VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

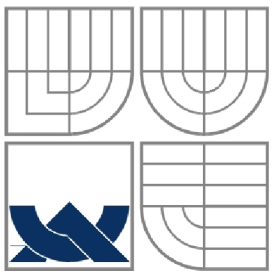
METÓDY AUTENTIZÁCIE NAPOJENIA K WIFI SIETI

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

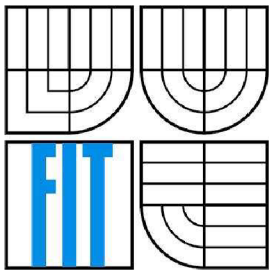
AUTOR PRÁCE
AUTHOR

Bc. FILIP VALAŠEK

BRNO 2007



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

METÓDY AUTENTIZÁCIE NAPOJENIA K WIFI SIETI

METHODS OF AUTHENTICATION TO WIFI NETWORK

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. FILIP VALAŠEK
AUTHOR

VEDOUCÍ PRÁCE — Ing. PETR LAMPA
SUPERVISOR

BRNO 2007

Metody autentizace napojení k WiFi síti

Methods of Authentication to WiFi Network

Vedoucí:

Lampa Petr, Ing., CVT FIT VUT

Oponent:

Kašpárek Tomáš, Ing., CVT FIT VUT

Přihlášen:

Valašek Filip, Bc.

Zadání:

1. Prostudujte způsoby autentizace klientů na úrovni L2 k počítačové síti typu WiFi dle standardu IEEE 802.1x.
2. Seznamte se s dostupnými implementacemi Radius serveru a způsoby jejich konfigurace.
3. Otestujte funkčnost a spolehlivost implementací autentizace klientů v různých operačních systémech (WinXP, Linux, BSD) ve spojení se zvolenými servery Radius a WiFi AP HP, Asus, Avaya a Cisco.
4. Otestujte vliv použitého šifrování a rotace klíčů na přenosovou rychlost.
5. Zvolte vhodnou kombinaci autentizace a serveru, vypracujte nástroje pro konfiguraci a správu včetně uživatelské dokumentace.
6. Zhodnoťte použitelnost tohoto způsobu autentizace s dalšími možnostmi.

Část požadovaná pro obhajobu SP:

První 3 body zadání.

Kategorie:

Počítačové sítě

Literatura:

1. http://www.open1x.org/
2. http://www.freeradius.org/
3. http://www.ieee802.org/1/pages/802.1X-rev.html

Licenčná zmluva

Licenčná zmluva je uložená v archíve Fakulty informačních technologií Vysokého učení technického v Brně.

Abstrakt

Diplomová práca sa zaoberá autentizáciou pomocou protokolu RADIUS a autentizačnými metódami podľa štandardu IEEE 802.1X. Na začiatku sa nachádza stručná charakteristika vybraných autentizačných metód, najmä PAP, CHAP a niektorých EAP typov. Obsahuje tiež prehľad implementácií protokolu RADIUS, bližšie sa venuje serveru FreeRADIUS. Cieľom je implementovať nástroj na správu servera FreeRADIUS.

Kľúčové slová

Autentizácia, autorizácia, WiFi, FreeRADIUS, AAA protokol, RADIUS, EAP

Abstract

This diploma thesis deals with authentication using RADIUS protocol and authentication methods in accordance with standard IEEE 802.1X. At the beginning there are shortly characteristics of chosen authentication methods, such as CHAP, PAP and some EAP types. Document includes summary of RADIUS protocols implementations, especially the FreeRADIUS server. Our goal is to implement a management tool to adminitrate FreeRADIUS server.

Keywords

Authentication, authorization, WiFi, FreeRADIUS, AAA protocol, RADIUS, EAP

Citácia

VALAŠEK, Filip. Metódy autentizácie napojenia k WiFi sieťam. [s.l.], 2007. 50 s. FIT VUT v Brně. Vedúci diplomovej práce Petr Lampa.

Metódy autentizácie napojenia k WiFi sieti

Prehlásenie

Prehlasujem, že som túto diplomovú prácu vypracoval samostatne pod vedením Ing. Petra Lampu. Uviedol som všetky literárne pramene a publikácie, z ktorých som čerpal.

.....
Filip Valašek
22. 5. 2007

Poďakovanie

Touto cestou by som sa chcel poďakovať vedúcemu práce Ing. Petrovi Lampovi za ochotu pri riešení tejto práce. Tiež mojim blízkym a známym, ktorí mi pomohli udržať si optimizmus a dobrú náladu pri práci.

Obsah

Obsah 1
1 Úvod 3
2 Spôsoby autentizácie 4
2.1 Tri používané spôsoby autentizácie 4
2.2 Autentizácia podľa štandardu IEEE 802.1X 4
2.2.1 Základné pojmy 4
2.2.2 Princíp IEEE 802.1X 5
2.3 Autentizačné metódy 6
2.3.1 PAP 7
2.3.2 CHAP 7
2.3.3 EAP 7
2.3.4 EAP-TLS 9
2.3.5 EAP-TTLS 9
2.3.6 PEAPv0/EAP-MSCHAPv2 10
2.3.7 PEAPv1/EAP-GTC 10
2.3.8 EAP-SIM 10
2.3.9 EAP-LEAP 10
2.3.10 Sumarizácia vlastností autentizačných metód 10
3 Dostupné implementácie protokolu RADIUS 11
3.1 Prehľad implementácií 11
3.2 Testované implementácie 11
3.2.1 OpenRADIUS 11
3.2.2 FreeRADIUS 12
3.2.3 JRadius 12
3.2.4 Cistron RADIUS 12
3.2.5 GNU Radius 13
3.3 Zhodnotenie 13
4 Testovanie funkčnosti a spoľahlivosti 14
4.1 Autentizačný server – FreeRADIUS 14
4.2 Autentizátor – prístupové body (AP) 14
4.3 Suplikant 14
5 Vplyv šifrovania a rotácie kľúčov na prenosovú rýchlosť 16
5.1 Základné pojmy 16
5.2 Bezpečnosť podľa 802.11i 16

5.2.1 Pre-RSN bezpečnosť 17
5.2.2 RSN bezpečnosť 18
5.3 Testovanie 20
6 Konfiguračné nástroje 21
6.1 Požiadavky na konfiguráciu 21
6.1.1 Konfiguračné súbory 21
6.1.2 FreeRADIUS a MySQL 21
6.2 Požiadavky na aplikáciu 23
6.3 Architektúra 23
6.4 Rozhranie klient–server 24
6.5 Používateľské rozhranie 25
6.6 Podrobnejší popis implementácie 26
6.6.1 Databázová vrstva 26
6.6.2 Prezentačná vrstva 26
7 Zhodnotenie použiteľnosti 27
7.1 Iné možnosti autentizácie 27
7.1.1 DIAMETER 27
7.1.2 TACACS 27
7.1.3 TACACS+ 28
8 Záver 29
Literatúra 30
Zoznam príloh 32

1 Úvod

Bezdrôtové komunikácie je rýchlo sa rozvíjajúci odbor. Umožňujú ľuďom komunikovať bez potreby spájania komunikačných zariadení prostredníctvom vodičov – prenosovým médiom je vzduch. Takéto „spojenie“ zariadení je veľmi pohodlné a poskytuje používateľom možnosť istej mobility.

Exitujú viaceré technológie umožňujúce bezdrôtovú komunikáciu (GSM, GPRS, WiMAX,…), no my sa zameriame na WiFi. WiFi štandard (IEEE 802.11) je najrozšírenejší pri budovaní bezdrôtových sietí WLAN (Wireless LAN).

Ako to však býva, žiadna služba nie je zadarmo a skrýva v sebe aj isté riziká, či dodatočné náklady na prevádzku. V prípade WLAN je dosť podstatným problémom *bezpečnosť*. Z tohto hľadiska nás bude zaujímať najmä *autentizácia* a *autorizácia*.

Autentizácia znamená potvrdenie, že používateľ požadujúci služby je platným používateľom poskytovaných sieťových služieb. Autentizácia je dosiahnutá pomocou predstavenia identity a istého poverenia alebo tajomstva. Medzi rôzne typy tajomstva patria napríklad heslá, poverenia na jedno použitie, digitálne certifikáty alebo telefónne čísla (či už volajúce alebo volané). [4]

Autorizácia znamená udelenie špecifického typu služby (vrátane „žiadna služba“) používateľovi na základe jeho autentizácie, služieb, ktoré požaduje a aktuálneho stavu systému. Autorizácia môže byť založená na obmedzeniach, napríklad obmedzenie na určité hodiny v rámci dňa, alebo obmedzenie na fyzickú polohu, alebo obmedzenie viacnásobného prihlásenia jedného používateľa. Autorizácia určuje povahu služby, ktorá je poskytnutá používateľovi. Tieto služby sú napríklad: filtrovanie IP adries, pridelenie adresy, pridelenie cesty, QoS, riadenie šírky pásma, tunelovanie do konkrétneho koncového bodu, alebo šifrovanie. [4]

Pre poskytovateľa služieb býva často dôležitá možnosť sledovať využívanie sieťových služieb používateľmi – **účtovanie**. Tieto informácie môžu byť použité pre správu, plánovanie alebo ďalšie účely. [4]

Na autentizáciu, autorizáciu a účtovanie sa využíva **AAA protokol** (authentication, authorization, accounting protocol). Medzi AAA protokoly patria napríklad RADIUS, DIAMETER, TACACS, TACACS+ apod. V tejto práci sa budeme zaoberať protokolom RADIUS a jeho voľne šíriteľnými implementáciami.

V druhej kapitole uvedieme prehľad spôsobov autentizácie na úrovni L2 podľa štandardu IEEE 802.1X. V tretej sa zasa zameriame na rôzne „Open Source“ implementácie protokolu RADIUS. Vo štvrtej kapitole predstavíme výsledky testov funkčnosti a spoľahlivosti implementácií autentizácie klientov v rôznych operačných systémoch (WinXP, Linux, BSD) v spojení so zvolenými servermi RADIUS a WiFi AP HP, Asus a D-Link.

2 Spôsoby autentizácie

Stručne sme sa o autentizácii zmienili v úvodnej kapitole. Autentizačné faktory pre ľudí sú všeobecne rozdelené do troch kategórií. Používateľ niečo:

- JE – odtlačok prstov, DNA,
- MÁ – mobilný telefón, kreditná karta, hardvérový token alebo
- VIE – PIN, heslo.

Málokedy sa však používa trojfaktorová autentizácia. Väčšinou je to iba dvojfaktorová, ktorá sa tiež nazýva **silná autentizácia**. Najjasnejším príkladom je banková karta. Jej vlastník niečo má (samotná karta) a niečo vie (PIN kód).

