které útočník zahltí AP iracionálními daty ve velkém množství. AP tyto data zpracovává a dojde k jeho zahlcení nebo zhroucení. Zahlcení AP má za následek zpomalení připojení ostatních uživatelů. Takovýto útok bývá často jen málo podařeným vtípkem náctiletých uživatelů, tzv skript-kidies. V horším případě je útok DoS předzvěstí útoku Man in the middle. Nasazením DoS útočník prvně odpojí klienta od AP aby je pak nechal připojit na svoje pdostrčené AP. Obranou proti tomuto může být filtrování MAC adres. V případě, že jsou útoky vedeny z internetu, je vhodné předřadit firewall s dobrou analýzou paketů.

Tabulka 2: Další způsoby útoku na síť

Typ útoku	Technologie napadení
Odepření služby	(Denial of Service, DoS). Při tomto útoku se hacker snaží dostat systém oběti do poruchového stavu, v něm odepírá běžné služby ostatním, i právoplatným uživatelům. Možností vyvolání takového stavu je několik, například zaplavení cíle množstvím požadavků na spojení.
Distribuované odepření služeb	(Distributed Denial of Service, DDoS). Tento typ operace útočí na vyhlédnutý cíl z většího množství různých napadených nic netušících systémů.
Útoky se záplavou paketů SYN	V rámci tohoto útoku se síť zahltí pakety SYN, které normálně znamenají zahájení požadavku na spojení. Výsledkem je naprosté vytížení procesoru, paměti a síťového rozhraní, že systém již nemůže obsluhovat právoplatné požadavky spojen a vzniká odepření služeb (DoS)

Útok se záplavou paketů UDP	Tento útok je podobný záplavě ICMP paketů a opět znamená zasílání paketů v takovém množství, že se cílový systém výrazně zpomalí a nedokáže zpracovávat platná spojení. Naprosto typickým zástupcem je záplava paketů na port 53, který obsluhuje službu DNS.
Prohledávání portů	Útok s prohledáváním portů znamená vysílání paketů s různými čísli portů a jeho cílem je nalezení dostupných služeb.
Smrtelný ping	Specifikace protokolu TCP/IP určuje pro přenos datagramu jistou velikost paketu. Mnohé implementace protokolu ping umožňují ale uživateli podle potřeby i zadání jiné, větší velikosti paketu. Výrazně nadměrný paket ICMP může přitom v systém vyvolat množství nejrůznějších reakcí, jako je odepření služeb, havárie systému, jeho zablokování či restart.
Falšováni IP adres	Při tomto útoku se útočník pokouší obejít bezpečnostní kontroly tím, že napodobuje IP adresu, e-mailovou adresu nebo uživatelský ID platného klienta. To je pro hackera důležité především při zneužití vztahu důvěry mezi počítači, které v sítích bývají často definovány
Pozemní útok	(land attack). Kombinace útoku záplavou paketů SYN a falšováním IP adresy. Útočník zasílá do cílové sítě zfalšované SYN, jejichž zdrojovou i cílovou IP adresu tvoří skutečná IP adresa oběti.Přijímací systém na tyto pakety reaguje odesíláním paketu SYN-ACK sobě samému a vytvoří tak prázdné spojení , které zůstává otevřené do vypršení časového limitu. Záplava prázdných spojení může systém zcela zahltit a dostat jej tak do stavu odepření služeb (DoS).
Tear drop	Tento útok zneužívá mechanizmus rekonstrukce neboli opětovného sestavení fragmentovaných paketů IP. Jedním z údajů hlavičky IP je totiž offset (relativní adresa). Pokud se součet offsetu a velikosti jednoho paketu liší od stejného součtu v dalším fragmentovaném paketu, znamená to, že se oba pakety překrývají a server může při pokusu o jejich rekonstrukci zhavarovat.

Prohledávání s dotazy ping	Podobný jako prohledávání portů. Útočník při této operaci zasílá požadavky opakování echo ICMP neboli ping, a to na různé cílové adresy. Přitom sleduje, jestli mu některý z cílů odpoví a on se tak dozví IP adresu potenciální oběti.
Soubory Java/ActiveX/ZIP/EXE.	Do této kategorie spadají různé zlomyslné javové Applety nebo komponenty ActveX, skryté ve webových stránkách. Po stažení na počítač se nainstalují jako trojský kůň. Tyto trojské koně mohou být skryty také v různých souborech typu .zip, .gzip a .tar, nebo ve spustitelných souborech .exe. Vhodným nastavením bezpečnostních mechanismů je možné všechny javové Applty a objekty ActiveX ve webových stránkách zablokovat a stejně tak nepropouštět ani přílohy typu .zip, .gzip, .tar a .exe v elektronické poště.
Útok WinNuke	Výraz WinNuke označuje hackerskou aplikaci, jejímž jediným úkolem je přivést k havárii jakýkoliv počítač Windows, připojeným do Internetu. Aplikace WinNuke odesílá do hostitelského systému s navázaným spojením data mimo NETBIOS, které u mnoha počítačů vede k havárii.
Hrubá síla	U této metody se útočník pokouší uhodnout hesla do systému pomocí primitivních technik, jako je opakované přihlašování pod určitý účet s výrazy převzatými ze slovníku možných hesel.
Zdrojové směrování	Mechanismus zdrojového směrování je variantou hlavičky paketu IP, v níž samotný zdroj definuje způsob směrování paketů. Směrovací informace v hlavičkách IP mohou například obsahovat jinou IP adresu, než samostatný zdroj v hlavičce. Pakety se tak odešlou jiným směrem. Směrování paketů ICMP je možné ovládat několika dalšími způsoby
Záznam cesty	Útočník odesílá pakety s volbou IP 7 (Rekord route, záznam cesty). Zaznamenanou cestu tvoří posloupnost internetových adres, jejichž analýzou může vnější pozorovatel zjistit zajímavé informace o schématu adresování a topologii vnitřní sítě

Volné zdrojové směrování	Útočník odesílá pakety s volbou IP 3 (Loose source routing). To znamená, že zdroj paketu může určit směrování, podle něhož se bude paket odesílat do cíle přes jednotlivé brány. Každá z bran a hostitelů může ale odesílat paket na další trasu v požadované cestě přes libovolný počet mezilehlých bran. Proto hovoříme o volném zdrojovém směrování.
Striknízdrojové směrování	Útočník odesílá pakety s volbou IP 9 (Strict source routing). Zdroj paketu v takovém případě určí přesné směrování paketu do cíle. Každá z bran a hostitelů musí ale odeslat datagram na další adresu v požadované cestě přímo a pouze přes přímo připojenou síť. Proto hovoříme o strikním směřování
Záplava paketů ICMP	Tento útok znamená, že dotazy ICMP neboli ping přetíží cílový systém takovým množstvím požadavků na opakování (echo), že systém zcela vyčerpá své prostředky na odpovědi a nemůže zpracovávat normální, platný provoz. Zpráv ICMP existuje několik typů přičemž každá má svůj význam a každá může být užitečná i pro útočníka:
ICMP Echo Reply	Odpověď na opakování, kód 0. Jedná se o odpověď ping. Mnohé firewallu jejich průchod povolují, aby se uživatelé uvnitř sítě mohli dostat k externím prostředkům. Zároveň jsou i účinnou metodou k vedení útoku
ICMP Host Unreachable	Hostitel je nedosažitelný, kód 3. Chybová zpráva z hostitele či směrovače, která znamená, že odeslaný paket nedorazil do cíle
ICMP Source Quench	Zpomalení zdroje, kód 4. tato odpověď indikuje zahlcení určitého místa v Internetu. Pokud se někdo rozhodne zahltit naši síť takovými pakety, pokouší se fakticky přesvědčit počítače o zpomalení vysílání dat.
ICMP Redirect	Přesměrování, kód 5. Zpráva se žádostí o přesměrování provozu. Útočník tak může změnit chování výchozího směrovače a může například vést útok s mužem uprostřed, kdy veškerý náš provoz přesměruje na svůj počítač

ICMP Echo Request	Žádost o opakování, kód 8. Tyto pakety s požadavkem ping se používají velice běžně. Mohou sice znamenat nežádoucí aktivity průzkumu počítače, ale z velké části bývají součástí normálního provozu sítě
ICMP Time Exceeded for a Datagram	Překroční času pro přenos datagram, kód 11. Uvedená zpráva znamená, že paket nedorazilo cíle z důvodu překroční určitého časového limitu.
ICMP Parameter Problem on Datagram	Problém v parametru datagram, kód 12. U této zprávy se děje něco neobvyklého. Často je indikátorem útoku
Velký paket ICMP	Paket ICMP o délce přes 1024 bajtů může u některých zařízení znamenat problémy, protože tato velikost již není považována za normální
Odposlech paketů	Tato technika představuje pasivní metodu útoku, při níž se karta síťového rozhraní přepne do promiskuitního režimu.Pokud se útočníkovi podaří dostat do lokální sítě LAN nástroj na odposlech, znamená to, že již došlo k velmi vážnému narušení bezpečnosti. A protože útočník vidi většinu paketů v síti LAN

6 PENETRAČNÍ TEST SÍTĚ

Pro zjištění nebezpečí, které v sobě každá WLAN skrývá je nejlepší provést tzv. penetrační test. Otestováním možností průniku do sítě se o jejich slabinách dozvíme nejvíce. Penetrační test by měl provádět spolehlivý, na zřizovateli sítě nezávislý odborník. Tento odborník by měl mít dobré znalosti chování bezpečnostních opatření bezdrátových sítí a také by měl mít povědomí o chování rádiového signálu.

6.1 Vybavení pro penetrační test

Vybavení pro testování WLAN je velmi podobné tomu, které by použil hacker, jedná se zejména o:

- laptop s podporou dvojí PCMCI, měl by podporovat linux a/nebo BSD
- PCMCI karty s konektory pro externí antény, karty by měly být od různých výrobců
- alespoň dvě antény (všesměrová a směrová)
- specifické prostředky pro bezdrátové testování
- volitelné doplňky – náhradní baterie, přijímač GPS, zesilovače signálu apod.

6.2 Site survey

Základem pro testování, podobně jako pro samotné budování sítě, je detailní průzkum místa (site survey). Z pohledu testování penetrace se pomocí site survey můžeme dozvědět následující:

- místa, která jsou vhodná pro výchozí útok narušitele, tedy místa, kde mohou nerušeně odposlouchávat signál a zpracovávat informace
- neautorizované přístupové body
- sousední sítě, odkud může přijít útok (náhodný a/nebo záměrný)
- stávající zdroje šumu – poslouží jako základ pro pozdější odhalení zdrojů nadměrného šumu
- další problémy, spojené spíše s návrhem sítě, které ovšem nemusí souviset s bezpečností sítě

Poslední bod, ač to tak nemusí vypadat, je velice důležitý. Vzhledem k odlišnému typu nosiče informace oproti pevným sítím může správce sítě dojít k chybným závěrům. Špat-

nou konfiguraci sítě lze snadno zaměnit útok typu DoS (např. vysoký počet paketů na WLAN, toto může být způsobeno nevhodnou maximální délkou rámce – 2312 oproti 1500 na ethernetu)

6.3 Speciální prostředky pro testování penetrace

Prostředků pro audit bezdrátové bezpečnosti je dostatek a jejich počet i nadále rostoucí. Většina jich je ve statusu freeware a jsou tedy dostupné zdarma. Většina z těchto nástrojů se v síti chová specificky. Je tedy vhodné pozorovat jak se konkrétní tool projevuje, protože se pravděpodobně bude nacházet také v arsenálu narušitele. Specifické prostředky pro penetrační test jsou tedy následující:

- prostředky pro rozbití šifry – pro rozbití WEP (např. AirSnort, Wepcrack, Dweputils, Wep_tools, WepAttack), pro získání klíčů na klientských stanicích, pro napadení systému autentizace 802.11x
- prostředky pro generování rámců 802.11 – např. AirJack, File2air, Libwlan, FakeAP, Void11, Wnet
- prostředky pro podsunutí šifrovaného provozu – např. Wepedgie
- software pro management přístupových bodů

7 POLITIKA DATOVÉ BEZPEČNOSTI ORGANIZACE

Datová bezpečnost by měla být zakotvena v bezpečnostních směrnicích organizace. Při návrhu zabezpečené sítě je vhodné vycházet z dokumentu, který měl obsahovat alespoň základní pravidla postupu při realizaci bezpečné sítě, říkejme mu „Rozvaha projektu datové bezpečnosti organizace“. Tento dokument by měl vznikat za spolupráce širokého okruhu zaměstnanců, zejména pak vrcholného managementu, IT specialisty a facility managera organizace. Tento dokument je rozdělen na tři základní kapitoly, kterými jsou:

- určení cíle
- určení strategie
- určení politiky

7.1 Určení cíle

Určení cíle je konkrétní popsání stavu, do kterého je třeba danou síť přestavět. Měly by být definovány prioritní oblasti, kterým je třeba věnovat největší pozornost. Obecně je se dá říci, že cílem by mělo být:

Vyloučení přímých a nepřímých ztrát, které jsou způsobeny zneužitím, zničením, poškozením a/nebo nedostupností informací. Zároveň je nutné vytvořit fungující, vyrovnaný a cenově výhodný systém zabezpečení informací

V této kapitole by měla být finanční rozvaha projektu datového zabezpečení.

7.2 Určení strategie

V této části našeho dokumentu je vhodné určit, jakým způsobem chce daná organizace dosáhnout cíle, spočívajícího v kvalitním zabezpečení sítě. Nutností je definování typu dat a informací a složek informačního sytému, které jsou obsaženy v koncepci bezpečnostního řešení. Měly by být popsány divize společnosti a partneři, kteří se budou účastnit Je vhodné zvážit, nakolik jsou daná opatření funkční a zda například příliš nekomplikují provoz firmy.

7.3 Určení politiky

Určení politiky při návrhu vhodného bezpečnostního systému spočívá v definování pravidel, která vedou k zajištění adekvátního zabezpečení datové sítě.

Politika bezpečnosti společnosti v oblasti zabezpečení dat je obecně založena na rozpoznání vhodného (autorizovaného) a nevhodného (neautorizovaného) přístupu k informacím a datům. Cílem vhodného zabezpečení datové bezdrátové sítě, je zajistit datům:

- autenticitu
- integritu
- dostupnost
- prokazatelnost a nepopiratelnost odpovědnosti
- spolehlivost a důvěrnost

7.4 Koncepce ochrany

Budovat informační systém s řízenou datovou bezpečností je méně nákladné (časově, finančně) než datové zabezpečení implementovat v již existujícím (nezabezpečeném) informačním systému.

7.4.1 Důvěra

Otázka důvěry v organizaci je velice důležitá a pro dobré fungování hraje velkou roli. Je nutné definovat, komu v organizaci je možné důvěřovat zcela a komu již méně. Definování důvěry by mělo pokrýt všechny oblasti fungování firmy (zejména pak zaměstnance a technologie). Základním omylem je teze, že důvěřovat nelze nikomu ani ničemu. I opačný způsob přístupu k problému, tedy že důvěřovat lze každému, je velice scestný. Bezpečnostní zásady je nutné nastavit tak, aby vznikla rovnováha mezi důvěrou a bezpečností

Vhodné zabezpečení informačního systému postaveného na standardu IEEE802.11 je založeno na kombinaci několika základních opatření. Primární body, kterých je třeba si všímat jsou následující:

- celkový pohled
- řízení
- administrativa
- technologie

- právní stránka
- psychologická, sociální

7.4.2 Celkový pohled

Navrhovat bezpečnostní opatření je nutné až po provedení celkového auditu stávajících opatření. Tento audit by měl být zaměřen zejména na zkoumání technického stavu použitých zařízení, dále pak na samotné uživatele informačního systému a celkové klima ve firmě.

