UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Bezpečné autentifikované bezdrátové připojení

Petr Moravec

Bakalářská práce
2010

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 12.8.2010 Petr Moravec

Poděkování

Děkuji Mgr. Tomáši Hudcovi za vysvětlení celého řešeného problému, připomínky a vedení celé mé práce. Dále děkuji rodičům a kamarádům za podporu během studia.

Anotace

Cílem práce bylo vytvořit souhrn a popis dostupných zabezpečení bezdrátových sítí, posoudit jejich bezpečnost a popsat možné útoky na ně. Další částí bylo navrhnout zabezpečení bezdrátové sítě tak, aby nebylo možné se připojit bez zadání uživatelského jména a heslo nebo osobního certifikátu nebo dalších zabezpečení.

Vlastní návrh je realizován pomocí serveru FreeRADIUS a klienta RADIUS serveru RouterBoard s RouterOS od firmy MikroTik. Server vyžaduje pro připojení vlastnictví certifikátu a znalost vlastní kombinace uživatelského jména a hesla. Server také ukládá do databáze všechny přístupy a pokusy o připojení.

Klíčová slova

WEP, WPA, WPA2, 802.1x, RADIUS server, FreeRADIUS, MySQL, RouterOS, MikroTik, Wi-Fi, autorizace

Title

Secure authenticated wireless connection

Annotation

The aim of the thesis was to create a summary and description of available security measures of wireless networks, judge their security and describe possible attacks on them. Design of security measures of wireless network that would not allow connection without user name and password, or personal certificate or additional security was done next.

Design itself is realized using the FreeRADIUS server and RADIUS client of RouterBoard with RouterOS from the MikroTik company. Ownership of certificate and knowledge of valid user name and password is required by the server for successful connection. All access info and connection attempts are saved into database by the server as well.

Keywords

WEP, WPA, WPA2, 802.1x, RADIUS server, FreeRADIUS, MySQL, RouterOS, MikroTik, Wi-Fi, authorization

Obsah

Seznam zkratek

AES	Advanced Encryption Standard
AP	Access point
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CRC-32	Cyclic redundancy check
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
FMS	Fluhrer, Mantin and Shamir attack
IEEE	Institute of Electrical and Electronics Engineers
MAC	Media Access Control
MD5	Message-Digest algorithm
MIC	Message Integrity Code
PEAP	Protected Extensible Authentication Protocol
PPP	Point-to-Point Protocol
PSK	Pre-shared key
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

Seznam obrázků

Seznam tabulek

Úvod

Cílem této práce je popsat dostupné zabezpečení bezdrátových sítí, popsat jejich slabiny a možné útoky na ně. Dále u každého zabezpečení posoudit jeho bezpečnost, náročnost použití a přehled potřebného hardware k implementaci.

V další části je za cíl návrh zabezpečení bezdrátové sítě tak, aby nebyla možnost připojit se k síti bez autentifikace (např. kombinací jména a hesla, soukromým klíčem apod.). Pro tento návrh je nutné také specifikovat nutný hardware, který musí být použit pro realizaci připojení.

Poslední částí práce je část praktická, kde je popsána realizace návrhu. Konfigurace je uvedena navrženým způsobem tak, že ukládá přístupy, dobu připojení a neoprávněné pokusy o připojení do databáze.

Bezdrátové připojení v dnešní době je jedním z nejrozšířenějších přenosových medií internetu ke koncovému uživateli, protože mobilita je jeho velkou předností. Existuje několik druhů připojení, které se dělí podle rychlosti připojení, kvality, možnosti vzdálenosti přenosu a také cenou zařízení. Bezdrátové sítě se používají v domácnostech, přednáškových sálech a stále častěji ve veřejných prostorech. Tyto veřejná místa je nutné chránit z důvodu neoprávněného zneužití. Nebezpečí, kterých hrozí, je mnoho, protože v dnešní době se snaží mnoho lidí využít slabin k páchání přestupků, někdy i trestných činů.

1 Jednotlivá zabezpečení

Jednotlivá zabezpečení jsou rozdělena podle stupně zabezpečení, na začátku kapitoly je uveden souhrn základních zabezpečení, které mohou být součástí ostatních zabezpečení.

1.1 Základní pravidla a doporučení pro bezpečnost

Při budování bezdrátové sítě je nutno praktikovat několik základních opatření, která nám zvýší bezpečnost a ochrání síť před lehkým prolomením pomocí zjištění klíče nebo nezabezpečeného přístupu k hardwaru.

1.1.1 Volba SSID

Volba SSID je důležitým prvkem v zabezpečení. SSID je nutno volit tak, aby neobsahoval klíč zabezpečení a ani žádnou spojitost s ním. Špatná volba SSID by mohlo napomoci útočníkovi při útoku. SSID by nemělo ani obsahovat umístění vysílače, aby nebylo ulehčeno nalezení vysílače a útok na něj.

Pomocí SSID je možnost lehce zabezpečit síť pomocí skrytí SSID. Skrytím SSID je síť neviditelná navenek. Klient, který se chce připojit, musí znát parametry nastavení sítě (včetně samotného skrytého SSID), podle kterých má ve správci bezdrátových sítí vytvořený profil sítě a když je síť v dosahu, je možno se na ní připojit. Skrytí SSID je velmi jednoduché zabezpečení, protože jednoduchým odposlechem se dá tato síť detekovat. Avšak pokud je tato metoda v součinnosti s některým z šifrování nebo jiným druhem zabezpečení, působí kladně pro zvýšení bezpečnosti.

Problémy tohoto zabezpečení mohou nastat na straně klientů, velkým problémem může být chybějící správce bezdrátových sítí – nemožnost nastavení sítě, dalším problémem je pomalejší připojení. V neposlední řadě zde nastává problém pro správce bezdrátové sítě, protože ve veřejných prostorech může nastat situace, že SSID budou mezi sebou kolidovat díky volbě stejného SSID. [15][1]

1.1.2 Nastavení DHCP

DHCP je server pro automatické nastavení klienta při připojení k síti. Jeho použití je obvyklé, protože s jejím použitím odpadá nutnost nastavování klienta při každém připojení. Toto můžeme ale brát i jako nevýhodu pro bezpečnost, protože útočník po prolomení zabezpečení nemusí zjišťovat nastavení rozsahu IP adres, výchozí brány a dalších parametrů, proto správce sítě by měl zvážit zda DHCP server skutečně potřebuje. Pro poskytovatele internetu domácnostem nebo firmám je DHCP

server zcela zbytečný, protože jednotlivým klientům mohou přidělit staticky IP adresu. Pro šíření internetu na veřejnosti jako je např. pokrytí škol, veřejných center nebo restaurací je DHCP téměř nezbytné. [15][1]

1.1.3 Zabezpečení vysílače

Zabezpečení vysílače je nutné, aby nedošlo k poškození hardwaru nebo útoku na síť pomocí přímého napojení na vysílač. Důležitým zabezpečením vysílače je volba přístupového hesla do administrace přístroje. Je nutné volit přístupové jméno a heslo velmi bezpečně. Dalším důležitým zabezpečením je umístění vysílače nebo serveru. Vysílač by měl být umístěn na hůře dostupném místě, aby nebylo možno se k němu lehce dostat.

1.1.4 Klíč zabezpečení

Klíč je využíván pro zabezpečení pomocí šifrování. Klíč by měl být volen, aby byl bezpečný podle pravidel pro bezpečná hesla – měl by obsahovat kombinaci velkých a malých písmen, číslic a speciálních znaků. Mezi klíčem a SSID by neměla být žádná vazba.

1.2 MAC restrikce

Adresa MAC je unikátní adresa každého síťového zařízení. Pomocí MAC restrikce můžeme určit, které zařízení bude mít přístup do sítě nebo naopak, které nebude mít přístup. Při nastavování této metody musí správce ručně nastavit každé nové zařízení, aby mu mohl povolit přístup do sítě. Toto avšak platí jen pro případ, že je povolen přístup jen vypsaným adresám MAC.

Svoji správnou funkci plní tato metoda při udělování zákazů přístupu k síti, pokud například správce potřebuje zakázat přístup do sítě uživateli, který se dopouští přestupků (šíření spamu), a zná jeho adresu MAC, může tomuto uživateli pomocí MAC restrikce zakázat přístup do sítě ze současného zařízení. [1]

1.2.1 Možnosti útoku

Na toto zabezpečení existuje jednoduchý útok. Stačí získat povolenou adresu MAC a nahradit svou adresu získanou. Získání povolené adresy MAC je jednoduché, protože stačí odchytit ARP dotaz, který obsahuje adresu IP a následně adresu MAC.

Odchycení se provede pomocí nástroje na skenování sítě (např. Wireshark), pro odchycení okolní komunikace se musí wi-fi karta přepnout do monitorovacího módu (tuto funkci neumí každá wi-fi karta). V nástroji Wireshark se zachytí veškerá ko-

munikace, kde lze najít i potřebné údaje pro útok na MAC restrikci. Aby bylo možné zachytit komunikaci, musí probíhat v tu dobu komunikace povoleného klienta. Pak již stačí přepsat adresu MAC útočníka na získanou adresu a připojit se.

Útočník může donutit původního majitele k odpojení pomocí DoS útoku nebo se může i připojit zároveň s původním majitelem, ale to hrozí riziko, že při komunikaci se stejným serverem může dojít ke kolizi. Mimo tuto výjimku původní majitel a ani ostatní zařízení v síti nezjistí kolizi a může takto útočník zůstat neodhalen.