2.1 Tri používané spôsoby autentizácie

Pri autentizácii k počítačovým sieťam sa používajú najmä nasledujúce tri spôsoby.

Autentizácia pomocou webového formulára – Po pripojení je potrebné spustiť webový prehliadač, vyplniť prístupové meno a heslo a až potom je používateľovi umožnený prístup k službám podľa výsledku autorizácie. Autentizáciu a autorizáciu vykonáva AAI (authentication and authorization infrastructure).

Autentizácia pomocou VPN spojenia – Po celý čas komunikácie je umožnený prístup iba k určeným VPN serverom. Po zadaní prihlasovacích údajov k VPN sieti je umožnený prístup ku všetkým službám danej siete. V tomto prístupe nevystupuje AAI a autentizácia a autorizácia prebiehajú výhradne na VPN serveri.

Autentizácia pomocou 802.1X – Tomuto spôsobu autentizácie sa hovorí aj riadenie prístupu k sieti pomocou portov. Vyžaduje si prístupové zariadenia, ktoré dokážu v spolupráci s autentizačným serverom umožniť klientskemu zariadeniu sprístupniť služby siete. Podrobnejšie sa autentizácii podľa 802.1X budeme venovať v ďalšom texte.

2.2 Autentizácia podľa štandardu IEEE 802.1X

2.2.1 Základné pojmy

Na potreby problematiky autentizácie podľa štandardu IEEE 802.1X boli zavedené nasledujúce pojmy [3]:

Autentizátor – Entita na jednom konci LAN segmentu bod-bod, ktorá zabezpečuje autentizáciu entity na druhom konci tejto linky.

Autentizačný server – Entita, ktorá poskytuje autentizačnú službu autentizátoru. Táto služba určuje, z údajov poskytnutých suplikantom, či suplikant je autorizovaný na prístup k službám poskytovaným autentizátorom. Funkcia autentizačného servera môže byť spojená s autentizátorom, alebo môže byť prístupná vzdialene cez sieť, ku ktorej má autentizátor prístup.

Prístupový port siete – Bod pripojenia systému k LAN. Môže to byť fyzický port, napríklad jeden LAN MAC priradený k fyzickému segmentu LAN, alebo logický port, napríklad IEEE 802.11 asociácia medzi stanicou a prístupovým bodom (AP). Pojem port je používaný ako skratka pre prístupový port siete.

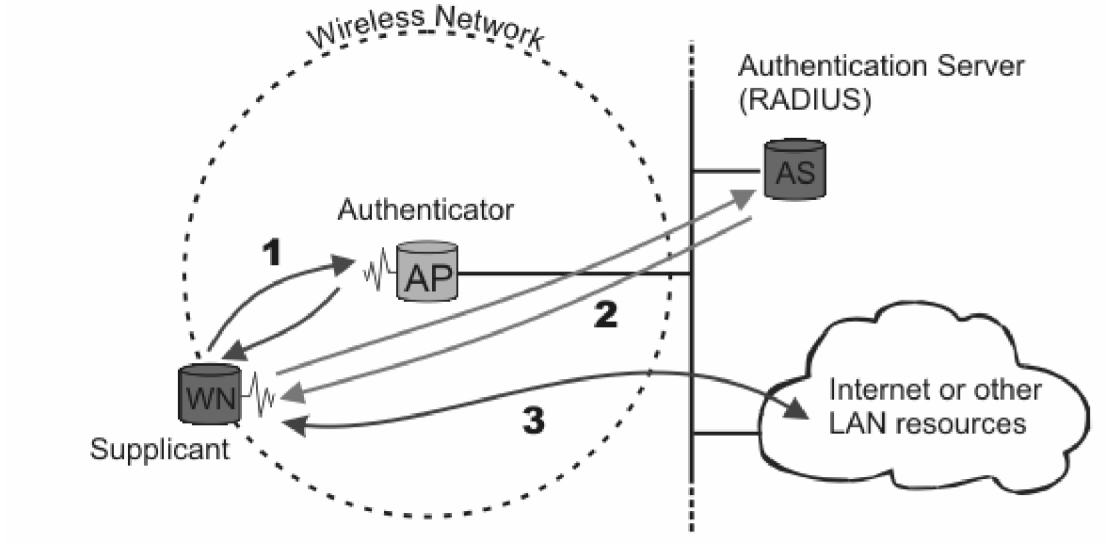
Port access entity (PAE) – Protokolová entita asociovaná s portom. Môže podporovať protokolovú funkcionalitu spojenú s autentizátorom, suplikantom, alebo s oboma.

Suplikant – Entita na jednom konci LAN segmentu bod-bod, ktorá je autentizovaná autentizátorom pripojeným k druhému koncu linky. Termín suplikant je používaný v štandarde 802.1X namiesto častejšieho termínu **peer**, používaného v ostatných špecifikáciách riadenia prístupu.

Systém – Zariadenie pripojené k LAN pomocou jedného alebo viacerých portov. Príklady systémov sú koncové stanice, servery, MAC mosty, routre atď.

2.2.2 Princíp IEEE 802.1X

Všeobecná schéma vysvetľujúca princíp autentizácie podľa štandardu 802.1X je zobrazená na Obr. 1.



Obr. 1 Princíp autentizácie podľa štandardu 802.1X [2]

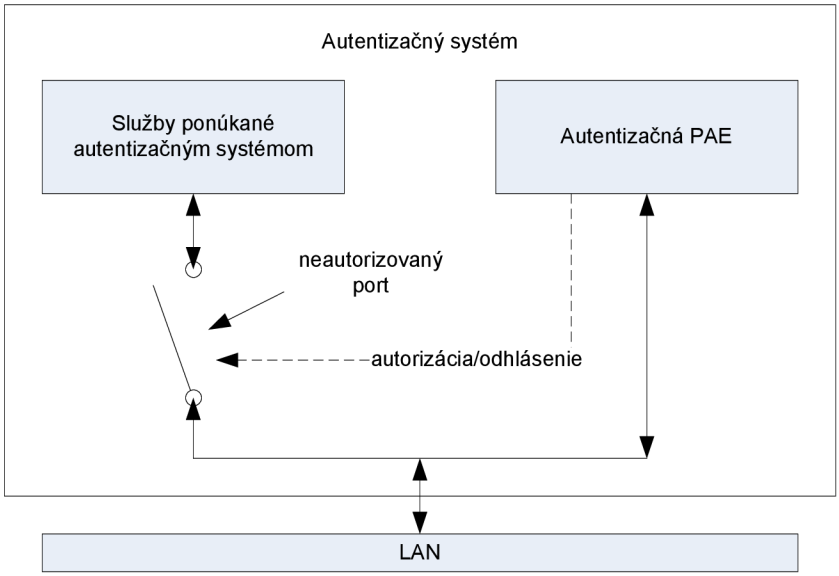
Je zrejmé že na autentizovanie je potrebné zariadenie nazývané autentizátor, ktoré má schopnosť blokovať porty. Inak by bolo možné sa pripojiť úplne voľne a autentizácia by tak strácala svoj zmysel.

Autentizácia prebieha takto (podľa Obr. 1):

1. Keď bezdrôtový uzol (WN) požiada o prístup k LAN zdrojom, prístupový bod (AP) sa spýta na identitu WN. Žiadna iná komunikácia ako autentizácia nie je dovolená pokiaľ WN nie je autentizovaný.

   WN, ktorý žiada o autentizáciu obsahuje suplikant. Suplikant je zodpovedný za posielanie žiadosti autentizátoru. Takisto prístupový bod obsahuje autentizátor, ktorý môže byť aj mimo neho ako externý komponent.
2. Ako náhle bola zaslaná identita, autentizačný proces začína. Autentizátor počas celého autentizačného procesu iba preposiela autentizačné pakety medzi autentizačným serverom a suplikantom. Keď tento proces skončí, autentizačný server pošle potvrdzovaciu správu (alebo chybovú správu pri neúspechu). Pri kladnej odpovedi autentizátor otvorí pre suplikant port.
3. Zároveň je suplikant oprávnený pristupovať k požadovaným službám.

Princíp otvárania portov je možné pochopiť aj na Obr. 2. Autentizátor musí mať neustále voľne prístupnú entitu na autentizáciu (PAE), ale služby, o ktoré suplikant žiada, tie musia byť neprístupné. Sprístupnia sa až po ukončení autorizácie, prípadne príslušný port ostane zatvorený, ak autorizácia skončila neúspechom.



Obr. 2 Otváranie portov

2.3 Autentizačné metódy

Existuje veľké množstvo autentizačných metód. Niektoré sú menej bezpečné, niektoré viacej. Pri bezdrôtovom prenose je ich bezpečnosť omnoho dôležitejšia ako pri káblových rozvodoch. Fyzické oddelenie prenosového média od okolitého prostredia znemožňuje v bežných podmienkach možnosť odpočúvania.

WiFi je však známe svojím veľmi slabým zabezpečením prenosu. Tak je veľmi jednoduché odchytávať komunikáciu priamo „zo vzduchu“. Aj keď zabezpečenie prenosu nie je to isté ako autentizácia, spolu veľmi úzko súvisia. Nie je možné totiž autentizovať bez prenosu citlivých informácií, ktoré by prípadný útočník mohol zneužiť pri predstieraní identity niekoho iného. Preto je dôležité dbať aj na vybratý spôsob autentizácie v spojení s vhodným zašifrovaním komunikácie.

2.3.1 PAP

Spolu s metódou CHAP patria medzi najjednoduchšie a zároveň aj najmenej bezpečné. Na použitie v bezdrôtových sieťach sú takmer nepoužiteľné bez pridania inej bezpečnejšej metódy (napríklad EAP-TTLS).

Password Authentication Protocol, skrátene PAP, je jednoduchý autentizačný protokol používaný na na autentizáciu používateľa voči vzdialenému serveru. PAP býva vnorený v PPP protokole (Point-to-Point). Takmer všetky sieťové operačné systémy podporujú PAP.

Metóda PAP prenáša cez sieť heslo v jeho čistej nezmenenej podobe a preto je považovaná za nebezpečnú. Je používaná ako posledná možnosť, keď vzdialený server nepodporuje iný silnejší autentizačný protokol.

2.3.2 CHAP

Challenge-Handshake Authentication Protocol (CHAP) je používaný na periodickú verifikáciu identity používateľa použitím 3-cestného handshaku. Toto je vykonané po zostavení spojenia a môže byť opakované kedykoľvek, keď je už spojenie zostavené.

1. Po zostavení spojenia autentizátor pošle správu *challenge* používateľovi.
2. Peer odpovie hodnotou vypočítanou pomocou hash funkcie, napríklad MD5.
3. Autentizátor skontroluje odpoveď podľa jeho vlastného výpočtu. Ak sú hodnoty rovnaké, autentizácia skončí úspechom, inak je spojenie ukončené.
4. V náhodných intervaloch posiela autentizátor nové *challenge* správy a opakuje sa vykonanie úloh podľa bodov 1 až 3.

