VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

AUDIT PODNIKOVÝCH WIFI SÍTÍ ZALOŽENÝCH NA STANDARDU 802.1X

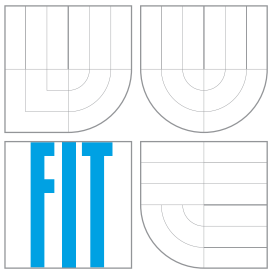
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. LUKÁŠ ANTAL

BRNO 2012

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

AUDIT PODNIKOVÝCH WIFI SÍTÍ ZALOŽENÝCH NA STANDARDU 802.1X

802.1X BASED WIRELESS NETWORK SECURITY AUDIT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. LUKÁŠ ANTAL
AUTHOR

VEDOUCÍ PRÁCE — Ing. MICHAL DROZD
SUPERVISOR

BRNO 2012

Abstrakt

Tato diplomová práce se zabývá analýzou zabezpečení bezdrátových WiFi sítí založených na standardu 802.1X a metodou auditu těchto sítí. V práci jsou popsány jednotlivé verze metod autentizačního protokolu EAP používané v bezdrátových sítích, rizika vyplývající z jejich nasazení a doporučení pro zmírnění těchto rizik. Součástí práce je také návrh a implementace aplikace určené pro audit 802.1X bezdrátových sítí se zaměřením na zpracování protokolu EAP.

Abstract

This master's thesis analyzes the security of 802.1X based wireless networks and presents the methodology for auditing these networks. The thesis describes various methods of the EAP authentication protocol used in wireless networks, security risks arising from their usage and recommendations for mitigating these risks. The paper also includes implementation of the application for 802.1X based wireless networks audit focusing on the EAP protocol processing.

Klíčová slova

802.11, 802.1X, RADIUS, EAP, Bezpečnost, Audit

Keywords

802.11, 802.1X, RADIUS, EAP, Security, Audit

Citace

Lukáš Antal: Audit podnikových WiFi sítí založených na standardu 802.1X, diplomová práce, Brno, FIT VUT v Brně, 2012

Audit podnikových WiFi sítí založených na standardu 802.1X

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana Ing. Michala Drozda

.....
Lukáš Antal
20. května 2012

Poděkování

Rád bych poděkoval vedoucímu mé práce panu Ing. Michalovi Drozdovi za odborné vedení a čas věnovaný konzultacím. Dále bych rád poděkoval panu Ing. Marošovi Barabasovi za poskytnuté rady a připomínky. Děkuji také své přítelkyni za trpělivost a rodině za podporu během studia.

Obsah

1 Úvod **3**
1.1 Cíle práce . . . 4

2 Bezpečnost WLAN sítí **6**
2.1 IEEE 802.11 . . . 8
2.1.1 Vývoj standardu . . . 8
2.1.2 Service Set . . . 10
2.1.3 802.11 rámce . . . 10
2.2 Filtrace MAC adres a skrývání SSID . . . 15
2.3 WEP . . . 16
2.4 WPA Personal . . . 18
2.4.1 WPA . . . 19
2.4.2 WPA2 . . . 20
2.5 WPA Enterprise . . . 21
2.5.1 RADIUS . . . 22
2.5.2 EAP, EAPOL . . . 24
2.5.3 EAP-MD5 . . . 27
2.5.4 LEAP . . . 28
2.5.5 EAP-FAST . . . 29
2.5.6 PEAP . . . 30
2.5.7 EAP-TLS . . . 32
2.5.8 EAP-TTLS . . . 34
2.5.9 Shrnutí . . . 34

3 Slabiny bezpečnostních mechanismů WLAN sítí **35**
3.1 Filtrace MAC adres a skrývání SSID . . . 36
3.2 WPA Enterpise . . . 37
3.2.1 EAP-MD5 . . . 37
3.2.2 LEAP . . . 38
3.2.3 EAP-FAST . . . 40
3.2.4 PEAP . . . 41
3.2.5 EAP-TTLS . . . 44
3.2.6 EAP-TLS . . . 44
3.3 Shrnutí . . . 45

4 Bezpečnostní audit **48**
4.1 Základní pojmy . . . 48
4.2 Historie . . . 49
4.3 OSSTMM . . . 50
4.4 Metodika auditu 802.1X bezdrátové sítě . . . 51

5 EAPtool **56**
5.1 Návrh . . . 57
5.1.1 Pasivní režim . . . 57
5.1.2 Aktivní režim . . . 59
5.1.3 Penetrační režim - EAP-MD5, LEAP . . . 60
5.1.4 Penetrační režim - PEAP . . . 62
5.1.5 WIDS režim . . . 64
5.2 Implementace . . . 65
5.2.1 Odhalení skrytého SSID . . . 65
5.2.2 Překlad MAC adres . . . 66
5.2.3 Multithreading . . . 66
5.2.4 Ukládání zachycené komunikace . . . 67
5.2.5 Volba WiFi kanálu . . . 67
5.2.6 Použité technologie . . . 67
5.3 Podobné projekty . . . 69
5.3.1 Nmap eap-info NSE script . . . 69
5.3.2 EAPeak . . . 69
5.4 Možná rozšíření . . . 70
5.5 Použití . . . 70

6 Ukázkový audit **73**
6.1 Detekce použité metody . . . 73
6.2 Získání přístupu . . . 74
6.2.1 LEAP . . . 75
6.2.2 PEAP . . . 76
6.3 Enumerace uživatelských jmen . . . 77
6.4 Audit zařízení služeb . . . 78
6.5 Závěr auditu . . . 78

7 Závěr **79**
7.1 Zhodnocení výsledků . . . 80

A Instalace nástroje EAPtool **85**

B Obsah přiloženého CD **86**

Kapitola 1

Úvod

Bezdrátové WiFi sítě jsou v současné době součástí síťové infrastruktury téměř každé společnosti a organizace. V případě klasických LAN[1] sítí jsou data přenášena v rámci uzavřeného systému spojů. Aby se klient připojil k LAN síti, musí svůj počítač či jiné zařízení fyzicky propojit kabelem s danou síťovou infrastrukturou. Útočník by pro neautorizované připojení k takové síti potřeboval fyzický přístup do dané budovy, kde by se již vystavil vysokému riziku odhalení.

U bezdrátových sítí je situace zcela jiná. Bezdrátový signál se prostředím šíří do všech směrů a navíc podléhá fyzikálním zákonitostem, jakými jsou například odraz, lom, rozptyl, stínění či difrakce. Šíření WiFi signálu[2] je obecně obtížné předpovědět[26] či přímo omezit na vyhrazené prostory. Útočník se tak může nacházet na veřejném místě mimo prostory společnosti a přesto mít dostatečný signál pro pokusy o neautorizovaný přístup do sítě.

Z toho důvodu je nutné věnovat bezpečnostnímu nastavení bezdrátové sítě náležitou pozornost, hlavně pokud je bezdrátová síť součástí síťové infrastruktury organizace či společnosti, jejíž kompromitace by s sebou nesla finanční, reputační či jiná rizika.

Následují příklady z nedávné doby, kdy kompromitace slabě zabezpečené WiFi sítě vedla k finančním ztrátám. V prosinci roku 2006 byla kompromitována počítačová síť společnosti TJX Companies[3], vlastníka největšího řetězce obchodních domů v USA. Incident byl společností oznámen v lednu roku 2007[4] a následně bylo zjištěno, že celý útok trval již roku 2005 a měl za následek krádež 45,6 milionů čísel kreditních a debetních karet, 450 tisíc SSN[5], čísel řidičských průkazů a dalších osobních údajů[13]. Příčinou úniku tak velkého množství citlivých informací bylo nasazení v té době již nevyhovujícího bezpečnostního mechanismu WEP na bezdrátové sítě platebních terminálů. Jeden z dopadených útočníků Albert Gonzalez později vypověděl, že útok probíhal pomocí notebooku a volně dostupného software z auta na parkovišti před jedním z obchodních domů ve městě St. Paul, Minnesota[18].

Zabezpečení bezdrátových WiFi sítí vykonalo za posledních deset let dlouhou cestu[7]. Přesto v současné době není použití zastaralých bezpečnostních mechanismů v podnikových WiFi sítích stále žádnou výjimkou. V srpnu roku 2011 byla skupina útočníků z města Seattle schopna během krátké doby kompromitovat více než deset nedostatečně zabezpečených podnikových WiFi sítí s cílem krádeže a následného prodeje citlivých údajů[32].

[1] Pojmem LAN budou nadále v této práci označované metalické sítě, zatímco bezdrátové sítě budou označovány jako WLAN

[2] Obecně i jakéhokoliv jiného bezdrátového signálu

[3] http://www.tjx.com/

[4] http://www.businesswire.com/news/tjx/20070117005971/en

[5] Social Security number - Unikátní devítimístné číslo sloužící jako identifikace každého občana USA.

Výše uvedené příklady slouží jako připomenutí, že bezpečnost bezdrátových sítí je stále aktuálním tématem, jež by v žádném případě nemělo být podceněno, a to zvlášť v případě společností a organizací nakládajících s osobními a dalšími citlivými daty.

1.1 Cíle práce

Práce má za cíl analyzovat bezpečnostní mechanismy používané u WiFi sítí implementujících autentizaci dle standardu 802.1X, popsat jejich slabá místa, zranitelnosti, možnosti zneužití a následně uvést doporučení pro zmírnění popsaných rizik. Celkově je tak cílem vytvořit ucelenou metodiku pro analýzu bezpečnostních mechanismů těchto WiFi sítí, rizik plynoucích z jejich nasazení a případných doporučení. Metodika má za cíl sloužit administrátorům bezdrátových sítí jako bezpečnostní příručka pro bezpečnostní konfiguraci a provoz bezdrátových sítí, stejně jako bezpečnostním auditorům či penetračním testerům pro provedení technicky zaměřeného bezpečnostního auditu.

Primárním cílem práce jsou bezdrátové WiFi sítě postavené na standardu 802.1X a analýza jednotlivých typů metod autentizačního protokolu EAP. Práce se věnuje bezdrátovým sítím dle standardu IEEE 802.11, označovaným souhrnně akronymem WiFi. Práce se nevěnuje bezpečnosti dalších bezdrátových technologií jako je například Bluetooth či ZigBee. Dále v práci bude bezdrátovou sítí vždy myšlena WiFi síť, pokud nebude uvedeno jinak.

V kapitole 2 budou podrobně popsány nejrozšířenější bezpečnostní mechanismy používané v bezdrátových sítích. Největší pozornost bude věnována mechanismům zabezpečení bezdrátových sítí využívající autentizaci dle standardu IEEE 802.1X (2.5). V této kapitole bude popsána architektura bezdrátové sítě využívající 802.1X autentizaci, podrobně bude popsán autentizační protokol EAP (2.5.2) a protokol RADIUS (2.5.1). Taktéž zde budou představeny jednotlivé metody protokolu EAP a popsán princip každé z nich. Kapitola se bude také zabývat bezpečnostními mechanismy založenými na principu sdíleného klíče, jakými jsou bezpečnostní algoritmy WEP (2.3), WPA-Personal a WPA2-Personal (2.4).

Kapitola 3 bude svoji strukturou téměř ekvivalentní s předchozí kapitolou a bude popisovat bezpečnostní slabiny a rizika vyplývající z nasazení jednotlivých bezpečnostních mechanismů. Kromě popisu a nástinu zneužití jednotlivých slabin bude vždy uvedeno doporučení týkající se bezpečného nasazení a použití dané technologie. Tato kapitola bude již zaměřena čistě na bezpečnost jednotlivých metod protokolu EAP využívaného v rámci 802.1X autentizace a nebude popisovat zranitelnosti mechanismů založených na použití sdíleného klíče, jakými jsou WEP, WPA-Personal a WPA2-Personal.

Kapitola 4 bude zaměřena na problematiku realizace bezpečnostních auditů. Budou zde zmíněny standardizované postupy a metodiky, jejich principy a možná aplikace v kontextu auditu bezdrátových WiFi sítí. Na základě existujících postupů bude vymezen rozsah a seznam činností pro provedení auditu bezdrátové sítě s autentizací dle standardu 802.1X.

V praktické části práce je cílem navrhnout a implementovat aplikaci usnadňující audit podnikových sítí se zaměřením na analýzu použitých metod EAP protokolu. Aplikace bude vytvořena s důrazem na implementaci funkcionalit pro testování sítí založených na standardu 802.1X, které v současné době nejsou podporovány žádnou existující volně dostupnou aplikací. Návrhem, implementací a praktickými ukázkami aplikace se bude zabývat kapitola 5.

V kapitole 6 bude navržená metodika využita při realizaci bezpečnostního auditu bezdrátové sítě menší společnosti. Audit bude také z velké části realizován prostřednictvím aplikace navržené a implementované v rámci praktické části této práce. V kapitole bude

popsán postup auditu, detekované zranitelnosti a z nich vyplývající rizika a také bezpečnostní doporučení vedoucí ke snížení či úplnému odstranění těchto rizik.

Výsledky a výstupy práce, zhodnocení dosažených cílů a návrhy na další možná rozšíření budou shrnuty v závěrečné kapitole 7.