7.4.3 Řízení

Je nutné, aby management organizace pochopil důležitost bezpečnostních opatření na úseku informačních technologií a byl odhodlán aplikovat bezpečnostní opatření

7.4.4 Administrativa

Část firmy, zabývající se administrativou je oblastí, kde dochází nejvíce k unikům informací, proto je třeba věnovat této části organizace zvýšenou pozornost. Tato část firmy by také měla být velmi otevřená principům a potřebám aplikace bezpečnostních opatření.

7.4.5 Technologie

Technologie užité k dosažení datové bezpečnosti jsou kritickou složkou celého systému. Je ale scestné si myslet, že pokud mám špičkové zařízení, bude celý systém bezchybný.

7.4.6 Právní složka

Při návrhu bezpečného informačního systému je třeba dbát na platné právní ustanovení státu. Veškeré bezpečnostní opatření proto musí být v souladu se zákony.

7.4.7 Psychologická, sociální

Při provádění auditu se zaměřujeme také na celkové vyznění psycho-sociálního klimatu ve firmě. Je třeba eliminovat zejména nespolehlivé a labilní jedince, kteří mají přístup k citlivým datům.

7.5 Zásady zabezpečení firemní bezdrátové sítě

Jak již bylo řečeno, zásady zabezpečení bezdrátové sítě jsou zásadním a důležitým prvkem při tvorbě zabezpečené bezdrátové sítě. Vhodně definované zásady popisují chování objektů a subjektů v síti a vytvářejí tak normu, podle které je posuzováno veškeré další dění v síti. Naše zásady by neměly omezovat běžný provoz sítě ale také musí zajišťovat vhodné chování všech objektů a subjektů v síti i vně sítě. Pokud tedy aplikujeme bezpečnostní zásady, je jasné, jakým způsobem mají být nastaveny servery, jaké firewally mají být použity atp. Jedná se o souhrn následujících vlastností a dějů:

- Kompletní a aktuální přehled o bezdrátových zařízeních – kontrola, registrace, aktualizace a monitorování používaných zařízení pro možnosti zabezpečení, aktualizace MAC adres pro filtraci, kontinuální upgrade bezpečnostních zařízení
- Vzdělání a zodpovědnost uživatelů – důkladná znalost bezpečnostní politiky a podmínek používání bezdrátových zařízení, přísný zákaz neautorizované instalace a používání jakéhokoliv bezdrátového zařízení (WLAN, Bluetooth, apod.)
- Fyzické zabezpečení – umístění prvků bezdrátové sítě, tak aby bylo zabráněno krádeži nebo zničení, venkovní zařízení má být hlídáno podobně jako objekt sám.
- Zabezpečení na fyzické vrstvě – EIRP v povolených mezích, vhodná volba a umístění antény, v případě potřeby je vhodné použít blokovací reflektory pro šíření signálu nevhodným směrem.
- Instalace sítě – více přístupových bodů zvyšuje odolnost sítě proti útokům typu Man in the Modele a DoS. WLAN by měla být v jiné doméně než pevná část sítě, u přístupových bodů připojených k různým přepínačům by všechny tyto přepínače měli patřit do stejné WLAN. Brána mezi bezdrátovou a pevnou částí by měla obsahovat správné oddělení a podporovat implementaci autentizaci a šifrování.
- Zabezpečení sítě – u WLAN by identifikátor sítě SSID neměl obsahovat žádné informace užitečné pro potenciálního útočníka (např. SSID bezdrátové sítě použité na fakultě aplikované informatiky ve formě UTB_U5 je tedy silně nevyhovující). Měla by být nastavena filtrace MAC, 8021x, WPA/WPA2, prověřit všechny protokoly ve WLAN a odstranit všechny nepotřebné pro omezení propustnosti sítě a bezpečnostních slabin.
- Politika hesel – volba délky a stylu hesel, tak aby se minimalizovali všechny možnosti útoku na hesla jak hrubou silou (dostatečná délka a kombinace malá/VELKÁ písmena) tak na základě slovníku (dostatečná délka)

- Monitoring sítě a reakce na narušení bezpečnosti – důkladná dokumentace a řešení zjištěných problémů
- Pravidelný audit bezpečnosti sítě – pravidelné prověrky externími specialisty s cílem odhalit všechna slabá místa a navrhnout řešení.

7.5.1 Konkrétní aplikace použité k zajištění zásad zabezpečení

Následující tabulka shrnuje základní principy, které je nutné dodržet při aplikaci zásad zabezpečení. Všechny by měly být dodrženy v co největší míře – pokud je jedna z nich podceněna, snižuje se účinnost všech ostatních.

Tabulka 3: Zásady zabezpečení firemní sítě

Typ zásady	Obecný popis zásady
Bezdrátová komunikace	Určuje pravidla pro přístup do podnikové sítě prostřednictvím zabezpečených mechanismů bezdrátové komunikace
Virtuální privátní sítě (VPN)	Stanovuje zásady vzdáleného přístupu přes síť VPN s IPSec nebo L2TP do vnitřní firemní sítě
Zabezpečení serverů	Vymezuje standarty pro základní konfiguraci interních serverů, které jsou ve vlastnictví firmy, případně pracují ve webovém hostovaném prostoru.
Zabezpečení směrovačů a přepínačů	Popisuje povinnou minimální bezpečnostní konfiguraci všech směrovačů a přepínačů, připojených do ostré provozní sítě, nebo požívaných v jakémkoliv ostrém provozním prostředí
Vzdálený přístup	Definuje standarty pro připojení libovolného hostitele do firemní sítě. Tyto standarty sledují minimalizaci různých potenciálních hrozeb, jako je ztráta citlivých nebo důvěrných firemních dat, duševního vlastnictví, poškození image firmy na veřejnosti, poškození kriticky důležitých vnitřních systémů atd.

Posuzování rizik	Zmocňuje oddělení informační bezpečnosti k provádění pravidelného posuzování rizik bezpečnosti informací, jehož účelem je zjištění zranitelných míst v síti a zahájení nápravných opatření
Hesla	Zavádí standarty pro vytváření silných hesel, ochranu šifer a frekvenci změn hesel.
Antivirová ochrana	Vymezuje požadavky, jež musí splňovat počítače připojené do podnikové sítě s ohledem na účinnou detekci virů a jejich prevence.
Citlivost informací	Napomáhá zaměstnancům určit, které informace smí sdělovat cizím osobám (mimo zaměstnanců), a také relativní citlivost informací, které bez oprávnění sdělovat nesmí
Extranet	Určuje zásady, podle nichž se do firemní sítě připojit cizí organizace za účelem provádění transakcí
Vytáčený přístup	Stanovuje pravidla pro ochranu elektronických informací před neúmyslným ohrožením, jestliže zaměstnanec pracuje s nad vytáčeným připojením
Přístupové informace k databázím	Určuje požadavky na bezpečné ukládání a načítání uživatelských jmen a hesel k databázím, které budou využívat programy při přístupu k databázi provozované na firemní síti
Automaticky přeposílaná pošta	Zakazuje neoprávněné i neúmyslné prozrazování citlivých firemních informací
Audit	Členům oddělení informační bezpečnosti přiděluje oprávnění k výkonu bezpečnostního auditu nad libovolným systémem, který je ve vlastnictví společnosti nebo který je v jejích prostorách nainstalován.
Standardy poskytovatelů aplikač-	Definuje minimální bezpečnost, kterou musí splňovat každý poskytovatel aplikačních služeb (ASP)

ních služeb	
Poskytovatelé aplikačních služeb	Vyjadřuje požadavky firmy na poskytovatele aplikačních služeb (Application Service Providers, ASP). Tito poskytovatelé zajišťují společně softwarové, hardwarové i síťové technologie. Součástí těchto zásad jsou také samostatné standardy poskytovatelů
Analogové linky	Popisuje způsoby přípustného využívání analogových telefonních linek a linek ISDN a nařizuje příslušné zásady a postupy pro schvalování. Pro linky, určené výhradně pro faxování a příjem hovorů, a linky zapojené do počítačů platí samostatná pravidla
Přípustné užití	Vymezuje osoby, které smí pracovat s počítačovým zařízením a sítěmi ve vlastnictví společnosti. Týká se firemních počítačů, umístěných ve firemních prostorách i v domácnostech zaměstnanců.
Přípustné šifrování	Stanovuje pravidla, která omezují šifrování jen na obecně známé, prověřené a účinné algoritmy. Navíc určuje potřebné postupy, které zajišťují naplnění příslušných zákonů a nižších předpisů

7.6 Zavádění zabezpečené datové sítě

Zavádění bezpečnostních opatření do praxe bývá zpravidla doprovázeno velkými obtížemi. Profesionální zabezpečení sítě vyžaduje velké investice do technického vybavení a zvýšení povědomí uživatelů datové sítě zejména na úseku pravidel bezpečnosti. Nová pravidla také zpravidla omezují stávající praktiky uživatelů sítě, takže je nutné je dostatečně poučit o důvodech, které firmu vedly k zavedení nových pravidel a opatření. Důležitou částí realizace nových opatření je plná podpora managementu organizace.

7.6.1 Časté chyby při aplikaci nových opatření

Aby bylo zavedení nových opatření co nejvíce bezproblémové, je nutné postupovat zodpovědně a vyvarovat se několika častých chyb. Je nutné postupovat dle „Rozvahy projektu datové bezpečnosti organizace“. Pokud dojde k odklonu od základních pravidel „Rozvahy“ může dojít ke snížení funkčnosti celého systému opatření, případně k jeho celkové nefunkčnosti. Protože je zřízení zabezpečené datové sítě finančně náročné, měla by si organizace také vytvořit dostatečnou finanční zálohu, aby byla schopná projekt dostatečně finančně zajistit. Při výstavbě zabezpečené sítě by organizace neměla spoléhat pouze na vlastní zaměstnance, ale měla by oslovit společnosti erudované v oblasti datové bezpečnosti, na druhou stranu není příliš vhodné si vytvořit závislost na externích partnerech. Zároveň je nutné si uvědomit, že nejslabším článkem zabezpečené sítě je lidský faktor. Proto se nespoléháme pouze na technologie, ale snažíme se zajistit jejich vhodnou kooperaci s poučenými uživateli sítě.

8 BEZDRÁTOVÉ SÍTĚ 802.11

Před zavedením normy 802.11 se bezdrátové přenosy dat používaly výjimečně a byly doménou zejména sektoru obrany státu a příbuzných oblastí. Protože v této oblasti nebyla zavedena funkční a jednotná standardizace, většina použitých zařízení byla vzájemně nekompatibilní

8.1 Historie

Hlavním důvodem pro vznik normy 802.11 v roce 1997 byla právě vzájemná nekompatibilita mezi zařízeními a protokoly v bezdrátové komunikaci. Standard 802.11 je oficiální normou bezdrátových sítí LAN (WLAN, wireless lan area network) a byl vydán organizací IEEE. Tato organizace se zabývá normalizací bezdrátových sítí v rámci výboru 802. O evropská specifika normy 802.11 se stará organizace ETSI a o její severoamerickou příbuznou se stará organizace FCC. Mimo sítí 802.11 se IEEE zabývá i několika dalšími typy bezdrátových rádiových sítí. Jedná se zejména o tyto v rámci výboru **802:**

- IEEE 820.11 – bezdrátové lokální sítě (WLAN)
- IEEE 820.15 – bezdrátové osobní sítě (WPAN)
- IEEE 820.16 – širokopásmový bezdrátový přístup (WMAN)
- IEEE 820.20 – širokopásmové mobilní sítě (MBWA)
- IEEE 820.21 – roaming mezi sítěmi (Media Independent Handoff)
- IEEE 820.22 – WRAN (Wireless Regional Area Network)

O přesné vyznění normy 802.11 a zejména o praktické věci se stará organizace Wi-Fi Alliance (Wi-Fi, wireles fidelity). Tato organizace uděluje výrobkům logo Wi-Fi, které potvrzuje kompatibilitu se standardem.

Obrázek 10: Logo Wi-Fi aliance

Výše znázorněné logo zaručuje, že je jeho nositel kompatibilní se všemi jinými nositeli loga lze je v vzájemně kombinovat. Výjimkou je pouze vzájemná nekompabilita mezi standardy 802.11a a 802.11b/g. Tyto výrobky mezi sebou propojit nelze.

Následující tabulka shrnuje všechny etapy vývoje IEEE 802.11 a zabývá se také blízkou budoucností tohoto tématu.

Tabulka 4: Historie bezdrátových sítí 802.11x

Standard	Rok	Vlastnosti
802.11a	1999	Standard definuje fyzickou vrstvu, která pracuje v pásmu 5GHz, používá metodu modulace OFDM (*Orthogonal Frequency Division Multiplexing*) a podporuje přenosovou rychlost 54 Mb/s.
802.11b	1999	Standard definuje fyzickou vrstvu, která v pásmu 2,4 GHz pracuje s metodami modulace FHSS a DSSS. Podporuje přenosovou rychlost 11 Mb/s.
802.11d	2001	Pro země, kde pásmo 2,4 GHz není přístupné.
802.11c	2003	Mosty (*Bridge*) mezi přístupovými body. Využívají ho přístupové body (*access points)*
802.11e	2003	Podpora pro QoS (*Quality of Service*) na MAC vrst-

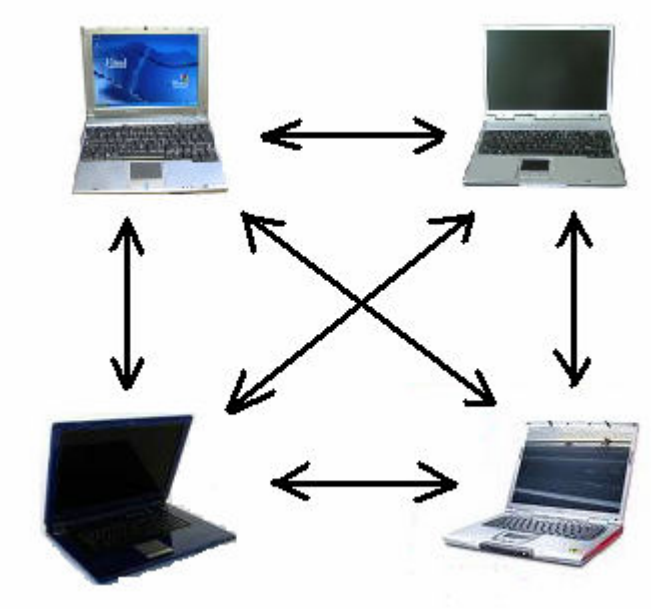
		vě. Zlepšení přenosu zvuku a obrazu.
802.11f	2003	Spolupráce přístupových bodů od různých výrobců. Umožňuje přecházet mezi jednotlivými přístupovými uzly (*roaming*)
802.11g	2003	Standard zavádí do pásma 2,4 GHz modulační metodu OFDM, která svými parametry překonává FHSS i DSSS a umožňuje rychlost až 54 Mb/s.
802.11h	2003	Umožňuje v Evropě používat WLAN v pásmu 5 GHz. Dynamický výběr kanálu a regulace výkonu.
802.11i	2004	Zabezpečovací a ověřovací mechanismy na MAC vrstvě. Zvýšení bezpečnosti přenášených dat.
802.11j	2004	Využití pásma 4,9 a 5 GHz v Japonsku.
802.11k	BUDOUCTNOST	Měření rádiových prostředků.
802.11m		Revize standardů.
802.11n		Vysoká propustnost.
802.11p		Bezdrátový přístup pro mobilní zařízení.
802.11r		Rychlý roaming.
802.11u		Spolupráce s externími sítěmi.
802.11.2		Měření a testování WLAN zařízení.
802.11v		Management bezdrátových zařízení.
802.11s		Multi-hopping.
802.11w		Podpora integrity, autenticity, utajení a ochrany dat.