2.3.3 EAP

Extensible Authentication Protocol [10], alebo EAP, je univerzálny autentizačný rámec, nie je špecifickým autentizačným mechanizmom, často používaný v bezdrôtových sieťach, ale je často používaný aj v drôtových sieťach. Podporuje množstvo autentizačných metód. Typicky beží priamo na linkovej vrstve ako PPP protokol alebo IEEE 802, bez potreby IP adresovania. Fragmentácia nie je podporovaná, ale jednotlivé EAP metódy môžu mať jej podporu.

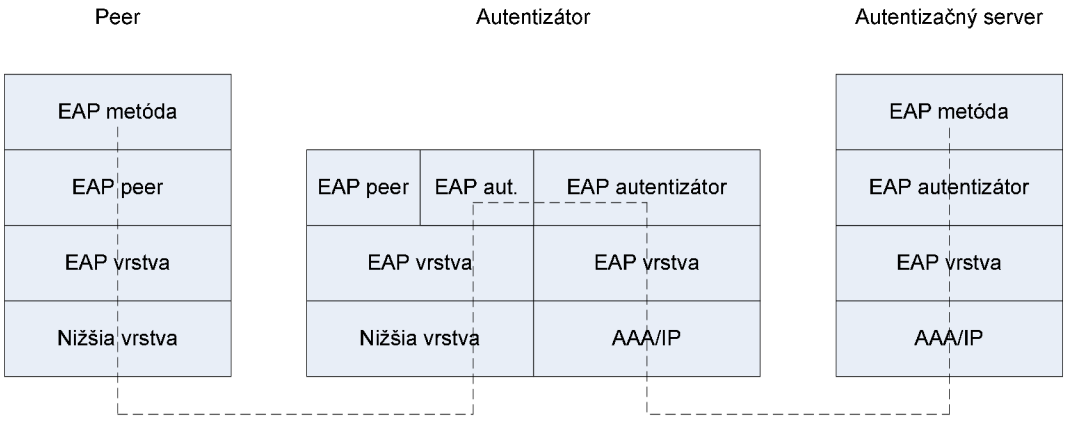
Štandardu EAP sa venujeme preto, lebo určuje všeobecný spôsob komunikácie medzi suplikantom, autentizátorom a autentizačným serverom.

Nedávno WPA a WPA2 štandardy oficiálne prijali tieto EAP typy ako ich oficiálne autentizačné mechanizmy:

- EAP-TLS – podporovaný od začiatku,
- EAP-TTLS/MSCHAPv2,
- PEAPv0/EAP-MSCHAPv2,
- PEAPv1/EAP-GTC,
- EAP-SIM,
- EAP-LEAP.

Autentizačných mechanizmov existuje viacej (približne 40), ale predchádzajúcich 6 je najvýznamnejších.

Pri EAP hrá autentizátor úlohu sprostredkovateľa komunikácie medzi suplikantom a autentizačným serverom (Obr. 3). Výhodou je, že autentizátor nemusí poznať jednotlivé autentizačné EAP metódy, ale jednoducho iba preposiela pakety ďalej.



Obr. 3 Preposielanie EAP cez Pass-through autentizátor

Podľa [3] na komunikáciu medzi suplikantom a autentizátorom služi vnáranie. Toto vnáranie je známe ako EAP over LAN, alebo EAPOL. V tomto čase EAPOL je popísané pre 802.3/Ethernet MAC a Token Ring/FDDI MAC. EAPOL používané s 802.3/Ethernet MAC môže byť aplikované na ostatné LAN technológie, ktoré zdieľajú rovnaký základný formát rámca ako Ethernet. V predchádzajúcom obrázku nižšia vrstva znamená práve EAPOL rámec, ktorého presnejšia špecifikiácia je vidieť na Obr. 4.

	Číslo oktetu
PAE Ethernet Type	1-2
Protocol Version	3
Packet Type	4
Packet Body Length	5-6
Packet Body	7-N

Obr. 4 EAPOL formát rámca pre 802.3/Ethernet

PAE Ethernet Type je pole s dĺžkou 2 oktety, obsahuje hodnotu 88-8E. **Protocol Version** určuje zasa verziu EAPOL protokolu podporovanú odosielateľom EAPOL rámca. **Packet Type** hodnota znamená typ paketu (EAP-Packet, EAPOL-Start, EAPOL-Logoff, EAPOL-Key alebo EAPOL-Encapsulated-ASF-Alert), ktorý sa bude prenášať. **Packet Body Length** definuje dĺžku **Packet Body**, v ktorom sa nachádza taký paket, ako je definovaný v poli Packet Type.

V prípade, ak sa jedná o EAP-Packet, pole Packet Body obsahuje EAP paket so štruktúrou podľa Obr. 5.

	Číslo oktetu
Code	1
Identifier	2
Length	3-4
Data	5-N

Obr. 5 EAP paket formát

Code určuje typ EAP paketu. Kódy sú priradené nasledovne: 1 – Request, 2 – Response, 3 – Success, 4 – Failure. **Identifier** identifikuje paket a umožňuje spárovanie žiadosti a odpovede. **Length** je dĺžka paketu, do ktorej sa započítava dĺžka polí Code, Identifier, Length a Data. **Data** obsahuje nakoniec dáta podľa typu paketu.

Vnorenie EAP do IEEE 802 podľa IEEE 802.1X neobsahuje PPP a tiež podporu pre linkovú a sieťovú negociáciu. Výsledkom je, že nie je možné prenášať iné ako EAP autentizačné mechanizmy, napríklad PAP alebo CHAP, čo však nie je problém vzhľadom na ich slabú autentizačnú bezpečnosť.

2.3.4 EAP-TLS

EAP-TLS je definovaný v [11] a je dobre podporovaný u výrobcov bezdrôtových zariadení. Ponúka vynikajúcu bezpečnosť. Používa PKI na bezpečnú komunikáciu s RADIUS serverom. Aj napriek dobrej bezpečnosti jeho nevýhodou je správa klientskych certifikátov, kedy pre každého používateľa musí byť jeden vydaný, čím vznikajú vyššie náklady pre prevádzkovateľa systému.

2.3.5 EAP-TTLS

EAP Tunneled TLS Authentication Protocol Version 1 [13] je EAP typ, ktorý používa TLS na vytvorenie bezpečného spojenia medzi klientom a serverom, cez ktoré môžu byť vymieňané ďalšie údaje. Začiatočný TLS handshake vzájomne autentizuje klienta a server, alebo môže vykonať jednosmernú autentizáciu, počas ktorej je autentizovaný iba server. Bezpečné spojenie je potom používané na autentizáciu klienta použitím zložitejších autentizačných infraštruktúr, napríklad RADIUS. Autentizácia klienta môže prebiehať samotným EAP, alebo to môže byť iný autentizačný protokol ako PAP, CHAP, MS-CHAP alebo MS-CHAP-V2.

2.3.6 PEAPv0/EAP-MSCHAPv2

PEAPv0/EAP-MSCHAPv2 [14] je technický termín pre častejšie používanú skratku PEAP. Po EAP-TLS, PEAPv0/EAP-MSCHAPv2 je druhý najčastejšie podporovaný EAP štandard. Je podobný s EAP-TTLS, pretože potrebuje iba certifikát servera na vytvorenie bezpečného tunela na ochranu autentizácie používateľa.

2.3.7 PEAPv1/EAP-GTC

PEAPv1/EAP-GTC bol vytvorený firmou Cisco ako alternatíva k PEAPv0/EAP-MSCHAPv2. EAP-GTC nechráni autentizačné dáta v žiadnom smere.

Aj keď sa Microsoft podieľal na vývoji PEAP, nikdy nepridal podporu pre PEAPv1 do systému Windows. Bez záujmu Microsoftu o podporu PEAPv1 a malý záujem Cisco o jeho propagáciu, PEAPv1 autentizácia je veľmi zriedka používaná.

2.3.8 EAP-SIM

EAP-SIM je používaný pre autentizáciu a distribúciu session kľúča s použitím GSM SIM.

2.3.9 EAP-LEAP

Lightweight Extensible Authentication Protocol je proprietárna EAP metóda vyvinutá firmou Cisco. Cisco vyvinulo veľké úsilie na presadenie LEAP metódy, ale vzhľadom na neexistujúcu podporu zo strany Microsoftu sa im to nepodarilo. Je považovaná za menej bezpečnú a náchylnú na dictionary attack. Cisco však argumentuje tým, že je potrebné voliť dostatočne silné heslá, toto je však v bežnom živote nemysliteľne a nedosiahnuteľné.

Podpora tejto technológie je veľmi slabá a je preto málo rozšírená v porovnaní s EAP-TTLS/MSCHAPv2 alebo PEAPv0/EAP-MSCHAPv2.

2.3.10 Sumarizácia vlastností autentizačných metód

Z hľadiska bezpečnosti je na tom najlepšie EAP-TLS a je tiež podporovaná takmer každým výrobcom zariadení. Skrýva však náklady na prevádzku certifikačnej autority. Menej bezpečná ale zato flexibilnejšia je EAP-TTLS/MSCHAPv2 (prípadne PEAPv0/EAP-MSCHAPv2). Strata na bezpečnosti je však malá v porovnaní s potrebou vydávať pre každého používateľa certifikát.

3 Dostupné implementácie protokolu RADIUS

3.1 Prehľad implementácií

V Tab. 1 je stručný prehľad softvérových implementácií RADIUS servera. Sú tam uvedené aj *open source* (OS) aplikácie, ale aj *komerčné* (kom.). Podporu pre RADIUS majú aj niektoré hardvérové zariadenia, ale jedná sa väčšinou o produkty, ktorých cena je neporovnateľne vyššia oproti ich SW konkurentom.

Radius server	Typ
FreeRADIUS GNU Radius JRadius OpenRADIUS Cistron RADIUS	OS
Microsoft IAS Radiator Elektron Aradial RADIUS Steel-Belted Radius	kom.

Tab. 1 Prehľad implementácií RADIUS serverov

3.2 Testované implementácie

Funkčnosť sme testovali najmä pri open source projektoch RADIUS serverov. Cieľom bolo preskúmať dostupné autentizačné metódy a zistiť spôsoby konfigurácie. V budúcnosti bude potrebné vytvoriť k serveru aj konfiguračné prostriedky, takže je výhodná taká implementácia, ktorá dokáže spolupracovať s niektorou voľne dostupnou databázou (napr. MySQL).

3.2.1 OpenRADIUS

OpenRADIUS je RADIUS server, ktorý dovoľuje používanie externých súborov pre všetko – zdieľané tajomstvo, kontá a heslá, profily, databázu sedení, NAS list atď. Jeho správanie je plne konfigurovateľné. Používa vlastný jednoduchý jazyk, ktorý umožňuje získať plnú kontrolu nad požiadavkami a odpoveďami. Obsahuje aj LDAP a SQL moduly.