Omezením tohoto útoku může být, že změnu adresy MAC nepodporuje každá wi-fi karta. Proti tomuto útoku neexistuje účinná obrana, která by zabránila zkušenému útočníkovi prolomit zabezpečení.[1]

1.2.2 Náročnost použití a implementace

Samotná implementace spočívá pouze v povolení MAC restrikce, zvolení metody povolování (povolí všechny nebo zakáže všechny) a vypsání adres MAC do seznamu. V případě všech povolených a zakázaných jen vypsaných v seznamu probíhá připojení obvyklým způsobem, jen se zařízení ověří, zda není na seznamu zakázaných zařízení. Pokud jsou všichni klienti zakázaní a povolení jen vypsaní, je použití složitější. Při připojení nového klienta je nutno zadat jeho adresu MAC na seznam povolených zařízení.

Náročnost na samotné zařízení má pouze na straně vysílače, které musí podporovat MAC restrikci, to ovšem není záležitost samotného hardware, ale software vysílače. Na straně klienta není žádný požadavek, protože adresu MAC má každé bezdrátové síťové rozhraní.

1.2.3 Shrnutí

MAC restrikce je nejjednodušší zabezpečení bezdrátové sítě. Samotné je velmi neefektivní a nebezpečné. Samotná MAC restrikce se nedoporučuje používat, ale s některým z dalších zabezpečení kladně přispívá k bezpečnosti. Dnes může být MAC restrikce využita k zabránění přístupu do sítě určitému zařízení, ale tato funkce není spolehlivá, protože se může obejít útokem, který je popsán v kapitole o možnostech útoku.

Jedinou výhodou je, že nemá žádné nároky na zařízení uživatele, ale tato výhoda měla své opodstatnění dříve, když jednoduchá zařízení neuměla žádné zabezpečení, ale v dnešní době už toto neplatí.

1.3 WEP

WEP je základním zabezpečením wifi, který je obsažen v základní standardu 802.11. Šifrování probíhá na druhé síťové vrstvě, takže jsou šifrovány všechny rámce, které prochází. WEP využívá šifrovací mechanismus RC4 a zabezpečení pomocí cyklického kódu pro výpočet kontrolního součtu CRC-32. Odesílatel i příjemce potřebují mít stejný klíč, který se používá pro šifrování a dešifrování. Tento klíč je statický, proto by se měl pro větší bezpečnost obměňovat.

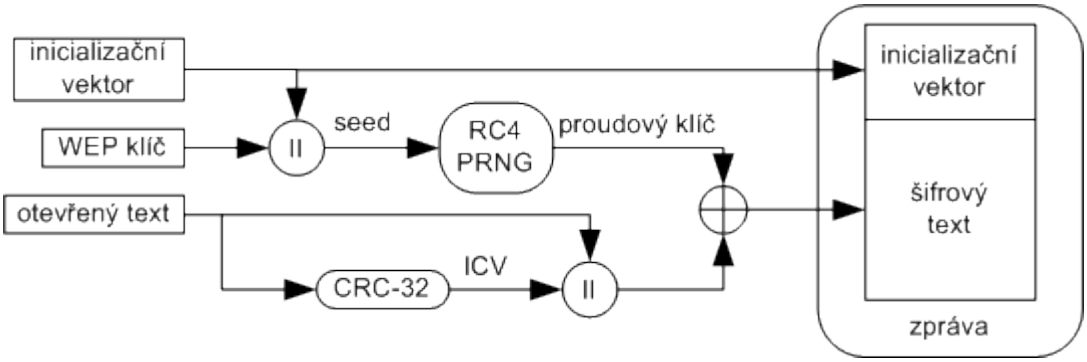
Základní verzí WEP je 64bitová forma, která se skládá z 40bitového klíče a 24bitového inicializačního vektoru, další verzí je 128bitová a někteří výrobci implementují i 256bitovou verzi. V každé této verzi je obsažen 24bitový inicializační vektor a zbytek je klíč (104 bitů, resp. 242 bitů). [1][15]

Inicializační vektor je část řetězce, která zajistí, že bude zašifrovaný řetězec unikátní a nezávislý na ostatních řetězcích generovaných pomocí stejného klíče, protože zašifrování stejné zprávy symetrickou šifrou pokaždé vygeneruje stejnou šifrovanou zprávu a tím by se snadněji mohl klíč uhodnout. Inicializační vektor se mění s každým paketem. Vytvoření inicializačního vektoru provádí vysílací strana, která ho použije k sestavení šifrované zprávy a také ho přiloží v otevřené podobě do záhlaví rámce. Unikátních inicializačních vektorů je jen 224 a stále se opakují dokola, proto inicializační vektor nevyřeší problém s útoky. Inicializační vektor má i nevýhodu, že celý klíč prodlužuje a tím je potřeba více času k dešifrování. [1][15]

CRC-32 (Cyclic Redundancy Check) zajišťuje integritu šifrované zprávy. To znamená, že kontroluje, zda zpráva nebyla změněna mezi odesláním a přijetím. Hodnota kontrolního součtu je obsažena v těle zprávy. CRC-32 je lineární funkce, která lze obejít určitou záměnou bitů, které nedokáže odhalit.

RC4 je šifrovací metoda, která byla zveřejněna roku 1994 Ronem Rivestem. Algoritmus využívá proudovou symetrickou šifru, která používá klíč o délce 40, 104 nebo 232 bitů. Největším problémem je, že musí být uložen u klienta statický klíč, podle kterého se šifruje a dešifruje. Někteří výrobci ukládají klíč do speciální paměti síťové karty. Naopak někteří ukládají klíč do registrů v nezabezpečené podobě.

WEP neřeší distribuci klíče, proto tento klíč musí být zadáván ručně do zařízení. Tím je snížena bezpečnost, protože klíč zná oprávněný uživatel a to často pomáhá útočníkovi k lehkému získání přístupu do sítě. Proudová šifra vytváří pseudonáhodný stream o délce jakou má zpráva. Samotné šifrování probíhá pomocí operace XOR mezi streamem a daty. Dešifrování probíhá naopak. [14][15]



Obrázek 1 – Šifrování WEP

1.3.1 Možnosti útoku

Možností útoku na WEP existuje velké množství, protože díky malému zabezpečení lze použít i jednoduché útoky. Již v roce 2000 byla publikována práce na téma zranitelnosti protokolu WEP. Následně bylo publikováno několik prací, které popisovaly možnosti útoků. Od roku 2004 po útoku KoreK se začal protokol WEP považovat jen za identifikátor, který označoval síť jako soukromou, ale již se nedal považovat za bezpečný.[14]

Útok hrubou silou (brutal-force attack) – tento útok spočívá v postupném zkoušení možných hodnot klíče. Lze postupovat podle slovníku nebo různými kombinacemi znaků. Avšak v přijatelném čase lze tento útok uskutečnit jen proti 40bitovému šifrovacímu klíči, kde útok trvá několik hodin. Při úspěšném útoku získá útočník šifrovací klíč, který poslouží pro připojení k síti. [15]

V dnešní době je tento útok velmi neefektivní. Obranou je častá změna šifrovacího klíče nebo omezení počtu pokusů o autentizaci za určitý čas, ale toto ošetření může přinést i problém v podobě neprovedení autentizace oprávněného uživatele. Deautentizaci lze provést jednoduše a tím vše může vést k DoS útoku.

Injekce paketu – tento útok je proveditelný díky tomu, že se inicializační vektor u každého paketu nemusí měnit. Toho se dá využít při útoku na šifrovací sekvenci, kdy se analýzou dvou paketů odvozených od stejného IV zjistí sekvenci šifrovacího klíče. Principem je, že XOR dvou zašifrovaných zpráv a XOR dvou původních zpráv dává stejný výsledek.

Injekce paketu proběhne díky zjištěné šifrovací sekvenci k vytvoření libovolné nové zprávy. Vezme se nová nezašifrovaná zpráva, provede se operace XOR se známou sekvencí a vytvoří se tak nová šifrovaná zpráva. Příjemce vzniklý paket dešifruje a akceptuje jako platná data. Tímto útokem může posílat útočník do sítě falešná data, která můžou mít různé následky.[15][16]

FMS útok – útok byl popsán již v roce 2001. Útok počítá s tím, že se vyskytují inicializační vektory, podle kterých se dá určit privátní část klíče. Útočník pro uskutečnění musí znát několik počátečních bajtů šifrovaného textu, ale díky tomu, že všechny IP a ARP pakety začínají hodnotou 0xAA není toto problém.

První verzí byl BF-FMS (brutal-force FMS), který se liší s klasickým BF v potřebě výkonu a počtu paketů. Pro klasický BF stačí jeden paket, ale je potřeba velký výpočetní výkon, oproti tomu BF-FMS potřebuje velké množství paketů, ale stačí menší výpočetní výkon.

V roce 2002 byl představen optimalizovaný FMS. Ten pomocí ARP dotazů generuje síťový provoz. Cílem tohoto útoku je získat šifrovací klíč pro připojení. Nejznámějším programem, který využívá FMS útok, je Aircrack –ng, pomocí kterého lze vykonat útok řádově v minutách.

Obranou proti tomuto útoku je jedině v aktualizace firewall, aby se nepoužívaly slabé třídy inicializačních vektorů. [15]

1.3.2 Náročnost použití a implementace

Implementace do hardwaru bezdrátových zařízení je snadná a tudíž nemá vliv šifrování na výkon počítače. Z administrátorského hlediska aktivace zabezpečení WEP spočívá v nastavení daného zabezpečení a nastavení klíče. Z uživatelského hlediska je připojení jednoduché, pro připojení musí znát uživatel pouze klíč, který zadá ve svém správci bezdrátových připojení.

1.3.3 Shrnutí

WEP je první zabezpečení, které v počátku svou funkci vykonávalo dobře, ale po úspěšném útoku a po letech zdokonalování útoků se WEP stalo jen znakem, že není síť veřejná.