8.2 Typy sítí

Bezdrátové sítě mají dle svých norem definovány dva základní druhy sítí, dle kterých je pak odvozena topologie.V prvním případě se klienti připojují přímo mezi sebou. Tento režim se nazývá IBSS neboli ad-hoc. V druhém případě se klienti v sítí připojí k centrálnímu přístupovému bodu (acces pointu). Takovýto režim se nazývá BSS/ESS neboli režim infrastrukturní.

8.2.1 Sítě Ad-hoc

Síť koncipovanou jak ad-hoc jsou výhodné v tom, že nepotřebují k činnosti žádný přístupový bod. Tyto sítě pracují v režimu peer-to-peer a každý klient je v podstatě autonomní přístupový bod. Při takto strukturované síti je nutné, aby všichni účastníci byli blízko u sebe a jejich počet je omezený. Sítě ad-hoc se využívá například pokud je nutné krátkodobě spojit několik počítačů při konferenci atp. Bezpečnostní podmínky u takovéto sítě jsou jednoduché: stačí pouze znát použitý kanál a SSID. U ad-hoc lze použít i WEP.

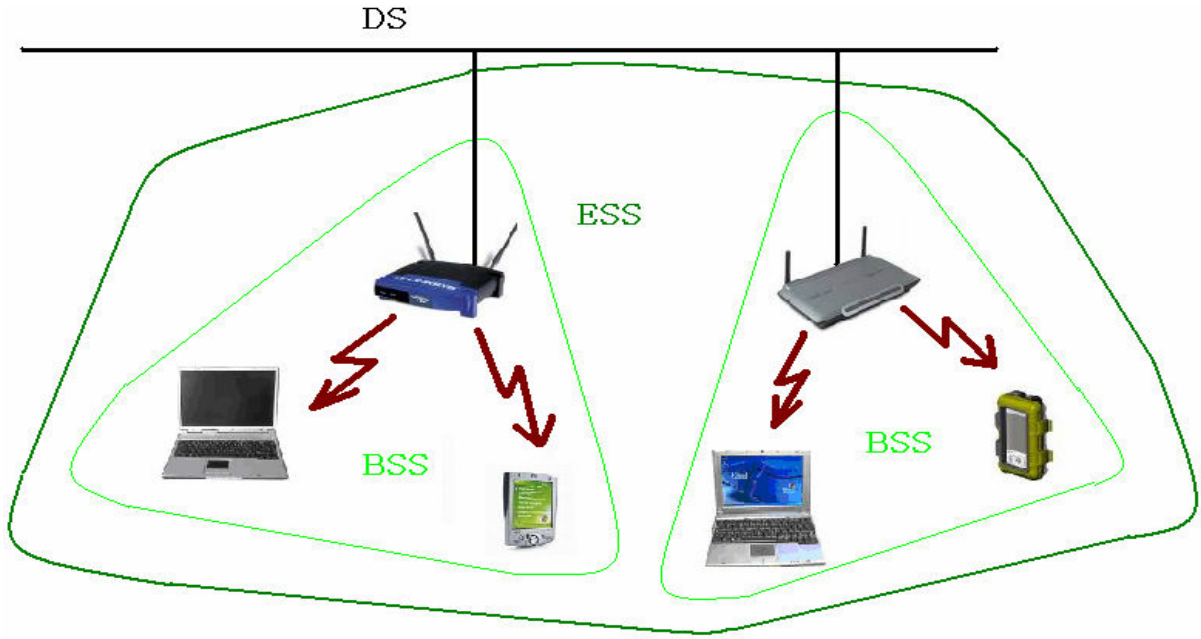


Obrázek 11: Schéma Ad-Hoc sítě

8.2.2 Infrastrukturní sítě - BSS/ESS

V těchto sítích musí být alespoň jeden přístupový bod AP (BSS). BSS (Basic service set) je přístupový bod, který může být připojen k nějakému uzlu (např. Ethernet, přes něj může

být do sítě distribuován internet). Jednotlivé bezdrátové stanice se připojí k tomuto AP a veškerý provoz v síti je jim řízen.ESS (extended service system) jsou dvě nebo více propojených BSS, které jsou navzájem propojeny přes distribuční systém. Distribučním systém bývá ethernet, ale může to být i WDS (wireless distribution system). Tento typ sítě se používá mnohem častěji než typ ad-hoc.



Obrázek 12: Schéma infrastrukturní sítě BSS/ESS

9 ZABEZPEČENÍ SÍTÍ 802.11 (WLAN)

Zabezpečit síť postavenou na standardu 802.11 je složitější než vhodně zajistit běžnou metalickou síť. Důvodů proč tomu tak je několik. První vychází ze samotného principu šíření radiového signálu prostředím. Nelze přesně definovat, kde bude signál dosažitelný a kde už dosažitelný nebude. V všech místech, kde je signál zachytitelný, lze pomocí volně dostupného software a vhodného hardware síť odposlouchávat a analyzovat. Bezpečnostní prvky v normě 802.11a/b/g se ale zaměřují pouze na autentizaci, šifrování a integritu dat. Autorizace není součástí specifikace a musí se provádět externími mechanismy (např. mechanismem pro řízení přístupu 802.1x). Z tohoto důvodu byly do bezdrátové sítě implementovány speciální externí bezpečnostní mechanismy, které měly bezdrátovou síť přiblížit klasické metalické. Bohužel, jejich kvalita je na různé úrovni a ne vždy vyhovují alespoň základním požadavkům zabezpečení.

9.1 Přístupový bod – AP

Principem funkce AP v bezdrátové síti je podpora komunikace mezi klientskými zařízeními v síti na základě normy 802.11. Působí jako mezilehlé zařízení , kdy rámce vysílané jednou stanicí v dané WLAN musí AP vyslat na adresu cílové stanice. AP nejen propojuje dvě a více stanic a plní taky roli spojky bezdrátové sítě a sítě pevné (zpravidla ethernetu). V tomto případě plní všechny funkce mostu – sledování MAC adres, jaká MAC se skrývá za jakým portem, předávání rámců mezi klienty na základě tabulky adres a filtrace klientů apod.

Existuje několik pravidel pro zvýšení bezpečnosti funkcí samotného AP, mezi ně patří zejména tyto:

- je vhodné pořizovat AP s pamětí typu Flash – tato paměť usnadňuje aplikaci bezpečnostních záplat a opatření
- AP by měl podporovat VLAN (Virtual LAN), pomocí kterého lze sdružovat uživatele do skupin a přidělit každé ze skupin konkrétní přístupová oprávnění. VLAN také umožní oddělit běžný provoz od managementu sítě.
- AP je nutno mechanicky chránit, aby jej nebylo možné snadno resetovat (po resetu dojde k obnovení výrobních nastavení zařízení, která jsou všeobecně známá), ukrást nebo poškodit.

- na rozhraní pro management aplikovat silná hesla a šifrování, pro vzdálený přístup na AP (přístup na AP lze také omezit pouze na konkrétní místa na ethernetu), aby neautorizovaný personál nebyl schopen provádět změny v konfiguraci
- protokol pro management SNMP používat až od verze 3

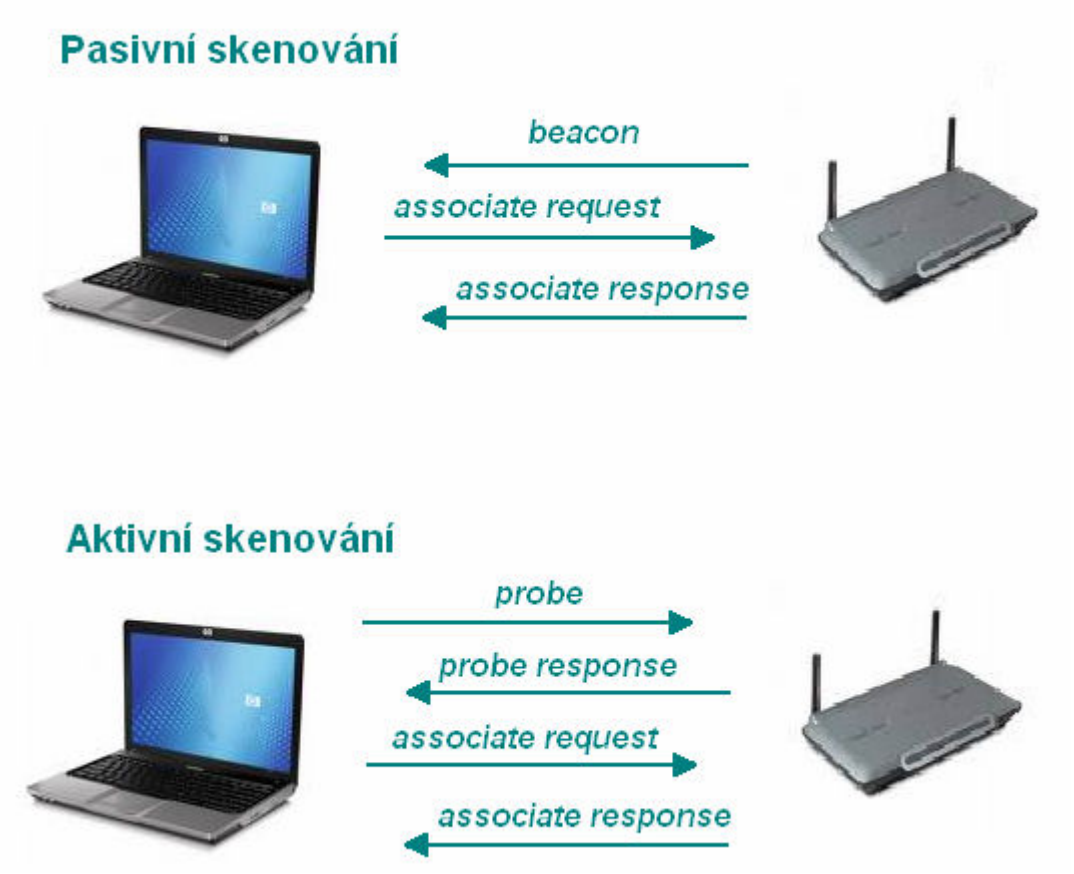
9.1.1 AP ve funkci bezdrátového směrovače

Bezdrátový směrovač bývá často integrován v některých AP a doplňuje funkce AP na fyzické a spojové vrstvě o funkci síťové vrstvy, tedy o směrování. Běžně podporovanou je také funkce NAT (překlad adres IP) nebo DHCP (dynamické přidělování IP adres klientským stanicím). Klientské IP jsou pak v AP přeloženy na jedinečnou, často globálně unikátní IP adresu, která je pak komunikována. NAT představuje jeden z bezpečnostních prvků, protože interní adresy se nezveřejňují na internetu (byl jsem ale svědkem použití techniky, která neměla s identifikací IP za překladem nejmenší problém). Naopak aplikace DHCP je bezpečnostním rizikem, protože lze IP adresu získat vcelku jednoduše.

9.2 Přidružení k WLAN

Přidružení k WLAN probíhá na základě skenování provozu v síti. Skenování probíhá vždy při poklesu intenzity signálu a při zvýšené chybovosti. Skenování může být také spuštěno uživatelem nebo operačním systémem. Při pasivním skenování stanice jen určitou dobu a zajímají ji jen specifické rámce *(beacon)*, které implicitně AP vysílá a které obsahují informace o AP (SSID). Při aktivním skenování klient vysílá na jednotlivých kanálech pokusné rámce *(probes)* a čeká od dostupných AP odezvu. Před samotným přidružením k AP musí klient splnit požadavky autentizaci. Autentizace může být otevřená (open-systém), nebo prostřednictvím klíče, který sdílí všechny stanice WLAN (shared-key). Při přidružování k AP prochází klient těmito stavy:

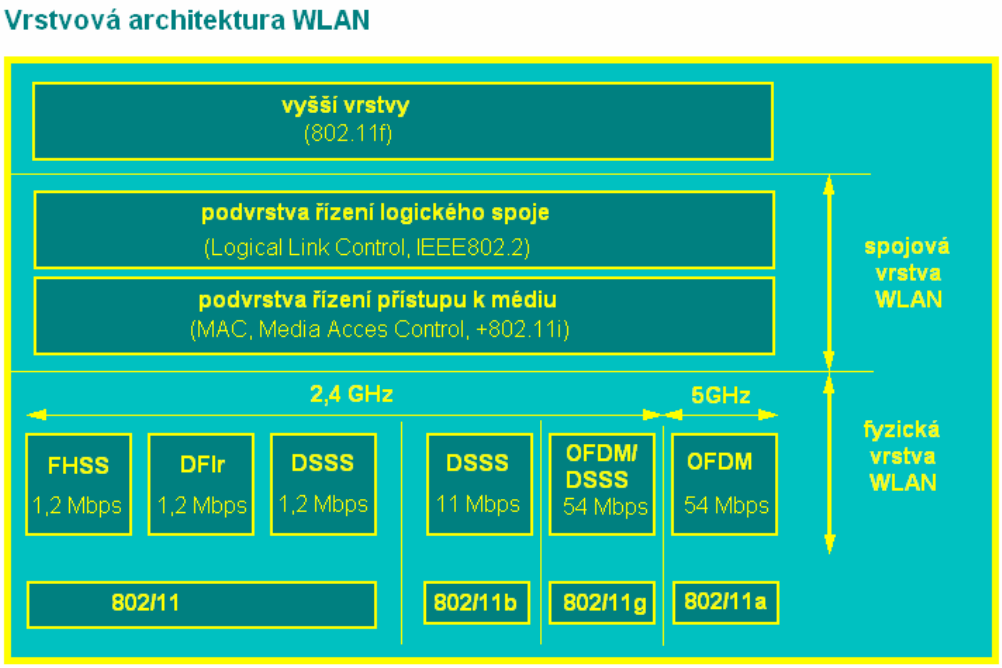
- neautentizován a nepřidružen
- autentizován a nepřidružen
- autentizován a přidružen



Obrázek 13: Pasivní a aktivní skenování sítě

9.3 Typy WLAN

Všechny WLAN pracují v bezlicenčním pásmu 2,4 nebo 5 GHz. Obrázek níže popisuje, které vrstvy/podvrstvy referenčního modelu ISO/OSI jsou v rámci 802.11 použity.