Výhodou je možnosť veľmi podrobnej konfigurácie, čo je aj zároveň nevýhoda, pretože mne osobne sa zdala konfigurácia zložitá. Navyše nie je dostatok dostupných webových zdrojov o nastavovaní.

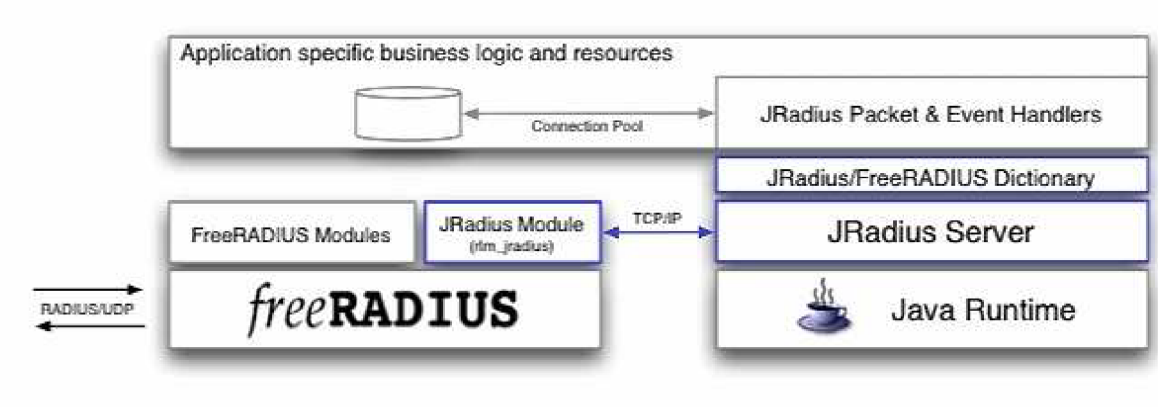
3.2.2 FreeRADIUS

Je asi najrozšírenejším voľne šíriteľným RADIUS serverom. Jeho konfigurácia sa uskutočňuje pomocou konfiguračných súborov, ktoré zároveň obsahujú dôkladnú dokumentáciu jednotlivých atribútov. Pri začiatkoch vychádzal čiastočne z iného servera – Cistron RADIUS.

Má implementované množstvo autentizačných metód (EAP-TLS, PEAPv0/EAP-MSCHAPv2,…). Obsahuje tiež SQL modul, pomocou ktorého je možné konfiguráciu oddeliť od servera a umiestniť ju v databáze. Sú dostupné moduly pre spoluprácu s databázami DB2, Firebird, Oracle, PostgreSQL a samozrejme aj MySQL.

3.2.3 JRadius

JRadius je zaujímavým riešením. Na Obr. 6 je vidieť, ako funguje. Využíva na svoju činnosť FreeRADIUS server. Ten má viacej modulov a jedným z nich môže byť aj JRadius modul (rlm_jradius).



Obr. 6 Architektúra JRadius [5]

Vzhľadom na to, že tento produkt nemožno používať ako samostatný, nie je použiteľný pre naše potreby a teda sa ním nebudeme ďalej zaoberať. Jeho miesto je skôr pri zložitejších autentizačných úlohách, v ktorých je potrebná integrácia s inými autentizačnými systémami a protokolmi.

3.2.4 Cistron RADIUS

Na stránke [7] tohto projektu nás autor informuje, že na dosiahnutie lepších výsledkov a pre svetlú budúcnosť jeho serveru, je potrebné úsilie viacerých ľudí a tak spojil svoje sily s autorom FreeRADIUS a spojili svoje implementačné úsilie. Výsledným produktom je teda FreeRADIUS a tiež je nasledovníkom Cistron RADIUS servera.

Z Cistron RADIUS bolo neskôr odvodených viacej implementácií, ale ich použiteľnosť nie je príliš dobrá. Cistron RADIUS sa už ďalej nevyvíja, ale existujú neoficiálne doplnky.

3.2.5 GNU Radius

Momentálne nepredstavuje príliš zaujímavú implementáciu, pretože tak ako väčšina open source RADIUS serverov, nepodporuje také množstvo autentizácií, ako FreeRADIUS. Avšak do budúcnosti je plánovaná implementácia EAP-TLS a EAP-MSCHAPv2.

3.3 Zhodnotenie

Všetky servery boli skúšané na distribúcii systému Ubuntu 6.06 Dapper Drake, ich inštalácia by však nemala byť problémom ani na inom operačnom systéme.

Na zhodnotenie kvalít jednotlivých implementácií nám poslúži Tab. 2. V prvej polovici sa nachádzajú dostupné autentizačné metódy a v druhej možnosti konfigurácie.

Radius server	FreeRADIUS	GNU Radius	OpenRADIUS	Cistron RADIUS
EAP-SIM	●	○	○	○
EAP-TLS	●	○	○	○
EAP-TTLS	●	○	○	○
EAP-MD5	●	○	○	○
CHAP	●	●	●	○
PAP	●	●	●	○
Cisco-LEAP	●	○	○	○
EAP-MSCHAPv2	●	○	○	○
Meno a heslo	●	●	●	●
SQL modul	●	●	●	○
Súbory	●	●	●	●

Tab. 2 Prehľad autentizačných schopností RADIUS serverov

Rozhodujúcimi kritériami pre výber vhodnej implementácie boli:

1. implementované autentizačné mechanizmy,
2. rozsah spôsobov konfigurácie, najmä možnosť konfigurácie prostredníctvom databázy.

Prvé kritérium najlepšie splnil FreeRADIUS a pri druhom obstáli všetky okrem Cistron RADIUS.

Zo všetkých testovaných serverov je práve FreeRADIUS tým najlepším riešením. Podporuje veľké množstvo autentizačných mechanizmov (určite zo všetkých testovaných najviacej) a je možné ho konfigurovať pomocou SQL databázy.

4 Testovanie funkčnosti a spoľahlivosti

4.1 Autentizačný server – FreeRADIUS

Vzhľadom na to, že väčšina klientských WiFi kariet by mala podporovať EAP-TLS, zvolili sme na testovanie túto autentizačnú metódu. Bolo potrebné vytvoriť certifikačnú autoritu a v súlade s použitím EAP-TLS nakonfigurovať aj FreeRADIUS. Certifikačná autorita bola vytvorená pomocou známeho prostriedku OpenSSL. Vychádzali sme pri tom z dokumentu [12].

V štandardnej konfigurácii bolo potrebné vykonať zmeny v súbore **klientov**, ktoré boli nastavené podľa testovacej siete na 192.168.122.0/24, ďalej v súbore **používateľov** bol pridaný nový používateľ podľa vydaného certifikátu („Filip Valasek“) a nakoniec v súbore **eap.conf** bolo treba nastaviť odkazy na certifikát servera a ostatné atribúty. Obsah podstatných častí konfigurácie sa nachádza v Prílohe A.

4.2 Autentizátor – prístupové body (AP)

Na testovanie sme mali k dispozícii štyri prístupové body (AP):

- HP ProCurve Wireless Access Point 420 WW (J8131A),
- HP ProCurve Access Point 530 WW (J8987A),
- D-Link DWL-2000AP+ a
- ASUS WL-300g.

HP ProCurve 420 a HP Procurve 530 patria medzi drahšie zariadenia, a tak podľa očakávaní fungovali spoľahlivo. D-Link dokázal tiež spolupracovať so serverom veľmi dobre. ASUS síce uvádza, že toto zariadenie vie spracovávať protokol 802.1X, ale vôbec to nefungovalo.

4.3 Suplikant

Ako WiFi karty sme testovali:

- staršiu PCI kartu s čipom Realtek RTL 8180L (používaný aj v niektorých PCMCIA kartách),
- Wireless 11a/b/g PC Card with XJACK Antenna (3CRPAG175B) – chipset Atheros AR5414 a
- Intel Pro Wireless 2200BG – chipset Intel 2200.

V systéme **Windows XP** nenastali pri inštalácii žiadne problémy. Windows v sebe obsahuje už štandardný vstavaný suplikant, ale autentizácia pomocou neho prebiehala dlhšie ako napríklad pri použití štandardnej konfiguračnej utility dodávanej k Intel 2200.

Pri **BSD** (FreeBSD) a **Linuxe** (Ubuntu) bola situácia zložitejšia. Najprv bolo potrebné správne nainštalovať a nastaviť Xsupplicant (http://open1x.sourceforge.net) a potom už pripojenie prebehlo v poriadku.

Rozsiahly test iných WiFi kariet (v Linuxe a WinXP) je dostupný napríklad na adrese http://www.eduroam.cz/doku.php?id=cs:uzivatel:hw:karty:uvod.

5 Vplyv šifrovania a rotácie kľúčov na prenosovú rýchlosť

Bez toho, aby sme vykonali akékoľvek testy, každého určite napadne, že neexistuje žiadna bezpečnosť bez réžie a teda aj bez nákladov na túto bezpečnosť. V prípade metalických (káblových) či optických spojov sa tieto náklady strácajú v prenosovej rýchlosti a nie sú také podstatné. Pri bezdrôtových je však frekvenčné spektrum obmedzené a tiež kódový pomer je značne nevýhodnejší. Z toho dôvodu nás to núti zamyslieť sa nad výhodami, či nevýhodami rôznych druhov šifrovania.

V tejto kapitole si najprv stručne vysvetlíme všetky potrebné pojmy, ktoré neskôr využijeme pri testovaní vplyvu rôznych druhov šifrovania na prenosovú rýchlosť.

5.1 Základné pojmy

Organizácia IEEE vydala dodatok ku štandardu 802.11 s označením 802.11i [16], ktorý určuje princípy, ako vytvárať robustnú bezpečnú sieť (RSN).

Robust security network (RSN): Je bezpečnostná sieť, ktorá umožňuje vytvárať iba robustné bezpečnostné asociácie (robust security network associations – RSNA).

Robust security network association (RSNA): Typ spojenia používaný párom staníc (STA), ak procedúra na vytvorenie tohto spojenia medzi nimi obsahuje 4-cestný handshake. Treba si uvedomiť, že existencia páru RSNA-zariadení ešte nevytvára RSN. RSN je to iba vtedy, ak všetky zariadenia v sieti používajú RSNA.

Robust-security-network-association-(RSNA-) capable zariadenie: Stanica (STA), ktorá je schopná vytvoriť RSNA. RSNA-capable zariadenie ešte nemusí byť v súlade s RSNA Protocol Implementation Conformance Statement (PICS). Zariadenie, ktoré bolo upgradované na podporu Temporal Key Integrity Protocol (TKIP) môže byť RSNA-capable, ale nemusí byť ešte v súlade s PICS, ak nepodporuje aj CCM [counter mode (CTR) with cipher-block chaining (CBC) with message authentication code (MAC)] Protocol (CCMP).