Proběhly i pokusy o oživení zabezpečení WEP tím, že se vydaly nové verze, které jsou označované jako WEP+ a WEP2. WEP+ je vylepšený WEP a snaží se odstranit slabé inicializační vektory, které poskytují útočníkovi velmi rychlé spočítání klíče. Toto vylepšení musí obsahovat obě vysílající strany, jinak probíhá komunikace přes klasické WEP. Vylepšení WEP2 se snaží odstranit další bezpečnostní chyby – rozšíření inicializačních vektorů a zesílení 128bitového šifrování. Byl použit na zařízeních, kde nebylo možná implementace WPA nebo WPA2, ale bohužel WEP2 má stejné bezpečnostní problémy, takže útočníkovi prolomení tohoto zabezpečení zabere akorát více času.

WEP a ani jeho novější verze (WEP+ a WEP2) se rozhodně nedoporučuje používat v místech, kde by mohla probíhat citlivější komunikace. V ostatních sítích je použití na vlastní nebezpečí. Dříve mělo WEP opět výhodu, že nové zabezpečení nebylo podporováno ve všech zařízeních, ale v dnešní době už opět většina zařízení umí novější typ zabezpečení. Pokud tedy není síť omezena použitím starších zřízení, nedoporučuje se používat zabezpečení WEP.

1.4 WPA

Na konci roku 2002 vydalo IEEE zabezpečení WPA, které bylo dopředně kompatibilní s vyvíjeným standardem 802.11i (WPA2). WPA umožňuje implementaci na AP, na kterých se používal WEP bez hardwarových úprav, stačil jen upgrade software. WPA se tedy stalo dočasným řešením. WPA lze použít s autentizačním serverem IEEE 802.1x, který poskytuje jednotlivým uživatelům rozdílné klíče. Další použití je v režimu PSK (pre-shared key – předsdílený klíč), které vychází z toho, že všichni uživatelé mají stejný šifrovací klíč. [1]

Data jsou šifrována proudovou šifrou RC4 se 128bitovým klíčem a 48bitovým inicializačním vektorem. Největší změna oproti WEP je v použití TKIP, které využije zadaný klíč pouze jako první hodnotu, z níž se matematicky vypočítají další šifrovací klíče. Tímto je zaručeno, že stejný klíč nebude použit dvakrát, jako tomu je u WEP. Díky delším inicializačním vektorům a použití TKIP je WPA mnohem bezpečnější a odolává útokům, které byly použity na WEP. Pro kontrolu integrity se využívá MAC (Message Autentication Code), který se zde nazývá MIC (Message Integrity Code).

TKIP – protokol, který obsahuje dynamické generování klíčů a kontrolu integrity MIC. Obsahuje i ochranu proti útoku přeposíláním pomocí číslování paketů. Útočník nemůže odposlechnout dostatek paketů, aby odhalil šifrovací klíč, protože TKIP mění klíč pro každý paket. TKIP vyžívá 128bitový klíč pro šifrování a 64bitový klíč pro kontrolu integrity dat. Na začátku klient získá tyto dva klíče bezpečnou cestou při první komunikaci pomocí protokolu 802.1x. [1]

Klíč, který zajišťuje integritu, se označuje MIC. Jako první při šifrování se provede XOR mezi hodnotou klíče (Temporal Key) a adresou MAC odesilatele, tím vznikne první klíč. Dále se první klíč sloučí se sekvenčním číslem a vzniká druhý klíč, který je určen pouze pro jeden paket. Mechanismu WEP se druhý klíč předá jako standardní 128bitový WEP klíč. Dále přenos probíhá jako u přenosu pomocí WEP. Největším rozdílem oproti WEP je, že díky výpočtu prvního klíče už nepoužívají všichni klienti stejný klíč a díky výpočtu druhého klíče už není vztah mezi hodno-

tou inicializačního vektoru (v tomto případě sekvenčním číslem) a samotným šifrovacím klíčem. [15]

MIC – Message Integrity Code je hashovaní funkce, která má na výstupu délku osm bytů, což je dvojnásobná délka oproti kontrole integrity u WEP. Integrita se ověřuje pomocí digitálního podpisu, který se přidává ke každému rámci. Počítá se z datové části rámce, pořadového čísla paketu, zdrojové a cílové adresy MAC a náhodné hodnoty. Tím, že pracuje i se zdrojovou a cílovou adresou, je možné ověřit integritu adres MAC. Když se objeví kolize, tak téměř s jistotou je síť pod útokem. Po odhalení útoku se okamžitě změní klíče na nové a staré se přestanou používat. [14]

Sekvenční číslo (inicializační vektor) – problém s inicializačními vektory řeší TKIP pomocí dvou pravidel. Velikost inicializačního vektoru se zvětšila z 24b na 48b. Což znamená, že při přenosové rychlosti 54 Mbps se vyčerpá za dobu delší než 1000 let. A za druhé nařizuje, aby hodnota IV rostla inkrementálně od nuly a hodnoty mimo pořadí se ignorovaly. Z pohledu bezpečnosti znamená rozšíření prostoru IV (resp. sekvenčního čísla) eliminaci kolizí IV a na nich založené útoky. [14]

1.4.1 Možnosti útoku

I když došlo k úpravám jako je prodloužení inicializačních vektorů a klíčů, odstranění paketů s podobným klíčem a změně kontroly ověřující zprávy je v dnešní době WPA v kombinaci s TKIP některými útoky snadné prolomit. Tato kombinace je považována za stejně nebezpečnou jako je WEP. Sdílené heslo se dá odhalit například slovníkovým útokem. Stačí odchytit jedinou výměnu paketů při autentizaci klienta a pak spustit slovníkový útok off-line. Při dnešním výkonu tento je uskutečnitelný v několika hodinách.[16]

1.4.2 Shrnutí

WPA se dá rozdělit do dvou druhů použití WPA-TKIP a WPA-AES. WPA-TKIP neposkytuje takovou ochranu jako WPA-AES, proto se nedoporučuje používat pro sítě s citlivějšími daty a pokud vše dovolí, doporučuje se používat WPA-AES. To poskytuje již dostatečnou ochranu, ale v dnešní době již není problém podpory WPA2, takže pokud opět vše dovolí, je nejlepší řešení zvolit WPA2-AES, které je v současné době nejlepší řešení s předsdíleným klíčem (PSK).

1.5 WPA2 a RADIUS server

WPA bylo pouze jako provizorní řešení, které zastoupilo WPA2 do roku 2004 kdy se v praxi nasadilo část řešení skupiny 802.11i. Hlavním rozdílem oproti WEP a WPA bylo nasazení šifry AES, která avšak nebyla zpočátku ještě dokončena. TKIP je možné použít pro zachování zpětné kompatibility s WPA. WPA2 pro správu klíčů nově implementuje protokol CCMP a pro kontrolu integrity zprávy zůstává MIC z WPA. Někdy se WPA2 označuje jako RSN – Robust Security Network.

***CCMP* (Counter Mode with CBC-MAC Protocol)** – je šifrovací protokol, který nahrazuje TKIP. CCMP je povinnou součástí WPA2. Protokol využívá šifrovací standard AES. Na šifrování je použit režim CCM, to je kombinace čítačového režimu a CBC-MAC. Čítačový režim zajišťuje šifrování a CBC-MAC zajišťuje autentizaci a integritu dat s využitím MIC. Čítačový režim převádí blokovou šifru na proudovou. [14]

Vstup pro šifru je skupina bitů, kde je část čítač a část náhodná. Tento vstup se zašifruje blokovou šifrou a výsledek je stejně dlouhý jako blok zašifrovaných dat. Ze zašifrovaných dat se vezme každým posunutím čítače jeden byte a tato získaná data se pomocí XOR spojí s textem a tím vznikne šifrovaný text. Hodnoty čítače se nesmí nikdy opakovat.

Pro kontrolu integrity MIC se používá CBC-MAC (Cipher Block Chaining - Message Authentification Code). Šifra probíhá stejně jako v CBC, ale použije se pouze poslední blok jako MAC, z kterého slouží jako MIC horních 64 bitů.

AES – Advanced Encryption Standard je bloková šifra. AES je standard amerického federálního standardu FIPS. Šifra Rijndael, která je využita v AES, byla vyvinuta Joanem Deamenem a Vincentem Rijmenem z Belgie. Na federální šifrovací AES byla vypsána 2. 1. 1997 soutěž, do které se přihlásilo několik algoritmů, ale z pětice, která se dostala do užšího výběru, vyšel jako nejlepší algoritmus Rijndael. AES používá stejně jako RC4 symetrický klíč, takže se šifruje i dešifruje pomocí stejného sdíleného klíče. Délka klíče může být 128, 192 nebo 256 bitů. Hlavním rozdílem oproti RC4 je, že AES šifruje celé 128bitové bloky (RC4 šifruje lineárně operací XOR každý bajt). Odtud získala šifra název bloková. Hlavní výhodou Rijndaelu jsou veliká rychlost a snadná softwarová i hardwarová implementace.[1]

Autentizace – Autentizace je možná stejně jako u WPA dvěma možnostmi, buď PSK nebo podle 802.1x. U WPA2 je však navíc ještě definovaná předběžná autentizace (pre-authentication), která umožňuje autentizovat se vůči AP, který ještě nemá

v dosahu, tak že vyšle autentizaci prostřednictvím přístupového bodu, se kterým již autentizován je. Tohoto mechanismu se využívá při roamingu mezi WLAN.