Obrázek 14: Vrstvová architektura WLAN

V dnešní době lze použít tři typy WLAN. Jsou to tyto:

- IEEE 802.11a - pracuju v pásmu 5,1 – 5,53 GHz a 5,725 – 5,825 GHz s dosahem 50-70m, nabízí maximální datovou rychlost 54Mbit/s
- IEEE 802.11b – (Wi-Fi) pracuje v pásmu 2,4 Ghz na bázi rozprostřeného spektra, s dosahem 100-300m a maximální rychlost na fyzické vrstvě je 11Mbit/s. V České republice se používá 13 kanálů v rozsahu kmitočtů 2,412 - 2,472 GHz. Odstup mezi kanály je 5 MHz, celkem lze použít tři nepřekrývající se kanály.
- IEEE 802.11g – rychlejší verze Wi-Fi, v pásmu 2,4 Ghz, zpětně slučitelná s IEEE 802.11b s maximální rychlostí 54 Mbit/s

9.4 Protokol řízení přístupu k médiu MAC

Důležitou vrstvou bezdrátové sítě je podvrstva nazývána MAC (*Media Access Control*). MAC podvrstva slouží jako rozhraní mezi fyzickou vrstvou a hostitelským zařízením. Pro podvrstvu MAC jsou důležité dvě vlastnosti.

- CRC (Cyclic Redundancy Check), kontrolní cyklický součet – kontrola přenosu paketů
- fragmentace paketů – rozdělení paketů na menší části, přenáší se postupně.

Podvrstva MAC je zodpovědná za přenos dat, přidružení stanice, autentizaci, utajení dat a management napájení. Pro koordinaci přístupu k médiím slouží dvě funkce:

- DCF (Distributed Coordination Function) funkce distribuované koordinace
- PCF (Point Coordination Function) funkce koordinace s jedním bodem

Funkce DCF se používá pro standard 802.11 navržený pro datové přenosy a založený na metodě přístupu CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Jedná se o systém předcházení kolizím. U bezdrátových sítí se špatně detekují kolizní stavy. Stanice nejprve naslouchá, zda někdo nevysílá a pokud je médium volné,může stanice začít vysílat. Příjemce poté pošle stanici potvrzovací paket. Funkce PCF je vhodná pro aplikace reálného času, například k přenosu videa. Používá se ale jen zřídka.

Dále může nastat situace, kdy stanice na sebe „nevidí“. Typicky tato situace nastává ve venkovním prostředí. Kdy vznikne tzv. skrytý uzel (*hidden node*), stanice slyší vysílání jenom některých stanic, ale ne všech. Často by tedy mohlo docházet ke kolizím ve vysílaní. Z tohoto důvodu byl vyvinut mechanizmus RTS/CTS (*Request-To-Send/Clear-To-Send)*, který zabraňuje vzniku kolizí.

9.5 Bezpečnost WLAN na jednotlivých vrstvách

9.5.1 Bezpečnost na fyzické vrstvě

Fyzická vrstva obstarává technické problémy komunikace. Jedná se zejména o modulaci, řešení šumu a rušení a vazbu mezi propustností dat a modulací. Bezpečnost na úrovni fyzické vrstvy se dá zajistit vhodnou volbou následující vlastností:

- vymezení prostoru a omezení průniku signálu – je vhodné použít stavební materiály s omezenou propustností rádiového signálu (kovové prvky je třeba uzemnit). Okna by měla být opatřena termální izolací. Dobrou volbou je i nátěr na bázi kovu aplikovaný uvnitř i vně budovy (tyto kroky sice dobře zabezpečí vnitřní WLAN společnosti, ale utlumí používání dalších bezdrátových zařízení komunikujících směrem ven, např. mobilní telefony, proto je třeba každý krok dobře uvážit).
- Anténa – směrovost antény je důležitá pro vymezení prostoru, kam bude distribuován signál (je nutné změřit směrovost antény i směrem, kam by dle reglementu neměla zářit – setkal jsem se anténou typu síto, která zářila více směrem za anténu než směrem v před).

- Modulace – pro průnik do WLAN musí útočník použít stejný typ modulace, který je použit v síti (jedná se o DSSS nebo OFDM).
- Identifikátor sítě – ve stejném fyzickém prostoru můžou existovat maximálně tři virtuální sítě – tyto sítě musí být odlišeny identifikátory SSID nebo ESSID. Klient se nemůže bez znalosti identifikátoru do sítě přihlásit.

9.5.2 Bezpečnost na spojové vrstvě

Funkcí spojové vrstvy je zejména obstarávání spojovacích mostů *(STP, Spanning Tree Protocol)* mezi stranami komunikace. Další prací je přepínání a VLAN. Součástí spojové vrstvy je podvrstva MAC, která má za úkol chybové řízení, management zahlcení sítě *(CSMA/CA)*, agregace paketů a volitelné šifrování. Bezpečnost na spojové vrstvě se dá zajistit následovně:

- MAC adresy - adresy NIC jednotlivých stanic mohou být spárovány s IP adresami klientů. Takovýto seznam IP a MAC klientů se ukládá do přístupového seznamu (ACL, Acces Kontrol List) – pomocí MAC lze jasně popsat pravidla přístupu. Při použití bezdrátových mostů lze také povolit/zakázat komunikaci mezi dvěma držiteli MAC adres.
- Protokol – v případě podpory více síťových protokolů ve WLAN (která mezi protokoly nijak nerozlišuje, rámce jsou vždy stejné), lze filtrovat provoz (např. zakázat IPX, AppleTalk, apod.)
- Autentizace – ověřování identity klienta probíhá na druhé vrstvě otevřeně (open-systém) nebo pomocí sdíleného klíče (shared-key), nebo na základě 802.1x EAP, s využitím autentizačního protokolu (zpravidla Radius).
- Šifrování – na bázi mechanismů specifikovaných ve WEP nebo DES/3DES (64bitový klíč), či AES (802.11i, 128bitový klíč), tyto mechanismy jsou použitelné pouze pro bezdrátový spoj.

9.5.3 Bezpečnost na síťové vrstvě

Funkcemi síťové vrstvy jsou následující činnosti: směrování, management přidělování šířky pásma, podpora QoS, roaming na 3. vrstvě (fyzické předávání klientů mezi AP). Bezpečnost na úrovni síťové vrstvy zajišťují:

- filtrace IP adres – bezdrátové směrovače dovolují aplikovat řízení přístupu na základě přístupových seznamů IP adres

- firewall – některé bezdrátové směrovače mají zabudovanou funkci firewall, jedná se zejména o blokován provozu z internetu do AP.
- VPN – IP VPN se budují zejména pomocí mechanizmů nejnižších tří vrstev. Šifrování pomocí IPSec a tunelování pomocí L2TP, nebo PPTP (zajišťují koncové zašifrování mezi WLAN stanicí a VPN serverem)

9.5.4 Bezpečnost na aplikační vrstvě

Aplikační vrstva má za úkol monitorovat provoz v síti. Zabývá se také managementem a návrhem sítě. Bezpečnost aplikační vrstvy zajišťuje:

- **RADIUS server –** komunikace s RADIUS serverem pro autentizaci klientů.

9.6 SSID

Access point zpravidla vysílá takzvanou administrativní signalizaci – beacon. Pomocí tohoto signálu dává AP najevo svoji existenci v dané lokalitě a zároveň se pomocí ní orientují připojená zařízení. Jednou z částí beaconu je SSID (service set identifier) a je společně s technologií WEP základním pilířem zabezpečení sítí 802.11. Beacon poskytuje základní informace o AP, zejména pak podporované rychlosti, označení sítě a o intenzitě signálu. Klienti přistupující k síti se mohou připojit pouze k síti, jejíž SSID znají. Tímto je také zamezeno klientskému zařízení, aby se připojilo k AP, které v dané lokalitě působí paralelně, ovšem není naše cílové. Vhodnou technikou může být nakonfigurování AP tak, aby nevysílal beacon pravidelně. Tím lze datovou sít částečně zakrýt před útočníkem. Tato technika je ovšem pouze primárním opatřením a zcela jistě dokonale nezabrání informovanému útočníkovi aby byl síť schopen napadnout (k obejití nepravidelně vysílaného beaconu se používá tzv. technika falešného požadavku). Často se také používá rozšířené verze SSID, tzv. ESSID (extended SSID), které slouží pro řízení přístupu k síti. ESSID se nikdy nevysílá, ale je uloženo přímo v AP. Stanice které znají ESSID mají povolen přístup k AP. Všechny ostatní jsou z komunikace vyloučeny. Síť, ve které je aplikováno ESSID se nazývá uzavřená.

Tabulka 5: Výchozí hodnoty SSID různých výrobců

Výrobce	Výchozí hodnota SSID
3Com	101,comcomcom
Proxim	Tsunami,WaveLAN
Dlink	WLAN
Linksys	Linksys, wireless
NetGear	Wireless
SMC	WLAN
Zyxel	Wireless
Ovislink	Airlive
Compex	Any

9.7 WEP

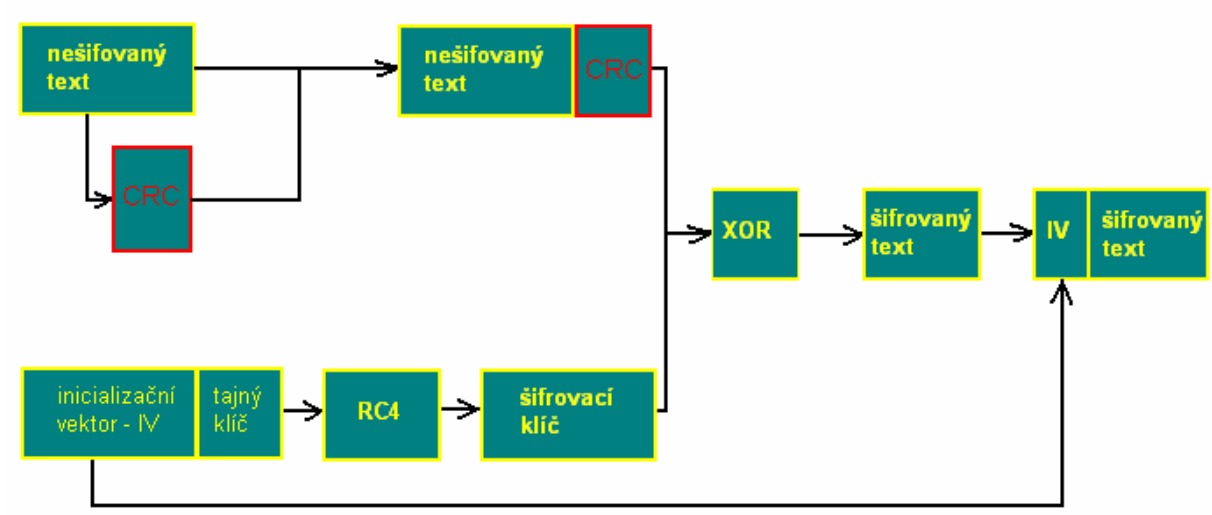
WEP – wired equivalent privacy – soukromí odpovídající metalické síti. Tento typ bezpečnostního protokolu byl implementován do bezdrátových sítí už od normy 802.11b. Cílem WEP je zajistit uživatelům sítě stejnou úroveň bezpečnosti, jakou mají k dispozici uživatelé metalické sítě (například ethernetu). Překotný a zároveň nejednotný vývoj WEP měl za následek to, že samotný protokol obsahuje mnoho nedostatků a chyb. WEP nebyl navrhován jako hlavní bezpečnostní aplikace, ale pouze jako jakási platforma pro finální a rozhodující aplikaci, která měla vlastností WEP využívat. WEP byl navržen jako nástroj k autentizaci a pro ochranu dat šifrováním osobním (privátním) klíčem. WEP tedy používá symetrický způsob šifrování (jako klíč se obvykle používá slovo nebo sekvence znaků).

9.7.1 Funkce protokolu WEP

Ke správnému pochopení funkce protokolu WEP je třeba se seznámit s průběhem jeho aplikace.

Prvním krokem při aplikaci WEP je spočítání 32-bitového cyklického redundantního součtu (CRC). CRC se pak připojí k přenášenému textu. Přenášená informace se zašifruje

64/128 bitovým klíčem. Tento klíč sestává z uživatelského klíče v délce 40/104 bitů a dynamicky se měnícího inicializačního vektoru (IV). IV má délku vždy právě 24 bitů. Nakombinováním tohoto klíče a IV vznikne za pomocí generátoru čísel RC4 šifrovací klíč. Následuje aplikace logické funkce XOR mezi přenášenou informací s kontrolním součtem a IV. Výsledkem aplikace XOR je šifrovaný text, ke kterému se připojuje IV. Šifrovaný text s připojeným IV pak přenášíme.

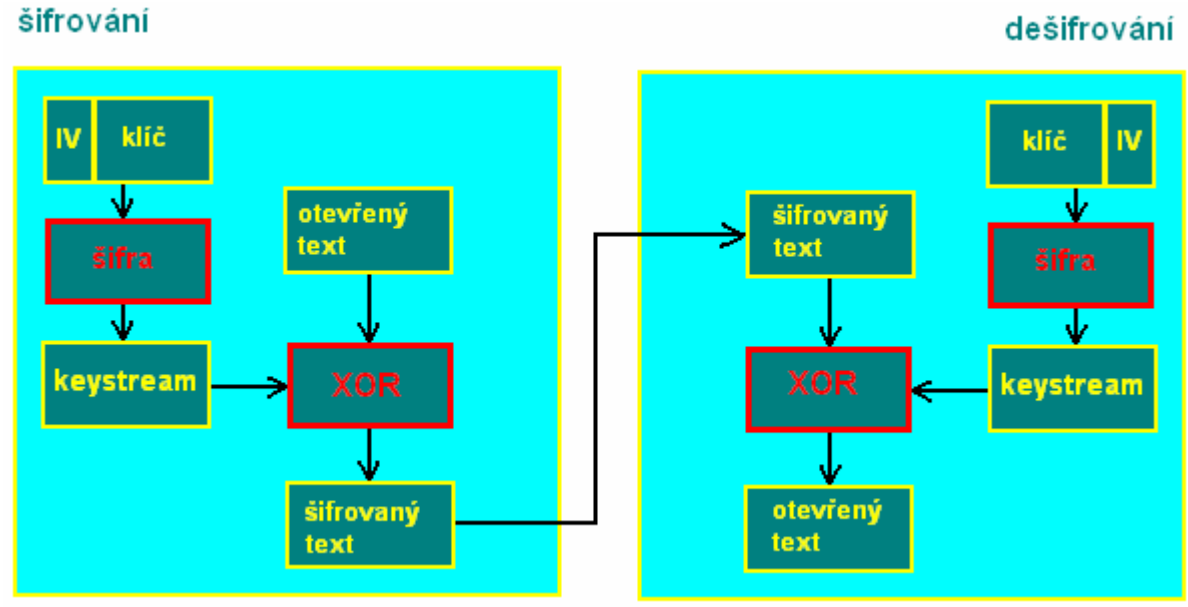


Obrázek 15: Princip WEP

Inicializační vektor IV se používá pro zmírnění statičnosti klíče. Protože stejná zpráva by vedla ke stejnému zašifrovanému textu. Množina IV může nabývat celkem 2^{24} kombinací. Velmi rychle se při velkém provozu sítě vyčerpá. Potom musíme použít použitou hodnotu IV a právě tímto bude porušeno pravidlo RC4, že nesmí být klíč použít opakovaně. Problémem WEP je, že žádná norma nám neříká, jak IV měnit. Výrobci IV s každým paketem většinou mění, ale často je znám vzorec nastavení IV. Při inicializaci karty vždy začít na 0 a každým paketem IV zvyšovat o 1. To ulehčuje útočníkům práci.