Protokoly CCMP a TKIP si ešte popíšeme neskôr.

5.2 Bezpečnosť podľa 802.11i

Ako prvé si vysvetlíme princíp bezpečnosti podľa štandardu IEEE 802.11i [16]. Ako aj ostatné bezdrôtové technológie, aj WLAN si vyžaduje splnenie niekoľkých bezpečnostných cieľov. Tieto sú dosiahnuté pomocou bezpečnostných vlastností zabudovaných do bezdrôtových sieťových štandardov. Najbežnejšie ciele pre WLAN sú tieto:

- **Dôvernosť** – zabezpečuje, aby komunikácia nemohla byť sledovaná neautorizovanou stranou,
- **Integrita** – deteguje zámerné alebo náhodné zmeny dát, ktoré nastanú počas ich prenosu,
- **Dostupnosť** – zaručuje prístup zariadení a jednotlivcov ku sieti a k jej zdrojom v ktoromkoľvek čase, keď potrebujú,
- **Riadenie prístupu** – obmedzuje prístupové práva zariadení a jednotlivcov pri prístupe k sieti prípadne k jej zdrojom v rámci siete.

Bezpečnostné ciele pre bezdrôtové a drôtové LAN sú rovnaké. Rovnaké sú aj hlavné kategórie hrozieb, ktorým čelia. Tab. 3 poskytuje prehľad hlavných kategórií hrozieb pre LAN.

Najviac hrozieb typicky spôsobuje útočník s prístupom k linkovej vrstve medzi STA a AP alebo medzi dvoma STA. Niektoré z hrozieb obsiahnutých v Tab. 3 sa spoliehajú na útočníkovu schopnosť zachytiť sieťovú komunikáciu a napojiť sa na ňu.

Tieto hlavné črty sú najviac viditeľné rozdiely medzi ochranou drôtovej a bezdrôtovej siete: relatívna jednoduchosť zachytenia komunikácie a vkladanie novej, z čoho sa dá iba odhadnúť, či ide o autentický zdroj. V drôtových LAN, útočník by musel mať fyzický prístup k LAN alebo vzdialene kompromitovať systémy alebo LAN. V bezdrôtových LAN, útočníkovi stačí iba byť v rozsahu pokrytia WLAN infraštruktúry. Navyše, útočník môže mať výhodu pri použití citlivejších smerových antén, ktoré dokážu značne rozšíriť rozsah WLAN.

Kategória hrozby	Popis
Denial of Service	Útočník zabráni alebo znemožní normálne používanie alebo správu siete alebo sieťového zariadenia.
Odpočúvanie	Útočník pasívne pozoruje sieťovú komunikáciu a hľadá dáta, ktoré obsahujú autentizačné údaje.
Man-in-the-Middle	Útočník aktívne prerušuje komunikačnú cestu medzi dvoma legitímnymi stranami komunikácie, aby zachytil autentizačné údaje a dáta. Útočník sa môže vydávať za legitímneho komunikujúceho. V súvislosti s WLAN, man-in-the-middle atak môže byť dosiahnutý pomocu falošného AP, ktorý sa komunikujúcim javí ako autorizovaný AP.
Masquerading	Útočník sa vydáva za autorizovaného používateľa a získava tak určité privilégiá.
Modifikácia správ	Útočník pozmení skutočnú správu jej vymazaním, pridaním novej, zmenou alebo preusporiadaním správ.
Reprodukcia správ	Útočník pasívne monitoruje prenos a preposiela správy, pričom sa správa ako legitímny používateľ.
Analýza prenosu	Útočník pasívne monitoruje prenos, aby identifikoval komunikačné vzory a účastníkov komunikácie.

Tab. 3 Hlavné hrozby pre LAN bezpečnosť [15]

5.2.1 Pre-RSN bezpečnosť

Predtým, ako IEEE uviedlo dodatok 802.11i a jeho rámec, IEEE 802.1 malo veľa problémov s vážnymi bezpečnostnými hrozbami. Niektorí výrobcovia pridali proprietárne vlastnosti do ich IEEE 802.11 implementácií, aby kompenzovali bezpečnostné trhliny v štandarde. Avšak tieto proprietárne

vlastnosti často znemožňujú interoperabilitu. Pre-RSN bezpečnosť je reprezentovaná v 802.11 protokolom WEP, o ktorom je známe, že nie je bezpečný a existuje niekoľko dobre známych slabých miest.

Riadenie prístupu a autentizácia – Pre-RSN IEEE 802.11 vykonáva riadenie prístupu buď pomocou otvorených systémov (open system) alebo zdieľaným kľúčom (shared key). Open system autentizácia nevyžaduje žiadne prístupové údaje od STA, teda je použiteľná iba ako verejný prístup k WLAN. Shared key autentizácia používa schému výzva-odpoveď, ale má slabé stránky, ktoré môžu dovoliť man-in-the-middle útok a tiež iné kompromitácie. Napokon ani open system a tiež shared key autentizácia neumožňujú STA overiť identitu AP, takže útočník môže vystaviť falošné AP a takto nalákať STA na jeho použitie. Takto sa naruší i dôvernosť, integrita a dostupnosť

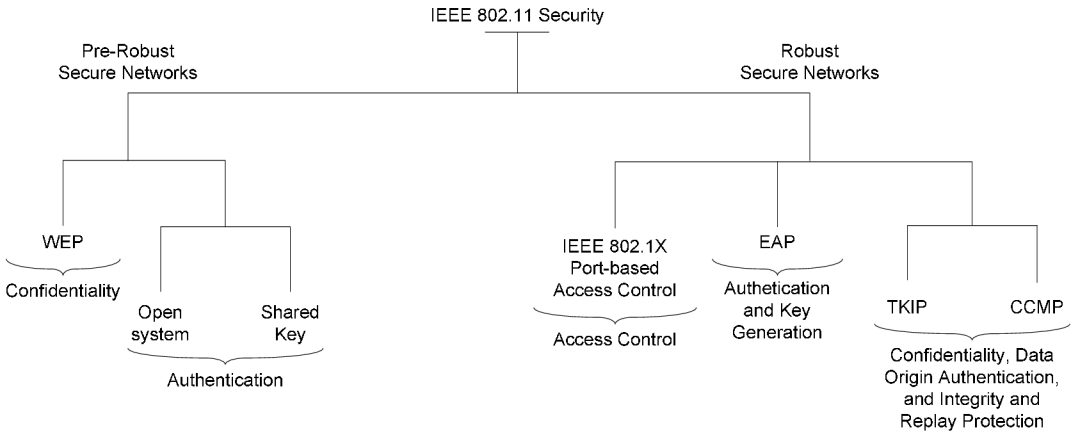
Šifrovanie – WEP trpí množstvom bezpečnostných slabín, ktoré umožňujú potenciálnemu útočníkovi s ľahko dostupným softvérom dešifrovať zachytené dáta, niekedy aj s dátami zachytenými behom pár minút. Tieto slabiny sú výsledkom toho, že WEP používa RC4 šifrovanie a 24-bitový inicializačný vektor, ktorý je príliš malý, aby sa uchránil na zaťaženej sieti WLAN.

Dátová integrita – WEP sa pokúša vykonávať kontrolu integrity dát kontrolovaním správ a odmietne tie, ktoré boli zmenené počas prenosu. Používa pri tom jednoduchý ne-kryptografický kontrolný súčet a chráni tento súčet šifrovaním. Nanešťastie, toto šifrovanie neposkytuje žiadnu ochranu proti bit-flipping útokom, čo znamená, že v mnohých prípadoch môže útočník zmeniť oboje – aj dáta aj prislúchajúci kontrolný súčet – bez možnosti detekcie.

Dostupnosť – Jednotlivci bez fyzického pristúpu k WLAN môži napadnúť jej dostupnosť dvomi spôsobmi: jamming a flooding. Jamming sa vyskutne, keď zariadenie vysielajúce elektromagnetické žiarenie spraví sieť nepoužiteľnú. Flooding zasa vzniká posielaním veľkého množstva správ vysokou rýchlosťou. IEEE 802.11 štandard neobsahuje žiadnu obranu proti týmto dvom typom útokov. Útočníci môžu tiež vytvoriť falošné AP, ktoré spôsobí nedostupnosť legitímnej WLAN.

5.2.2 RSN bezpečnosť

S pridaním dodatku IEEE 802.11i v roku 2004, IEEE 802.11 ponúka dve všeobecné triedy bezpečnostných schopností pre 802.11 WLAN. Prvá trieda, pre-RSN bezpečnosť, obsahuje zdedené bezpečnostné schopnosti vyvynuté v originálnej IEEE 802.11 špecifikácii: open system a shared key autentizácia pre overenie identity bezdôtových staníc, a WEP pre ochranu dôvernosti prenášaných dát. Druhá trieda bezpečnostných schopností obsahuje množstvo bezpečnostných mechanizmov na vytvorenie RSN. RSN obsahuje bezpečnostné rozšírenia na opravu všetkých známych závad, s ktorými sa stretával WEP a poskytuje robustnú ochranu pre bezdrôtové spojenie, vrátane dátovej integrity a dôvernosti. Nasledujúci obrázok túto taxonómi názorne reprezentuje.



Obr. 7 Taxonómia pre Pre-RSN a RSN bezpečnosť [15]

5.2.2.1 TKIP

Temporal Key Integrity Protocol (TKIP) je myslený ako dočasné riešenie pre 802.11 WLAN na rýchle pokrytie množstva nedostatkov, ktorými trpí WEP. TKIP môže byť implementovaný prostredníctvom zmeny softvéru, nepotrebuje nahradenie hardvéru v AP a v STA.

5.2.2.2 CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) je považovaný za dlhodobejšie riešenie pre IEEE 802.11 WLAN siete. CCMP vyžaduje zmenu hardvéru a vyžaduje si tiež, aby organizácia nahradina jej pre-RSN IEEE 802.11 zariadenia.

5.2.2.3 Porovnanie

Porovnanie je v nasledujúcej tabuľke [15].