Kapitola 2

Bezpečnost WLAN sítí

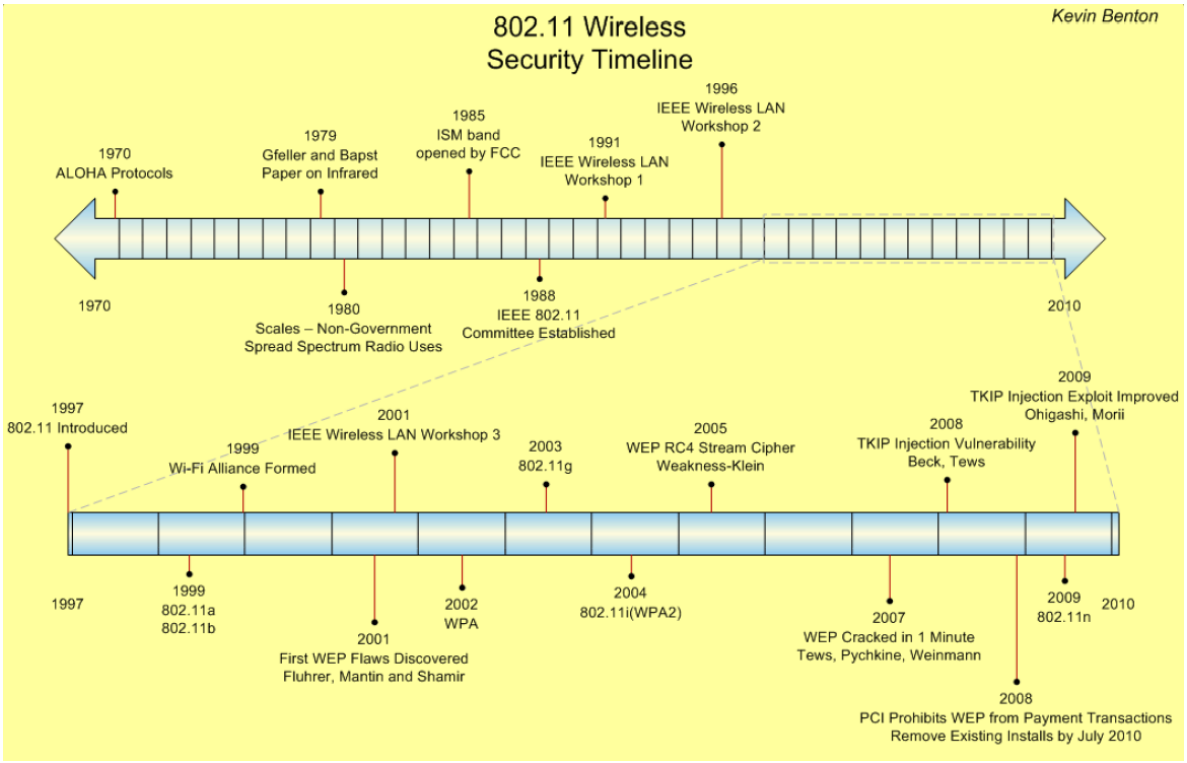
Od doby vzniku standardu IEEE 802.11 prošlo zabezpečení bezdrátových sítí poměrně rušným vývojem. Již původní verze standardu z roku 1997 podporovala šifrování bezdrátové komunikace prostřednictvím kryptografického algoritmu WEP (Wired Equivalent Privacy). První bezpečnostní nedostatky tohoto algoritmu byly publikovány v roce 2001. Spolu s postupným objevováním bezpečnostních trhlin šifrovacího algoritmu RC4, na kterém je algoritmus WEP postaven, sílila potřeba modernějšího a bezpečnějšího kryptografického mechanismu pro bezdrátové sítě. Tím se stal v roce 2002 mechanismus WPA (Wi-Fi Protected Access) využívající algoritmus TKIP (Temporal Key Integrity Protocol). Zabezpečení WPA vychází z draftu standardu 802.11i a bylo vydáno s důrazem na rychlou opravu nedostatků zabezpečení WEP bez nutnosti zásahů do hardware bezdrátových zařízení. Plnohodnotný standard IEEE 802.11i byl vydán v roce 2004 a nese označení WPA2. WPA2 přináší podporu šifrování pomocí algoritmu AES (Advanced Encryption Standard), který je do dnešní doby považován za bezpečný. Od roku 2008 se začínají objevovat první náznaky bezpečnostních nedostatků algoritmu TKIP, umožňující injekci dat do šifrované komunikace[38]. Průběh vývoje standardu 802.11 a jeho zabezpečení je stručně shrnut na obrázku 2.1.

Zajištění důvěrnosti

Jak již bylo uvedeno výše, bezdrátový signál je velice obtížné omezit pouze na vyhrazené prostory. Kdokoliv v dosahu signálu daného přístupového bodu tak má možnost odposlouchávat probíhající komunikaci. Z toho důvodu řešíme otázku zajištění důvěrnosti bezdrátově přenášených dat. Důvěrnost definujeme jako zajištění toho, že se k datům nedostane osoba, jíž data nejsou určena. Jinými slovy důvěrnost definuje, že přístup k informaci je umožněn pouze autorizovanému příjemci. V případě bezdrátové sítě se informace šíří prostorem nekontrolovaně a kdokoliv s dostatečným signálem tak může danou informaci odposlechnout. Obrana proti odposlechu je u (nejen) bezdrátových WiFi sítí řešena šifrováním. Šifrování WiFi sítí je realizováno na druhé vrstvě ISO/OSI modelu. Různé typy šifrování využívané u WiFi sítí jsou popsány dále v této kapitole.

Zajištění integrity

Zároveň se zajištěním důvěrnosti přenášených dat je nutné zajistit jejich integritu, tedy ochranu proti neautorizované modifikaci. Integrita dat je u bezdrátových sítí zajištěna mechanismy WEP a WPA. Ty jsou podrobně popsány dále v této kapitole.



Obrázek 2.1: Vývoj bezpečnostních mechanismů WiFi sítí. Převzato z [7]

Řízení přístupu

Řízení přístupu slouží k zajištění přístupu k dané síti pouze autorizovaným klientům. V případě bezdrátových sítí ho můžeme rozdělit na základě informace sloužící pro udělení oprávnění přístupu do sítě na tři typy:

- **MAC adresa** - Řízení přístupu na základě MAC adresy je jedinou možností řízení přístupu u nešifrovaných WiFi sítí. Zároveň je však možné tento typ řízení přístupu zkombinovat s dále uvedenými typy. Je založené na existenci seznamu povolených MAC adres, který je uložen na přístupovém bodě. Ten před autentizací klienta ověří, zda je MAC adresa jeho bezdrátového síťového adaptéru v seznamu povolených klientů a na základě tohoto porovnání je rozhodnuto, zda bude klientovi umožněno připojení k síti. Více o tomto mechanismu pojednává kapitola 2.2.

- **Sdílený klíč** - Řízení přístupu na základě znalosti sdíleného klíče je uplatněno prostřednictvím bezpečnostních mechanismů WEP a WPA-Personal popsaných v kapitolách 2.3 a 2.4.

- **Přístupové údaje/certifikát** - Přihlašování uživatelů na základě znalosti vlastních přihlašovacích údajů (jméno a heslo), případně vlastnictví klientského certifikátu je použito v případě nasazení autentizace dle standardu 802.1X. Tento standard je popsán v kapitole 2.5.

2.1 IEEE 802.11

V této kapitole je popsán vývoj standardu IEEE 802.11 pro lokální bezdrátové sítě včetně popisu jeho předchůdců. Dále jsou definovány pojmy týkající architektury bezdrátových WiFi sítí jakými jsou například ESS a BSS. Nakonec jsou podrobně rozebrány jednotlivé typy 802.11 rámců související s bezpečností bezdrátových sítí.

2.1.1 Vývoj standardu

Při bezdrátovém přenosu dat je nutné vyřešit přístup ke sdílenému médiu tak, aby se jednotlivé vysílací stanice navzájem nerušily[1]. Jednou z prvních technologií řešení přístupu ke sdílenému médiu byl protokol ALOHA (1970) a jeho nástupce Slotted ALOHA (1972)[29]. Tyto protokoly potom tvoří základ současných metod pro řešení sdíleného přístupu:

- **CSMA/CD** - *Carrier sense multiple access with collision detection* je metoda používaná u metalických ethernetových LAN sítí.
- **CSMA/CA** - *Carrier sense multiple access with collision avoidance* je metoda používaná u sítí standardu IEEE 802.11 popsaného dále v této kapitole.

Datové bezdrátové sítě se začaly rozšiřovat zhruba od poloviny osmdesátých let 20. století. V té době využíval každý výrobce vlastní navzájem nekompatibilní proprietární technologie a postupy[7]. Tato situace vyústila v nutnost potřeby jednotného otevřeného standardu pro bezdrátovou datovou komunikaci.

Tímto standardem se stal IEEE 802.11 dokončený v roce 1997. Standard podporoval maximální přenosovou rychlost 2Mbps ve frekvenčním pásmu 2,4 GHZ. Prvním masově rozšířeným standardem se však staly až **802.11a** a **802.11b** publikované v roce 1999[16]. Tyto standardy přinášejí zvýšení přenosové rychlosti a podporu frekvenčního pásma 5 GHz (802.11a). Další zvýšení rychlosti až na 54Mbps pak nabízí standard **802.11g** z roku 2003, který je zpětně kompatibilní s 802.11b. V roce 2009 byl schválen zatím poslední z této rodiny standardů, a to **802.11n**[2]. Jeho základem je podpora technologie *Multiple In, Multiple Out* - MIMO, která za pomocí více antén sloužících pro příjem a odesílání podporuje přenosy rychlostí teoreticky až 600Mbps[21]. Standard podporuje použití až osmi antén, dnešní AP však většinou využívají pouze tři. Vývoj a specifika standardu IEEE 802.11 popisuje tabulka 2.1.

Standard	Vydání	Maximální rychlost [Mbps]	Šířka pásma [Hz]	Pásmo [GHz]	Fyzická vrstva
802.11	1997	2	20	2,4	DSSS, FHSS
802.11a	1999	54	20	5/3,7	OFDM
802.11b	1999	11	20	2,4	DSSS
802.11g	2003	54	20	2,4	OFDM
802.11n	2005	150	20/40	2,5/5	OFDM

Tabulka 2.1: IEEE 802.11 standardy

Kromě verzí standardu 802.11 uvedených v tabulce 2.1 existuje ještě množství dalších revizí a derivátů tohoto standardu, které jsou dále stručně popsány.

[1] Viz problém skrytého terminálu

[2] http://standards.ieee.org/getieee802/download/802.11n-2009.pdf

- **802.11c** - Standard definující možnosti přemosťování v rámci bezdrátových sítí na úrovni komunikační podvrstvy MAC (*Media Access Control*). Standard byl ratifikován v roce 1998 a od roku 2001 je zahrnut v rámci standardu 802.11d.

- **802.11d** - 802.11d je označovaný jako globální harmonizační standard definující využití různých frekvenčních pásem (především pásmo 5 GHz). Standard definuje požadavky na fyzickou vrstvu a taktéž například podporuje uvádění informací o daném státě v rámci *Beacon* a *Probe* rámců tak, aby se klienti mohli automaticky přizpůsobit požadavkům a regulacím dané země. Standard byl ratifikován v roce 2001 a v roce 2007 byl zapracován do standardu IEEE 802.11-2007.

- **802.11e** - Definuje vylepšení služby QoS (Quality of Service) na úrovni komunikační podvrstvy MAC (*Media Access Control*). Tato vylepšení jsou velice důležitá pro aplikace citlivé na zpoždění přenosu, jakými jsou VoIP over WLAN či streamování multimédií. Standard byl ratifikován v roce 2005 a v roce 2007 byl zapracován do standardu IEEE 802.11-2007.

- **802.11f** - Definuje implementaci protokolu IAPP (*Inter-Access Point Protocol*), který slouží pro komunikaci mezi přístupovými body různých výrobců a pro zajištění roamingu, kdy uživatel přechází od jednoho přístupového bodu k dalšímu. Standard byl ratifikován v roce 2003.

- **802.11h** - Doplnění standardu 802.11a tak, aby bylo možné frekvenční pásmo 5 GHz používat i v evropských podmínkách mimo budovy a zároveň aby bylo minimalizováno rušení s jinými systémy (například meteorologické radary). Standard byl ratifikován v roce 2004 a v roce 2007 byl zapracován do standardu IEEE 802.11-2007.

- **802.11i** - Bezpečnostní standard WPA2 popsaný v kapitole 2.4.2. Standard byl ratifikován v roce 2004.

- **802.11j** - Obdoba standardu 802.11h, avšak pro japonské podmínky. Standard byl ratifikován v roce 2003 a v roce 2007 byl zapracován do standardu IEEE 802.11-2007.

- **802.11k** - Vylepšení správy a řízení rádiových zdrojů pro vysoké frekvence. Standard byl ratifikován v roce 2008.

- **802.11p** - Definuje tzv. WAVE (*Wireless Access for the Vehicular Environment*) umožňující využití WiFi v rámci vozidel jako součást Inteligentního dopravního systému (ITS - *Intelligent Transportation Systems*). Systém využívá frekvenční pásmo 5.9 GHz. Standard byl ratifikován v roce 2010.

- **802.11r** - Standard definující WiFi připojení z rychle se pohybujících objektů, včetně řešení handoveru mezi různými základnovými stanicemi. Standard byl ratifikován v roce 2008.

- **802.11r** - Standard definující topologii *Mesh*[3] v rámci WiFi sítě. Standard byl ratifikován v roce 2011.

- **802.11u** - Standard definující propojení WiFi sítí se sítěmi jiných typů (například buňkové mobilní sítě). Standard byl ratifikován v roce 2011.

[3]Síťová topologie, ve které je většina síťových zařízení propojena navzájem.

- **802.11v** - Standard definující konfiguraci klientských zařízení během jejich připojení k síti. Standard byl ratifikován v roce 2011.
- **802.11w** - Definuje metody pro zvýšení zabezpečení rámců typu *Management*. Standard byl ratifikován v roce 2009.
- **802.11y** - Podpora pro provoz WiFi sítě ve frekvenčním pásmu 3650 – 3700 MHz. Standard byl ratifikován v roce 2008.

2.1.2 Service Set

Pod obecným pojmem *Service Set* - SS označujeme množinu zařízení připojených k lokální WLAN síti. V rámci terminologie bezdrátových sítí potom rozlišujeme pojmy BSS, ESS, BSSID a SSID[17]:

- **BSS** - *Basic Service Set* je označení pro jeden přístupový bod (AP - Access Point) a všechny klientské stanice (STA - Station) k němu připojené.
- **IBSS** - *Independent Basic Service Set* je označení pro množinu klientských stanic komunikujících přímo mezi sebou v režimu Ad-Hoc.
- **ESS** - *Extended Service Set* vzniká propojením dvou a více BSS pomocí distribučního systému. Vztah mezi BSS a ESS je ilustrován na obrázku 2.2.
- **BSSID** - *Basic Service Set Identifier* je jednoznačný identifikátor BSS. Tímto identifikátorem je MAC adresa[4] přístupového bodu.
- **SSID** - *Service Set Identifier* je identifikátor jedné WLAN sítě obsahující nula[5] a více přístupových bodů. Jinými slovy se jedná o element určující identitu ESS nebo BSS. Identifikátor má formu až 32 znaků dlouhého řetězce. SSID nemusí být unikátní, v jedné lokalitě se tak může nacházet více bezdrátových sítí se stejným SSID. Někdy je tento identifikátor nesprávně označován jako ESSID. Takový termín však není v IEEE 802.11 standardu definován[4].

2.1.3 802.11 rámce

Nejmenší jednotka pro přenos dat v rámci WiFi sítě se nazývá rámec. Nepočítáme-li fyzickou vrstvu, 802.11 rámec začíná MAC (*Media Access Control*) hlavičkou, následuje LLC (*Logical Link Control*), data vyšších vrstev (IP, UPD, TCP,...)[6] a FCS (*Frame Check Sequence*). MAC hlavička bude podrobně popsána dále. Vrstva LLC - *Logical Link Control*, která je součástí spojové vrstvy, určuje protokol vyšší vrstvy pro přenos dat. V TCP/IP sítích se jedná o protokol IP. FCS - *Frame Check Sequence* obsahuje 32b dlouhý kontrolní součet obsahu paketu. Pro výpočet kontrolního součtu je obvykle použit algoritmus CRC - *Cyclic Redundancy Check*.