802.1x a EAP – 802.1x je protokol, který umožňuje autentizaci na portu. Původně byl tento standard určen pro kabelové sítě, ale lze jej použít ke zlepšení bezpečnosti v prostředí bezdrátových sítí. Protokol 802.1x pochází z protokolu PPP (Point-to-Point Protocol). PPP má však nevýhodu, že umožňuje autentizaci pouze na základě uživatelského jména a hesla. Protokol EAP (Extensible Authentication Protocol) byl nejdříve vytvořen jako doplněk protokolu PPP. Tvůrci chtěli vytvořit platformu pro různé autentizační metody, takže se tedy jedná o PPP s přídavnými autentizačními doplňky. Díky tomu je autentizace uživatelů možná více způsoby. Pro autentizaci mohou být využity hesla, certifikáty, PKI, tokeny, biometriky, čipové karty a mnoho dalších. EAP je otevřený standard, proto ho je možné v budoucnu doplňovat o nově vyvinuté doplňky. [1][14]

802.1x – 802.1x je protokol, který umožňuje využívat EAP na drátových i bezdrátových sítích. Je založen na třech komponentech – žadatel (cílový počítač), autentizátor (router nebo AP) a autentizační server (RADIUS). Pro fungování celého protokolu musí být podporováno 802.1x i EAP na všech komponentách, ale to dnes již není problém, protože podpora těchto komponent je standardně všude.

Autentizátor funguje podobně jako dynamický firewall, dokud neproběhne autentizace, nepropustí nic kromě zpráv protokolu 802.1x a až po úspěšné autentizaci je povolen všechen provoz. Jsou použity dva virtuální porty – řízený a neřízený. Neřízený port je pouze pro komunikaci autentizátora s autentizačním serverem. Řízený port je na začátku v neautorizovaném stavu, takže je blokován veškerý provoz. Po autentizaci klienta se řízený port přepne do autorizovaného stavu a může jím procházet síťový provoz. [14][1]

***Průběh autentizace* [1]**

1. Žadatel (klient) začne odesláním rámce EAP Start. Tím se autentizátor dozví, že se chce někdo připojit do sítě.

2. Autentizátor odpoví rámcem EAP Request/Identity, kterým žádá o určení totožnosti.

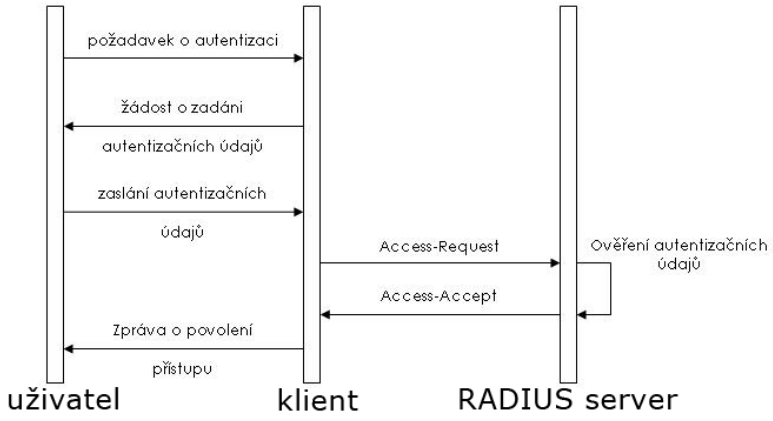
3. Žadatel odpoví také rámcem EAP Request/Identity, ve kterém se identifikuje (uživatelské jméno). Autentizátor tuto informaci předá autentizačnímu severu.

4. Autentizační server zjistí, zda účet existuje a pošle autentizátoru rámec EAP Request, který obsahuje výzvu na informaci (například na zadání hesla). Autentizátor tento rámec předá žadateli.

5. Žadatel odpoví požadovanou informací. Autentizátor opět předá odpověď autentizačnímu serveru.

6. Autentizační server provede ověření a odpoví autentizátoru rámcem EAP Success při kladném ověření nebo EAP Failure při zamítnutí o autentizaci.

7. Pokud autentizátor obdrží rámec EAP Success, přepne autentizátor řízený port z neautorizovaného stavu do stavu autorizovaného a povolí normální síťovou komunikaci. Při EAP Failure zamítne žádost žadatele a nechá uzavřený port.



Obrázek 2 – průběh autentizace

Použití 802.1x s WEP – Protokol 802.1x lze také využít k bezpečnému šíření klíčů pro jednotlivé stanice. V prostředí WEP používali všichni stejný sdílený klíč WEP, ale pomocí protokolu 802.1x může každý klient dostat svůj vlastní klíč WEP. Pokud se útočníkovi podaří klíč WEP rozluštit, bude s ním moci rozluštit pouze komunikaci daného uživatele nebo dané relace. Tato technika, kdy nelze jedním klíčem rozluštit veškerou komunikaci, se označuje jako dynamický WEP a slouží jako metoda snižující některá rizika vyplývající z WEPu a jeho známé zranitelnosti. Protože 802.1x navíc umožňuje automatické obnovení klíče, může klienty donutit pravidelně žádat o nový klíč, čímž se sníží počet kolizí IV. V krajním případě se může generovat klíč každých 30 sekund.

Jednou z nejdůležitějších možností je, že lze klienty individuálně identifikovat a autentizovat. V původním prostředí WEPu sdíleli všichni uživatelé stejný klíč. Když došlo k autentizaci uživatele, jediná informace, kterou bylo možné získat, byla ta, že daný uživatel zná klíč, takže útočníka nemohl nikdo rozeznat, když získal klíč. U protokolu 802.1x je každý autentizovaný uživatel jednoznačně identifikován. [1]

Autentizační metody protokolu EAP – V současnosti podporuje protokol EAP mnoho metod autentizace. Jednotlivé metody se liší v náročnosti použití, ale i v bezpečnosti. Nejznámější autentizační metody jsou MD5, PEAP, TTLS, LEAP, TLS.

MD5 – MD5 (původně CHAP) je metoda, která se nejsnadněji implementuje, ale také poskytuje nejnižší úroveň zabezpečení, protože je napadnutelná celou řadou útoků mezi které patří i prostý slovníkový útok. Kromě velkého množství útoků neumí ani vzájemnou autentizaci, takže je zranitelná i útokem přeposílání přes útočníka. Umí pouze jednosměrnou autentizaci, to znamená, že klient se může ověřit u AP, klient už ale nemá možnost ověřit pravost AP. Další nevýhodou je, že metoda MD5 nepodporuje dynamické generování WEP/TKIP klíčů, protože neobsahuje žádné mechanismy umožňující vytvářet jednotlivé klíče pro klienty. Tato metoda by se neměla vůbec používat, protože má velice mnoho nevýhod, někteří výrobci tuto metodu ani nepovolují.[15]

PEAP – Protokol PEAP (Protected EAP) podporuje vzájemnou autentizaci a dynamickou obnovu WEPových klíčů. Vyžaduje certifikát pouze na straně serveru. Autentizace klientů probíhá zabezpečeným kanálem, takže je možno použít méně bezpečnou metodu. Prostřednictvím certifikátu dojde k autentizaci serveru a následně se může použít jiné metody protokolu EAP k autentizaci klienta. Může se tedy teo-

reticky použít PEAP a MS-CHAP verze 2 a celý postup bude bezpečný, protože komunikace protokolem MSCHAP probíhá v zabezpečeném tunelu. [15][14]

TTLS – Protokol TTLS (Tunneled Transport Layer Security) podporuje také vzájemnou autentizaci i dynamickou obnovu WEPových klíčů. Podobně jako PEAP vyžaduje TTLS certifikát na straně serveru a u klienta není potřeba. Klient se autentizuje pomocí hesel. TTLS je bezpečný a jeho implementace je jednoduchá. [15][14]

LEAP – Protokol LEAP (Lightweight Extensible Authentication Protocol) poskytuje rovněž vzájemnou autentizaci i dynamickou obnovu WEPových klíčů. Tento protokol navrhla v roce 2000 společnost Cisco jako dočasné řešení před schválením standardu 802.1x. Podporovala jej pouze zařízení Cisco a nedočkala se široké podpory ostatních výrobců. [15]

TLS – Protokol TLS (Transport Layer Security) představuje z pohledu bezpečnosti nejsilnější řešení, jeho implementace je ale zároveň nejobtížnější. TLS poskytuje také vzájemnou autentizaci i dynamickou obnovu WEPových klíčů. Protokol prostřednictvím PKI (Public Key Infrastructure) vytváří šifrovaný tunel, jímž probíhá výměna autentizačních údajů. Aby bylo možné TLS použít, musí být na straně serveru i na straně klientů instalovány certifikáty. [15]

1.5.1 Možnosti útoku

Na zabezpečení WPA2-PSK zatím neexistuje žádný spolehlivý útok, který by byl uskutečnitelný cizím útočníkem. Podle posledních zpráv je objevený útok, který dokáže odposlouchávat provoz, ale útočník musí být autorizovaným uživatelem. AirTight Networks provedla útok na síť s WPA2-Enterprise, která má vylepšení, že klienti sítě nepoužívají klíče odvozené od stejného sdíleného hesla, ale každý uživatel má vlastní klíč pro ověření přístupovým bodem. To je za normálních okolností praktické a velmi účelné řešení, díky kterému jednotliví účastníci sítového provozu nemohou odposlouchávat datovou komunikaci ostatních uživatelů.

Útok proběhne tak, že autorizovaný uživatel s platnými přístupovými údaji do sítě podvrhne falešné „broadcast pakety“, ty totiž jsou zabezpečené pouze Group Temporal klíčem, který nechrání proti zfalšování. Díky tomu se útočník může vydávat za gateway a odposlouchávat tak veškerou komunikaci v síti.[13]

2 Rozdělení zabezpečení podle použití a úrovně zabezpečení

Existuje několik zabezpečení, která se liší v úrovni zabezpečení, složitosti, ale také ve vhodném použití. Některá se hodí více pro domácí použití a některá se naopak hodí více pro použití ve veřejných prostorech.