Bezpečnostná vlastnosť	Manual WEP	Dynamic WEP	TKIP	CCMP
Kryptografický algoritmus	RC4	RC4	RC4	AES
Veľkosť kľúča	40 alebo 104 bitov (šifrovanie)	40 alebo 104 bitov (šifrovanie)	128 bitov (šifrovanie), 64 bitov (ochrana integrity)	128 bitov (šifrovanie aj ochrana integrity)
Paketový kľúč	Vytvorený spojením WEP kľúča a 24-bitového IV	Odvodený z EAP autentizácie	Vytvorený pomocou TKIP mixing function	Nie je, postačuje temprary key
Mechanizmus integrity	Šifrované CRC-32	Šifrované CRC-32	Michael MIC	CCM
Ochrana hlavičky	Žiadna	Žiadna	Zdrojová a cieľová adresa ochránená pomocou Michael MIC	Zdroj. a cieľ. adresa ochránená pomocou CCM
Replay ochrana	Žiadna	Žiadna	Vynútené IV poradie	Vynútené IV poradie

Autentizácia	Open system alebo shared key	EAP metóda s IEEE 802.1X	EAP metóda s IEEE 802.1X alebo PSK	EAP metóda s IEEE 802.1X alebo PSK
Distribúcia kľúča	Manuálne	IEEE 802.1X	IEEE 802.1X alebo manuálne	IEEE 802.1X alebo manuálne

5.3 Testovanie

Testovanie vplyvu rýchlosti sme vykonali vcelku jednoduchým spôsobom. Na vzdialený server sme umiestnili súbor s veľkosťou 710 MB a merali sme čas, ktorý je potrebný na jeho skopírovanie na klientsky počítač. Pritom sme skúšali tieto tri varianty šifrovania:

- open system,
- TKIP a
- CCMP.

V nasledujúcej tabuľke sú výsledky zhrnuté a vypočítali sme aj percentuálny pomer času vzhľadom na referenčnú hodnotu pri open system. V jednotlivých stĺpcoch sú časy uvedené v sekundách. Predposledný riadok tabuľky udáva priemerný čas vypočítaný ako aritmetický priemer z desiatich nameraných hodnôt a posledný riadok vyjadruje percentuálny pomer vzhľadom na hodnotu pri open system infraštruktúre.

Celkovo je možné v tabuľke vidieť, že šifrovanie TKIP alebo CCMP má náklady rovné približne 4 až 5 % vzhľadom k otvorenej (nešifrovanej) komunikácii. Je to prirodzene spôsobené réžiou, ktorú predstavuje šifrovanie.

Open system	TKIP	CCMP
315	327	325
310	330	333
308	335	330
330	338	340
327	340	335
300	310	338
305	300	336
300	337	310
310	325	312
290	320	315
309,5	326,2	327,4
100 %	94,88 %	94,53 %

Tab. 4 Štatistické výsledky merania rýchlosti prenosu

6 Konfiguračné nástroje

Ešte pred tým, ako sa budeme venovať implementácii konfiguračných nástrojov, musíme najskôr vybrať vhodnú kombináciu autentizačného servera a autentizácie. V predchádzajúcich častiach tejto práce sme sa už venovali rôznym implementáciám protokolu RADIUS a tiež najpoužívanejším spôsobom autentizácie.

Spomedzi všetkých RADIUS implementácií, ktoré pripadajú do úvahy, je jednoznačne FreeRADIUS najpokročilejší a obsahuje najväčšie možnosti použitia spôsobov autentizácie. Jedná sa o „živý“ projekt, ktorý sa neustále vyvíja a teda je do budúcnosti predpoklad jeho použiteľnosti.

Pri spôsobe autentizácie nie je situácia až tak jednoduchá ako pri serveri.

6.1 Požiadavky na konfiguráciu

FreeRADIUS server sa implicitne konfiguruje pomocou konfiguračných súborov. Nebudeme sa venovať opisu celej konfigurácie, ale pozrieme sa iba na tie časti, ktoré pre nás budú zaujímavé z pohľadu správy používateľov a účtovania.

6.1.1 Konfiguračné súbory

Súbor **radius.conf** – v tomto súbore sa konfigurujú v podstate všetky podstatné parametre týkajúce sa autentizačných metód. V prílohe A je časť z tohto súboru, ktorá určuje konfiguráciu EAP-TLS metódy. Jednotlivé logické časti sú oddelené párovými zloženými zátvorkami.

Súbor **client.conf** zasa obsahuje údaje o klientskych zariadeniach (predovšetkým NAS), ktoré sa pripájajú „priamo“ k serveru a môžu slúžiť ako autentizátor. Zápis konfigurácie je vcelku jednoduchý a zrozumiteľný.

Súbor **users** nie je potrebné meniť v prípade ak používame externú databázu. Všeobecne je používaný na nastavenie atribútov používateľov ako je meno, heslo, spôsob autentizácie,….

Kompletné konfiguračné súbory, tak ako sme ich používali pri práci, sú obsiahnuté na priloženom CD.

6.1.2 FreeRADIUS a MySQL

Server FreeRADIUS umožňuje vcelku pohodlne konfigurovať (pridávať, odoberať,…) informácie o používateľoch pomocou databázy. Nasledujúce tabuľky popisujú model databázy, ktorá slúži práve na konfiguráciu servera.

usergroup
Väzobná tabuľka – určuje príslušnosť používateľa k určitej skupine

id	primárny kľúč
UserName	meno používateľa
GroupName	meno skupiny

radcheck	
Nastavenie používateľov a ich hesiel	
id	primárny kľúč
UserName	meno používateľa
Attribute	atribút (User-Password)
Value	hodnota
op	operátor (==)

radgroupcheck	
Nastavenie skupín a spôsobov autentizácie	
id	primárny kľúč
GroupName	meno skupiny
Attribute	atribút (Auth-Type)
Value	hodnota
op	operátor (:=)

radreply	
Nastavenie atribútov, ktoré budú zaslané v odpovedi od servera	
id	primárny kľúč
UserName	meno používateľa
Attribute	atribút
Value	hodnota
op	operátor (:=)

radgroupcheck	
Podobne ako radreply, ale tentoraz pre skupiny	
id	primárny kľúč
GroupName	meno skupiny
Attribute	atribút
Value	hodnota
op	operátor (:=)

radacct	
Účtovacia tabuľka – vypĺňa výhradne server na základe údajov od autentizátora	
id	primárny kľúč
UserName	meno používateľa
...	množstvo atribútov, ale najmä: množstvo prenesených dát, doba sedenia

6.2 Požiadavky na aplikáciu

Konfiguračný nástroj by mal umožňovať pridávať používateľov, meniť im priradené atribúty a samozrejme aj mazať používateľov. FreeRADIUS je schopný vytvárať aj používateľské skupiny. Preto by mala aplikácia obsahovať funkcionalitu správy skupín a tiež pridávania používateľov do nich. Vzhľadom na to, že RADIUS je AAA protokol, je možné vykonávať aj účtovanie prenesených dát používateľom.

Z uvedeného vyplýva, že celkový koncept navrhovanej aplikácie sa dá rozdeliť na tri relatívne samostatné časti:

- správa používateľov,
- správa skupín,
- štatistické výstupy.

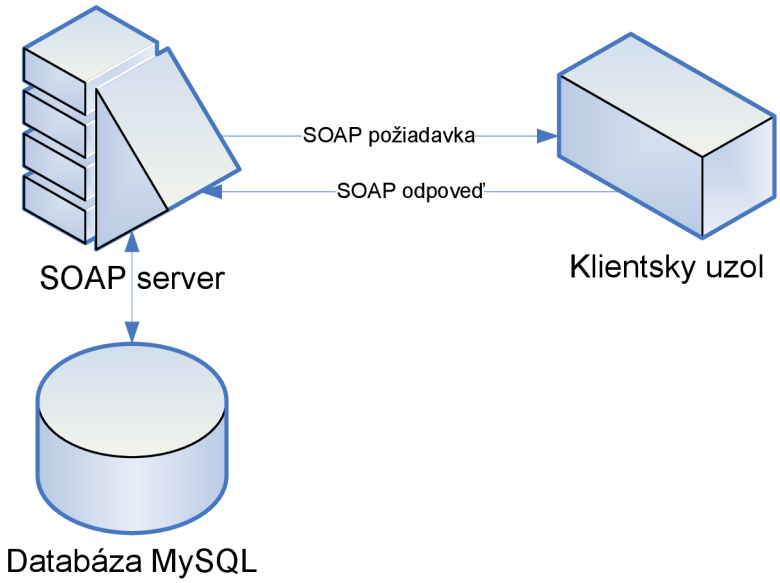
6.3 Architektúra

Ako základná architektúra bola zvolená architektúra klient-server. Aj keď implementácia bude prebiehať výhradne (aj klient aj server) v programovacom jazyku PHP s databázou MySQL, v budúcnosti by mohla vzniknúť potreba vytvoriť klientsku aplikáciu, ktorá by bola umiestnená nezávisle od servera na ľubovoľnom počítači v sieti. Zvolená architektúra umožní tiež dodatočne jednoducho implementovať ďalšie funkčné prvky na strane klienta, prípadne uľahčí správu servera aj z iných aplikácií.

Ako komunikačný protokol sme zvolili SOAP, čo postačuje pre naše účely. Výhodou SOAP je jeho podpora takmer vo všetkých programovacích jazykoch, čím je zachovaná možnosť ďalšieho rozširovania aplikácie.

Na nasledujúcom obrázku je vidieť koncept architektúry klient-server s použítím komunikačného protokolu SOAP. Na jednej strane je klientska aplikácia, ktorá posiela požiadavku smerom k serveru. Ten spracuje správu a vytvorí odpoveď, ktorú pošle späť ku klientovi. Komunikácia prebieha najčastejšie pomocou HTTP, ale je možná aj cez TCP alebo SNMP. Formát vymieňaných dát je odvodený z XML, čo na jednej strane zvyšuje množstvo prenesených dát, ale zasa pre naše účely to plne postačuje.

Využitá bude databáza MySQL, pre ktorú má FreeRADIUS distribúcia vytvorené aj SQL skripty na vytvorenie tabuliek.



Obr. 8 Architektúra konfigurácie servera FreeRADIUS

6.4 Rozhranie klient–server

Vytvorili sme tri základné rozhrania pre komunikáciu klient–server. Sú rozdelené v zmysle kapitoly 0 na rozhranie:

- používateľ (skript soap_user.php),
- skupina (soap_group.php) a
- štatistiky (soap_statistics.php).

Presnejší popis jednotlivých rozhraní a ich metód (funkcií) je opísaný v nasledujúcich tabuľkách.

SOAP_USER		
Funkcia	**Vstupy**	**Výstup** ***Akcia***
add	*name* – meno používateľa *password* – heslo	Výsledkom je počet vložených riadkov, teda 1 v prípade úspechu a -1 v prípade neúspechu. *Do databázy sa vložia údaje o používateľovi.*
remove	*name* – meno používateľa	0 – neúspečné, 1 – úspech *Odstráni používateľa z databázy.*
changePassword	*name* – meno *password* – heslo	0 – neúspech, 1 – úspešná zmena. *Zmení používateľské heslo.*
doAttribude	*user* – používateľ *attribute* – atribút *op* – operátor *value* – hodnota	0 – neúspech, 1 – úspech. *Vloží, prípadne zmení požadovaný atribút pre používateľa.*
removeAttribute	*user* – používateľ *attribute* – atribút	0 – neúspech, 1 – úspech. *Odtráni atribút.*
getAll	*void*	Vráti pole, kde sú všetky údaje z tabuľky radcheck.
getUser	*name* – meno	Vráti všetky údaje o používateľovi ako pole.