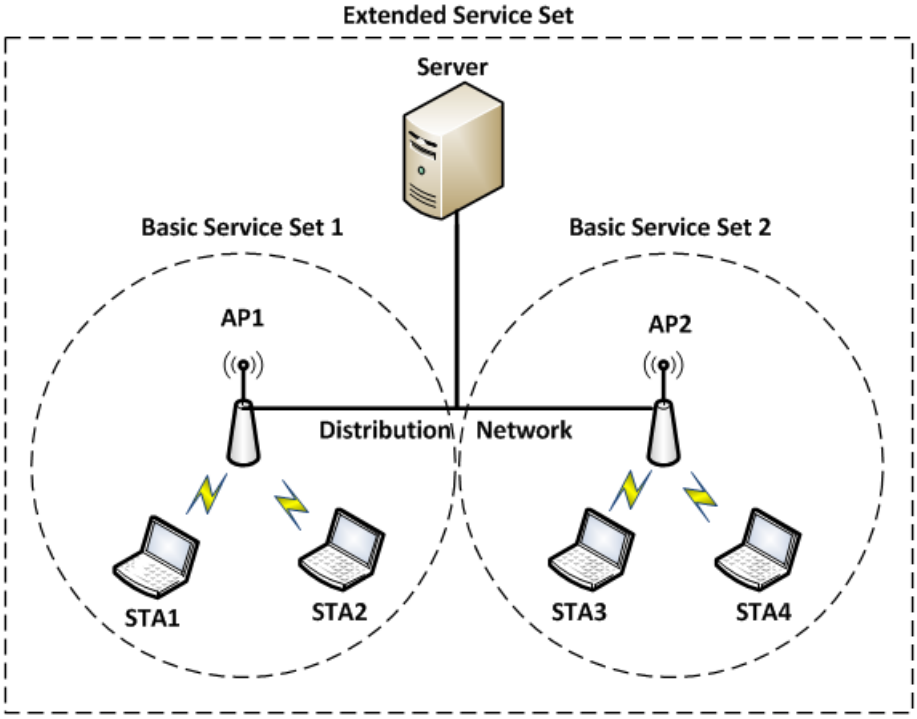
MAC hlavička se skládá z následujících částí[4]:

- **Frame Control**: 4 bajty dlouhé pole obsahující následující informace:

[4] 48b dlouhá hodnota jednoznačně identifikující síťovou kartu (Network Interface Controller - NIC) každého zařízení

[5] V případě Ad-Hoc sítě

[6] Vrstvy LLC a výše jsou přítomny, pouze pokud se jedná o datový rámec



Obrázek 2.2: Extended Service Set

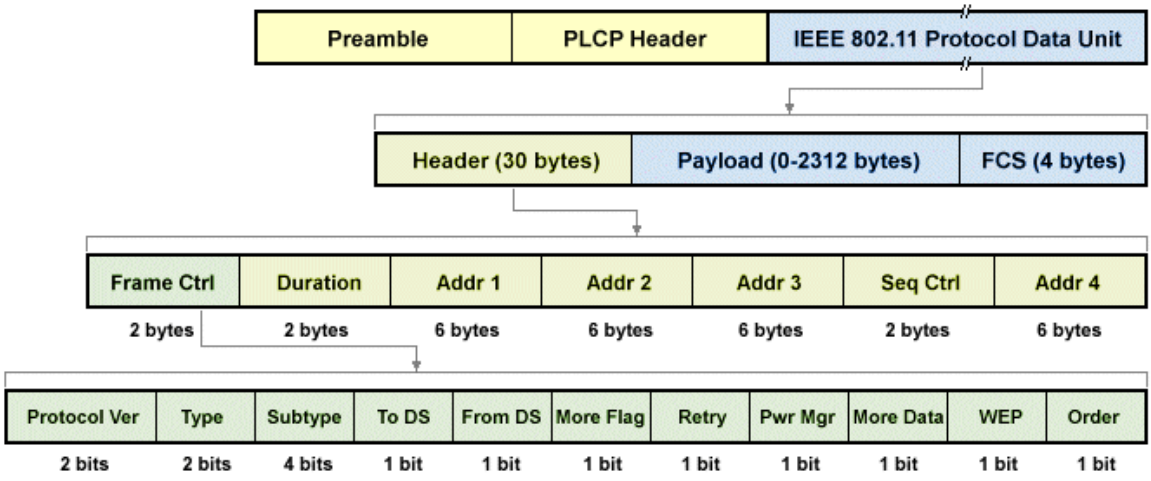
- **Protocol Version**: Obsahuje verzi použitého protokolu, nastaveno na hodnotu 0, hodnoty 1 až 3 jsou rezervovány pro případné další použití. (2b)
- **Type/Subtype**: Identifikace významu rámce. Hlavní typy 802.11 rámců jsou *Control*, *Management* a *Data*. Jednotlivé typy a podtypy 802.11 rámců jsou popsány dále v této kapitole. (6b)
- **To DS/From DS**: Význam kombinací těchto dvou bitových příznaků je uveden v tabulce 2.2 (2b)
- **More fragments**: Určuje, zda byl rámec při přenosu fragmentován. (1b)
- **Retry**: Určuje, zda se jedná o znovu zaslaný rámec. (1b)
- **Power Management**: Indikuje, zda je použit mód úspory energie. Hodnota určuje, v jakém stavu bude STA po odeslání rámce. Hodnota 0 značí, že stanice bude v aktivním módu. Hodnota 1 značí, že stanice přechází do úsporného módu. Rámce odeslané přístupovým bodem mají tento bit vždy nastaven na hodnotu 0. (1b)
- **More data**: Určuje, zda má STA další data k odeslání ve svém bufferu. Tento příznak je používán pouze u rámců typu *Data* a *Management*. (1b)
- **Protected Frame**: Určuje, zda byl rámec zpracován kryptografickým algoritmem. Tento příznak může být nastavený na hodnotu 1 pouze v u rámců typu *Data* a rámců typu a podtypu *Management - Authentication.*, a to v případě, že je na dané síti použito šifrování WEP nebo WPA. (1b)
- **Order**: Příznak Order značí, zda je rámec přenášen prostřednictvím třídy StrictlyOrdered. (1b)

- **Duration ID**: Slouží pro rezervování doby obsazení média (8b)
- **Station ID**: Slouží pro funkci úspory energie (8b)
- **BSSID adresa**: MAC adresa AP v rámci BSS. (48b)
- **Zdrojová adresa**: MAC adresa odesílatele rámce. (48b)
- **Cílová adresa**: MAC adresa příjemce rámce. (48b)
- **Sequence control**: 2 bajty dlouhé pole obsahující následující hodnoty:
  - **Sequence number**: Slouží pro zjištění správného pořadí přijatých rámců a také jako ochrana proti přijetí duplikátních zpráv. (12b)
  - **Fragment number**: Určuje, zda se jedná o fragmentovaný paket, případně o jakou část fragmentu se jedná. (4b)
- **Volitelná adresa**: Čtvrtá MAC adresa může být volitelně použita, pokud rámec prochází bezdrátových mostem. (48b)

To DS	From DS	Význam
0	0	Rámec je zasílán mezi dvěma STA v rámci IBSS
0	1	Rámec je zasílán ze STA na AP
1	0	Rámec je zasílán z AP na STA
1	1	Rámec je zasílán z AP na AP v rámci ESS

Tabulka 2.2: Význam kombinací bitových příznaků *To DS* a *From DS*. Převzato z: [4]

Struktura WiFi rámce se zapouzdřením MAC hlavičky a pole Frame Control je ilustrována na obrázku 2.3.



Obrázek 2.3: IEEE 802.11 rámec. Převzato z: [36]

Jak již bylo uvedeno výše, 802.11 rámce můžeme dle typu rozdělit na tři hlavní skupiny: *Control*, *Management* a *Data*. Každý z těchto typů potom můžeme rozdělit na několik

podtypů dle specifické funkce rámce. Jelikož na jednotlivé typy rámců bude v dalších částech této práce odkazováno, následuje popis jednotlivých typů a podtypů rámců standardu 802.11. Souhrn všech podtypů není úplný, vybrány byly především podtypy rámců nějakým způsobem související s bezpečností bezdrátových sítí.

Rámce typu management

Rámce typu management slouží pro řízení procesu asociace a autentizace klienta k bezdrátové síti. Rozlišujeme následující podtypy:

- **Authentication request/response frame**: Autentizační rámce slouží pro autentizaci klienta vůči přístupovému bodu. Autentizace dle standardu 802.11 je proces, při kterém dojde k ověření identity klienta a na základě výsledku tohoto ověření je identita klienta přístupovým bodem přijata nebo odmítnuta. Komunikaci započne klient posláním autentizačního rámce obsahujícího svoji identitu (typicky MAC adresa) na přístupový bod. V případě, že je použita tzv. *Open system* autentizace, klient zašle jediný autentizační paket, na který přístupový bod odpoví přijetím anebo odmítnutím identity klienta. V případě, že je použita autentizace na základě sdíleného klíče (*Shared key authentication*), odpoví přístupový bod klientovi na autentizační požadavek rámcem obsahujícím challenge řetězec. Tento challenge řetězec zašifruje klient sdíleným klíčem a odešle na přístupový bod. Ten ověří, zda byl použit správný klíč a pošle klientovi odpověď s výsledkem tohoto ověření. Oba typy autentizace včetně jejich zranitelností jsou popsány v kapitole 2.3.

- **Deauthentication frame**: Deautentizační rámec posílá klient přístupovému bodu za účelem ukončení komunikace. Zneužitím těchto rámců pro vykonání útoku DoS (*Denial of Service*) a jeho detekcí se zabývá kapitola 5.1.5.

- **Association request/response frame**: Po tom, co se klient úspěšně autentizoval, následuje proces asociace, při kterém přístupový bod vyhradí prostředky pro daného klienta. Klient zahájí komunikaci zasláním asociačního požadavku. Přístupový bod rozhodne o asociaci a zašle klientovi odpověď. Posloupnost akcí vedoucích k asociaci klienta je ilustrována na obrázku 2.4.

- **Reassociation request/response frame**: Pokud se klient pohybuje mezi jednotlivými přístupovými body v rámci ESS, vzdálí se od AP, ke kterému je právě asociován a zároveň detekuje AP s vyšším signálem, vyšle požadavek na reasociaci. Nové AP se následně postará o přeposlání dat, která mohla zůstat ve vysílacím bufferu předchozího přístupového bodu. Veškerá další komunikace poté probíhá přes nové AP.

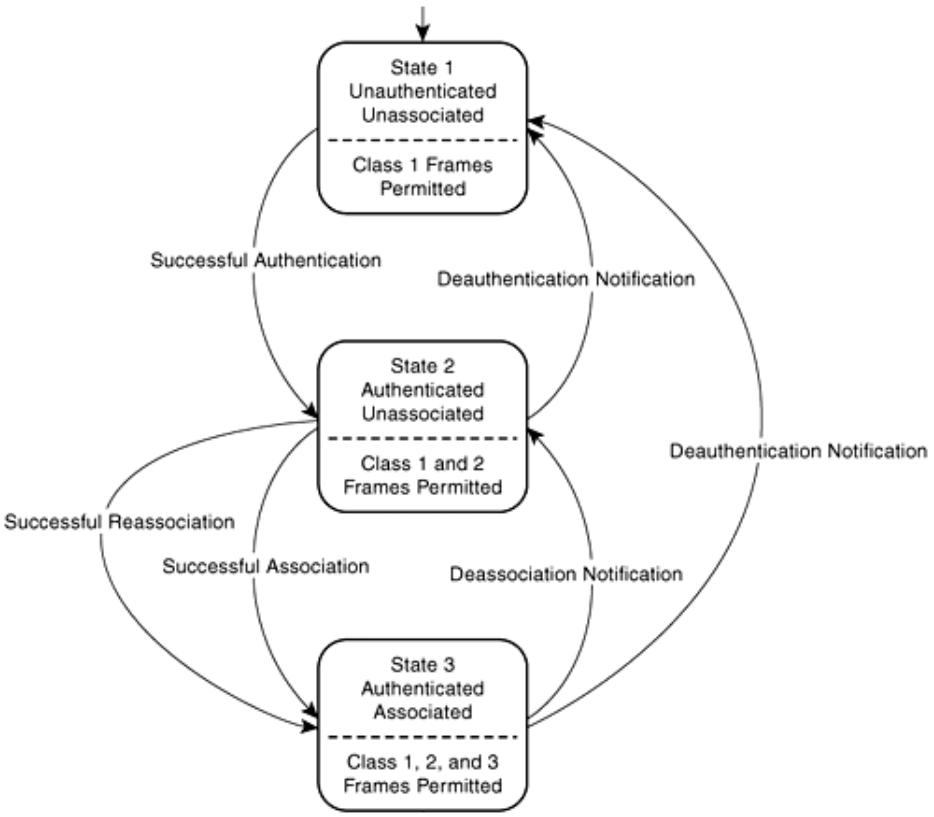
- **Disassociation frame**: Klient zasílá přístupovému bodu požadavek na deasociaci jako upozornění, že končí současnou asociaci s AP. Přístupový bod pak může uvolnit prostředky vyhrazené pro tohoto klienta.

- **Beacon frame**: Přístupový bod periodicky posílá *Beacon* rámce za účelem upozornění klientů, že se v jejich blízkosti nachází WiFi síť. *Beacon* rámec obsahuje SSID dané sítě, časové razítko, informaci o podporovaných modulacích a kryptografických algoritmech, verzi 802.11 standardu[7], číslo kanálu a další informace odvíjející se od

[7] a,b,g,n nebo jejich kombinace

výrobce daného AP, například jméno výrobce či podpora WPS[8]. *Beacon* rámce jsou vždy posílány na broadcastovou adresu spojové vrstvy[9]. Funkcionalitu periodického vysílání *Beacon* rámců lze na většině přístupových bodů deaktivovat jakožto zabezpečení proti neoprávněnému přístupu do sítě. O tomto způsobu zabezpečení pojednává kapitola 2.2.