Jednotlivá zabezpečení jsou MAC restrikce, WEP, WPA-PSK, WPA2-PSK a RADIUS server. Podrobně budou zabezpečení rozebrána v další kapitole.

Dnes je několik druhů prostředí, které je nutné chránit a zabezpečit proti útočníkům. Prostředí se liší použitím sítě, ale také rozsahem a nutností kontroly. Prostředí lze rozdělit na dvě velké skupiny – domácí prostředí a veřejné prostředí.

2.1 Domácí prostředí

Zde se jedná o použití pro osobní účely, nejčastěji za účelem šíření internetu nebo vytvoření domácí sítě. Signál pokrývá většinou neveřejné prostory a předpokládá se použití jen velice úzkým okruhem lidí. Zabezpečení zde nemusí být na vysoké úrovni, protože většinou útočníci se nezaměřují na takovéto sítě. Pro domácí sítě jsou vhodné všechny uvedené zabezpečení. Pokud uživatel používá některé ze starších zařízení, které neumí žádné zabezpečení, může použít restrikci na MAC, která je sice velice slabé zabezpečení, ale pro osobní účely dostačující.

Pokud ale není důvod použít toto slabé zabezpečení, je vhodné použít zabezpečení pomocí WEP, WPA-PSK a WPA2-PSK. Všechny zabezpečení jsou na vyšší úrovni než MAC restrikce. Z vyjmenovaných zabezpečení je nejlepší WPA2-PSK, které poskytuje velice dobrou ochranu a je v současnosti doporučovaným zabezpečením pro domácí sítě.

V domácím prostředí lze použít i RADIUS server, který je ale zbytečně složitý a náročný na implementaci, proto se nedoporučuje použít k zabezpečení domácí sítě.

2.2 Veřejné prostředí

Veřejné prostředí zahrnuje především použití ve veřejných prostorech, firmách, školách apod., kde je nutné ochránit síť důsledněji. Předpokládá se, že signál veřejné sítě bude šířen ve veřejně dostupných prostorech nebo prostorech, které využívá velké množství lidí (např. firmy, školy).

Sítě ve veřejném prostředí by se daly rozdělit na více druhů. Jedním druhem je síť kam má přístup každý, kdo je v dosahu signálu (např. restaurace). V tomto druhu se síť ve většině případů používá bez zabezpečení, aby odpadl nutný kontakt se správcem sítě.

Dalším druhem je síť, do které má být umožněn přístup pouze několika zařízením (např. firma). U těchto sítí je předpoklad, že je nutné, aby byla síť dostatečně chráněna, protože může probíhat po síti citlivá komunikace. Pro tyto sítě je naprosto nevyhovující MAC restrikce, ale také zabezpečení pomocí WEP, které je velmi slabé. Oboje zabezpečení neposkytuje ochranu, která je důležitá pro ochránění citlivých dat. Dostatečným zabezpečením je WPA-PSK a WPA2-PSK, která poskytují ochranu pro přenos dat. Nejlepším řešením pro tyto sítě je server RADIUS, který umožňuje vysoké zabezpečení přístupu do sítě, ale také možnost kontrolovat přístupy.

Posledním druhem je veřejná síť, která má kontrolovaný přístup. Jedná se většinou o sítě ve veřejném prostředí, které jsou dostupné pouze pro registrované uživatele (např. škola, poskytovatel internetu). Síť ve většině případů slouží pro sdílení internetu a pokrývá běžně dostupné prostory pro veřejnost. Do sítě je možný přístup například na základě kombinace uživatelského jména a hesla, po předchozí registraci nebo zanesení do systému správcem sítě. Síť má velkou výhodu, že přístup je kontrolovaný a umožněn pouze pro ověřené uživatele. Zde je naprosto nevyhovující MAC restrikce, WEP, WPA-PSK i WPA2-PSK, protože tyto zabezpečení neumožňují ověření uživatele na základě vlastní kombinace uživatelského jména a hesla. Zde je jedinou možností použít RADIUS server, který umožňuje spravovat databázi uživatelů. [1]

V tabulce je uvedeno shrnutí výhod a nevýhod, které mají zabezpečení v jednotlivých prostředích.

Název zabezpečení	Výhody	Nevýhody
Domácí prostředí		
MAC restrikce	Možnost připojení zařízení, které nemá podporu šifrování (např. mobilní telefony)	Pro připojení nového zařízení je nutné přidat adresu MAC do zařízení
WEP	Jednoduché šifrování, má podporu i u starších zařízení	Stupeň ochrany není vysoký a v dnešní době snadno prolomitelné zabezpečení
WPA-PSK	Vysoké zabezpečení šifrovaného přenosu	Menší podpora u starších zařízení
WPA2-PSK	Nejnovější a vysoce zabezpečené šifrování	Menší podpora u starších zařízení
RADIUS server	Nejvyšší zabezpečení	Složitost pro domácí použití
Veřejné prostředí		
MAC restrikce	Nemá výhody	Pro připojení k síti nutno kontaktovat správce sítě - zdlouhavé
WEP	Možnost připojení všech zařízení, jednoduchost připojení	Nízké zabezpečení, nutno znát klíč pro připojení k síti
WPA-PSK	Obvyklá metoda zabezpečení, vysoké zabezpečení	Nutno znát klíč pro připojení k síti
WPA2-PSK	Neexistuje dnes přímý útok, takže má vysoké zabezpečení	Není podpora u všech zařízení a operačních systému
RADIUS server	Služba HotSpot, kontrolovaný přístup do sítě, možnost omezovat uživatele	Dražší realizace díky nutnosti mít v síti RADIUS server

Tabulka 1 – rozdělení zabezpečení podle použití a úrovně zabezpečení

3 Hardware a software pro realizaci

Pro splnění zadání je třeba, aby navržené řešení umožňovalo ověření uživatelů na základě kombinace uživatelského jména a heslo.

Dnešní možnosti zabezpečení se dají rozdělit do dvou druhů. Na jedné straně je zabezpečení pomocí společného klíče a na druhé straně zabezpečení pomocí přihlášení vlastní kombinací uživatelského jména a heslo, certifikátem apod., které jsou vystaveny jednotlivým uživatelům.

Při zabezpečení pomocí společného klíče stačí pro realizaci samotné AP, které poskytuje možnost zabezpečení pomocí WEP, WPA-PSK nebo WPA2-PSK, ale toto cíl zadání neumožňuje splnit.

Další možností je použití protokolu 802.1x, který umožňuje ověření uživatele pomocí mnoha metod, jednou z metod je kombinace uživatelského jména a hesla, která je požadována v zadání práce. Protokol 802.1x je založen na třech komponentech – žadatel (cílový počítač), autentizátor a autentizační server. Jako autentizační server je nejrozšířenější RADIUS server – server, který obsahuje seznam uživatelů, kteří mají přístup do sítě, a obsahuje nástroje na ověření těchto uživatelů Autentizátor je nejčastěji router nebo AP, ke kterému se uživatel připojuje.

Ve výběru samotného RADIUS serveru se nabízí několik variant. RADIUS server je součástí Windows Server, dále existují RADIUS servery určené pro Windows. Například TekRADIUS je distribuován jen pod Windows. Velká část RADIUS serverů pro GNU/Linux má i verze pod Windows, ale to je spíše nedoporučované řešení. Windows jsem však vyřadil z důvodu ceny. RADIUS serverů pro GNU/Linux existuje větší množství. Nejznámějším a nejpoužívanějším je FreeRADIUS, jeho distribuce probíhá zdarma, obsahuje velké množství konfigurací a vyznačuje se dobře zpracovanou dokumentací na internetu i v samotných konfiguračních souborech.

RADIUS server potřebuje pro svou funkci server, který bude stabilní a s co nejmenší pravděpodobností výpadku, na tuto pozici se nabízí celá škála serverů běžně prodávaných. RADIUS server není hardwarově náročný, proto stačí pro provoz i méně výkonnější server nebo server pro jiné služby.

Z pohledu operačních systémů se nabízí také více řešení, ale nejlepším dostupným řešením je GNU/Linux. Výběr GNU/Linux má mnoho výhod, největší výhodou je, že distribuce je zdarma, celý systém je stabilní a nabízí také větší možnosti adminis-

trace. Oproti tomu konkurence v podobě Windows a MAC OS přináší výhody, ale také nevýhody, které jsou rozhodující při výběru. Hlavní nevýhodou je cena a v případě použití MAC OS je nutné použít Apple Macintosh.

Volba distribuce GNU/Linux závisí již na osobních zkušenostech administrátora. Do návrhu byl vybrán operační systém Ubuntu 10.04, protože s Ubuntu mám dlouhodobější zkušenosti. Pro profesionální použití se doporučuje použít serverovou edici Debian(bude se mírně lišit umístění konfiguračních souborů) nebo serverovou edici Ubuntu. Cena serveru se pohybuje od 15 000 Kč.

Klient nebo klienti RADIUS serveru jsou bezdrátové routery. Stejně jako u serveru pro RADIUS server je v nabídce celá škála produktů, které jsou vhodné pro realizaci. Mezi nejlepší dostupné řešení patří routery od firmy MikroTik a od firmy Cisco. V porovnání vychází v některých parametrech lépe MikroTik a jinde Cisco. Možnosti konfigurace je u obou řešení podobná a i samotné rozhraní pro konfiguraci (konzole) vypadá podobně s podobnými příkazy. Zde volba závisí opět na zkušenostech se jmenovanými routery. Další možností jsou routery od firem HP, Asus, OvisLink, D-Link apod., řešení od těchto firem jsou také použitelná, avšak některé ze zařízení nepodporuje RADIUS accounting a nedosahují takových kvalit jako zařízení od firem MikroTik a Cisco.