SOAP_GROUP		
Funkcia	**Vstupy**	**Výstup** ***Akcia***
add	*name* – meno používateľa *auth_type* – heslo	Výsledkom je počet vložených riadkov, teda 1 v prípade úspechu a -1 v prípade neúspechu. *Do databázy sa vložia údaje o používateľovi.*
remove	*name* – meno používateľa	0 – neúspečné, 1 – úspech *Odstráni používateľa z databázy.*
changeAuthType	*name* – meno *auth_type* – heslo	0 – neúspech, 1 – úspešná zmena. *Zmení používateľské heslo.*
doAttribude	*user* – používateľ *attribute* – atribút *op* – operátor *value* – hodnota	0 – neúspech, 1 – úspech. *Vloží, prípadne zmení požadovaný atribút pre používateľa.*
removeAttribute	*user* – používateľ *attribute* – atribút	0 – neúspech, 1 – úspech. *Odtráni atribút.*
getAll	*void*	Vráti pole, kde sú údaje o všetkých skupinách.
getGroup	*name* – meno	Vráti všetky údaje o skupine ako pole.
addUser	*group* – skupina *user* – používateľ	Po úspešnej asociácii vráti 1, inak 0 alebo -1. *Pridá používateľa do skupiny.*

SOAP_STATISTICS		
Funkcia	**Vstupy**	**Výstup** ***Akcia***
getUser	*name* – meno používateľa *first* – počet vrátených výsledkov, ak je rovné 0, vráti všetky údaje pre konkrétneho používateľa	Vráti pole jednotlivých prihlásení aj so štatistickými údajmi.
getCount	*name* – meno používateľa	Vráti počet účtovacích záznamov pre používateľa.

6.5 Používateľské rozhranie

Na pridávanie používateľov a skupín a na ich správu sme vytvorili používateľské rozhranie, ktoré umožňuje vykonávať základné operácie údržby. Celé rozhranie pracuje ako klientska aplikácia, ktorá sa prostredníctvom popísaných bodov z predchádzajúcej časti pripája na SOAP server a tak konfiguruje server FreeRADIUS. Celá aplikácia je implementovaná, tak isto ako server, v PHP, teda jej spustenie neprebieha priamo u používateľa, ale na serveri.

Pripájanie prebieha až po autentizácii, ktorá je nastavená pomocou súboru .htaccess. Rovnako sa autentizuje aj klientska aplikácia voči SOAP serveru. Súbor .htaccess poskytuje možnosť dodatočne nastaviť aj iné obmedzenia ako prihlasovanie pomocou mena a hesla. Je možné ho nastaviť aj tak, aby bol obmedzený iba na určité IP adresy.

6.6 Podrobnejší popis implementácie

Ako už sme naznačili, architektúra aplikácie je viacvrstvová. Základná vrstva je vrstva databázová, ktorá pracuje priamo s databázou, nad ňou je vrstva SOAP, ktorá obsahuje metódy na pohodlnejšiu prácu s aplikáciou a na najvyššej vrstve sú prezentačné PHP skripty, ktoré už priamo zobrazujú údaje, prípadne posielajú údaje vrstve SOAP. SOAP vrstvu sme si popísali už v predchádzajúcom texte, teraz sa pozrieme na databázovú a na prezentačnú.

6.6.1 Databázová vrstva

Databázová vrstva pracuje priamo s databázou a vystupuje ako adaptér pre vyššiu vrstvu SOAP. Obsahuje presne tie triedy, ktoré korešpondujú s tabuľkami z databázy, ktoré využívame:

- radacct – účtovanie,
- radcheck – používatelia,
- radreply – atribúty používateľov,
- radgroupcheck – podobne ako radcheck ale pre skupiny,
- radgroupreply – atribúty pre skupiny,
- usergroup – práca s priraďovaním používateľov do skupín (väzobná trieda).

6.6.2 Prezentačná vrstva

Prezentačná vrstva je vlastne jediná vrstva, ktorú môže „vidieť“ používateľ. Nižšie vrstvy mu ostanú ukryté. Základ tvoria tri PHP skripty a k nim prislúchajúce adresáre:

- **user.php** – prístup k prípadom použitia súvisiacich s používateľmi,
- **group.php** – správa skupín,
- **statistic.php** – zobrazenie štatistík.

Jednotlivé adresáre (user, group a statistic) obsahujú pre každú akciu vlastný PHP skript. Všetky zdrojové kódy, aj s komentárom, sú uložené na priloženom CD.

7 Zhodnotenie použiteľnosti

Počas používania a konfigurácie sa nevyskytli žiadne vážnejšie chyby. Aplikácia nebola testovaná na to, akú záťaž zvládne, ale podľa dostupných testov, FreeRADIUS patrí medzi veľmi dobre použiteľné autentizačné servery. Na stránke produktu sa píše, že FreeRADIUS používa veľké množstvo inštitúcií a že je používaný aj pre systémy s niekoľko tisíc používateľmi.

7.1 Iné možnosti autentizácie

Okrem RADIUS existuje viacej podobných AAA protokolov. Medzi ne patria DIAMETER, TACACS a tiež TACACS+. Postupne si ich porovnáme a popíšeme.

7.1.1 DIAMETER

Názov je odvodený od protokolu RADIUS, ktorý je jeho predchodcom (priemer je dvakrát polomer). DIAMETER nie je spätne kompatibilný, ale poskytuje upgrade pre RADIUS. Základné rozdiely sú napríklad:

- Používa spoľahlivý transportný protokol (TCP alebo SCTP, nie UDP).
- Môže prenášať aj bezpečnostné protokoly vyššej úrovne – IPsec alebo TLS.
- Má podporu pre RADIUS.
- Má väčší adresový priestor pre pár atribút–hodnota a pre identifikátory (32 bitov namiesto 8 bitov).
- Môže byť používaný aj stavový aj bezstavový model.
- Má notifikáciu chýb.
- Obsahuje lepšiu podporu pre roaming.
- Je lepšie rozšíriteľný – môžu byť definované nové atribúty a príkazy.
- Má základnú podporu pre používateľské sedenia a účtovanie.

Komplexnosť tohto protokolu má však aj svoje nevýhody – nie je príliš jednoduché implementovať celý štandard tak, ako je popísaný v RFC dokumentoch. DIAMETER je totiž ešte viac komplexný a je zložitejší ako RADIUS.

7.1.2 TACACS

Terminal Access Controller Access-Control System (TACACS) je autentizačný protokol, ktorý sa používa na komunikáciu s autentizačným serverom najmä v UNIXových sieťach. TACACS umožňuje vzdialenému serveru komunikovať s autentizačným serverom na zistenie, či používateľ má prístup k sieti.

TACACS umožňuje klientovi zadať meno a heslo a poslať požiadavku na TACACS autentizačný server, niekedy nazývaný TACACS démon alebo zjednodušene TACACSD. Tento server je bežne program bežiaci na serveri. Ten rozhodne či akceptuje alebo odmietne požiadavku a pošle späť odpoveď.

Neskoršie bola uvedená verzia XTACAXS. Obe predchádzajúce verzie nahradila nová TACACS+ a tiež RADIUS. TACACS+ je úplne nový protokol a nie je kompatibilný s TACACS ani s XTACACS.

TACACS je definovaný v RFC 1492 a používa obvykle (buď TCP alebo UDP) port 49.

7.1.3 TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus) je protokol, ktorý poskytuje riadenie prístupu pre smerovače, sieťové prístupové servre a tiež pre ostatné sieťové zariadenia pomocou jedného alebo viacerých cetralizovaných serverov. TACACS+ vykonáva autentizáciu, autorizáciu a účtovanie oddelene.

Názov TACACS+ je odvodený od TACACS, ale napriek jeho menu, je to úplne nový protokol, ktorý je s predchádzajúcou verziou nekompatibilný.

Zatiaľ čo RADIUS kombinuje autentizáciu s autorizáciou v profile používateľa, TACACS+ oddeľuje tieto dve operácie. Ďalším rozdielom je použitie TCP pri TACACS+ a UDP pri RADIUS.

Existujú rozšírenia, ktoré poskytujú viacej typov autentizačných požiadaviek a viac typov odpovedí ako sú v originálnej špecifikácii.

TACACS+ používa TCP port 49, rovnako ako TACACS. Jeho špecifikácia sa však nachádza stále vo fáze vývoja a je to proprietárny protokol firmy CISCO.

8 Záver

V tejto práci bolo našou úlohou zistiť všeobecné podmienky použiteľnosti autentizácie na L2 úrovni podľa 802.1X v spojení s rôznymi RADIUS servermi a klientskymi zariadeniami. Zistili sme, že FreeRADIUS je asi najpoužiteľnejší z testovaných serverov. Jediný potenciálny „nepriateľ“ by mohol byť OpenRADIUS, no ten neobstál tak úspešne.

Otázka kompatibility klientskych zariadení je skôr o tom, do akej miery ich podporuje operačný systém, teda skôr či sú dostupné drivery. Situácia sa postupne zlepšuje aj pri unixových a linuxových systémoch, takže existuje dosť dobrá perspektíva použiteľnosti.

Ďalej sme sa zaoberali vplyvom použitého šifrovania na prenosovú rýchlosť. Zistili sme to, čo sme v podstate očakávali, že pri nešifrovanej komunikácii bez akejkoľvek autentizácie (open system) je prenosovná rýchlosť väčšia. Avšak pri testovaní TKIP a CCMP sme žiadny podstatný rozdiel nezistili.

Nakoniec bol vyvinutý konfiguračný nástroj a tiež jeho serverová časť (SOAP). Pomocou týchto prostriedkov je možné konfigurovať FreeRADIUS server a tiež sledovať niektoré štatistické údaje.

Jedným z novších protokolov je DIAMETER. Ten však neuspel medzi používateľmi najmä vďaka jeho zložitosti, ktorá je zbytočná. Princíp RADIUS servera zrejme plne vyhovuje drvivej väčšine aplikácií.

Literatúra

[1] HASSELL, Jonathan. *RADIUS*. [s.l.] : O'Reilly, 2002. 206 s. ISBN 0-596-00322-6.

[2] STRAND, Lars. *802.1X Port-Based Authentication HOWTO* [online]. 2004-08-18 [cit. 2006-12-27]. Dostupný z WWW: <http://www.linux.com/howtos/8021X-HOWTO/>.