- **Probe request/response frame**: Pomocí Probe požadavků klient aktivně vyhledává určitou síť na základě SSID, které je přenášeno uvnitř tohoto rámce. Požadavky jsou odesílány na broadcastovou adresu spojové vrstvy. Pokud přístupový bod přijme Probe požadavek a SSID uvnitř tohoto požadavku se shoduje s SSID propagovaným přístupovým bodem, je klientovi odeslána odpověď Probe response. Ta obsahuje stejné údaje, jaké jsou přenášeny uvnitř *Beacon* rámce. Klient také může odeslat požadavek Probe s prázdným SSID. Odpověď na takový požadavek potom zasílá každé AP v dosahu, avšak ne v případě, pokud má zakázanou propagaci vlastního SSID. Pokud klient na svůj požadavek obdrží více odpovědí od různých AP se stejným SSID, pokusí se připojit k přístupovému bodu s nejlepším signálem. Toto chování může být zneužito k útoku zvanému *Rogue AP*, jehož princip je popsán v kapitole 3.2.4.



Obrázek 2.4: Stavový diagram klienta podle IEEE 802.11. Převzato z [23]

[8] WiFi Protected Setup - Přihlašování na základě zadání PINu či stisknutí tlačítka na AP namísto konfigurace sdílených klíčů (WEP, WPA)

[9] Tvar broadcastové MAC adresy je následující: ff:ff:ff:ff:ff:ff

Kontrolní rámce

Kontrolní rámce slouží pro řízení rádiového vysílání tak, aby bylo zamezeno kolizím. Pomocí RTS, CTS a ACK kontrolních rámců je implementována metoda pro řešení problému skrytého terminálu. Ten spočívá v situaci, kdy stanice A prostřednictvím naslouchání média dostává informaci, že je médium volné a začne vysílat. Na přijímači C však může dojít ke kolizi vyslaných dat, spolu s daty stanice B, která byla pro vysílající stanici A skrytá, tedy nebyla v jejím dosahu. Rozlišujeme následující typy kontrolních rámců:

- **Request to Send (RTS) frame**: RTS rámec vysílá stanice připravená vysílat příjemci jako ověření, že je příjemce připraven data přijímat. Součástí RTS rámce je pak předpokládaná doba přenosu dat.
- **Clear to Send (CTS) frame**: CTS rámec je odesílán příjemcem RTS rámce jako potvrzení, že je připraven přijmout data. Součástí CTS rámce je pak předpokládaná doba přenosu dat z RTS rámce jako upozornění pro ostatní stanice, že po tuto dobu nemají vysílat.
- **Acknowledgement (ACK) frame**: Po obdržení CTS rámce vyšle stanice příjemci datové rámce. Pokud příjemce tyto pakety obdržel a úspěšně provedl kontrolu CRC, zašle potvrzení formou ACK rámce. Pokud odesílatel po odeslání dat neobdržel ACK rámec, předpokládá, že data nebyla úspěšně doručena a pokusí se o jejich znovu odeslání prostřednictvím RTS/CTS procedury.

Datové rámce

Datové rámce slouží k přenosu vlastních dat prostřednictvím zapouzdření protokolů vyšších vrstev. Datové rámce se dále dělí na 16 podtypů. Jejich popis však vzhledem k zaměření práce není zásadní, proto zde nebude uveden. Kompletní popis všech podtypů 802.11 rámců je uveden ve standardu IEEE 802.11 v tabulce 7-1[4].

2.2 Filtrace MAC adres a skrývání SSID

Jak již bylo uvedeno v kapitole 2.1.3, rámce typu *Beacon* jsou odpovědné za propagaci informace, že se v dané lokalitě nachází bezdrátová síť s určitým SSID. Většina přístupových bodů a bezdrátových routerů má možnost funkcionalitu propagace SSID vypnout jakožto další úroveň zabezpečení. Předpokladem je, že útočník nebude podnikat útok na síť, o jejíž existenci neví. Jedná se tedy o určitou aplikaci principu *Security through obscurity*. Klient, který se chce k takové síti připojit, musí ve svém suplikantu ručně zadat SSID bezdrátové sítě[10].

Další z možností mírného zvýšení zabezpečení bezdrátové sítě je zavedení řízení přístupu na základě kontroly MAC adresy klienta. Tento způsob řízení přístupu je obvykle implementován na přístupovém bodě, kde se nachází seznam MAC adres autorizovaných klientů. Pokud se klient, jehož MAC adresa není na seznamu povolených zařízení, pokusí o autentizaci a asociaci k síti, je přístupovým bodem odmítnut.

Způsob odhalení skrytého SSID stejně jako možnost obejití řízení přístupu na základě MAC adres jsou popsány v kapitole 3.1.

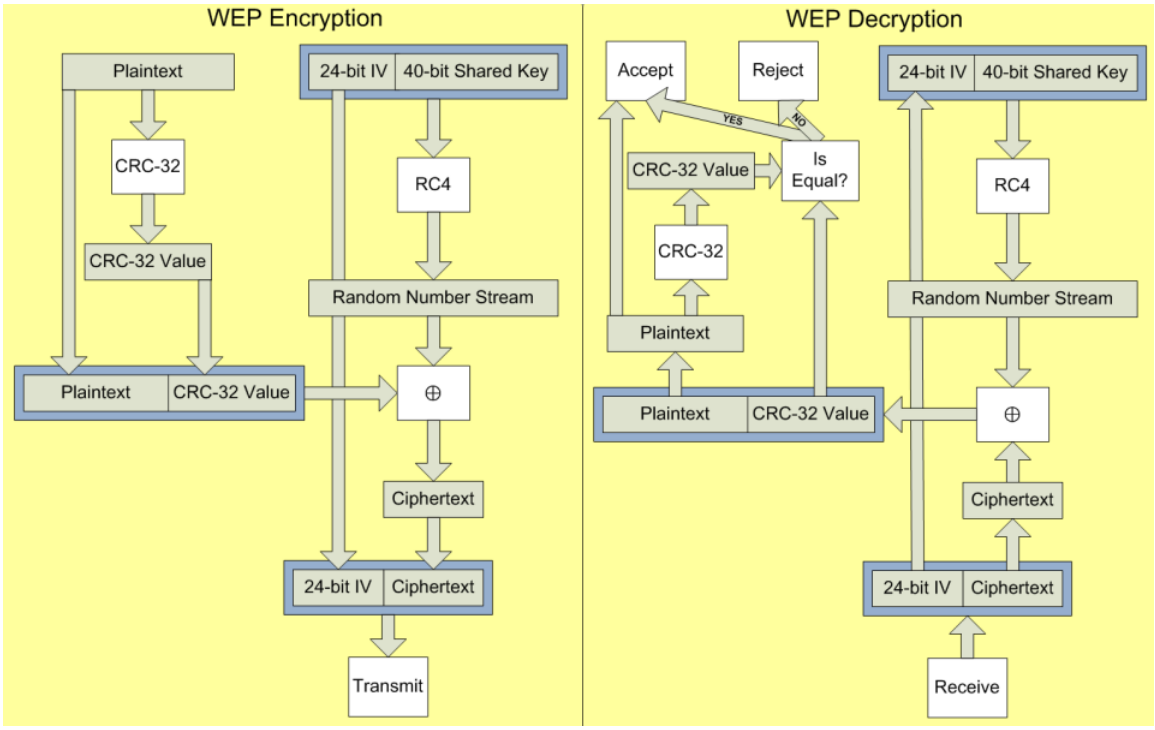
[10] Což je obvykle nutné pouze v případě prvního přihlášení, poté je možné využít možnost zapamatování daného SSID.

2.3 WEP

Protokol WEP (Wired Equivalent Privacy) se stal prvním bezpečnostním mechanismem sloužícím pro šifrování dat v rámci bezdrátového WiFi přenosu. Definice protokolu WEP byla součástí již původního standardu 802.11 z roku 1997. Jeho použití však nebylo standardem vynucováno, ale pouze doporučováno. WEP pro šifrování přenášených dat využívá symetrickou proudovou šifru RC4 (*Rivest Cipher 4*). Šifrování probíhá na druhé vrstvě ISO/OSI modelu.

Protokol podporuje použití 40 bitových nebo 104 bitových sdílených klíčů. Sdílený klíč je při operaci šifrování a dešifrování konkatenovaný s 24 bitovou hodnotou inicializačního vektoru. Tím je vytvořen 64 bitový nebo 128 bitový WEP klíč. Při šifrování algoritmem WEP je dále vytvořen 32 bitový kontrolní součet označovaný jako ICV (*Integrity Check Value*), který je připojen k přenášeným datům. WEP klíč, složený ze sdíleného klíče a inicializačního vektoru, je vstupem proudové šifry RC4, na jejímž výstupu je generována pseudonáhodná posloupnost nazývaná jako *Keystream*.

Vlastní šifrování je realizováno operací exkluzivního součtu mezi řetězcem *Keystream* a daty spolu s kontrolním součtem. K výsledným šifrovaným datům je připojen použitý inicializační vektor, který je příjemcem použit pro dešifrování. Operace dešifrování potom probíhá inverzním postupem. Celý proces šifrování a dešifrování je graficky znázorněn na obrázku 2.5.



Obrázek 2.5: Šifrování a dešifrování protokolem WEP. Převzato z [7]

V případě, že by ve výše uvedeném postupu nebyly využívány inicializační vektory, pak by zašifrování stejné zprávy symetrickou šifrou se stejným sdíleným klíčem pokaždé generovalo stejnou šifrovanou zprávu. To by mělo negativní vliv na bezpečnost a usnadnilo by kryptoanalýzu výsledných kryptogramů. Náhodně generované hodnoty inicializačního

vektoru tak slouží jako řešení tohoto problému.

Jak již bylo uvedeno výše, pro kontrolu integrity přeneseného rámce je využit 32 bitový kontrolní součet vytvořený algoritmem CRC-32 (*Cyclic Redundancy Check 32 bits*). Z lineární podstaty funkce CRC však vyplývá zranitelnost protokolu WEP spočívající v možnosti modifikace dat šifrovaného rámce a dopočítání korektního kontrolního součtu, a to následujícím způsobem[8]:

- Mějme šifrovaná data, kde *C* je vlastní šifrovaná správa a ICV je šifrovaný kontrolní součet.
- Vytvoříme bitovou masku *M* a provedeme *C' = M XOR C*, kde *C'* jsou šifrovaná data upravená pomocí masky na požadovanou hodnotu.
- Vypočteme *ICV' = CRC-32(M)*, kde *ICV'* je CRC kontrolní součet vytvořené masky.
- Vypočteme novou hodnotu kontrolního součtu *ICV" = ICV XOR ICV'*.
- Nyní máme šifrovaný rámec s daty *C'* a kontrolním součtem *ICV"*, který bude příjemcem korektně přijat.

Na tomto principu úpravy šifrovaných dat jsou založeny některé z útoků vůči protokolu WEP popsané níže.

Mechanismus WEP se sdíleným klíčem podporuje dvě metody autentizace klienta k síti. Ať je použita libovolná z těchto metod, vždy se jedná pouze o jednosměrnou autentizaci klienta vůči přístupovému bodu. Protokol WEP nepodporuje vzájemnou autentizaci. Následuje popis obou autentizačních metod:

- **Open System** - Prvním typem autentizace podporovanou protokolem WEP je tzv. *Open System* autentizace. V tomto režimu ve skutečnosti ani k žádné autentizaci nedochází. Klient zašle přístupovému bodu rámec *Authentication request* bez poskytnutí jakýchkoliv přístupových údajů a přístupový bod automaticky odpoví rámcem *Auhentication Success*. Po této autentizaci dojde k asociaci klienta k bezdrátové síti a započetí komunikace. Pokud však klient nezná sdílený klíč, asociace k síti se nezdaří. Faktická autentizace klienta tak prakticky probíhá právě až ve fázi asociace.
- **Shared Key** - Autentizace typu *Shared Key* probíhá následujícím způsobem. Klient stejně jako v předchozím případě započne komunikaci odesláním rámce *Authentication request* na přístupový bod. Přístupový bod klientovi odpoví rámcem, který obsahuje 1024 bitů dlouhou náhodnou hodnotu nazývanou *Challenge* a dále 24 bitový inicializační vektor. Klient hodnotu *Challenge* zašifruje pomocí sdíleného klíče a inicializačního vektoru a výslednou hodnotu pošle přístupovému bodu. Přístupový bod provede stejnou operaci a výsledek porovná s hodnotou obdrženou od klienta. Pokud se tyto hodnoty rovnají, klient prokázal znalost sdíleného klíče a je mu umožněno asociovat se k síti. Tento režim autentizace obsahuje vážnou zranitelnost, která může vést až ke kompromitaci sdíleného klíče. Pokud útočník odchytí zprávu *Challenge* zasílanou z přístupového bodu klientovi a zachytí taktéž odpověď klienta, může využít inverzní vlastnosti operace XOR a z těchto dvou odchycených hodnot získat platný *Keystream*. Ten poté může být využit k injekci paketů, které budou v rámci šifrované sítě přijaty. Injekcí podvržených ARP paketů může útočník vygenerovat v rámci sítě vysoký provoz s cílem nasbírat dostatečné množství inicializačních vektorů. Nad

množinou zachycených inicializačních vektorů může být poté zahájen statistický útok s cílem získat otevřenou podobu sdíleného klíče. Odchycený *Keystream* může být taktéž využit k provedení autentizace, kdy útočník nad obdrženým *Challenge* řetězcem provede operaci XOR se získaným řetězcem *Keystream* a vytvoří tak validní odpověď, na kterou přístupový bod reaguje asociací útočníka k síti. Z těchto důvodů je doporučované v případě nutnosti použít zabezpečení WEP využít *Open System* autentizaci, která netrpí výše uvedenou zranitelností.

První zranitelnosti protokolu WEP byly publikovány v roce 2001 v článku *Intercepting Mobile Communications: The Insecurity of 802.11*[8]. Ian Golberg v rámci tohoto článku upozornil na množství nedostatků přímo v návrhu symetrické šifry RC4, které umožňují narušení integrity, důvěrnosti a autenticity šifrované komunikace. Právě v tomto článku byla poprvé popsána metoda editace šifrovaného rámce a také zranitelnost autentizace v režimu *Shared Key*. V tom samém roce byla publikována statistická metoda založená na výskytu slabých inicializačních vektorů a jejich opakování v rámci šifry RC4, teoreticky popisující možnost zjištění sdíleného klíče[15]. Tato metoda byla pojmenována *FMS* podle prvních písmen jejích autorů[11]. V roce 2002 byla metoda *FMS* prakticky využita k útoku vedoucímu ke kompromitaci sdíleného WEP klíče. Tato metoda vyžadovala zachycení více než milionu paketů[34]. V roce 2004 publikoval bezpečnostní výzkumník s přezdívkou KoreK vylepšení předchozí metody, kdy ke kompromitaci WEP klíče postačuje zhruba 500 000 paketů. V roce 2007 přichází trojice vědců Pychkine, Tews a Weinmann s další optimalizací, jež k úspěšné kompromitaci vyžaduje již pouze zhruba 60 000 paketů[37].