Symetrická proudová šifra RC4 Jde o šifru, která se používá i v SSL (Secure Sockets Layer), kde slouží pro webové zabezpečení. Byla zvolena pro svoji jednoduchou implementaci přímo do hardwaru síťové karty. RC4 dovoluje klíč o délce do 256 bytů, 802.11 pro WEP zvolilo délku 40 bitů.

Šifra RC4 generuje pseudonáhodná čísla (PRNG, PseudoRandom Number Generator), která jsou základem kombinace tajného klíče a IV. Symetrická proudová šifra RC4 (obrázek 13) doplní klíč o IV a sestaví tak keystream. Šifrování spočívá v operaci XOR mezi otevřeným textem a keystreamem. Dešifrování znamená XOR mezi keystreamem a zašifrovaným textem. Funkce XOR umožňuje opětovným použitím na výsledek získat původní hodnotu. Proto je tedy WEP náchylný na útoky ze strany útočníka. Tato šifra se používá hlavně z důvodů snadné implementace do bezdrátových adaptérů a díky tomu to nemá vliv na výkon počítače.



Obrázek 16: Princip symetrické šifry RC4

9.8 Řízení přístupu do sítě

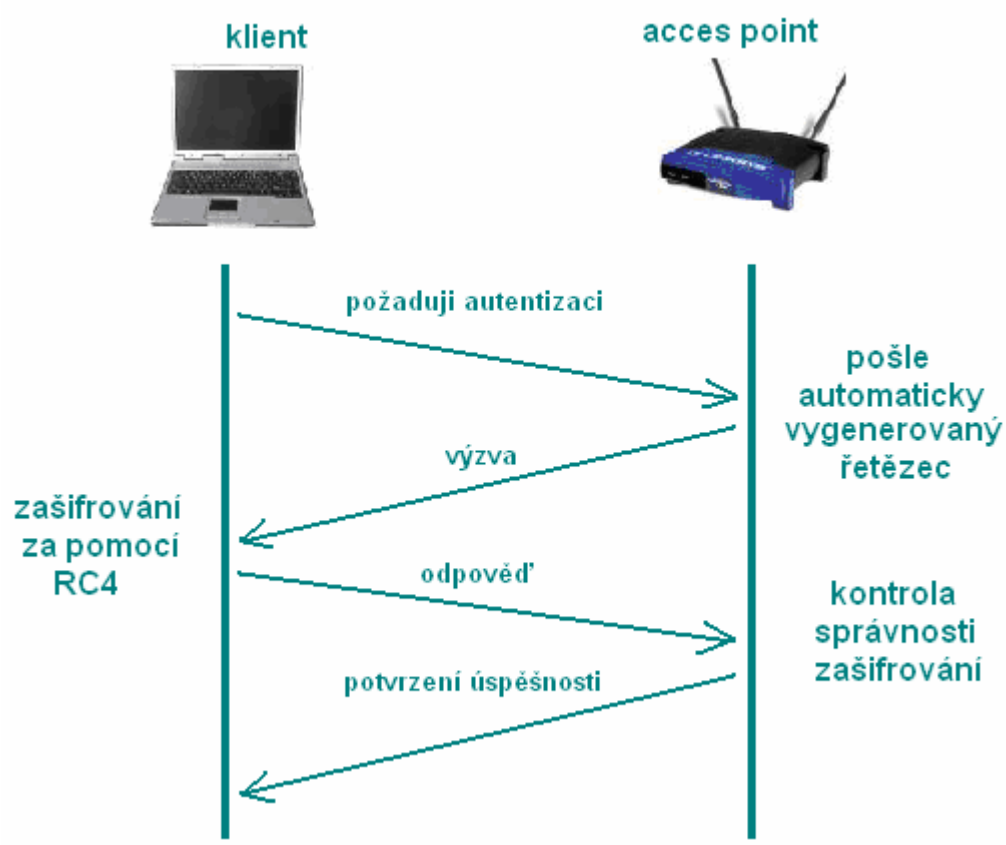
Řízení přístupu do sítě je jedním ze základních prvků bezpečnosti. Při řízení přístupu lze mluvit o autentizaci. Protokol 802.11 specifikuje dvě základní metody pro autentizaci. Jedná se o Open-system autentizaci a Shared-key autentizaci.

9.8.1 Open-system autentizace

Autentizace typu open-system je základním principem přístupu k síti 802.11. Průběh open-system autentizace je následující: klient odvysílá informaci o sobě v podobě SSID. Na tuto výzvu AP odpoví a pošle data zpět. Pokud je klientovi požadavek odepřen, je mu zakázáno přistupovat k síti. Tento způsob autentizace se běžně používá ve veřejných bezplatných sítí.

9.8.2 Shared-key autentizace

Použití shared key autentizace je z hlediska bezpečnosti vhodnější. Přístup do sítě je povolen jen stanicím, které se prokáží validním klíčem (např. WEP). Heslo není při provozu v síti komunikováno. Klient, který se chce do sítě přihlásit, dostane od AP žádost o autentizaci, kterou reprezentuje náhodně generovaný řetězec znaků. Klient tento řetězec zašifruje za použití síťového šifrovacího klíče a takto upravený jej zašle zpět. AP potom zkontroluje správnost šifrování a rozhodne o povolení/zamezení přístupu do sítě.



Obrázek 17: Shared-key autentizaci

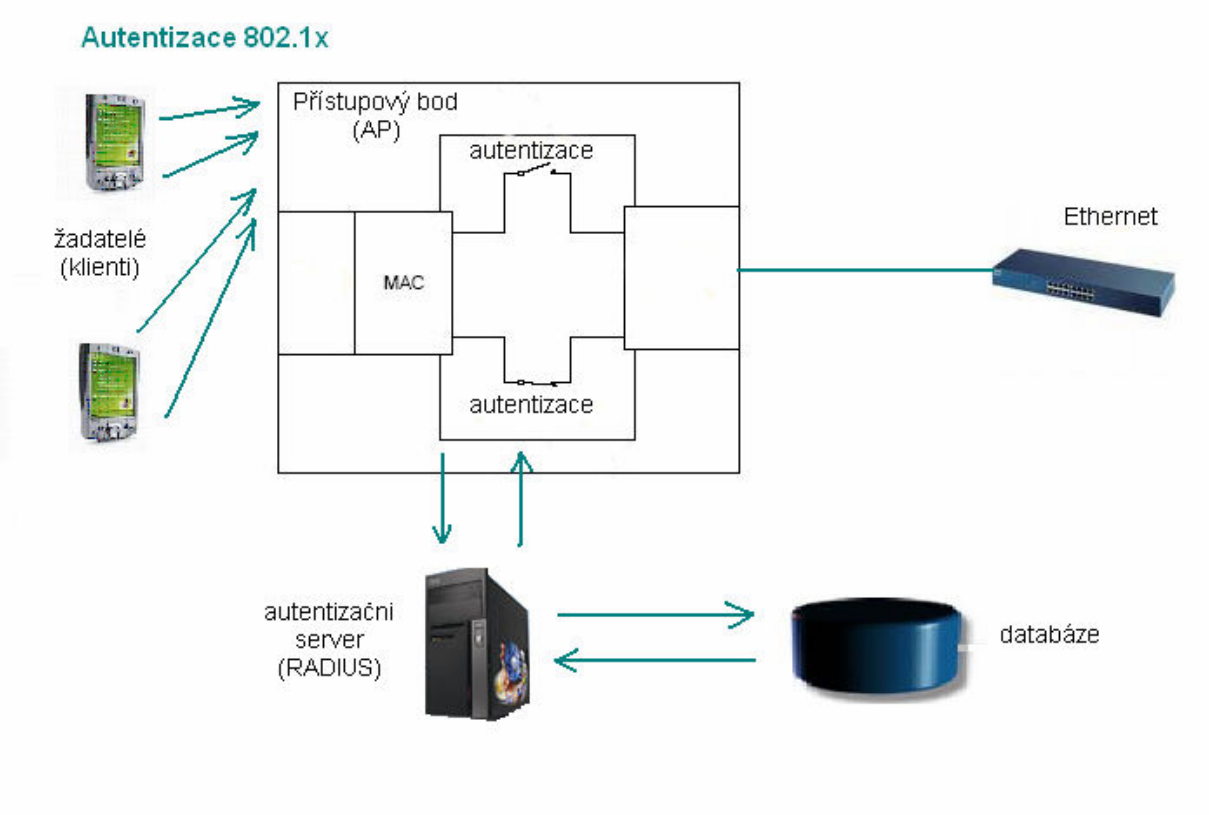
9.9 Flitrování MAC adres

MAC (media acces control) je unikátní adresa určitých síťových komponent (síťových karet, acces pointů, atp.). Tato hexadecimální adresa je definována již při výrobě karty výrobcem a je neměnná. Přístupový bod je schopen udržovat seznam autorizovaných MAC a povolí přístup pouze těm držitelům MAC, které jsou v seznamu. Neměnnost MAC je ale pouze relativní. Pokud je útočník dosti schopný, dokáže MAC adresy odposlechnout

a pomocí vhodného software je může simulovat. Touto technikou se útočník může vydávat za autorizovaný subjekt, i když jím nebude. V praxi se provádí také párování MAC s konkrétní IP adresou. V tomto případě musí být držitel MAC adresy také držitelem IP adresy - pokud IP nebo MAC neodpovídá informacím v databázi IP, není přístup povolen. Databáze informací o klientských MAC a IP musí být vhodně zabezpečena, protože se často stává terčem útoků.

9.10 IEEE 802.1x – řízení přístupu

Výše zmíněné mechanismy a postupy nezaručují příliš velký stupeň zabezpečení. Jistě lze najít aplikace, kde je třeba využít kvalitnější metody. Jako jedno ze standardních řešení se používá 802.1x pro řízení přístupu. Jedná se o obecný rámec pravidel aplikovaných ve všech druzích sítí (tedy nejenom v sítích bezdrátových). V našem případě se jedná o vylepšenou verzi protokolu WEP. Používá se pro autentizaci uživatelů, integritu dat a distribuci klíčů. Autentizace se aplikuje na úrovni portů přístupového bodu k WLAN. Protokol 802.1x tedy blokuje přístup segmentu lokální sítě pro neoprávněné uživatele.



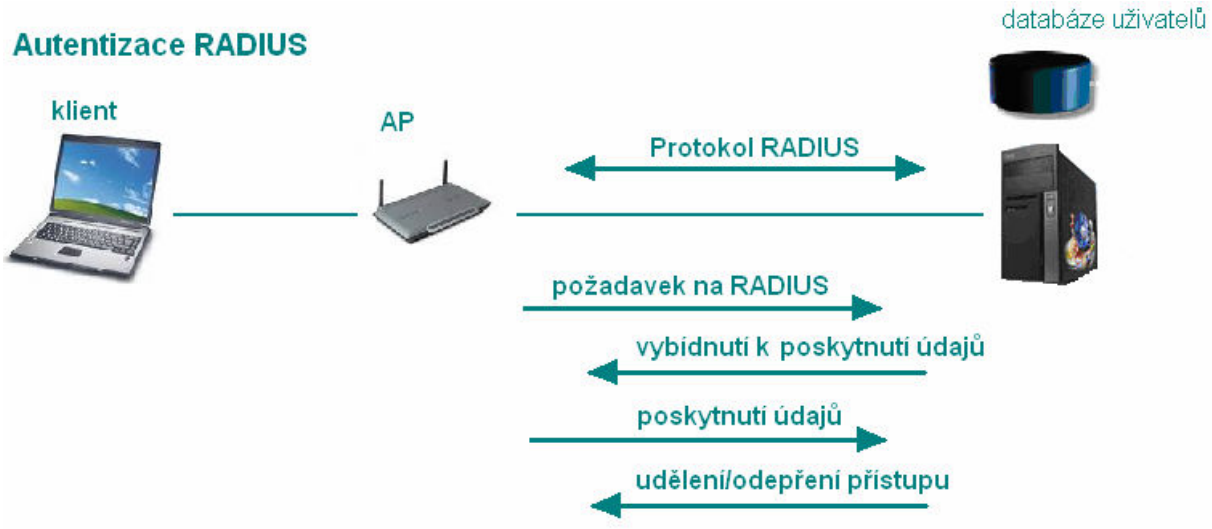
Obrázek 18: Autentizace pomocí RADIUS

Ověřování klienta provádí přístupový bod AP. Klient pošle výzvu k ověření AP a ten využije autentizačního serveru RADIUS (Repote Authentication Dial-IN User Service). Uživatel jehož ověření je pozitivní má přístup do systému. 802.1x tedy blokuje veškerý provoz na daném portu, než se uživatel autentizuje pomocí údajů na serveru RADIUS.

9.10.1 Radius

Využívá komunikace mezi klientem a serverem. Autentizace klientů se provádí pomocí hesla, které se v síti přenáší zašifrované. Server RADIUS je autonomní zařízení, které může být použito v celé podnikové síti, nikoli jen pro WLAN. Pokud v síti nemáme přímo server RADIUS, můžeme nakonfigurovat AP, aby simuloval RADIUS. Typický sled operací při autentizaci při užití RADIUS probíhá následovně:

- klient naváže spojení s AP, který od uživatele požaduje jméno a heslo.
- Po obdržení hesla a jména zašle AP serveru RADIUS žádost RADIUS ACCESS_REQUEST
- Požadevk RADIUS ACCESS_REQUEST je směrován na RADIUS přes lokální nebo rozlehlejší sít – pokud je v síti RADIUS zdvojen, může být využit alternativní server
- RADIUS ověří požadavek a správnost uživatelského jména a hesla na základě výzvy a zašle zprávu obsahující informaci o udělení/odepření přístupu do sítě RADIUS ACCESS_ACCEPT/DENY



Obrázek 19: Princip RADIUS

9.11 Autentizační metody protokolu EAP

Protokol 802.1x vychází z protokolu EAP (Extensible Authentication Protocol), který byl vyvinut pro PPP LCP (Point-to-Point Protocol Link Control Protocol) jako řízení systému RADIUS. Protokol PPP umožní autentizaci pouze s kombinací jména a hesla. Pomocí EAP lze podporovat různé metody autentizace. Tyto metody musí podporovat AP a autentizační server. Lze také použít paralelně více metod, ale musíme počítat se zvýšenými požadavky na provoz sítě.

9.11.1 MD5

MD5 (*Message Digest*) je nejslabší metodou a představuje nejnižší možnou úroveň zabezpečení. Je napadnutelná řadou útoků. Neměla by se používat tam, kde hrozí riziko odposlechu. Z tohoto důvodu je tato metoda nepoužitelná pro WLAN. Klient se autentizuje pomocí hesla.

9.11.2 LEAP

Protokol LEAP (*Lightweight Extensible Authentication Protocol*) je metoda, která byla navrhnuta firmou Cisco. Podporovala výhradně zařízení Cisco, proto se nedočkala široké podpory u ostatních výrobců. Autentizace probíhá na základě uživatelského jména a hesla prostřednictvím serveru RADIUS. Poskytuje dynamickou obnovu WEPových klíčů. Metoda je náchylná na slovníkové útoky na hesla.

9.11.3 TLS

Protokol TLS (*Transport Level Security*) podporuje autentizaci, ale i odvození klíčů. Jedná se o nejsilnější metodu, která je ale složitější pro implementaci. Identifikace klientů probíhá na základě dvou digitálních certifikátů (klient, server) podepsaných certifikační autoritou. Pomocí certifikačního serveru PKI se vytváří komunikační tunel, kde probíhá výměna autentizačních údajů. Tato metoda je implementována ve Windows XP.