[3] IEEE Computer Society. *IEEE Std 802.1X-2004, IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control.* New York : Institute of Electrical and Electronics Engineers, Inc., 2004. 142 s. Dostupný z WWW: <http://standards.ieee.org/getieee802/download/802.1X-2004.pdf>. ISBN 0-7381-4529-7.

[4] *Wikipedie: Otevřená encyklopedie: AAA protokol* [online]. c2006 [cit. 2006-12-28]. Dostupný z WWW: <http://cs.wikipedia.org/w/index.php?title=AAA_protokol&oldid=1059172>.

[5] *JRadius* [online]. 2006 [cit. 2006-12-31]. Dostupný z WWW: <http://jradius.org/>.

[6] *FreeRADIUS* [online]. 2006 [cit. 2006-12-31]. Dostupný z WWW: <http://http://www.freeradius.org/>.

[7] *Cistron RADIUS* [online]. 2006 [cit. 2006-12-31]. Dostupný z WWW: <http://www.radius.cistron.nl/>.

[8] *GNU Radius* [online]. 2006 [cit. 2006-12-31]. Dostupný z WWW: <http://www.gnu.org/software/radius/radius.html>.

[9] *OpenRADIUS* [online]. 2006 [cit. 2006-12-31]. Dostupný z WWW: <http://www.xs4all.nl/~evbergen/openradius/>.

[10] ABOBA, Bernard, et al. *RFC 3748 : Extensible Authentication Protocol (EAP)* [online]. 2004 [cit. 2007-01-02]. Dostupný z WWW: <http://tools.ietf.org/html/rfc3748>.

[11] ABOBA, Bernard, SIMON, Dan. *RFC 2716 : PPP EAP TLS Authentication Protocol* [online]. 1999 [cit. 2007-01-02]. Dostupný z WWW: <http://tools.ietf.org/html/rfc2716>.

[12] ROSER, Ken. *HOWTO: EAP/TLS Setup for FreeRADIUS and Windows XP Supplicant* [online]. 2002-04-18 [cit. 2007-01-02]. Dostupný z WWW: <http://www.freeradius.org/doc/EAPTLS.pdf>.

[13] FUNK, Paul, BLAKE-WILSON, Simon. *EAP Tunneled TLS Authentication Protocol Version 1 (EAP-TTLSv1)* [online]. 2006 [cit. 2007-01-02]. Dostupný z WWW: <http://tools.ietf.org/wg/eap/draft-funk-eap-ttls-v1-01.txt>.

[14] KAMATH, Vivek, PALEKAR, Ashwin, WODRICH, Mark. *Microsoft's PEAP version 0 (Implementation in Windows XP SP1)* [online]. 2006 [cit. 2007-01-02]. Dostupný z WWW: <http://tools.ietf.org/html/draft-kamath-pppext-peapv0-00>.

[15] SHEILA, Frankel, et al. *Establishing Wireless Robust Security Networks : A Guide to IEEE 802.11i*. [s.l.] : [s.n.], 2007. 162 s. Dostupný z WWW: <http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf>.

[16] IEEE Computer Society. *IEEE Std 802.11i-2004, IEEE Standard for Information technology : Medium Access Control (MAC) Security Enhancements.* New York : [s.n.], 2004. 190 s. Dostupný z WWW: <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>. ISBN 0-7381-4074-0.

Zoznam príloh

Príloha A: Príklad konfigurácie

Príloha B: Používateľská dokumentácia

Príloha C: CD s elektronickou verziou diplomovej práce a zdrojové kódy

Príloha A – Príklad konfigurácie

radius.conf

```
eap {
       default_eap_type = tls

       tls {
              private_key_password = whatever
              private_key_file = /root/myCA/cert-srv.pem
              certificate_file = /root/myCA/cert-srv.pem

              CA_file = /root/myCA/cacert.pem

              dh_file = /root/myCA/dh
              random_file = /root/myCA/random
              fragment_size = 1024      }
}
```

client.conf

```
client 192.168.122.0/16 {
       secret        = whatever
       shortname     = rtest
}
```

users

```
”Filip Valasek”     Auth-Type := EAP
```

Príloha B – Používateľská dokumentácia

Táto používateľská dokumentácia slúži na prácu s administračným rozhraním pre server FreeRADIUS. Je rozdelená na tri časti:

- Správa používateľov,
- Správa skupín a
- Štatistický výstup.

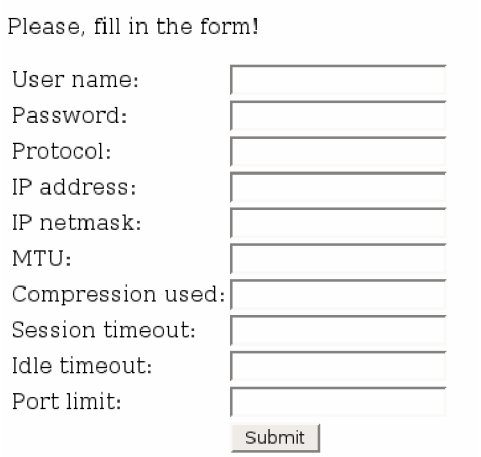
Hierarchia menu

Rozdelenie menu je nasledovné:

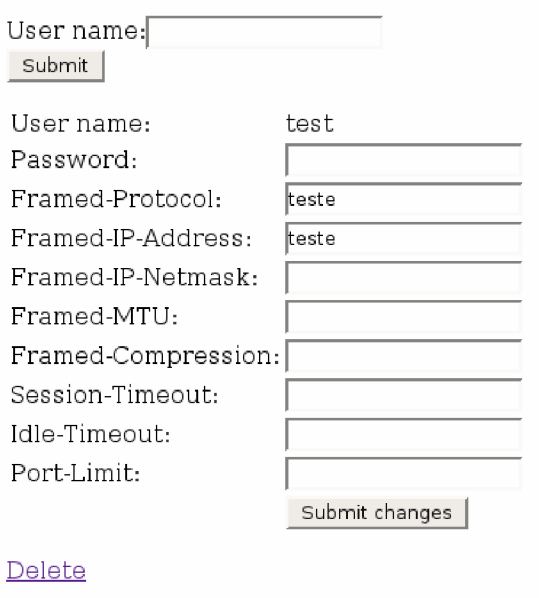
- **Users** – správa používateľov
  - **Add** – pridanie používateľa
  - **Find** – vyhľadanie používateľa
  - **Back** – návrat do hlavného menu
- **Groups** – správa skupín
  - **Add** – pridanie skupiny
  - **Show** – zobrazenie všetkých skupín
  - **Back** – návrat do hlavného menu
- **Statistics** – štatistické výstupy
  - **Find** – vyhľadanie štatistík podľa používateľa
  - **Back** – návrat do hlavného menu

Správa používateľov

Nového používateľa pridáme pomocou položky menu Users > Add. Položky User name a Password je možné jednoducho vyplniť. Význam ostatných atribútov je vysvetlený na konci tejto dokumentácie.



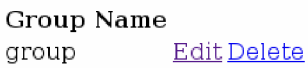
Používateľa môžeme aj **vyhľadávať** pomocou ponuky menu Users > Find. Potom po zadaní používateľa do poľa User name sa nám objavia všetky jeho údaje, ktoré môžeme **meniť a upravovať**. Ak je niektorý z atribútov vyplnený a my túto hodnotu vymažeme, atribút bude odstránený po stlačení tlačítka Submit changes. Používateľa jednoducho **vymažeme** stlačením odkazu Delete.



Správa skupín

Nová skupina sa pridáva podobne ako nový používateľ, ale teraz pomocou menu Groups > Add. Pri skupine nevypĺňame heslo ako pri používateľovi, ale autentizačný typ (EAP, Local,…). Ostatné atribúty sú rovnaké ako v pri používateľoch.

Pri skupinách si môžeme nechať **vypísať všetky skupiny** (Groups > Show). Následne môžeme tieto skupiny upravovať podobne ako používateľov a tiež ich vymazávať. Zmazaním skupiny či používateľa sa vymažú z databázy aj všetky atribúty, ktoré boli s touto skupinou alebo používateľom viazané.



Štatistický výstup

Na nasledujúcom obrázku je vidieť prehľad prihlásení pre používateľa xvalas06. Význam jednotlivých stĺpcov je zrejmý z ich popisov. Vyhľadať štatistiky pre iného používateľa je možné zadaním jeho mena do poľa User name. Ak je počet prihlásení vyšší ako sa vmestí na jednu stranu, funguje aj prepínanie medzi jednotlivými stranami.

User name:
Submit

0 1 2

User Name	Start Time	Stop Time	Session Time	Input Bytes	Output Bytes
xvalas06	2007-05-14 17:25:44	2007-05-20 08:49:20	33	0	0
xvalas06	2007-05-14 18:11:42	2007-05-20 09:07:16	1021	20978134	18402598
xvalas06	2007-05-14 18:59:28	2007-05-14 19:10:56	688	500060	1680447
xvalas06	2007-05-14 19:43:40	2007-05-14 19:44:11	32	0	0
xvalas06	2007-05-14 19:44:12	2007-05-14 19:44:15	4	0	0
xvalas06	2007-05-14 19:45:41	2007-05-14 19:50:13	273	0	0
xvalas06	2007-05-14 19:50:57	2007-05-14 20:06:18	920	0	0
xvalas06	2007-05-14 20:07:28	2007-05-14 20:08:29	61	70223	299074
xvalas06	2007-05-14 20:11:01	2007-05-20 10:05:37	15	13546	7053
xvalas06	2007-05-20 08:44:51	2007-05-20 08:48:43	232	0	0

Význam atribútov

Pri pridávaní používateľov a skupín sa stretávame s rôznymi atribútmi, ktorých význam nie je na prvý pohľad jasný. V nasledujúcej tabuľke sú všetky popísané.

Atribút	Popis	Možnosti
Framed-Protocol	Tento atribút určuje typ rámca.	PPP SLIP ARAP Gandalf Xylogics X.75 Synchronous
Framed-IP-Address	Tento atribút určuje adresu, ktorá bude priradená používateľovi.	napr. 192.168.2.100
Framed-IP-Netmask	Určuje IP sieťovú masku.	napr. 255.255.255.0
Framed-MTU	Určuje Maximum Transmission Unit, ktoré budú nakonfigurované pre používateľa.	
Framed-Compression	Kompresný protokol používaný spojením.	None VJ TCP/IP header compression IPX header compression Stac-LZS compression
Session-Timeout	Určuje maximálnu dĺžku doby v sekundách, ktorá je používateľovi poskytnutá pred ukončením sedenia alebo pred opätovnou výzvou.	
Idle-Timeout	Podobne ako pri Session-Timeout, ale ide o dobu nečinnosti.	
Port-Limit	Nastavuje maximálne množstvo portov, ktoré budú poskytnuté používateľov od NAS.	