Kromě postupného zlepšování statistické metody zaměřené na získání WEP klíče byly zveřejňovány útoky sloužící k vygenerování provozu v rámci dané sítě s cílem urychlit sběr požadovaného množství paketů. Těmito útoky jsou jmenovitě například *ARP injection*, *Fragmentation attack*, *KoreK Cochchop*, *Hirte* či *Caffe Latte*. V současné době existuje množství nástrojů, které automatizují útok vůči WEP klíčům a umožňují tak útok provést i méně zkušeným jedincům bez potřeby znát detaily či princip daného útoku. Uvedené útoky nebudou v rámci této práce podrobně popisovány, jelikož hlavní těžiště práce spočívá v popisu bezpečnostních technologií využívaných v případě WiFi sítí s autentizací dle standardu 802.1X.

Reakcí na zveřejňování slabin protokolu WEP bylo jeho postupné upravování spočívající například v zesílení šifrování[12], zvětšení prostoru inicializačních vektorů na 128 bitů či odstranění slabých inicializačních vektorů[11]. Žádná z těchto změn však nebyla standardizována a v současné době je doporučené jako náhradu za WEP využít protokol WPA, který je popsán v následující kapitole. Použití standardu WEP není doporučováno taktéž organizací WiFi Alliance a WEP tak postupně přestává být podporovaný firmwarem nových bezdrátových zařízení.

2.4 WPA Personal

Označení WPA Personal se vztahuje na použití standardu WPA (*Wi-fi Protected Access*) spolu se sdíleným klíčem. Použití WPA spolu s autentizací dle standardu 802.1X je souhrnně označováno jako WPA Enterprise a je popsáno v kapitole 2.5.

[11] Jimiž byli Scott Fluhler, Itsik Mantin a Adi Shamir
[12] Použití 256 bitových klíčů

2.4.1 WPA

Spolu s postupným objevováním bezpečnostních trhlin šifrovacího algoritmu RC4, na kterém je postaven protokol WEP, sílila potřeba modernějšího a bezpečnějšího kryptografického mechanismu pro bezdrátové sítě. Tím se stal v roce 2002 mechanismus WPA využívající algoritmus TKIP (*Temporal Key Integrity Protocol*) označovaný také jako WPA-TKIP. Zabezpečení WPA vychází z draftu standardu 802.11i a bylo vydáno s důrazem na rychlou opravu nedostatků zabezpečení WEP bez nutnosti zásahů do hardware bezdrátových zařízení. Jednalo se tak pouze o dočasné řešení, zatímco pokračovaly práce na dokončení standardu 802.11i[27].

Jedna z hlavních slabin protokolu WEP spočívá v použití sdíleného symetrického klíče všemi klienty po celou dobu jejich komunikace. Algoritmus TKIP použitý v rámci WPA využívá namísto jednoho sdíleného klíče celou hierarchii klíčů s cílem dynamické změny použitého šifrovacího klíče v rámci jedné komunikace[7]. Pro kontrolu integrity rámce je využit algoritmus MIC (*Message Integrity Check*) označovaný jako *Michael* generující 64 bitový kontrolní součet. Pokud algoritmus *Michael* detekuje během jedné minuty přijetí dvou rámců, které neprošly testem integrity, je okamžitě provedena reasociace klienta, mající za následek vygenerování nových šifrovacích klíčů. Oproti protokolu WEP je v rámci WPA implementována ochrana proti Replay útoku, a to za pomocí využití sekvenčního čísla rámce. Pokud je přijat rámec, jehož sekvenční číslo je nižší než aktuální, je rámec zahozen.

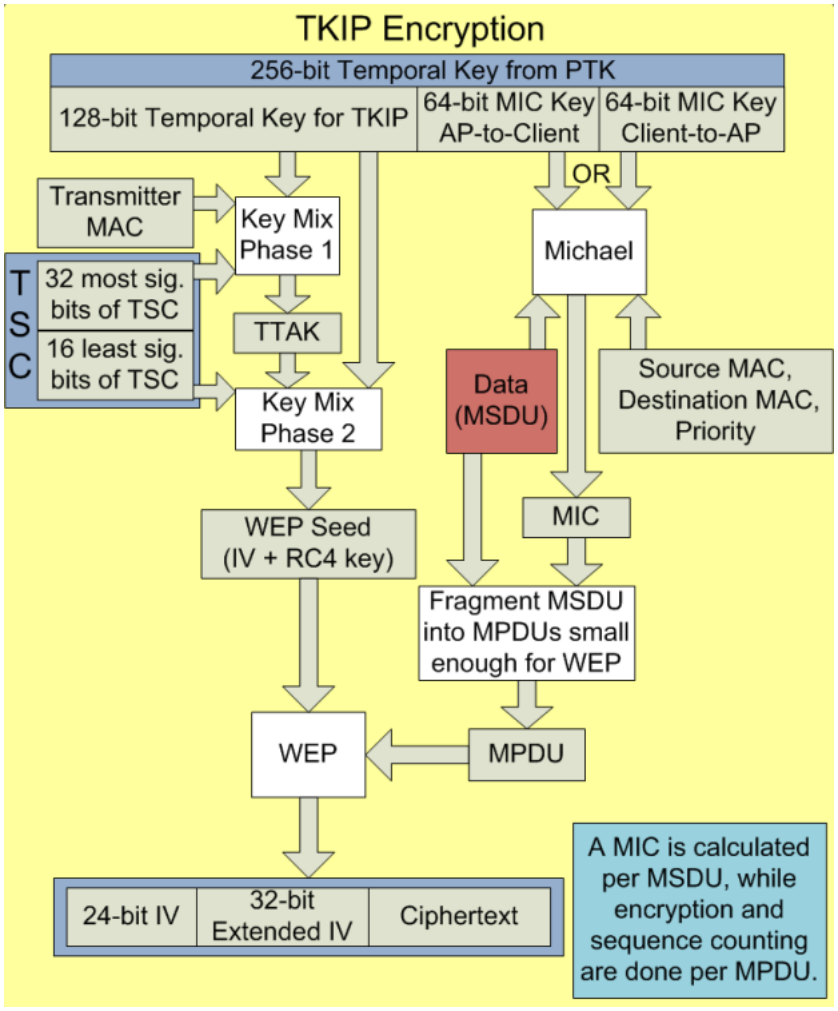
Výhodou protokolu WPA-TKIP oproti jeho nástupci WPA2 je možnost jeho použití v zařízeních, která původně podporovala pouze protokol WEP, a to bez jakékoliv hardwarové úpravy, pouze aktualizací použitého firmware. To z toho důvodu, že algoritmus TKIP tvoří jakousi „obálku“ protokolu WEP, zdokonalující jeho vlastnosti a přidávající mnohá vylepšení s cílem zabránit útokům popsaným proti protokolu WEP. Celý postup šifrování i zapouzdření protokolu WEP v rámci algoritmu TKIP je znázorněn na obrázku 2.6.

V roce 2008 byl publikován první útok na algoritmus TKIP nazvaný *Beck-Tews* po jeho autorech. Útok je rozšířením útoku *KoreK chochop* vůči protokolu WEP, který je založen na hádání hodnot jednotlivých bajtů zachyceného rámce, což vede k jeho kompletnímu dešifrování a následnému získání platného *Keystream*. Obranou proti útoku tohoto typu na TKIP je vlastnost algoritmu *Michael* popsaná výše, kdy je při detekci dvou rámců s porušenou integritou během jedné minuty provedena reasociace a následná změna použitých klíčů. Útok *Beck-Tews* však tomuto předchází vložením minutového intervalu před každý pokus o hádání hodnoty daného bajtu. Dešifrování rámce tak trvá déle[13] než v případě útoku *KoreK chochop*, ale přesto je možné dešifrovat celý paket a tím získat validní *Keystream*. Ochrana proti replay útoku je potom obejita prostřednictvím QoS (*Quality of Service*) kanálu a ve výsledku je tak možné do komunikace injektovat platný rámec[38].

V roce 2009 japonští vědci Toshihiro Ohigashi a Masakatu Morii zdokonalili *Beck-Tews* útok. *Ohigashi-Morii* útok předpokládá scénář MitM (*Man in the Middle*). Tím je odstraněna podmínka nutnosti podpory služby QoS přístupovým bodem a klientským zařízením a pomocí dalších optimalizací byl celkový čas na provedení útoku redukován na zhruba 1 minutu[25].

Ani jeden z výše uvedených útoků však nevede k získání otevřené podoby sdíleného šifrovacího klíče. WPA-TKIP splnil svůj cíl, a to překlenout období, kdy se WEP ukázal být z bezpečnostního hlediska naprosto nevyhovujícím. Přesto však není již v současné době doporučené protokol WPA-TKIP používat, hlavně pokud je daná bezdrátová WiFi síť součástí síťové infrastruktury organizace či společnosti, jejíž kompromitace by s sebou

[13] Autory je uváděn čas 12 - 15 minut



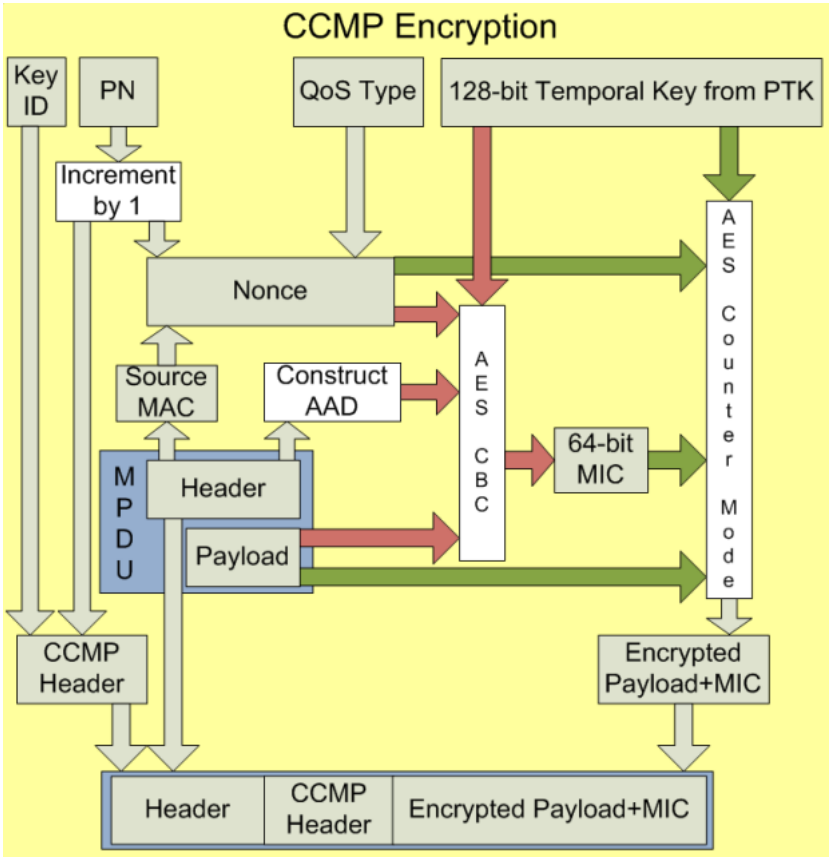
Obrázek 2.6: Šifrování algoritmem TKIP. Převzato z [7]

nesla finanční, reputační či jiná rizika. Namísto WPA-TKIP je doporučené použít jeho nástupce WPA2, který bude popsán v následující kapitole.

2.4.2 WPA2

Protokol WPA2 je definován standardem 802.11i z roku 2004 a je někdy též označován jako WPA2-CCMP či WPA2-AES. Tento standard již smazal veškeré vazby na zastaralý bezpečnostní protokol WEP a využívá protokol CCMP (*Counter Cipher Mode with Block Chaining Message Authentication Code Protocol*). CCMP používá šifrovací algoritmus AES (*Advanced Encryption Standard*) v režimu CCM (*Counter Mode with CBC-MAC*) se 128 bitovým klíčem a zajišťuje důvěrnost, integritu i autenticitu přenášených dat a eliminuje tak všechny předchozí útoky popsané vůči protokolu WEP nebo WPA-TKIP. Integrita dat uvnitř přenášeného rámce je zajišťována 64 bitovou hodnotu MIC (*Message Integrity Check*), která je šifrována spolu s daty. Celý proces šifrování prostřednictvím CCMP je zobrazen na obrázku 2.7. WPA2 může na některých zařízeních fungovat v tzv. WPA2-Mixed režimu, kdy je prioritně využit standard WPA2, avšak pokud daný klient tento

standard nepodporuje, je použit WPA-TKIP.



Obrázek 2.7: Šifrování algoritmem CCMP. Převzato z [7]

Přestože standard 802.11i eliminoval veškeré zranitelnosti předchozích protokolů WEP a WPA-TKIP, byl v roce 2010 publikován útok vedoucí k možnosti podvržení rámců v šifrované komunikaci. Při útoku je využit GTK (*Group Temporal Key*), což je jeden z klíčů klíčové hierarchie protokolu CCMP. Tento klíč je shodný pro všechny připojené klienty a slouží k šifrování komunikace přístupového bodu směrem ke skupině klientů. Z toho vyplývá, že před provedením útoku je nutné mít do dané sítě přístup. V rámci standardu 802.11i neexistuje žádný mechanismus, který by kontroloval podvrhnutí rámců šifrovaných GTK klíčem[3]. Útočník může tuto zranitelnost využít například pro provedení *ARP cache poisoning* útoku, pomocí kterého lze komunikaci autorizovaného klienta přesměrovat přes počítač útočníka. Takovýto útok je navíc z jeho podstaty velice těžko detekovatelný. Zranitelnost bývá označována jako *Hole 196*, a to z důvodu, že uvedená vlastnost GTK klíče je uvedena ve standardu 802.11i na straně 196[5].

I přes tento nedostatek zůstává WPA2 jediným doporučeným bezpečnostních mechanismem pro zabezpečení bezdrátové WiFi sítě s autentizací na základě sdíleného klíče.

2.5 WPA Enterprise

WPA-Enterprise je pojem, jehož význam není je standardu 802.11i definován. Obecně je takto označováno nasazení bezdrátové LAN v kombinaci s autentizačním standardem **IEEE**

802.1X. Pokud v této práci dále budou zmíněny pojmy WPA-Enterprise či podniková WiFi síť, bude jimi vždy myšlena bezdrátová LAN síť založená na protokolu 802.1X[14].