9.11.4 TTLS

Protokol TTLS (*Tunneled Transport Layer Security*) je podobný protokolu TLS, ale vyžaduje se pouze certifikát na straně autentizačního serveru. Klienti se autentizují pomocí hes-

la. TTLS je silnější autentizační metodou než LEAP a je také snadnější na implementaci než TLS, protože používá existující uživatelské identifikační údaje.

9.11.5 PEAP

Protokol PEAP (*Protected EAP*) podporuje vzájemnou autentizaci a dynamickou obnovu WEPových klíčů. Požaduje certifikát pouze na straně serveru. Klient nemusí mít certifikát a autentizuje se pomocí hesla a jména. Autentizace probíhá zabezpečeným tunelem, kde je možné použít různé metody autentizace. PEAP je silnější metoda než LEAP a je snadnější na implementaci než EAP-TLS. PEAP podporuje Microsoft a Cisco.

9.12 WPA

Z důvodu špatné použitelnosti protokolu WEP v produkčním prostředí, byl vyvinut protokol WEP2. Později byl změněn původní název na WPA (*Wi-Fi Protected Access)*. Protokol WPA je podmnožinou standardu 802.11i. Mnoho zařízení podporuje WPA šifrování v přímo v hardwaru. Slouží jak pro šifrování komunikace, tak i pro řízení přístupu.

Zabezpečení WPA je vybaveno rozšířeným inicializačním vektorem, technikou Re-Keying (automatická změna klíče) a kontrolu integrity (MIC), která zabraňuje změně dat na cestě od odesílatele k příjemci. Používá se šifrování TKIP a Per Packet Mixing (měnící se pozice inicializačního vektoru v paketu). Byl také nahrazen šifrovací algoritmus DES (*Data Encryption Standard*) u WEP algoritmem AES (*Advanced Encryption Standard*).

9.12.1 TKIP

Protokol TKIP (*Tempoval Key Integrity Protocol*) je určen k řešení hlavních nedostatků WEP. Obsahuje funkce dynamické regenerování klíčů (dočasných klíčů, odtud název protokolu), kontroly integrity zpráv a číslování paketů.

TKIP prodlužuje délku zprávy zašifrované pomocí WEP o 12bajtů: 4 bajty pro rozšířenou informaci IV a 8 bajtů pro kód integrity zprávy (MIC).

9.13 802.11i

Standard 802.11i byl navržen za účelem vyřešení bezpečnostních problémů s WEP. Dokáže podporovat protokol TKIP používaný u WPA, který je ovšem volitelný. Pro zabezpečení sítí se ale v 802.11i používá nový protokol CCMP, který strukturou vychází ze šifrování

AES. Hlavní oblast působení 802.11i je zkvalitnění autentizace a utajení datových rámců. 802.11i obsahuje dva režimy autentizace, jsou jimy PSK a 802.1x

9.13.1 CCMP a AES

CCMP (*Counter-mode CBC* (*Cipher Block Chaining*) *MAC* (*Message Authentication Code*) *Protocol*) zaručuje silnější šifrování. Používá se 128bitový klíč, který používá dynamické regenerování. CCMP zajišťuje najednou utajení, autenticitu, kontrolu integrity zpráv, číslování paketů na ochranu proti útokům. Prodlužuje datový rámec o 16 bytů.Pro šifrování přenášených dat se používá AES. AES (*Advanced Encryption Standard*) je náhradou za šifru RC4. Používá v režimu CCM čítačový režim s protokolem CBC-MAC (*Cipher Block Chaining-MAC)*. Čítačový režim zajišťuje šifrování, CBC-MAC zajišťuje autentizaci a integritu dat. CCM obsahuje funkci pro zajištění utajení CTR (*Counter Mode*). Stejně jako RC4 je i AES šifra se symetrickým klíčem. Text se šifruje i dešifruje stejným sdíleným tajným klíčem. AES pracuje s bloky o velikosti 128 bitů – *bloková šifra*. CCMP používá tedy 128 bitový dočasný klíč, odvozený od *master* klíče, který se získává v průběhu komunikace protokolem 802.1x.

CCMP obsahuje také mechanismus MIC, který ale funguje jinak než Michael v TKIP. Výpočet je založený na hodnotách vycházejících z IV a z dalších hlavičkových informací. Pracuje v 128bitových blocích a počítá se přes jednotlivé bloky až na konec originální zprávy, kdy se vypočte konečná hodnota.Používá se nový šifrovací mechanismus, který se liší od WEP/TKIP a RC4. Výstupem šifry AES je po inicializaci jen 128bitový blok. Celý vstupní text se rozdělí na 128bitových bloků a ty se postupně XORují s 128bitovým generovaným výstupem AES tak dlouho, dokud nedojde k zašifrování celé původní zprávy. Nakonec se čítač vynuluje, XORuje se hodnota MIC, která se přidává na konec rámce.Výsledkem je silnější šifra. Nevýhodou jsou ale zvýšené nároky na výkon zařízení, které tuto metodu podporují. Proto se vyrábějí výkonnější zařízení, které ale už nejsou kompatibilní s první generací bezdrátových sítí

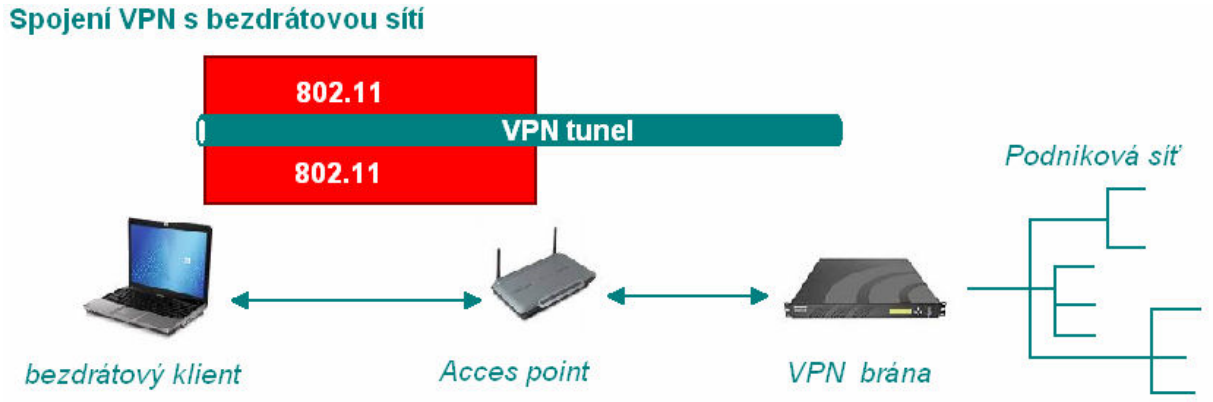
Základní vlastnosti protokolů WEP, WPA a 802.11i ukazuje následující tabulka.

Tabulka 6: Porovnání WEP, WPA a 802.11i

vlastnosti	WEP	WPA	802.11i
šifrovací algoritmus	RC4	RC4	CCMP (AES CCM)
délka klíče	40 nebo 104 bitů	dvě možnosti - 128 bitů pro šifrování, 64 bitů pro autentizaci a kontrolu integrity	128 bitů
inicializační vektor	24 bitů	48 bitů	48 bitů
kontrola integrity	32 bitů CRC	Michael MIC	CBC-MAC
autentizace a klíčový management	není	EAP na 802.1x	EAP na 802.1x

10 IMPLEMENTACE VPN V BEZDRÁTOVÉM PROSTŘEDÍ

Virtuální privátní sítě (VPN, *Virtual Private Network*) se používají pro vzdálený přístup k privátní síti prostřednictvím nedůvěryhodné sítě (Internet). Uživatelé mohou bezpečně používat prostředky firemní sítě i na cestách nebo mino kancelář. VPN lze použít pro řešení různých požadavků, které vyžadují bezpečnou komunikaci přes veřejnou síť. Bezpečnost VPN má dvě nedílné složky – první autentizaci uživatelů a druhou je utajení přenášených dat. Autentizace ověřuje identitu dvou koncových bodů komunikace ve VPN (klient VPN, brána VPN nebo směrovač) a uživatelů. VPN zajišťuje bezpečnost přenášených dat pomocí protokolů na vyšší úrovni. VPN se realizuje prostřednictvím tunelů veřejnou sítí, v rámci nichž se přenášené datagramy chrání proti útokům zvenčí (obrázek 19). Mnoho VPN implementací je založeno na IPSec bezpečnostním protokolu. IPSec představuje vysoce spolehlivou metodu zabezpečení pro budování VPN.



Obrázek 20: Spojení VPN s bezdrátovou sítí

VPN lze použít pro řešení mnoha požadavků, které v sobě zahrnují potřebu komunikovat přes zabezpečenou síť. Tyto požadavky mohou být následující:

- propojení jednotlivých LAN do velkého intranetu (site-to-site, LAN-to-LAN)
- vzdálený přístup – připojení vzdáleného uživatele k podnikovému intranetu. VPN klade zvýšené nároky na autentizaci klientů, protože uživatelé se mohou připojit skutečně odkudkoliv

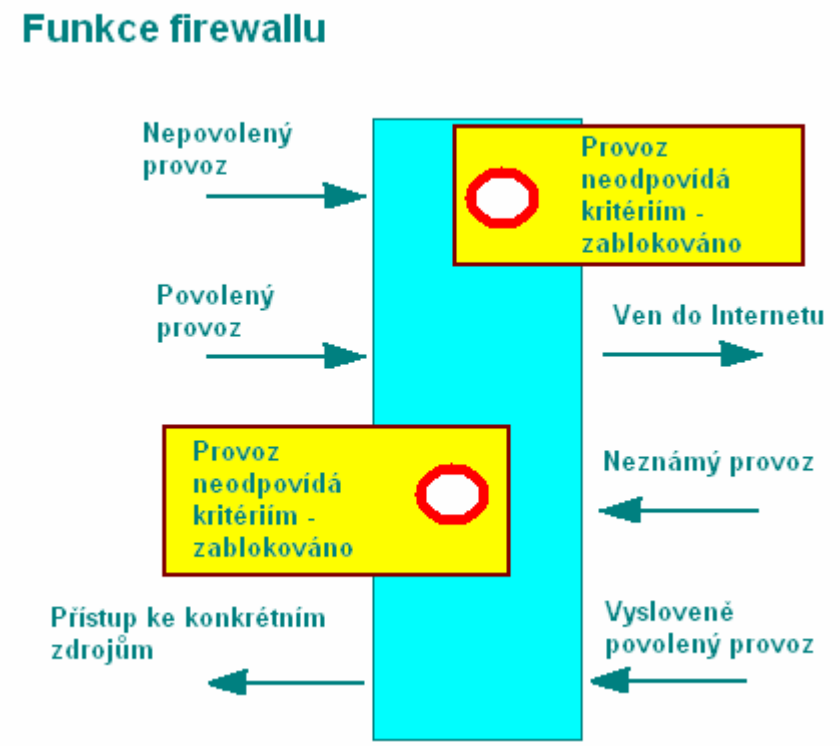
11 NÁSTROJE A TECHNIKY DATOVÉ BEZPEČNOSTI

11.1 Firewall

Firewall je bezpečnostní prvek, který je připojen na perimetru datové sítě. Funkcí firewallu je permanentně sledovat generovaný provoz směrem do sítě i směrem ven ze sítě. Podle prvidel, které definuje IT specialista společnosti pak firewall rozhodne o blokování/povolení přenosu dat. Firewall je primární prvek ochrany sítě a jeho přítomnost je tedy jednou z podmínek pro zajištění datové bezpečnosti.

11.1.1 Funkce firewallu

Firewall kontroluje síťový provoz a na základě definovaných pravidel povolí nebo zakáže provoz v síti.



Obrázek 21: Funkce firewallu

Podobně jako přístupové seznamy (ACL) často firewally filtrují síťový provoz na základě IP adres, podle použitého protokolu a také podle statusu připojení. Například vstup přes FTP firewall do vnitřní sítě firewall zpravidla nepovolí, ovšem pokud konkrétní relaci zahájí uživatel sítě, pak ji povolí. Defaultní nastavení, které je ovšem v řadě situací nepouži-

telné, spočívá v důvěře firewallu ve všechna vnitřní zařízení mající snahu komunikovat s externím zařízením (provoz do internetu)

- regulace přístupu vlastních uživatelů (uživatelů chráněné privátní sítě) do veřejného Internetu. Provozovatel firemní sítě může např. chtít zakázat svým zaměstnancům přístup k některým serverům (např. erotickým), nebo naopak povolit přístup jen k některým konkrétně určeným serverům, či tyto aktivity alespoň určitým způsobem regulovat (nebo i jen evidovat, tak aby mohl následně vyhodnotit chování uživatelů). Stejně tak může chtít regulovat využívání určitých služeb (např. ICQ apod.), či může chtít vázat příslušná omezení na konkrétní časové intervaly (například na stanovenou pracovní dobu) apod.
- antivirová ochrana - provozovatel připojené sítě může požadovat, aby firewall chránil tuto síť před nakažením počítačovými viry, což se může týkat jak přicházející elektronické pošty, tak například i pošty odcházející (aby nedošlo k zavirování externích uzlů), i dalšího druhu provozu (například přenosu textových souborů s makroviry)
- ptimalizace připojení - některé druhy firewallů mohou napomáhat efektivnějšímu využití přípojky dané sítě k vnějším sítím, typicky k Internetu. Jde o to, že v rámci firewallu může fungovat tzv. cache server, který v sobě uchovává některé objekty často požadované uživateli chráněné privátní sítě (nejčastěji: WWW stránky). Z vnějšího prostředí je pak sám stahuje (a tím zatěžuje přípojku) jen při prvním požadavku na ně, zatímco při dalších požadavcích na stejný objekt poskytne jeho kopii, kterou si uchoval. Díky tomu pak uživatelé připojené sítě mohou vystačit s pomalejší a tudíž lacinější přípojkou (k Internetu), než jakou by ke stejnému způsobu práce potřebovali bez právě popsané funkce firewallu.
- řešení problému s IP adresami - jedním z nepříjemných problémů dnešního Internetu je nedostatek číselných adres (IP adres). Každý uzel, který má být připojen k Internetu, musí mít přidělenu takovouto adresu, která je navíc unikátní (stejnou adresu nesmí mít žádný jiný počítač). Dnes jsou tyto adresy navíc závislé i na způsobu, jakým je připojení realizováno (jsou závislé na poskytovateli připojení). Se získáním potřebného počtu IP adres však mohou být v praxi spojeny určité problémy. Při použití firewallu (většiny druhů firewallů) však popsané pravidlo přestává platit

- za firewallem mohou být použity takové IP adresy, které nejsou unikátní a ani nejsou závislé na konkrétním providerovi, který připojení zajišťuje.

- veřejné zpřístupnění zdrojů - ačkoli se provozovatelé připojených sítí především snaží chránit své zdroje (včetně nejrůznějších informací) před neoprávněným přístupem zvenčí, přesto u některých konkrétních zdrojů (informací) mají zájem na jejich zpřístupnění i pro uživatele z vnějších sítí. Jde například o prezentaci firmy, její obchodní nabídky atd. - obecně o cokoli, co si provozovatel privátní sítě sám určí za veřejné. V rámci firewallu pak bývá takovéto zveřejnění realizováno - například formou WWW serveru či FTP serveru, který je přístupný jak "zevnitř" (z chráněné sítě), tak i "z vně".