Pro návrh v této práci bylo vybráno řešení od firmy MikroTik, která má v nabídce několik hardwarových prvků, zvaných RouterBoard, se softwarem RouterOS, který je součástí každého RouterBoard, ale je i samostatně ke stažení na stránkách výrobce. [9] Při výběru samotného RouterBoard se musí hledět na to, aby byl RouterBoard vybaven integrovaným bezdrátovým modulem nebo aby šel dodatečně připojit. Zajímavým produktem je například MikroTik RB411R. Je vybaven vším potřebným pro realizaci.

Na koncového klienta je požadavkem, aby uměl zvolený druh zabezpečení (nejlépe WPA2 se šifrováním AES). Dále je vyžadován protokol PEAP a metodu ověřování EAP-MSCHAP2. Toto vše je dostupné v operačním systému Windows od verze XP Service Pack 2.

4 Návrh zabezpečení bezdrátové sítě

V praktické části této práce jsem se věnoval jednotlivým zabezpečením, která jsou určitým způsobem napadnutelné. Zde bych chtěl navrhnout zabezpečení tak, aby se riziko napadení sítě snížilo na minimum. Vhodně poslouží RADIUS server. Připojení do sítě bude podmíněno vlastnictvím certifikátu a znalost svého uživatelského jména a hesla.

Podle výběru v minulé kapitole je nutné nainstalovat FreeRADIUS, modul MySQL pro FreeRADIUS a samotný MySQL server na vybraný server s operačním systémem GNU/Linux. Postup instalace je uveden v příloze A.

4.1 FreeRADIUS s MySQL

MySQL databáze není standardně obsažen v serveru FreeRADIUS, protože server využívá implicitně textové soubory pro uchování dat. Jedná se zejména o správu uživatelů. Správa těchto souborů by byla složitá a navíc by byl problém se sdílenou databází uživatelů, proto se doporučuje používat databázi. FreeRADIUS umožňuje využití několika typů databází (db2, Iodbc, mysql, oracle, postgresql, sybase, unixodbc). Výběr závisí na zkušenostech administrátora, ale já jsem zvolil MySQL, protože ho dlouhodobě využívám.

Databáze se využívá pro správu uživatelů, NAS serverů a ukládání dat z RADIUS accountingu. Tyto všechny údaje jsou standardně v souborech users, clients.conf a log souborech, které popíšu dále. Databáze má mnoho výhod proč jí použít, největší výhodou je snadná správa, která může probíhat přes aplikaci pro správu databáze nebo přes speciální aplikaci vyrobenou přímo pro s FreeRADIUS databází. Databáze lze vyrobit dvěma způsoby, buď použít schéma, které je obsaženo v souboru schema.sql a nas.sql nebo navrhnout vlastní tabulky. Schémata schema.sql a nas.sql jsou podrobně popsány v příloze B. Při návrhu vlastních tabulek by se muselo upravit pojmenování tabulek v sql.conf a samotné SQL dotazy v souboru dialup.conf. Dialup.conf je standardně nastavený pro použití se schématem ze souboru schema.sql.

Nastavení FreeRADIUS pro práci s MySQL je velice jednoduché. Jedná se o úpravu souborů *sql.conf* a */sites-available/default*. Konfigurace těchto souborů je uvedená v příloze C.

4.2 Správa uživatelů

Pokud z nějakého důvodu nechceme nebo nemůžeme použít databázi, řeší správu uživatelů textový soubor *users*. Soubor user je umístěn ve složce konfigurace serveru.

```
/etc/freeradius/users
```

Soubor *users* obsahuje nastavení parametrů autentizace pro jednotlivé uživatele. V možnostech nastavení je například IP adresa pro připojení (využitelné například u poskytovatelů připojení, kteří mají statické klienty), způsob autentizace nebo lze uživateli i zablokovat přístup do sítě. Nastavení obsahuje účty DEFAULT, které je vhodné smazat nebo zakomentovat (přidáním # na začátek každého řádku) pro větší bezpečnost. V souboru *users* je mnoho příkladů vložení uživatelů, ale jako standardní se využívá[4][7]

```
bob     Cleartext-Password := "hello"
```

Ale v mém návrh je server FreeRADIUS použit v kombinaci s MySQL a tím se veškerá správa uživatelů přesouvá do databáze. V databázi se dodržuje podobná struktura jako v souboru users (pojmenování atributů), to znamená, že příklad s bobem bude pro vložení do databáze vypadat takto:

```
INSERT INTO radcheck VALUES (1,'bob', 'Cleartext-Password',
':=', 'hello')
```

4.3 Vytvoření certifikátů

Certifikát je zašifrovaná informace, která spojuje veřejný klíč s pravou identitou subjektu. Vydavatel certifikátu se označuje jako certifikační autorita. Vydat certifikát může veřejná zákonně ověřená certifikační autorita (např. www.caczechia.cz, www.cacert.org) nebo vydat soukromý certifikát u kterého se předpokládá, že klienti budou věřit sami.

V mém návrhu je použit certifikát vydaný soukromou certifikační autoritou, ale lze jednoduše použít jakýkoliv jiný certifikát. FreeRADIUS potřebuje privátní a veřejný klíč a klient pro připojení potřebuje samotný certifikát. Tyto potřebné soubory jsem vygeneroval pomocí OpenSSL.

4.3.1 Vytvoření soukromého klíče

```
openssl req -new -out my-server.csr
```

v průběhu je nutné vyplnit několik údajů, včetně hesla pro soukromý klíč, toto heslo se zadává v konfiguračním souboru FreeRADIUS (bude uvedeno v jiné kapitole)

Výsledkem jsou soubory:

.rnd – soubor s náhodnými daty, podle kterých se vytvořil klíč

my-server.csr – certifikát

privkey.pem – soukromý klíč

4.3.2 Vytvoření serverového šifrovacího klíče

```
openssl rsa -in privkey.pem -out my-server.key
```

Výsledkem je soubor:

my-server.key – klíč kterým server šifruje komunikaci

4.3.3 Vytvoření certifikátu

```
openssl x509 -in my-server.csr -out my-server.cert -req -
signkey my-server.key -days 365
```

Výsledkem je certifikát s platností 365 dni

my-server.cert

4.3.4 Vytvoření samostatného certifikátu

```
openssl x509 -in my-server.cert -out my-server.crt -outform
DER
```

Výsledkem je certifikát

my-server.crt – certifikát pro instalaci do klientského počítače

Pro FreeRADIUS jsou důležité vygenerované soubory privkey.pem a my-server.key, které se standardně umístí do složky */etc/freeradius/certs.*

4.4 eap.conf

Soubor *eap.conf* obsahuje možnost povolit a nastavit autentizační metody podporované protokolem EAP. Pro můj návrh použiji režim PEAP, kde autentizace probíhá uživatelským jménem a heslem. Pro použití PEAP je nutné povolit a nastavit zabezpečené spojení TLS, které je použité pro vytvoření zabezpečeného kanálu mezi RADIUS serverem a uživatelem. Kanál se používá k poslání uživatelského jména a hesla. Protokol PEAP sám neurčuje metodu ověřování, ale poskytuje jen další zabezpečení jiným protokolům EAP, proto je nutné zvolit pro ověřování protokol MS-CHAP v2, který využije šifrovaný kanál TLS, který vytvoří PEAP.

Proces ověřování protokolem PEAP mezi klientem a RADIUS serverem se skládá ze dvou částí. V první fázi je vytvořen zabezpečený kanál a v druhé fázi dojde přes vytvořený kanál k ověření.

Protokol PEAP s protokolem MS-CHAPv2 lze snadněji nasadit než protokol EAP-TLS, protože ověření uživatele je provedeno pomocí kombinace uživatelského jména a hesla. Úspěšné ověřování protokolem MS-CHAP v2 vyžaduje, aby klient důvěřoval serveru RADIUS, to zajistí tím, že má příslušný certifikát certifikační autority nainstalovaný v úložišti certifikátů. [4][6][7]

Pro funkčnost návrh nastavíme v souboru eap.conf následujíci:

```
eap {
     default_eap_type = peap

     peap {
     default_eap_type = mschapv2
     }
     }

tls {
private_key_password = heslo soukromého klíče
private_key_file = ${certdir}/my-server.pem
certificate_file = ${certdir}/my-server.cert
}
```

Konfigurační volby `private_key_file` a `certificate_file` ukazují na soubory s privátním a veřejným klíčem, které získáte od certifikační autority (CA) nebo naše vygenerované soubory.

Pozornost by se měla věnovat nastavení `CA_file` a `CA_path`. Pokud budou nastavené špatně, může se umožnit přihlášení komukoliv, kdo má certifikát od zadané CA. Doporučuje se nechat `CA_file` nenastavené a `CA_path`, která defaultně ukazuje do adresáře, kde je testovací self-signed CA.

4.5 proxy.conf

V souboru *proxy.conf* se nastavuje, jak budeme požadavky směrovat. Požadavky s realmem „nas_realm.cz“ budeme směrovat na náš RADIUS server. Požadavky bez realmu (*realm NULL*) odmítneme a ostatní požadavky (*realm DEFAULT*) odmítneme nebo například v síti EDUROAM se tyto požadavky posílají na národní RADIUS server, kde jsou dále zpracovány a rozřazeny. Realm určuje RADIUS server, který je pro přihlašovaného uživatele domovský. V souboru proxy.conf jsou velké možnosti pro filtraci uživatelů, ale pro naše potřeby se využije málo. Jedná se prakticky jen o určení názvu realmu.