Hlavní výhodou WPA Enterprise sítí je pohodlná možnost správy vysokého počtu uživatelů. Zatímco u přechozích typů zabezpečení (WEP, WPA Personal) se všichni uživatelé bezdrátové sítě přihlašují se stejným (sdíleným) klíčem, ve WPA Enterprise síti má každý uživatel svůj vlastní pár přihlašovacích údajů, případně vlastní klientský certifikát. Tento fakt zpřehledňuje správu uživatelů a také zjednodušuje monitoring a možnost dohledání konkrétního uživatele v případě incidentu. Odebrání možnosti přístupu k síti určitému klientovi je otázka zablokování jednoho účtu, zatímco v síti se sdíleným heslem by tato situace musela být řešena změnou sdíleného klíče, čímž by tato změna zasáhla všechny uživatele dané bezdrátové sítě.

Autentizace klienta ve WPA-Enterprise sítích je založena na protokolu IEEE 802.1X, který slouží pro řízení přístupu k síti. Protokol byl původně vytvořen pro metalické LAN sítě, avšak s nástupem WiFi technologie našel uplatnění i u bezdrátových sítí. V architektuře WiFi sítě založené na standardu IEEE 802.1X vystupují následující tři entity:

- **Klient** - Někdy též označovaný jako suplikant. Klientem může být počítač, PDA, síťová tiskárna, mobilní telefon nebo například výrobní zařízení. Podmínkou je, aby software klienta podporoval autentizaci prostřednictvím 802.1X standardu.

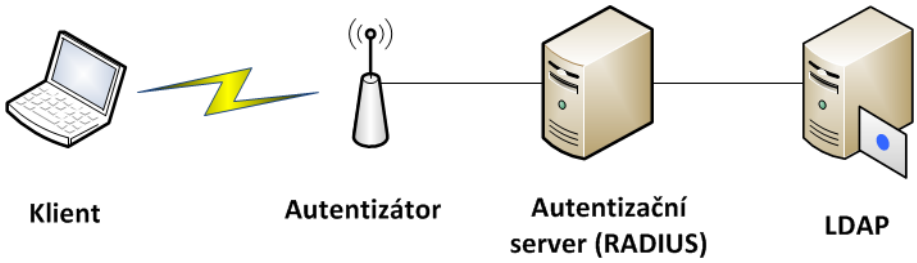
- **Autentizátor** - Autentizátor vystupuje v procesu přihlašování klienta k síti především jako prostředník, který přeposílá požadavky a odpovědi mezi klientem a autentizačním serverem. Autentizátorem je obvykle aktivní bezdrátový síťový prvek (Switch, Access Point) s podporou standardu 802.1X. Nejrozšířenějším komunikačním protokolem mezi autentizátorem a autentizačním serverem je RADIUS (Remote Authentication Dial In User Service). Protokol RADIUS je blíže popsán v kapitole 2.5.1.

- **Autentizační server** - Funkcí autentizačního serveru je na základě autentizačních údajů rozhodnout, zda bude klientovi umožněno připojení do sítě. Autentizační server vyhledává autentizační údaje v textových souborech, LDAP, Active Directory či SQL databázi. Pokud není databáze přihlašovacích údajů uložena přímo na autentizačním serveru, vystupuje v architektuře sítě s autentizací dle standardu 801.1X zvláštní server plnící právě tuto úlohu. Tímto serverem je většinou databázový server, LDAP server, Kerberos, případně kontroler Windows domény. Schéma WiFi 801.1X architektury je zachyceno na obrázku 2.8. V případě použití protokolu RADIUS je autentizační server označován jako RADIUS server. V současné době existuje mnoho komerčních (například implementace od firem Cisco System či RSA) i opensource (Freeradius[15], BSDradius[16]) implementací RADIUS serveru.

2.5.1 RADIUS

RADIUS je komunikační protokol používaný mezi autentizátorem (NAS, Network Access Server) a autentizačním serverem sloužící primárně k autentizaci klienta do sítě. Protokol kromě centralizované autentizace zajišťuje také autorizaci k síťovým službám a accounting

[14] Dále v práci pak taková síť bude zkráceně nazývána 802.1X WiFi síť
[15] http://freeradius.org/
[16] http://www.bsdradius.org/



Obrázek 2.8: Schéma WiFi 802.1X architektury

(tento termín je někdy překládán jako tarifikace). Tyto služby se obvykle označují zkratkou AAA (Authentication, Authorization, and Accounting) a jsou popsány v RFC 2865[17] a RFC 2866[18].

Protokol byl vyvinutý společností Livingston Enterprises v roce 1991 a v roce 1995 byl uznán jako IETF (Internet Engineering Task Force) standard[19]. RADIUS protokol používá protokol UDP, tedy nespojovaný protokol transportní vrstvy. RADIUS server obvykle naslouchá na UDP portu 1812 pro autentizaci a 1813 pro accounting. IETF v současné době připravuje drafty pro RADIUS protokol přes TCP[20] a také TLS/SSL šifrování pro RADIUS[21]. Autentizace klienta do sítě sestává z následujících zpráv:

- **Access-Request** – NAS posílá RADIUS serveru požadavek na autentizaci klienta. Tento požadavek obsahuje uživatelské jméno, heslo a dalšími údaje jako například IP adresu NAS serveru, číslo a typ portu či MTU. Heslo není mezi NAS a RADIUS serverem přenášeno v otevřené podobě, a to ani při použití autentizačního protokolu PAP (Password Authentication Protocol – nejjednodušší autentizační protokol, klient se autentizuje heslem, které je odesíláno v otevřené podobě). K zabezpečení hesla je použit tajný řetězec, jehož znalost je sdílena NAS i RADIUS serverem, v kombinaci s MD5 hashovací funkcí.
- **Access-Reject** - Tato zpráva je vrácena klientovi, pokud poskytl neplatné přihlašovací údaje či nemá povolený přístup do sítě.
- **Access-Challenge** – Tuto zprávu zasílá RADIUS server jako odpověď na Access-Request v případě použití sofistikovanějších autentizačních protokolů vytvářejících šifrované tunely. Server si tímto způsobem žádá o další informace.
- **Access Accept** – Zpráva Access Accept je vrácena klientovi v případě, že byl úspěšně autentizován do sítě.

Pro přenos informací v požadavcích a odpovědích je v rámci protokolu RADIUS použita datová struktura AVP - *Attribute Value Pairs*. Ta obsahuje vždy typ atributu, jeho délku a hodnotu.

Alternativou k protokolu RADIUS je protokol DIAMETER, která má ambice do budoucna RADIUS zcela nahradit[22][27]. Změnou oproti RADIUS protokolu je komunikace

[17] http://tools.ietf.org/html/rfc2865
[18] http://tools.ietf.org/html/rfc2866
[19] http://www.interlinknetworks.com/app_notes/History%20of%20RADIUS.pdf
[20] http://tools.ietf.org/html/draft-ietf-radext-tcp-transport-09
[21] http://tools.ietf.org/html/draft-ietf-radext-radsec-09
[22] Na nástupnictví upozorňuje i svým jménem: RADIUS (poloměr) vs. DIAMETER (průměr)

prostřednictvím spolehlivého protokolu (TCP nebo SCTP), podpora oznamování chyb nebo snadná rozšiřitelnost. Mírnou nevýhodou pro budoucí rychlé rozšíření může být skutečnost, že DIAMETER není plně zpětně kompatibilní s RADIUS protokolem. Vlastní autentizační protokol vyvinula i společnost Cisco System pod označením TACACS[23]. V současné době je využíván jeho nástupce TACACS+.

2.5.2 EAP, EAPOL

Srdcem standardu 802.1X je protokol EAP (Extensible Authentication Protocol). EAP bývá označován jako autentizační framework, jelikož poskytuje zapouzdření pro různé autentizační metody. Komunikace probíhá na druhé vrstvě ISO/OSI modelu. Protokol EAP je v rámci 802.1X architektury využit pro komunikaci mezi klientem a autentizátorem. V komunikaci mezi autentizátorem a autentizačním serverem pak dochází k jeho zapouzdření do protokolu RADIUS popsaného v předcházející sekci.

Obecně lze komunikaci pomocí EAP protokolu mezi klientem a autentizátorem popsat jako sérii následujících kroků[1]:

1. Klient započne komunikaci (EAPOL-Start)
2. Autentizátor vyžádá identitu klienta (EAP-Request-Identity)
3. Klient zašle svoji identitu (EAP-Response-Identity)
4. Autentizátor přepošle klientovi informace o zvolené EAP metodě, v závislosti na této metodě může zpráva obsahovat challenge řetězec (EAP-Request-Method)
5. Klient potvrdí použití dané EAP metody a v závislosti na této metodě přiloží challenge-response řetězec (EAP-Response-Method)
6. Výměna a kontrola certifikátů (Pouze u některých metod)
7. V případně validních přihlašovacích údajů je klient autentizován (EAP-Success), jinak je odmítnut (EAP-Failure)
8. Pokud na je WiFi síti nasazeno šifrování (WEP nebo WPA), proběhne výměna a generování šifrovacích klíčů (tzv. keyring material) (EAPOL-Key)

Metod protokolu EAP používaných v metalických LAN sítích existuje nepřeberné množství. Standard WPA v kombinaci s 802.1X z roku 2004 (jedná se o standard IEEE 802.11i-2004) původně zahrnoval pouze metodu EAP-TLS. V roce 2005 WiFi Alliance[24] certifikovala další 4 EAP metody pro použití v WLAN sítích[25]:

- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

[23] Terminal Access Controller Access-Control System

[24] Nezisková organizace zajišťující správu a řízení celosvětově uznávaných standardů pro adaptaci a lepší kompatibilitu hardware, použitého ve WLAN sítích

[25] http://www.wi-fi.org/news_articles.php?f=media_news&news_id=25

V roce 2009 byly certifikovány zatím poslední dvě EAP metody, a to[26]:

- EAP-FAST
- EAP-AKA.

Celkový výčet EAP metod certifikovaných organizací WiFi Alliance pro použití ve WiFi sítích spolu s roky certifikace zobrazuje tabulka 2.3.

EAP metoda	Rok certifikace
EAP-TLS	2003
EAP-TTLS/MSCHAPv2	2005
PEAPv0/EAP-MSCHAPv2	2005
PEAPv1/EAP-GTC	2005
EAP-SIM	2005
EAP-FAST	2009
EAP-AKA	2009

Tabulka 2.3: Metody protokolu EAP certifikované organizací WiFi Alliance

Porovnání jednotlivých EAP metod je uvedeno v kapitole zabývající se jejich bezpečností v tabulce 3.1. Konkrétní specifika jednotlivých EAP metod jsou podrobně popsána v následujících podkapitolách.

Struktura paketu

Struktura paketu protokolu EAP je znázorněna na obrázku 2.9. Prvních 16 bitů paketu udává typ paketu, který může nabývat následujících hodnot:

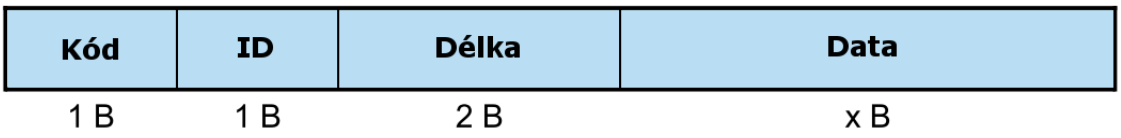
- 1 - Request (Žádost)
- 2 - Response (Odpověď)
- 3 - Success (Úspěšná autentizace)
- 4 - Failure (Neúspěšná autentizace)

Identifikátor slouží k identifikaci rámců náležejících ke stejnému komunikačnímu toku. Pole Délka udává délku celého rámce. V sekci Data jsou potom u určitých typů EAP paketů přenášena dodatečná data. Může se tak jednat například o uživatelské jméno nebo autentizační data. První bajt pole Data je vyhrazen pro určení typu EAP paketu. Typ EAP paketu může nabývat následujících hodnot[27]:

- 1 - Identity: požadavek/odpověď ohledně identity autentizovaného
- 2 - Notification: sdělení pro autentizovaného
- 3 - Nak: odmítnutí typu autentizace (pouze odpověď)

[26] http://www.wi-fi.org/news_articles.php?f=media_news&news_id=817
[27] Z důvodu velkého množství typů EAP paketů jsou uvedeny pouze základní typy

- 4 - EAP-MD5 Challenge (Message Digest 5)
- 5 - EAP-OTP (One Time Password)
- 13 - EAP-TLS
- 15 - RSA SecurID EAP (autentizace pomocí RSA tokenu)
- 17 - LEAP (Lightweight EAP)
- 21 - EAP-TTLS (Tunneled TLS EAP)
- 25 - PEAP (Protected EAP)
- 42 - EAP-FAST (EAP Flexible Authentication via Secure Tunneling)



Obrázek 2.9: Struktura EAP paketu

Možnost skrytí identity

U EAP metod, které pro autentizaci využívají šifrovaný point-to-point tunel mezi klientem a RADIUS serverem, dochází k přenosu uživatelského jména v rámci tohoto kanálu. Zároveň je však uživatelské jméno přenášeno v čitelné podobě ještě před sestavením šifrovaného kanálu prostřednictvím paketu EAP-Identity-Response. Na místo tohoto jména je možné nastavit libovolný řetězec (typicky je bezdrátovými klienty nastaven na „Anonymous“) jako obranu před odposlechnutím tohoto údaje. Možnost nastavit anonymizaci uživatelského jména v EAP-Identity-Response paketu závisí na použitém klientovi. Nativní klient MS Windows tuto možnost nenabízí, na rozdíl například od klienta Odyssey Access Client[28] od společnosti Juniper Networks.

Fast Reconnect

Fast Reconnect, někdy také *Session Resumption*, je vlastnost EAP metody, která dovoluje klientovi pohybovat se mezi jednotlivými přístupovými body dané sítě, aniž by musel po asociaci k novému přístupovému bodu znovu zadávat své přihlašovací údaje[29]. Tato vlastnost je podporována metodami PEAP a EAP-TTLS.

[28] http://www.juniper.net/us/en/products-services/software/ipc/odyssey-access-client/oac/
[29] http://technet.microsoft.com/en-us/library/cc757996%28WS.10%29.aspx

EAPOL

Protokol EAPOL (EAP over LAN) poskytuje zapouzdření protokolu EAP na LAN sítích. Původně byl navržen pro standard IEEE 802.3 (Ethernet), ale později byl uznán za vhodný i pro použití na IEEE 802.11 sítích. Rozlišujeme následující typy EAPOL paketů:

- **EAP-Packet** (typ 0) – Tento typ EAPOL paketu značí, že daný paket obsahuje zapouzdřený EAP paket.
- **EAPOL-Start** (typ 1) – Značí počátek komunikace, tímto typem EAPOL paketu dává klient autentizátoru na vědomí, že má zájem o autentizaci.
- **EAPOL-Logoff** (typ 2) – Tímto typem paketu dává klient autentizátoru na vědomí, že si přeje odpojení ze sítě. Autentizátor na tuto zprávu reaguje převedením portu klienta do neautorizovaného stavu až do doby další úspěšné autorizace.
- **EAPOL-Key** (typ 3) – V případě, že je na WiFi síti nasazeno šifrování (WEP, WPA), slouží tento typ zprávy pro výměnu šifrovacích klíčů mezi klientem a autentizátorem. Přesný postup výměny klíčů v původním standardu IEEE 802.1X-2001 chyběl a byl doplněn v aktualizovaném vydání IEEE 802.1X-2004.
- **EAPOL-Encapsulated-ASF-Alert** (typ 4) – zavedeno ASF (Alert Standards Forum) a slouží pro zasílání upozornění (například SNMP trap) přes neautorizované porty.