- vzdálený přístup oprávněných uživatelů - provozovatelé firemních sítí (intranetů) velmi často vyžadují, aby uživatelé měli přístup ke zdrojům a službám těchto chráněných sítí i v případě, kdy se nachází mimo dosah této sítě (jsou například v terénu, u zákazníka apod.). V takovémto případě jsou oprávnění uživatelé v pozici vzdálených uživatelů, a součástí řešení firewallu bývá i umožnění jejich vzdáleného přístupu.

- zabezpečená komunikace - veřejný Internet představuje nezabezpečený přenosový kanál, v tom smyslu že data která jsou přes něj přenášena nejsou žádným způsobem šifrována či jinak zabezpečena proti neoprávněnému "odposlechu". Potřebné zabezpečení je ale možné realizovat na vyšších úrovních (na úrovni transportní či aplikační vrstvy), a fakticky tak data šifrovat (kódovat) ještě před tím, než jsou předána k přenosu do veřejného Internetu. Takovéto řešení ale vyžaduje, aby "na druhé straně" byl někdo, kdo zakódovaná data vrací zpět do jejich původní podoby. V praxi mohou vše zajišťovat koncové uzly, které spolu komunikují. Stejně tak ale může potřebné šifrování (kódování) za účelem zabezpečení přenášených dat realizovat dvojice firewallů připojených k Internetu, která mezi sebou vytváří zabezpečený tunel. Díky němu pak mohou být propojeny například dvě chráněné privátní sítě skrze veřejný Internet, bez toho že by si jejich vnitřní uzly musely uvědomovat existenci zabezpečujících mechanismů a jakkoli se jí přizpůsobovat (bezpečný tunel mezi firewally je pro ně koncové uzly neviditelný) . Pomocí takovýchto tunelů

mezi jednotlivými firewally lze dokonce realizovat celé privátní sítě (VPN, Virtual Private Network) vedoucí skrze veřejný Internet.

- sdílení přístupu k Internetu - především u velmi malých sítí, tvořených jen několika málo počítači, je jedním z požadavků na jejich fungování to, aby vůbec umožňovaly přístup k Internetu všem uzlům připojené sítě. V zásadě jde o nahrazení funkce klasického směrovače, který je pro tuto roli jinak nezbytný.

11.1.2 Aplikace firewallu

Nabídka různých firewallů na trhu je velmi široká. Jsou k dostání firewally nejrůznějších velikostí, parametrů i tvarů. Konkrétní typ instalovaného firewallu závisí na přesný požadavcích ochrany a správy sítě a také na velikosti sítě či jiného chráněného systému. Firewally se obvykle dají rozdělit do několika kategorií :

- Osobní firewall, Tento typ firewallu má obvykle podobu speciálního softwaru, který chrání jediný osobní počítač (je také na něm nainstalovaný). S osobnímy firewally se nejčastěji setkáme na domácích počítačích širokopásmovým připojením k Internetu. Instalace takového firewallu na počítač je rozumná věc.
- Integrovaný firewall all in one. S těmito firewally pracují nejčastěji uživatelé širokopásmových přípojek (kabelový modem, DSL, Wifi) ti jsou k síti připojeni pomocí jediného zařízení, které současně plní funkci směrovače, ethernetového přepínače, a firewallu. Pokud se tento typ firewallů rozhodnete používat, pak se nesmí zapomenout prověřit jaké vůbec funkce nabízí, a při posuzování bezpečnosti být zdravě skeptičtí.
- Firewally pro malé a střední firmy. Tyto firewally zajišťují bezpečnost a ochranu menších sítí. Příkladem jsou produkty HAWEI AR 18-10 , AR -18-20 a CISCO PIX 501 a 506
- Firewally podnikové úrovně. Vyšší třída firewallů, například HUAWEI AR 28 a CISCO PIX 516. Jsou určeny pro organizace s tisíci jednotlivých uživatelů. Mají proto bohatší možnosti funkcí a nastavení . Také mají mnohdy více síťových rozhraní.

Firewall se zpravidla umisťuje do bodu, kde je vnitřní síť připojena k internetu. Takovét umístění preferují běžní uživatelé a menší společnosti. Ve velkých společnostech je možné firewally zapojit mezi různé části sítě, které vyžadují různou ochranu dat. Například pokud

firam dovolí svým obchodním partnerům vstup do sítě, bývá zpravidla bod přístupu chráněn firewallem.

11.1.3 Definice zásad přístupu

Síťový provoz mimo jiné podléhá pravidlům, které jsme definovali pomocí nastavení firewallu. Pokud by všechen provoz směřoval pouze z lokální sítě ven do internetu, bylo by nastavení firewallu velice jednoduché. Firewall by povoloval příchozí provoz jen takový, který by byl přímou odpovědí na požadavky uživatelů ve vnitřní síti. Může ale nastat situace, a s největší pravděpodobností nastane, kdy z internetu přijde požadavek, který je vhodné firewallem propustit. Přímý přístup z internetu do sítě by byl velmi riskantní, proto se definují porty, přes které je možné provozovat komunikace. Například port 80 (http) je vhodné povolit, ovšem je třeba si uvědomit, že nad protokolem 80 pracuje množství aplikací, z nichž mnoho může být škodlivých. Proto je třeba spojit síly firewallu s antivirovým systémem nebo personálním firewallem.

12 MODELOVÁ STUDIE

Zabezpečení sítě je přímo závislé na množství peněz, které jsme ochotni do tohoto zabezpečení investovat. Zároveň je závislé na složitosti sítě, jejím výkonu a způsobu administrace. Způsob zabezpečení je také silně odvislý od účelu zřízení sítě. Zcela jistě je třeba zajistit jiné zabezpečení pro domácí síť a jiné pro síť používanou v obchodní společnosti. Kvalitní zabezpečení by zvedlo nároky na administrování sítě. Zcela jinou kapitolou jsou pak veřejné bezdrátové sítě (tzv. hot spots). Tyto sítě jsou mnohem citlivější na úroveň zabezpečení, protože jsou otevřeny každému (zdarma nebo za poplatek) včetně nežádoucích uživatelů, kteří mohou jednoduše provoz sítě odposlouchávat.

12.1 Domácí síť

Cílem domácí bezdrátové sítě je propojení všech potřebných systémů v domácnosti. Bývají to zpravidla PC jednotlivých členů domácnosti. Výhledově se dá uvažovat o připojení dalších přístrojů, například fotoaparátu, kamery a užitkových spotřebičů, jako jsou ledničky, trouby, řídící prvky vytápění atp. Plusem takovéto sítě je snadná instalace a zřízení, vysoká mobilita a nízká cena. Mínusem pak zejména její malá spolehlivost z hlediska bezpečnosti. Středobodem domácí sítě bývá centrální AP, které slouží zpravidla i jako překlad NAT a router sítě. AP lze zpravidla ovládat přes jednoduché http rozhraní. Zároveň na takovémto AP může být přoveden roaming mezi metalickou a bezdrátovou částí sítě. Takováto síť je pro útočníka málo zajímavá a síly, které by musel vynaložit na její napadení se mu ani málo nevrátí v podobě vytěžených výhod.

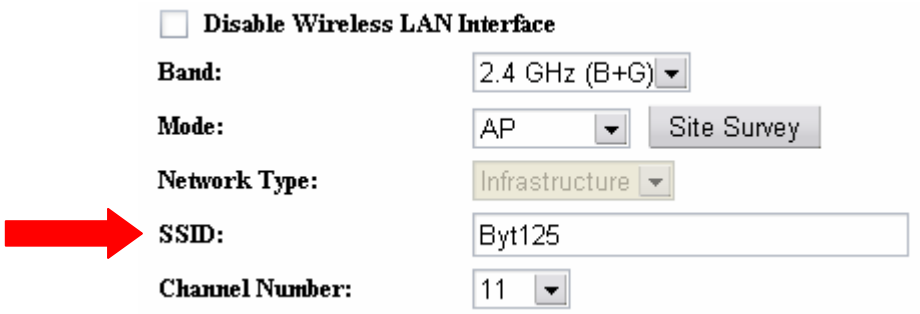
12.1.1 Doporučená nastavení bezdrátové domácí sítě

Výčet doporučených nastavení pro domácí bezdrátovou síť vychází z mých vlastních zkušeností, podobně ji mám nastavenou doma.

- Vypnout vysílání jména sítě (beacons)

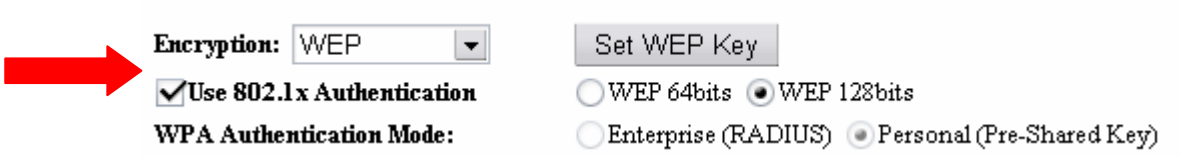
Obrázek 22: Vypnutí vysílání SSID

- Změnit výrobní hodnotu SSID od výrobce, vhodné SSID by nemělo obsahovat informace o lokalitě AP, jménu zřizovatele atp. Například SSID ve formě Novak_zlin je krajně nevhodné.



Obrázek 23: Změna SSID

- Pomocí firewallu na úrovni routeru vypnout všechny nepotřebné porty.
- Za každé situace používat šifrování WEP nebo WPA. U WEP je třeba nastavit dlouhý klíč (128bitový), který pravidelně měníme. Authentizace bude Open-systém.



Obrázek 24:Nastavení WEP

- Na každém PC používáme osobní firewall, který pravidelně aktualizujeme. Vhodné je například Kerio nebo ZoneAlarm. Pro pokročilejší uživatele doporučuji Kasperski firewall.

Takovéto zabezpečení zabrání v průniku méně zkušenému útočníkovi a představuje základní formu ochrany sítě. Pokud útočník bude chtít, dostane se přes bezpečnostní prvky.

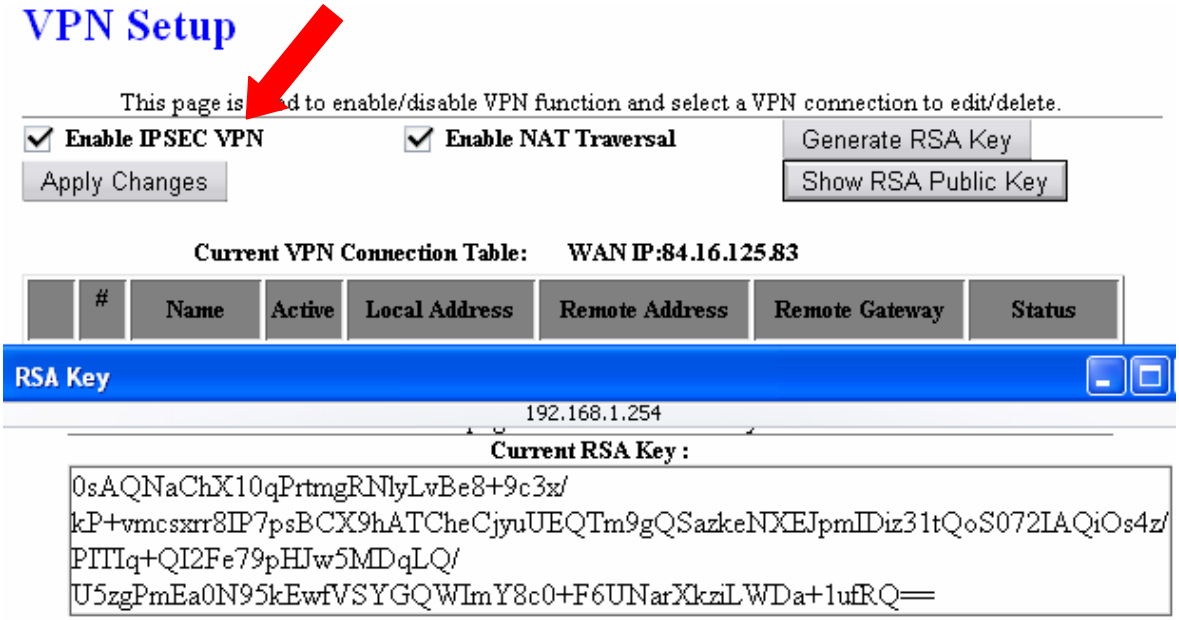
12.2 Firemní síť

Firemní bezdrátová síť bývá zpravidla instalovaná jako prodloužení ethernetu. V takovéto síti je používáno velké množství zařízení. Tato síť umožní vysokou mobilitu připojených účastníků v rámci firmy a bez přerušení spojení. Pokud použijeme nezabezpečený přenos dat, mohou se útočníci dostat k datům i přes dobrou úroveň autentizace. Proto je vhodné použití VPN, jež ve firemní síti patří mezi primární opatření.

12.2.1 Doporučená nastavení bezdrátové firemní sítě

Nastavení vhodná pro firemní bezdrátovou síť jsou obdobná jako u sítě domácí, pouze je třeba je ještě více zintenzivnit. Na níže uvedených obrázcích jsou uvedena nastavení, ilustračně provedena na mém domácím AP Realtek RTL 8186. Vhodná opatření pro zabezpečení firemní sítě jsou následující:

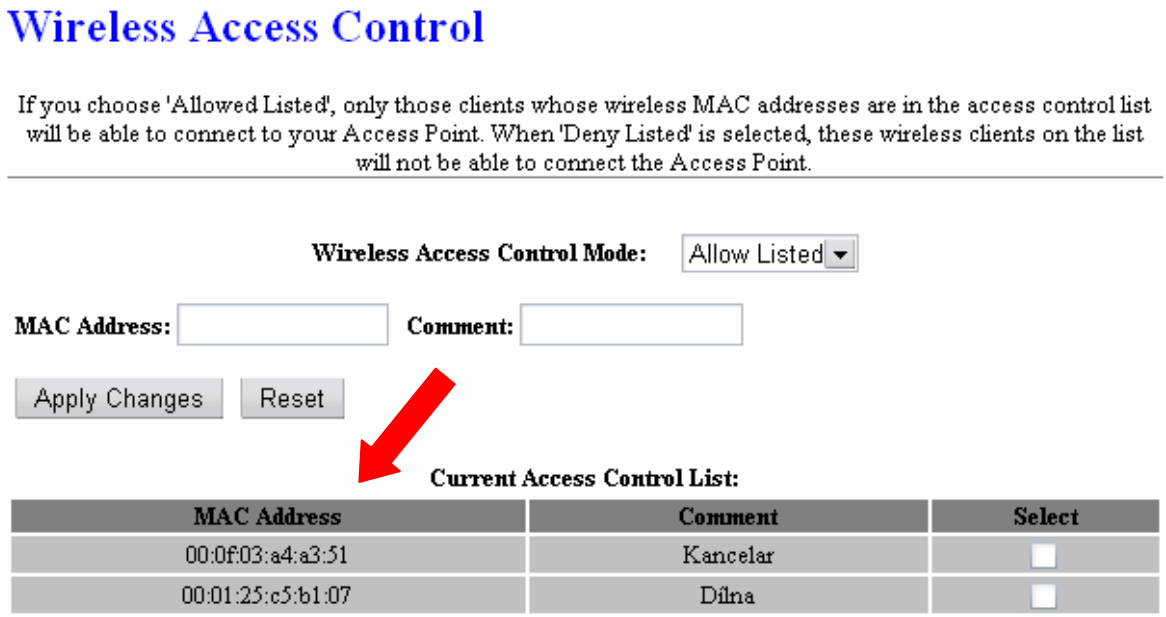
- Vypnout vysílání jména sítě (beacons)
- Změnit výrobní hodnotu SSID od výrobce, vhodné SSID by nemělo obsahovat informace o lokalitě AP, jménu zřizovatele atp.
- Ve všech firemních počítačích je třeba používat osobní firewall a antivir. Oba nástroje je nutné pravidelně aktualizovat. Bez aktualizace ztrácí svůj účel.
- Pro implementaci VPN používat AP s podporou IPsec, pro zajištění bezpečného tunelu mezi uživatelem a AP.