Po úpravách zbude v souboru pouze následující:

```
proxy server {
default_fallback = no
}

realm nas_realm.cz {
}

realm LOCAL {
}

realm NULL {
}
```

4.6 clients.conf

V souboru *clients.conf* je nastavení všech zařízení ověřující klienty, tedy všechny přístupové body. Tento soubor má opět význam pouze pokud nebudeme používat databázi. V databázi tento soubor zastupuje tabulka *nas*, která obsahuje opět všechny údaje jako tento soubor. Struktura tabulky *nas* je uvedena v příloze B.

Příklad definování klienta RADIUS:

```
client 192.168.1.10 {
        secret      = heslo
        shortname   = ap
}
```

4.7 Spuštění serveru

Pro testování se FreeRADIUS spustí příkazem

```
freeradius -X
```

Pro běžný provoz běží FreeRADIUS jako deamon na pozadí. Spuštění se provede příkazem (zastavení pouze výměnou start za stop)

```
/etc/init.d/freeradius start
```

5 Nastavení klienta

Klient RADIUS v RouterOS firmy MikroTik zvládne spoustu věcí. Autorizaci HotSpotu, PPP, PPPoE, PPTP, L2TP, ISDN atd.

Pro nastavení klienta RADIUS je potřeba přejít do jeho úrovně v konzoli příkazem */radius***.** Výpisem *print* je vidět, že na routeru není žádný záznam.

```
[admin@MikroTik] /radius>> print
Flags: X - disabled
# SERVICE CALLED-ID DOMAIN    ADDRESS   SECRET
```

Co je povoleno v této úrovni lze jednoduše zjistit zadáním příkazu ?. Pro účel nastavení připojení k RADIUS serveru je potřeba jen add.

```
[admin@MikroTik] /radius>> ?
MikroTik RouterOS can authenticate for PPP, PPPoE and PPTP
connections
.. -- go up to root
add -- Create a new item
```

add – volba přidá nové propojení k serveru RADIUS

RADIUS server se přidá příkazem add s následujícími parametry. Přidá se RADIUS server s adresou 192.168.1.1, heslo pro komunikaci je heslo a jako služby byly aktivovány wireless a dhcp.

```
[admin@MikroTik] /radius>> add address=192.168.1.1
secret=heslo service=wireless,dhcp
```

Pro ověřování byly učiněny všechny potřebné kroky. Doporučuji ověřit nastavení následovně:

```
[admin@MikroTik] /radius>> print detail
Flags: X - disabled
0 service=wireless,dhcp called-id="" domain="" add-
ress=192.168.1.1 secret="heslo" authentication-port=1812 ac-
counting-port=1813 timeout=300ms accounting-backup=no re-
alm=""
```

Parametry *called-id*, *domain* ani *realm* není potřeba primárně nastavovat, pokud pro jejich využití není opodstatnění. Nastavení *portů*, *timeout* a *accounting-backup* zůstane na výchozích hodnotách. [8][9]

5.1 Nastavení RADIUS Authorization

V předchozí kapitole se provedla konfigurace komunikačního mostu mezi serverem RADIUS a klientem RADIUS serveru. Dále se musí nakonfigurovat router tak, aby služby komunikovaly s autorizačním serverem

5.1.1 Wireless

Aby bylo možné ověřovat uživatele pomocí EAP, musí se tato volba aktivovat v natavení zabezpečení bezdrátové sítě. Pro aktivaci je nutné vytvořit nový bezpečnostní profil a aktivovat tento profil na bezdrátovém interface.

Pří přidání nového bezpečnostního profilu se mu přidělím jméno RADIUS a pomocí volby *radius-eap-accounting* se zapne accounting. To znamená, že všechny záznamy a požadavky, které obdrží router, pošle RADIUS serveru, který vše zpracuje a zapíše všechny údaje do databáze. V databázi lze pak dohledat všechny pokusy o připojení, úspěšné připojení a odhlášení jednotlivých uživatelů.

```
[admin@MikroTik] /interface wireless>> security-profiles add
name=RADIUS radius-eap-accounting=yes
```

Pro kontrolu lze využít opět volbu *security-profiles print* k vypsání seznamu profilů. Ve výpise by měla být vidět zapnuta volba *radius-eap-authentication=yes*. Aktivace na příslušný interface se provede přiřazením bezpečnostního profilu RADIUS k bezdrátovému interface

```
[admin@MikroTik] /interface wireless>> set bezdrat security-
profile=RADIUS
```

A ověřím opět příkazem print:

```
[admin@MikroTik] /interface>> wireless print
Flags: X - disabled, R - running
1    R    name="bezdrat"      security-profile=RADIUS
```

5.2 Server DHCP

Služba DHCP zajišťuje přiřazení IP adresy a dalších údajů pro připojení k síti nově připojeným uživatelům. V součinnosti s RADIUS serverem DHCP přispívá k větší bezpečnosti sítě, protože údaje přidělí pouze ověřeným uživatelům. Tato služba je nezbytná pro flexibilitu sítě, protože ušetří mnoho času, který by se strávil nastavováním příslušných údajů. Nastavení DHCP serveru je popsáno pouze stručně, jen pro aktivaci komunikace s RADIUS serverem, ostatní nastavení je nutno dohledat v dokumentaci RouterOS

Vypsání detailů o DHCP serveru se provede jednoduše příkazem print.

```
[admin@MikroTik] /ip>> dhcp-server print detail
Flags: X - disabled, I - invalid
0    name="dhcp"    use-radius=no
```

Aktivaci komunikace DHPC a RADIUS serveru se zapne nastavením *use-radius* na yes.

```
[admin@MikroTik] /ip>> dhcp-server set dhcp use-radius=yes
```

Tímto by měla být dokončena celá konfigurace klienta RADIUS serveru – RouterOS. RouterOS poskytuje mnoho dalšího nastavení, které je nutné pro plné zprovoznění sítě, ale toto je mimo rozsah této práce. [8][9]

Závěr

Celá práce se skládá ze dvou částí. V první části bylo cílem sestavit souhrn dostupných zabezpečení, popsat jejich slabiny a možnosti útoku. V této části je vytvořen popis základních bezpečnostních pravidel, která dobře přispívají k zabezpečení, jsou dobře kombinovatelná, ale samostatně jsou nedostatečná. Tyto pravidla je doporučeno používat v kombinaci s některým z dalších zabezpečení, která jsou popsána dále.

Zabezpečení WEP, WPA a WPA2 jsou už samostatně použitelné zabezpečení. WEP je zastaralé zabezpečení, které je dnes už téměř nepoužitelné, ale bohužel se může najít stále mnoho sítí, kde je WEP použito a tyto sítě jsou snadno napadnutelné. Malé vylepšení bezpečnosti přineslo další zabezpečení. WPA, které dočasně sloužilo, než byl dokončen vývoj WPA2. WPA posloužil jen ale na krátkou dobu, protože i toto zabezpečení bylo překonáno. Po dokončení WPA2 byla síť konečně bezpečně zabezpečena. Do dnešní doby neexistuje žádný spolehlivý útok proveditelný v reálném čase. Podle posledních novinek avšak i toto zabezpečení začíná oslabovat před útočníky.

V druhé části bylo cílem navrhnout zabezpečení bezdrátové sítě tak, aby nebylo možné se připojit bez zadání kombinace uživatelského jména a hesla. Zabezpečení bylo navrženo s ohledem na požadavky. Bylo vybráno zabezpečení PEAP s MS-CHAP v2, které pro připojení vytvoří TLS tunel a uživatele ověří pomocí kombinace uživatelského jména a hesla. Z nabídky RADIUS serverů a klientů RADIUS, které jsou uvedeny v textu, byl vybrán server FreeRADIUS v kombinaci s RouterBoard a RouterOS od firmy MikroTik. FreeRADIUS server poskytuje velké možnosti nastavení a vyniká kvalitní dokumentací. Jako vylepšení správy všech údajů byla použita databáze MySQL. V databázi jsou uložené všechny uživatelské účty, klienti RADIUS serveru.

Server zaznamenává všechny přístupy do sítě, ale také neúspěšné pokusy o přístup a to vše ukládá do databáze. Z databáze je pak možné vyčíst všechny potřebné údaje pro další zpracování statistik a zjištění pokusů o násilné prolomení zabezpečení.

Z vlastností tohoto řešení mohu jmenovat velmi zabezpečené připojení, které je dosaženou použitou kombinací protokolů. Další výhodou je plné logování přístupů, které je užitečné nejen pro statistiky, ale také pro obranu před nebezpečnými uživateli nebo útočníky. V neposlední řadě je výhodná cena celého řešení, finanční nároky jsou zde pouze na pořízení hardwaru pro server a klienta RADIUS serveru, kde

pro server není potřeba výkonný server a řešení od firmy MikroTik se mimo jiné vyznačuje svou dobrou cenou při zachování kvality.

Vhodným vylepšením by byla aplikace, která by spolupracovala s touto databází a ulehčila tak správu. Například aplikace, která by měla formulář pro vytváření nových účtů nebo také prohlížení logování přístupů a filtrování podle různých parametrů. V samotném textu jsou popsány změny v konfiguračních souborech, které jsou přiloženy na CD.

Navržené řešení by mohlo být použito pro poskytovatele internetu nebo veřejné instituce, které potřebují kontrolu svých přihlášených uživatelů.

Literatura

[1] ZANDL, Patrick. *Bezdrátové sítě WiFi : Praktický průvodce*. Brno: Computer Press, 2003. 204 s. ISBN 80-722-6632.

[2] DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP: Bezpečnost*. Brno: Computer Press, 2003. 571 s. ISBN 80-7226-849-X.

[3] CÍR, Lukáš. *Wi-Fi Router, Ověřování protokolem RADIUS a RADIUS Accounting*. Pardubice: Univerzita Pardubice. Fakulta elektrotechniky a informatiky, 2008. 70 s. Bakalářská práce.