Typy 5 až 255 EAPOL paketu jsou dle aktuálního standardu IEEE 802.1X rezervovány pro budoucí využití. Komunikace prostřednictvím EAPOL protokolu probíhá pouze mezi klientem a autentizátorem, není tedy dále přeposílána na autentizační server tak, jako je tomu v případě komunikace prostřednictvím protokolu EAP. Následuje popis jednotlivých metod protokolu EAP využíván v bezdrátových WiFi sítích.

2.5.3 EAP-MD5

Metoda EAP-MD5 je popsána v RFC 3748 a je zároveň IETF standardem. Jedná se o jednu z nejjednodušších EAP metod poskytujících velice nízkou úroveň bezpečnosti. Ta vyplývá z faktu, že heslo je přenášeno po síti ve formě MD5 hashe, který je náchylný vůči útoku hrubou silou a slovníkovému útoku. Metoda navíc podporuje pouze jednosměrnou autentizace, tedy že klient je autentizován vůči serveru, avšak klient již nezjistí autenticitu serveru. Metoda je tak zároveň náchylná na útok Man in the Middle.

EAP komunikace prostřednictvím metody EAP-MD5 probíhá následujícím způsobem (v závorkách jsou uvedeny typy EAP paketu):

- Autentizátor zašle klientovi výzvu na zadání identity. Volitelně je součástí tohoto EAP rámce také identita autentizátoru. (*EAP-Identity-Request*)
- Klient odpoví EAP rámcem obsahujícím jeho identitu - uživatelské jméno. (*EAP-Identity-Response*)
- Autentizátor zašle klientovi MD5 challenge, pseudonáhodně vygenerovaný šestnáct bajtů dlouhý řetězec (*EAP-MD5-Challenge*)

- Pokud si klient nepřeje použít metodu EAP-MD5, zašle autentizátoru zprávu Legacy Nak, která zároveň obsahuje typ metody, kterou si klient přeje dále použít (*EAP-NAK*).
- Klient vytvoří MD5 response řetězec (taktéž 16B), který získá aplikováním hashovací funkce MD5 nad konkatenací identifikačního čísla MD5 challenge rámce, hesla a MD5 challenge řetězce. Řetězec MD5 challenge hraje v rámci tohoto postupu roli ochrany proti replay útoku, jelikož k autentizaci nelze použít dříve odchycenou hodnotu MD5 response (*EAP-MD5-Response*)
- V případě, že klient zadal platné přihlašovací údaje, je úspěšně autentizován a připojen do sítě (*EAP-Success*).
- V případě, že klient zadá neplatné přihlašovací údaje nebo je jeho účet zablokován, obdrží od autentizátoru zprávu Failure a vstup do sítě mu není povolen (*EAP-Failure*).

Další nevýhoda EAP-MD5 metody spočívá v absenci podpory dynamického generování klíčů. Z toho důvodu není metoda kompatibilní s šifrováním pomocí dynamického WEP a WPA. Jediné možné šifrování bezdrátové WiFi sítě v kombinaci s EAP-MD5 metodou je tak statický WEP, jež byl popsán v kapitole 2.3.

Vzhledem k výše uvedeným skutečnostem není nadále doporučené metodu EAP-MD5 používat. Bezpečnostní nedostatky a rizika vyplývající z nasazení této metody jsou popsána v kapitole 3.2.1. Podpora této metody u operačních systémů Windows byla odstraněna počínaje verzí Windows Vista. Změnou v registrech lze však podpora metody opět povolit[30].

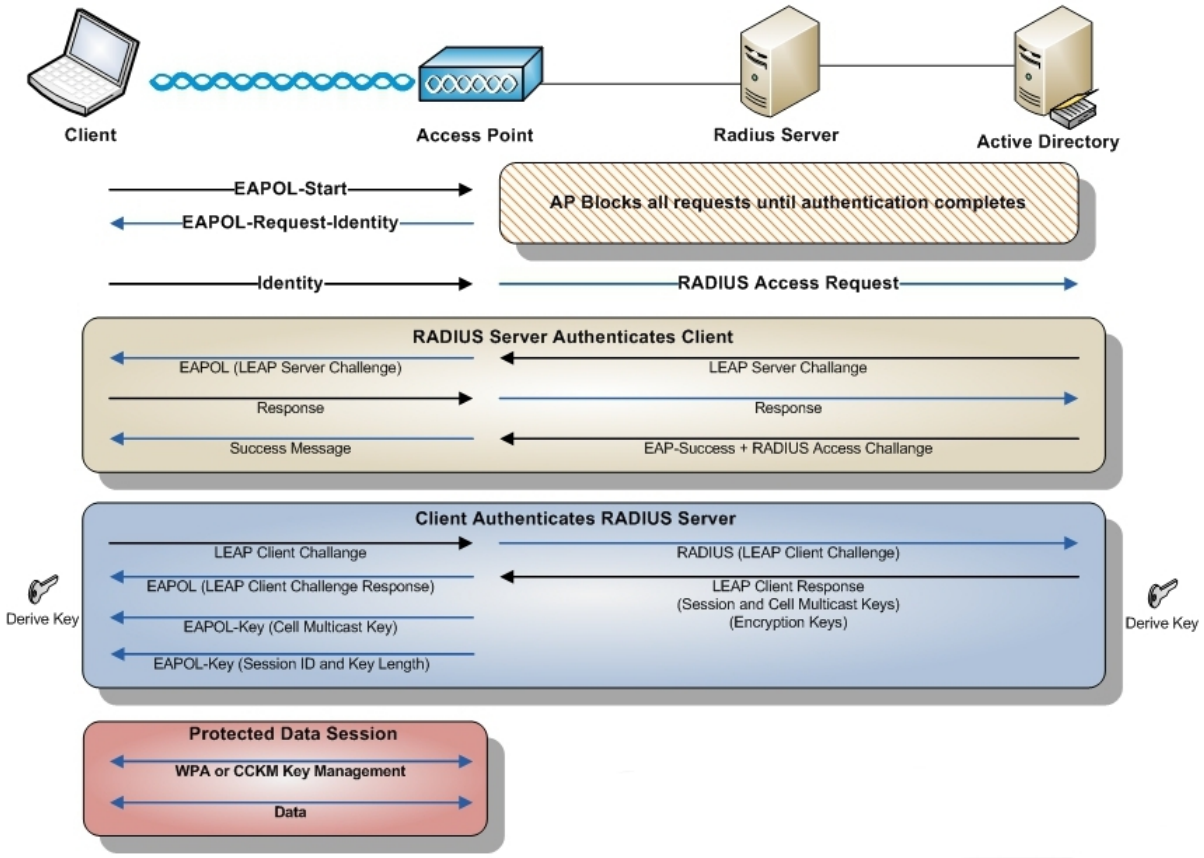
2.5.4 LEAP

EAP metoda LEAP, někdy též označovaná jako EAP-Cisco Wireless, je proprietární metoda publikovaná společností Cisco Systems[31] v roce 2000. Zkratka LEAP značí název *Lightweight Extensible Authentication Protocol*, ze kterého již vyplývá, že snahou bylo vytvořit odlehčenou metodu se zaměřením na snadnou použitelnost.

Stejně jako EAP-MD5 i LEAP používá pro autentizaci uživatelské heslo a jméno. Na rozdíl od EAP-MD5, kde je využit jednoduchý CHAP (*Challenge-handshake authentication protocol*) protokol pro autentizaci klienta vůči serveru, využívá LEAP modifikovaný protokol MS-CHAPv1(*Microsoft Challenge Handshake Authentication Protocol version 1*). Originální protokol MS-CHAP publikovaný společností Microsoft v roce 1998 a popsaný v RFC 2433[32] nepodporuje vzájemnou autentizaci. Právě v přidání podpory autentizace klienta vůči serveru i serveru vůči klientovi spočívá rozšíření tohoto protokolu společností Cisco[30]. Podpora vzájemné autentizace zvyšuje odolnost této metody vůči MitM (Man in The Middle) útoku. Přesná specifikace Ciscem upraveného MS-CHAPv1 protokolu je proprietární a tudíž není oficiálně popsána. Postup autentizace byl však získán metodou reverzního inženýrství[33].

Stejně jako u metody EAP-MD5 dochází k nešifrovanému přenosu challenge a challenge-response řetězce. Při znalosti algoritmu generování challenge-response řetězce je možné využít slovníkový útok pro získání původního hesla. Na tento nedostatek metody LEAP upozornil v roce 2003 jako první Joshua Wright[34]. Konkrétní popis zranitelnosti je uveden

[30] http://support.microsoft.com/kb/922574
[31] http://www.cisco.com
[32] http://tools.ietf.org/html/rfc2433
[33] http://lists.cistron.nl/pipermail/cistron-radius/2001-September/002042.html
[34] http://www.securityfocus.com/archive/1/340365/2003-10-03/2003-10-09/2



Obrázek 2.10: Autentizace prostřednictvím metody LEAP. Převzato z [12]

v kapitole 3.2.2.

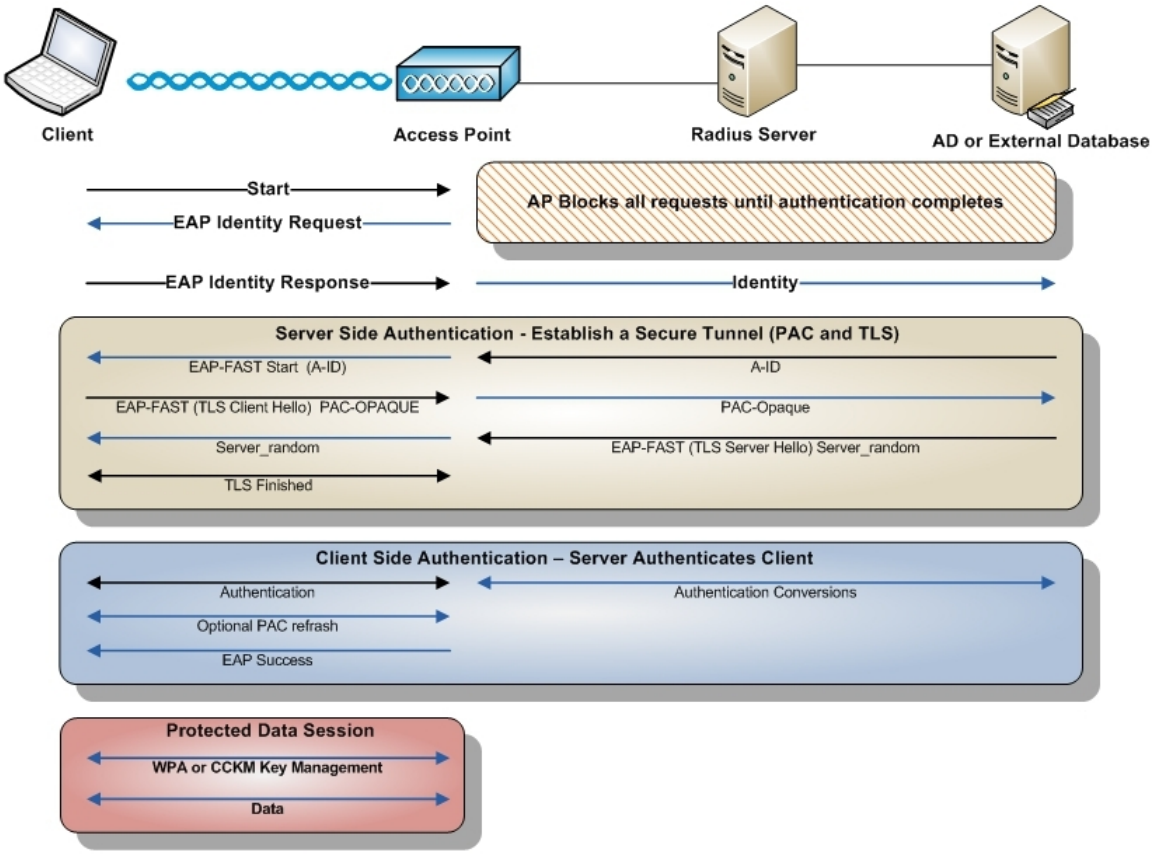
Komunikace mezi klientem a autentizátorem je obdobná jako u metody EAP-MD5 až na způsob, jakým je produkován *Challenge-Response* řetězec. Úspěšná autentizace klienta do sítě prostřednictvím metody LEAP je zachycena na obrázku 2.10.

Protokol LEAP nemá nativní podporu v žádné verzi OS Windows. V Mac OS X je LEAP podporován od verze OS X 10.4 Lion a v Linux s BSD systémech je podporován klientem wpa_supplicant.

Použití metody LEAP není nadále doporučováno samotnou společností Cisco Systems, která namísto ní doporučuje použít metodu EAP-FAST, která je brána jako faktický nástupce metody LEAP[2].

2.5.5 EAP-FAST

Metoda EAP-FAST (*Flexible Authentication via Secure Tunneling*) byla vytvořena společností Cisco Systems v roce 2007 jako reakce na objevení závažných bezpečnostních nedostatků v implementaci metody LEAP. Na rozdíl od svého předchůdce probíhá autentizace ve dvou fázích. V první fázi je sestaven zabezpečený šifrovaný point-to-point tunel mezi klientem a RADIUS serverem, autentizátor tak k této komunikace nemá přístup. Tunel je vytvořen na základě tzv. PAC (Protected Access Credentials), který je generován na RADIUS serveru a obsahuje unikátní klíč pro každého uživatele [30]. V druhé fázi proběhne



Obrázek 2.11: Autentizace prostřednictvím metody EAP-FAST. Převzato z [12]

skrze tento tunel autentizace pomocí algoritmu MS-CHAPv2, který zajišťuje vzájemnou autentizaci. Funkce jednotlivých fází metody EAP-FAST jsou uvedeny v tabulce 2.4. Autentizace prostřednictvím metody EAP-FAST je pak zachycena na obrázku 2.11.