Obrázek 25: Ukázka nastavení VPN za použití IPSec

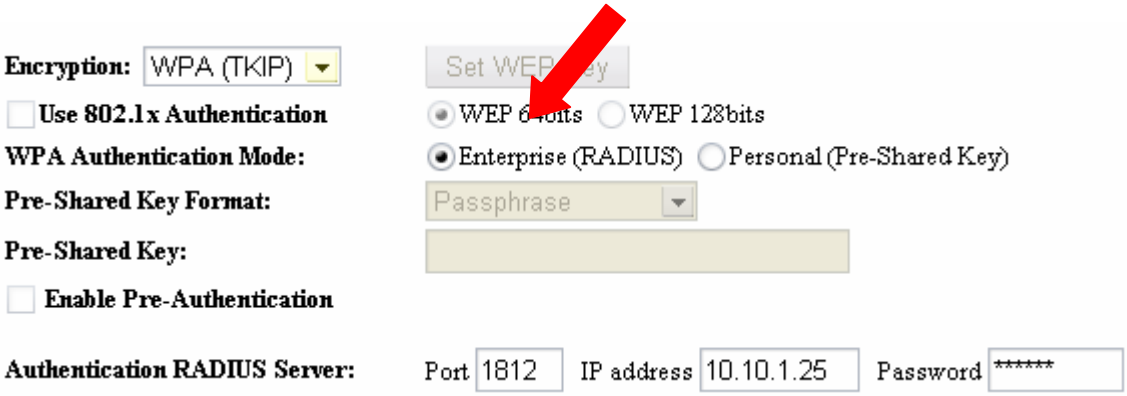
- Pravidelně provádět kontrolu všech AP, i fyzickou.
- Každé nové AP instalovat jen po provedení Site Survey a po instalaci provést penetrační test sítě.
- Zásadně používat infrastrukturní sítě na úkor ad-hoc sítí. Ad-hoc nedosahují takové úrovně bezpečnosti jako infrastrukturní.

- Definovat seznam povolených/zakázaných MAC adres



Obrázek 26: Nastavení seznamu MAC adres

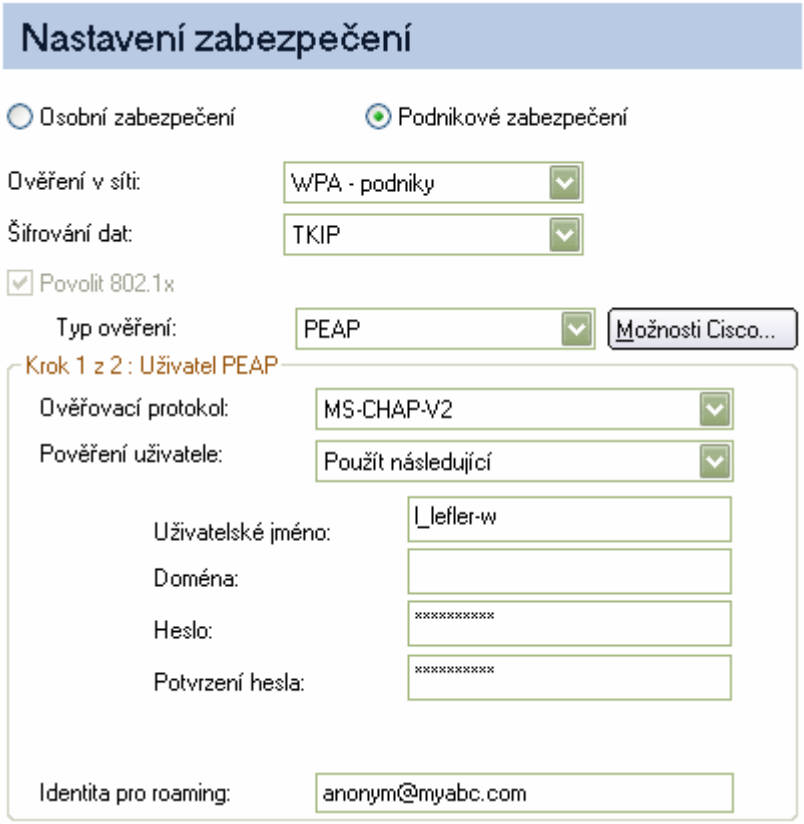
- Pravidelně aktualizovat firmware všech AP
- Maximalizovat použití statických IP adres na úkor dynamického přidělování DHCP.
- Pro autentizaci uživatelů aplikovat princip RADIUS nebo ekvivalentní. Šifrování WPA–TKIP.



Obrázek 27: Nastavení RADIUS a šifrování WPA-TKIP

Aby se klient správně připojil, je třeba nastavit i jeho bezdrátovou síťovou kartu. Pro ilustraci jsem použil síťovou kartu Intel PRO/Wireless 2200 BG integrovanou v mém notebooku. K nastavení této karty jsem použil utilitu Intel PROSet/Wireless ve verzi 10.1.0.6

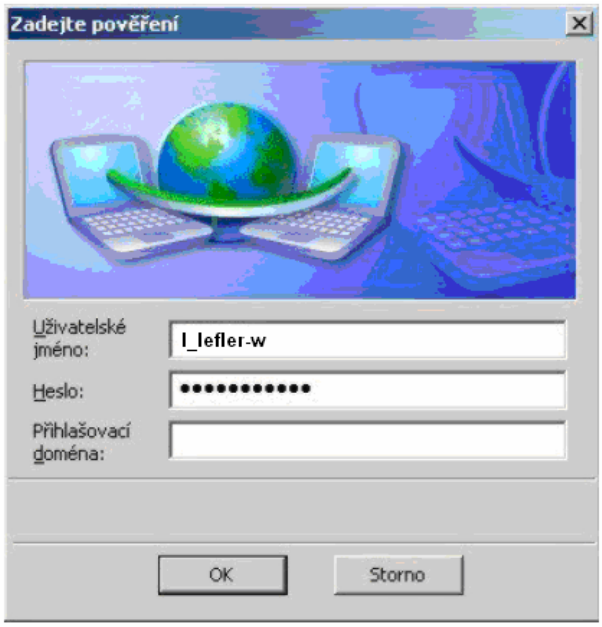
Následující obrázek popisuje nastavení, které je třeba provést, aby se počítač byl schopen připojit k výše uvedenému AP.



Obrázek 28: Nastavení klientského zařízení

Jako ověřovací protokol byl zvolen MS-CHAP-V2, která používá k ověření totožnosti uživatele pouze jméno a heslo. Metoda TLS používá k jménu a heslu ještě klientský certifikát.

Jak je vidět, nastavení přístupového bodu a síťové karty uživatele není jednoduchou záležitostí. Proto je třeba těmto činnostem věnovat zvýšenou pozornost zejména u AP, u kterého je výhodné po každém kroku uložit nastavení. Pokud byly všechny náležitosti acces pointu a bezdrátové síťové karty nastaveny dobře, při prvním přihlášení k síti se nám zobrazí toto dialogové okno (platí pouze pro výše uvedená nastavení):



Obrázek 29: Dialog přihlášení

ZÁVĚR

Při psaní této práce bylo mým cílem uvést základní informační rámec v oblasti datové bezpečnosti bezdrátových sítí zejména na standardu 802.11 ale diskutovány byly i sítě typu UWB a optické bezdrátové.

Bezdrátové sítě se s postupem doby stávají v určitých oblastech stále populárnější a začínají nahrazovat metalické sítě ethernet. Takovéto sítě poskytují vysoký uživatelský komfort, dostatečnou přenosovou rychlost a při vhodné konfiguraci i solidní úroveň zabezpečení.

Na druhou stranu je třeba uvést, že dokonalé zabezpečení je utopickou myšlenkou a je z principu nedosažitelné. Při definování a aplikování bezpečnostních pravidel musí administrátor (tedy domácí uživatel nebo firma) najít správnou rovnováhu mezi omezením funkce sítě a ochranou informací, které jsou v síti zpracovávány. Každé zvýšení bezpečnosti totiž velmi omezuje dynamiku a uživatelský komfort. Obecně se dá říci, že nutná úroveň zabezpečení je přímo úměrná hodnotě informací, které jsou v síti komunikovány. Dalšími faktory, jenž umocňují nutnost aplikace zabezpečení mohou být vysoce konkurenční prostředí, vysoká fluktuace zaměstnanců a jiné. Při definování bezpečnostních pravidel je třeba dávat důraz na lidský faktor, protože úmysl nebo chyba člověka bývají nejčastější místa úniku informací.

Jedním z dílčích cílů práce bylo popsání narušitele sítě a způsob jeho vniknutí do sítě. Velká část útoků je vedena tzv. skript-kids, což jsou svého druhu nepoučení amatéři. Průnik takovýchto útočníků končí zpravidla na perimetru bezdrátové sítě a skript-kids se nejsou schopni dostat k samotným datům v síti. Další skupinou jsou informovaní útočníci. Tito lidé jsou motivováni svým prospěchem z průniku do sítě a jejich techniky bývají často velmi pokročilé. Proti těmto lidem je třeba aplikovat silnější zabezpečení, pro ověření např. WPA-PEAP a šifrování TKIP. Vhodné je také použití VPN v kombinaci s IPSec.

Předposlední kapitola mojí bakalářské práce se věnuje problematice firewallu. Firewall je zásadní součástí informačního zabezpečení společnosti, zejména proto, že stojí na pomezí vnitřní sítě a vnějšího internetu. Firewall usnadní aplikaci bezpečnostních zásad společnosti, proto je jeho nasazení podmínkou k úspěchu.

Poslední kapitola se zabývá praktickou ukázkou nastavení některých zařízení v bezdrátové síti. Jednalo se o bezdrátovou síťovou kartu Intel PRO/Wireless 2200 BG a přístupový bod

Realtek RTL 8186. Na těchto zařízeních byla demonstrována doporučená nastavení bedrátových sítí v situaci domácího uživatele i nastavení pro firmu.

SEZNAM POUŽITÉ LITERATURY

[1] JIROVSKÝ, V., Vadenecum správce sítě. Nakl. Granada Publishing, spol s.r.o., Praha, 2001. ISBN 80-7169-745-1

[2] ZANDL, P., Bezdrátové sítě praktický průvodce. Nakl. Computer Press, Brno, 2003. ISBN 80-7226-632-2

[3] J. BIGELOW, S., Mistrovství v počítačových sítích, Správa, konfigurace, diagnostika a řešení problémů, Computer Press, Brno, 2004. ISBN 80-251-0178-9

[4] PUŽMANOVÁ, R., Bezpečnost bezdrátové komunikace, Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G, Computer Press, Brno, 2005. ISBN 80-251-0791-4

[5] BARKEN, L., Jak zabezpečit bezdrátovou síť, Computer Press, Brno, 2004. ISBN 80-251-0346-3

[6] JAŠEK, R., Ochrana znalostí a dat v podnikových informačních systémech. 1.vyd. Zlín: UTB ve Zlíně, 2002. ISBN 80-7318-095-2

[7] THOMAS, M., Zabezpečení počítačových sítí Nakl. CP Books, a.s., Brno, 2005. ISBN 80-251-0471-6

[8] KOHRE, T., Stavíme si bezdrátovou síť Wi-fi, Computer Press, Brno, 2004. ISBN 80-251-0391-9.

[9] PUŽMANOVÁ, R. WLAN konečně bezpečné [online]. [cit.2007-04-14]. Dostupné z <http://www.lupa.cz/clanky/wlan-konecne-bezpecne/>.

[10] PRAVDA, I. Přehled doplňků standardu IEEE 802.11 [online]. 2005. Dostupný z WWW: <http://access.feld.cvut.cz/view.php?cisloclanku=2005113002>.

[11] CISCO, Potokol LEAP [online]. [cit.2006-11-13]. Dostupné z <http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/netqa0900aecd801764f1.html>.

[12] PETERKA, J. Jak probíhají bezdrátové přenosy v sítích WLAN? [online]. Dostupný z WWW: <http://www.earchiv.cz/b02/b0900016.php3>.

[13] Internetový časopis Jupitermedia Corporation [online]. Dostupný z WWW: <http://www.80211-planet.com>.

[14] Bezpečně online, Výhody firewallu [online]. [cit.2007-03-10]. Dostupné z <http://www.bezpecneonline.cz/sekce1/s1001.htm>.

[15] *Cisco, NAT* [online]. [cit.2007-04-14]. Dostupné z < http://www.cisco.com/en/US/tech/tk648/tk361/technologies_q_and_a_item09186a00800e523b.shtml >.

[16] IETF,, Official Internet Protocol Standards [online]. [cit.2007-04-14]. Dostupné z <http://www.rfc-editor.org/rfcxx00.html>.

[17] IEEE 802.11 Wireless LAN Security with Microsoft Windows XP [online]. Dostupný z WWW: <http://www.microsoft.com/downloads>.

[18] Odvárka, Petr. ICMP - Internet Control Message Protocol [online]. [cit.2006-04-14]. Dostupné z <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=1&clanekID=6>.

[19] Internetový server Lupa.cz [online]. Dostupný z WWW: <http:www.lupa.cz>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAA	Authentication, Authorization, Accounting
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
ARP	Address Resolution Protocol
BSS	Basic Service Set
CA	Certification Authority
CCMP	Counter-Mode Cipher Block Chaining Message Authentication Code Protocol
CDMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CHAP	Challenge-Handshake Authentication Protocol
CRC	Vycliv Redundancy Check
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DSSS	Direkt Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
FDD	Frequency Division Duplex
FHSS	Frequency Hopping Spread Spectrum
IBSS	Institute of Electrical and Electronics Engineers
IDS	Intrusion detection Systém
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol

IPSec	Internet Protocol Security
IT	Information Technologies
IV	Initialization Vector
L2TP	Layer 2 Tunneling Protocol
LEAP	Lightweight Extensible Authentication Protocol
MAC	Message Authentication Code or Media Access Control
MD5	Message Digest 5
MIC	Message Integrity Code
OFDM	Orthogonal Frequency-Division Multiplexing
OSI	Open System Interconnect
PEAP	Protected EAP
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Repote Authentication Dial-in User Service
QoS	Quality of Service
RADIUS	Repote Authentication Dial In User Service
RC4	Symmetric stream cipher
RTS/CTS	Request-To-Send/Clear-To-Send
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TDD	Time Division Duplex
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol

TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
VPN	Virtual Private Network
WDS	Wireless Distribution Systém
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XOR	Nonekvivalence

SEZNAM OBRÁZKŮ

SEZNAM TABULEK