[4] *Eduroam.cz* [online]. 2009 [cit. 2010-08-12]. Dostupné z WWW: <www.eduroam.cz>.

[5] MIKOLÁŠEK , Václav. *Katedra informatiky a výpočetní techniky* [online]. 16.01.2005 [cit. 2010-08-12]. Napojení RADIUS serveru na SQL. Dostupné z WWW: <http://www.kiv.zcu.cz/~simekm/vyuka/pd/zapocty-2004/radius_mysql-mikolasek/index.html>.

[6] *FreeRADIUS Wiki* [online]. 2010 [cit. 2010-08-12]. Dostupné z WWW: <http://wiki.freeradius.org>.

[7] *FreeRADIUS - Documentation* [online]. 2010 [cit. 2010-08-12]. Dostupné z WWW: <http://freeradius.org/doc/>.

[8] *MikroTik Wiki* [online]. 2010 [cit. 2010-08-12]. Dostupné z WWW: <http://wiki.mikrotik.com>.

[9] *MikroTik Router and Wireless* [online]. 2000 [cit. 2010-08-12]. Dostupné z WWW: <http://www.mikrotik.com>.

[10] JE, David. *PCTuning* [online]. 12.10.2006 [cit. 2010-08-12]. Základy WiFi: jak zabezpečit bezdrátovou síť?. Dostupné z WWW: <http://pctuning.tyden.cz/component/content/7660/7660?task=view&start=2>.

[11] *Security-Portal.cz* [online]. 17 Březen, 2005 [cit. 2010-08-12]. WiFi sítě a jejich slabiny. Dostupné z WWW: <http://www.security-portal.cz/clanky/wifi-sítě-jejich-slabiny>.

[12] *Frontios.com* [online]. 2005-03-20 [cit. 2010-08-12]. FreeRadius and MySQL HowTo Notes. Dostupné z WWW: <http://www.frontios.com/freeradius.html>.

[13] *ITBiz.cz* [online]. 26. Červenec 2010 [cit. 2010-08-17]. WPA2 spojení bylo poprvé úspěšně napadeno. Dostupné z WWW: <http://www.itbiz.cz/wpa2-spojeni-bylo-uspesne-napadeno>.

[14] *HSC* [online]. 2005 [cit. 2010-08-20]. Bezpečnost Wi-Fi – WEP, WPA a WPA2. Dostupné z WWW: <http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf>.

[15] *Zabezpečení wifi sítí* [online]. 26. 12. 2008 [cit. 2010-08-20]. SOOM.cz. Dostupné z WWW: <http://www.soom.cz/index.php?name=usertexts/show&aid=652>.

[16] *Docupedia* [online]. 2005 [cit. 2010-08-20]. Cracking WEP and WPA Wireless Networks. Dostupné z WWW: <http://docs.alkaloid.net/index.php/Cracking_WEP_and_WPA_Wireless_Networks>.

Příloha A

Pro funkci FreeRADIUS s MySQL je nutné nainstalovat následující balíčky.

Instalace FreeRADIUS

```
sudo apt-get install freeradius
```

Instalace modulu MySQL

```
sudo apt-get install freeradius-mysql
```

Instalace MySQL serveru

```
sudo apt-get install mysql-server
```

Instalace PHPMyAdmina pro správu MySQL databáze, PHPMyAdmin potřebuje pro funkci Apache server s PHP

```
sudo apt-get install phpmyadmin
```

Příloha B

Pro práci FreeRADIUS s databází MySQL, která nahrazuje textové soubory, jsou vzorové tabulky umístěny v souborech *schema.sql* a *nas.sql*. Po importu souborů se nachází v databázi osm tabulek. Sedm tabulek je importováno ze *schema.sql* a tabulka *nas* je imporotvána z *nas.sql.* [3]

- Nas,
- radacct,
- radcheck,
- radgroupcheck,
- radgroupreply,
- radpostauth,
- radreply,
- usergroup.

Tabulky radcheck, radgroupcheck, readreply a radgroupreply mají podobnou strukturu, všechny obsahují pět sloupců.

- id – informativní, je využit pouze k řazení výsledků.
- UserName / GroupName – sloupec obsahuje uživatelské / skupinové jméno.
- Attribute – sloupec pro atributy stejné jako v souboru users.
- op – operátor např.: :=, =.
- Value – hodnota atributu, která je přiřazena operátorem.

Tabulka *nas* obsahuje jednotlivé NAS servery. Aby FreeRADIUS ale využíval tabulku *nas* je nutné aktivovat její funkci. Stačí odkomentovat parametr *readclients = yes* v souboru *sql.conf.* Tabulka *nas* obsahuje osm sloupců.

- id – informativní, je využit pouze k řazení záznamů.
- nasname – sloupec obsahuje IP adresy serveru NAS.
- Shortname – sloupec uchovává informace názvu serveru NAS.
- type – type říká serveru RADIUS, že klient může obsahovat specifické atributy, které jsou právě závislé na typu NAS.
- ports – sloupec udává počet dostupných portů NAS. Toto pole je informativní a slouží například programu dialupadmin, grafickému rozhraní pro správu databáze. Port jinak posílá sám NAS v rámci paketu Acces-Request. Pro využití čísla portu zaslané pomocí paketu Acces-Request, lze pole nastavit na hodnotu NULL.
- secret – sloupec uschovává heslo, které využívá server RADIUS a klient.
- community – sloupec udává název komunity SNMP; v případě, že SNMP není použito, je pole nastaveno na NULL.
- description – informativní, obsahuje popis záznamu.

Poslední tabulkou, které je důležitá při provozu, je *usergroup*. V této tabulce se přiřazují uživatelé ke skupinám. Obsahuje pouze tři sloupce.

- UserName – sloupec určuje uživatelské jméno.
- GroupName – název skupiny do které je přiřazen uživatel.
- Priority – nastavuje prioritu skupin uživatele; to se uplatní v situaci, kdy je uživatel ve více skupinách a díky prioritě skupin se zjistí, podle které se má server řídit.

Další tabulkou je tabulka *radpostauth*, tato tabulka má pouze informativní účel. FreeRADIUS sem zapisuje informace o autorizaci. Tabulka obsahuje pět sloupců.

- id – informativní, je využit pouze k řazení záznamů.
- user – sloupec obsahuje uživatelské jméno.
- pass – sloupec informuje o typu přihlášení.

- reply – sloupec obsahuje záznam o typu paketu přihlášení, např. Access-Accept.

- date – datum a hodina přihlášení.

Poslední tabulka v databázi je *radacct*, tabulka je určená pro RADIUS Accounting. Tabulka je pouze informativní vyplňovanou serverem RADIUS Accounting. Tabulka *radacct* obsahuje 25 sloupců.

- RadAcctId – udává identifikační číslo položky v tabulce.

- AcctSessionId – zde se zapisuji identifikační čísla sezení, přijaté od požadavku Accounting-Request.

- AcctUniqueId – obsahuje unikátní identifikační číslo.

- UserName – obsahuje uživatelské jméno klienta.

- Realm – Realm doména klienta.

- NASIPAddress – adresa IP serveru NAS, z něhož přišel požadavek.

- NASPortId – identifikace portu NAS.

- NASPortType – typ portu NAS. Např. Wireless-802.11.

- AcctStartTime – čas příchodu požadavku Start.

- AcctStopTime – čas příchodu požadavku Stop.

- AcctSessionTime – doba trvání sezení.

- AcctAuthentic – zaznamenání výběru autorizace RADIUS nebo Local authority.

- ConnectInfo_start – u této položky není zatím definované využití.

- ConnectInfo_stop – u této položky není zatím definované využití.

- AcctInputOctets – počet příchozích oktetů.

- AcctOutputOctets – počet odchozích oktetů.
- CalledStationId – identifikace služby odesílající požadavek.
- CallingStationId – v tomto poli se nachází identifikace klienta.
- AcctTerminateCause – obsahuje důvod ukončení sezení.
- ServiceType – u routeru MikroTik se používá jedině „Framed“.
- FramedProtocol – protokol linkové vrstvy. U routeru MikroTik se používá jedině „PPP“.
- FramedIPAddress – přidělená adresa IP klientovi.
- AcctStartDelay – doba po jakou se klient snažil odeslat požadavek Accounting-Request typu Start.
- AcctStopDelay – doba po jakou se klient snažil odeslat požadavek Accounting-Request typu Stop.
- XAscendSessionSvrKey – u této položky není zatím definované využití.

Příloha C

Hlavním souborem pro práci s databází je *sql.conf*. V tomto souboru je umístěna konfigurace samotného SQL. Nejprve se nastaví druh použité databáze a dále to jsou přístupové údaje k databázovému serveru, jako je adresa serveru, přihlašovací jméno, heslo a databáze. Soubor obsahuje i další nastavení jako je nastavení názvů tabulek nebo podrobnější nastavení databáze, ale pro správnou funkci stačí nastavit typ a přístupové údaje. [5]

Standardní nastavení

```
driver = "rlm_sql_mysql"
server = "localhost"
login = "radius"
password = "radpass"
radius_db = "radius"
```

Dalším krokem je nastavení FreeRADIUSu tak, aby využíval MySQL. To se lehce změní v konfiguračním souboru. Dříve toto nastavení bylo v hlavním konfiguračním souboru *radiusd.conf* (o přesunutí je v souboru napsaná poznámka na konci), ale nyní je přesunuto do souboru */sites-avalible/default.* V tomto souboru stačí odkomentovat sql a zakomentovat files v blocích *authorize, preacct a accounting.* Zakomentováním files docílíme toho, že server nebude hledat soubor users s uživateli.

```
authorize {
# files
sql
}

preacct {
# files
}

accounting {
sql
}
```

Po těchto jednoduchých krocích je vše nastaveno pro použití s MySQL.