V případě nasazení této EAP metody je nutné řešit distribuci PAC souborů jednotlivým uživatelům. To je obvykle řešeno zavedením nulté fáze autentizace, kdy automaticky dojde k předání obsahu PAC ze serveru klientovi prostřednictvím algoritmu Diffie-Hellman[30]. Případně může být distribuce řešena manuálně pomocí adresářů s výhradním přístupem pouze daného uživatele.

EAP-FAST také na rozdíl od metody LEAP přináší podporu serverových certifikátů. Jejich nasazení je povinné pouze v případě nastavení nulté fáze do režimu *Server-side authentication Diffie-Hellman mode*, v opačném případě je nepovinné.

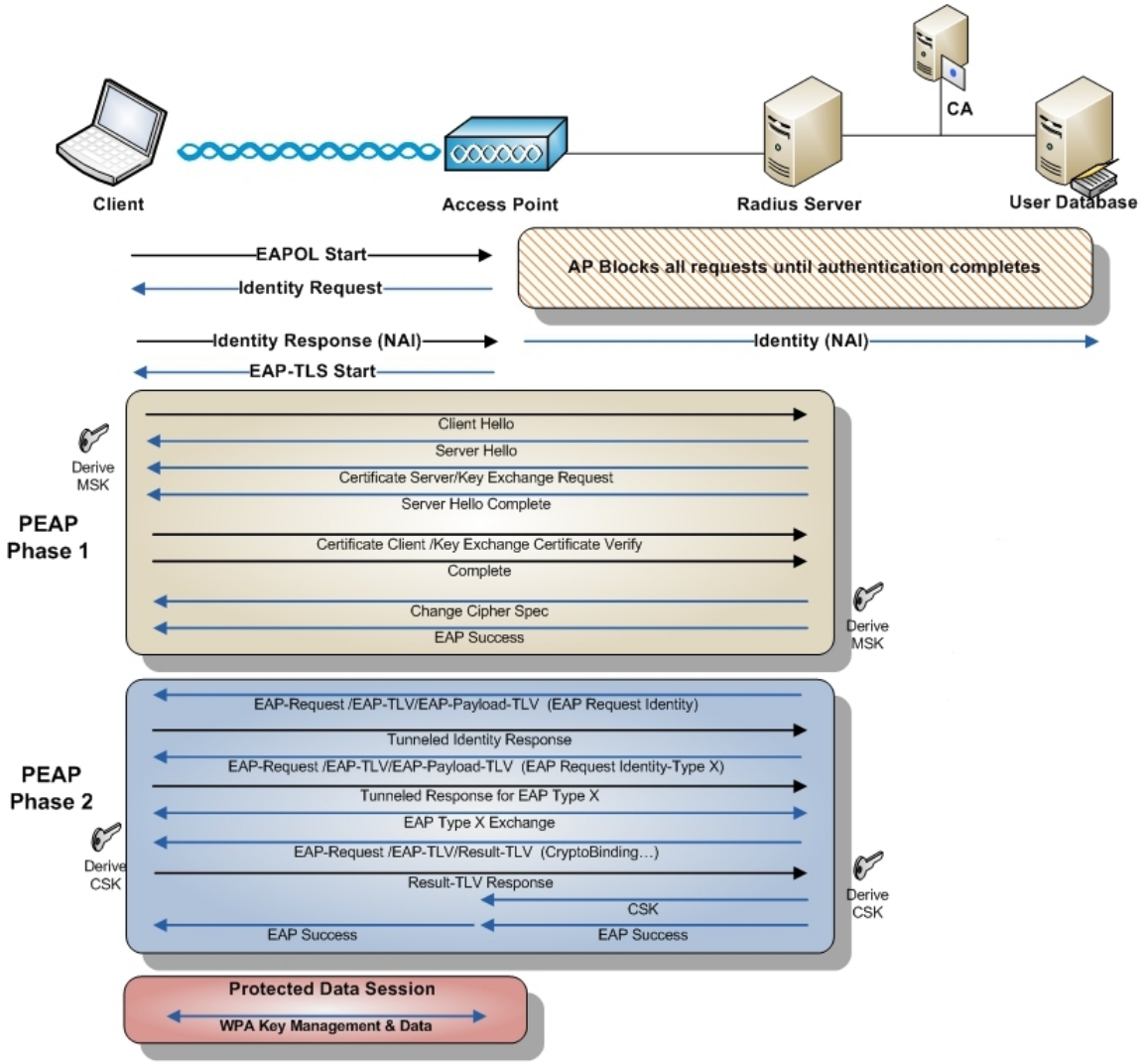
Metoda je náchylná na útok *RADIUS impersonation* (popsaný v kapitole 3.2.4) směřovaný na nultou fázi autentizace, kdy probíhá předání PAC souborů. Slabiny metody EAP-FAST jsou rozebrány v kapitole 3.2.3.

2.5.6 PEAP

PEAP (*Protected Extensible Authentication Protocol*) byl poprvé představen v roce 2002. Metoda byla vytvořena s důrazem na bezpečnost a vznikla kooperací společností Microsoft, Cisco Systems a RSA Security. Na rozdíl od dosud zmíněných EAP metod je PEAP popi-

Fáze	Funkce
Fáze 0	Přenos PAC z RADIUS serveru na klienta za použití Authenticated nebo Anonymous Diffie-Hellman protokolu
Fáze 1	Na základě PAC je vytvořen šifrovaný peer-to-peer tunel mezi klientem a RADIUS serverem
Fáze 2	V rámci šifrovaného tunelu dojde ke vzájemné autentizaci prostřednictvím protokolu MS-CHAPv2

Tabulka 2.4: Fáze metody EAP-FAST



Obrázek 2.12: Autentizace prostřednictvím metody PEAP. Převzato z [12]

sován jako samostatný protokol zapouzdřující EAP komunikaci do šifrovaného kanálu. Pro zabezpečení přenášených autentizačních údajů využívá tento kanál šifrování TLS. TLS/SSL komunikuje většinou na pomezí síťové a transportní vrstvy, v případě EAP protokolu je však použito *TLS over EAP* komunikující na spojové vrstvě ISO/OSI modelu. Autentizace

prostřednictvím protokolu PEAP je zobrazena na obrázku 2.12.

Na rozdíl od metody EAP-FAST, u které je použití serverového certifikátu volitelné, je v případě PEAP nasazení serverového certifikátu povinné. Certifikát slouží k prokázání autenticity RADIUS serveru za účelem snížení rizika *RADIUS impersonation* útoku popsaného v sekci 3.2.4. PEAP rozšiřuje EAP protokol o takzvané AVP – Attribute Value Pair[35], které slouží k přenosu dodatečných informací při autentizačním procesu.

Samotný PEAP definuje pouze vnější zapouzdření EAP komunikace, avšak nedefinuje použití žádného konkrétního vnitřního autentizačního mechanismu. Na základě použitého vnitřního protokolu rozlišujeme několik verzí PEAP protokolu, následuje popis dvou nejrozšířenějších:

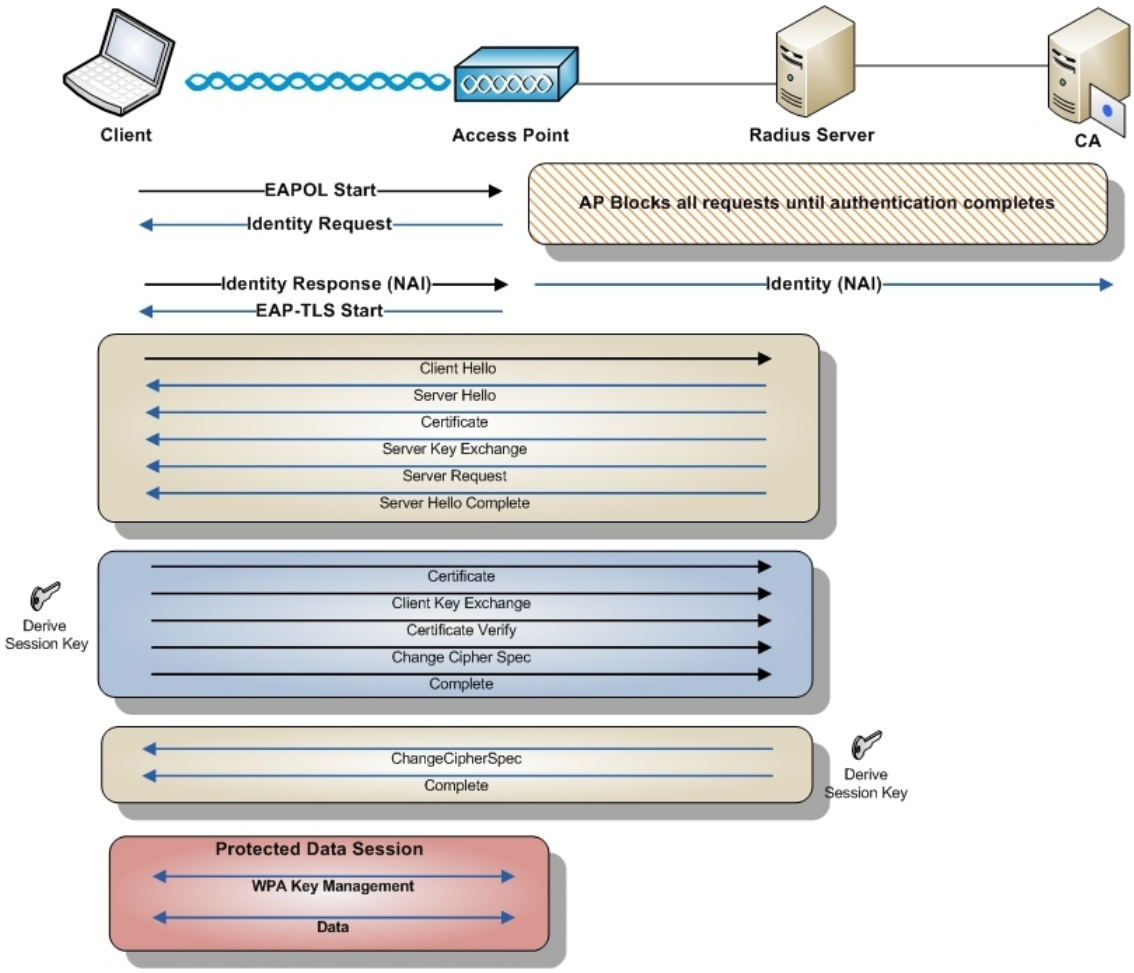
- **PEAPv0/EAP-MSCHAPv2** – PEAP verze 0 byla popsána v IETF draftu[36] vytvořeném společností Microsoft v roce 2002. Metoda využívá pro potřeby autentizace protokol EAP-MSCHAPv2 publikovaný společností Microsoft. EAP-MSCHAPv2 na rozdíl od své přechozí verze podporuje vzájemnou autentizaci. Toho je docíleno tím, že kromě *Challenge* řetězce ze serveru na klienta, posílá taktéž klient svůj tzv. *Challenge-peer* řetězec na server a ověřuje jeho odpověď[37]. Protokol PEAPv0 je nativně podporován operačními systémy Windows od verze Windows XP SP1 a MAC OS X od verze 10.3 Panther. Vzhledem k této podpoře, poměrně dobré úrovni bezpečnosti a snadné implementaci (oproti metodám založeným na klientských certifikátech) se jedná o jednu z nejrozšířenějších EAP metod.

- **PEAPv1/EAP-GTC** – Specifikace PEAP verze 1 je popsána v IETF draftech[38]. Metoda byla vytvořena společností Cisco Systems jako alternativa k PEAPv0. Přestože se Microsoft spolupodílel na vytvoření tohoto protokolu, dodnes není ve Windows nativní podpora pro PEAPv1. Společnost Cisco Systems navíc propaguje použití své jiné metody, a to EAP-FAST. Z těchto důvodů není PEAPv1/EAP-GTC příliš rozšířen. Jako vnitřní autentizační mechanismus je použita metoda EAP-GTC (EAP Generic Token Card) vytvořená společností Cisco Systems a popsaná v RFC 3748[39]. Tato metoda slouží pro přenos autentizačních údajů vygenerovaných bezpečnostním tokenem. Metoda pracuje s hesly typu OTP a není tudíž náchylná na replay útok. Bezpečnostním tokenem mohou být například RSA SecurID tokeny.

2.5.7 EAP-TLS

EAP-TLS (*EAP-Transport Layer Security*) je IETF standard definovaný v roce 1999 v RFC 2716[40] a v roce 2008 aktualizovaný v RFC 5216[41]. V roce 2003 byla tato EAP metoda jako první a do roku 2005 také jediná, certifikována organizací WiFi Alliance pro použití ve WiFi sítích a je tak široce podporována výrobci hardware. Spolu s PEAPv0/MS-CHAPv2 se jedná o nejrozšířenější EAP metodu používanou ve WiFi sítích založených na standardu 802.1X[16].

[35] http://tools.ietf.org/html/draft-kamath-pppext-peapv0-00#page-6
[36] http://tools.ietf.org/html/draft-kamath-pppext-peapv0-00
[37] http://technet.microsoft.com/en-us/library/cc957983.aspx
[38] http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-00 a http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-05
[39] http://tools.ietf.org/html/rfc3748
[40] http://tools.ietf.org/html/rfc2716
[41] http://tools.ietf.org/html/rfc5216



Obrázek 2.13: Autentizace prostřednictvím metody EAP-TLS. Převzato z [12]

EAP-TLS podporuje vzájemnou autentizaci mezi klientem a RADIUS serverem. Ta je založená na PKI, kdy se RADIUS server autentizuje klientům prostřednictvím serverového certifikátu a klienti se autentizují serveru každý svým vlastním klientským certifikátem. To s sebou přináší vyšší implementační (vybudování PKI infrastruktury, nutnost distribuce certifikátů na klienty) i finanční (zakoupení kvalifikovaných certifikátů centrální autority) náročnost nasazení této metody, avšak také vyšší úroveň bezpečnosti oproti dosud popsaným EAP metodám[14]. Certifikát uživatele může být uložený v souborovém systému nebo na čipové kartě.

Šifrovaný tunel mezi klientem a serverem je ustanoven prostřednictvím procedury nazývané TLS handshake. Ten probíhá následujícím způsobem[22]:

1. Klient požádá server o započetí ustanovení TLS kanálu a zároveň zašle serveru seznam podporovaných šifrovacích algoritmů a hashovacích funkcí.

2. Server ze seznamu vybere nejsilnější šifrovací algoritmus a hashovací funkci a poskytne klientovi svůj certifikát obsahující certifikační autoritu, jméno a veřejný klíč serveru.

3. Klient ověří přijatý certifikát, vygeneruje pseudonáhodné číslo označované jako Pre-

Master Secret (PMS), které zašifruje veřejným klíčem serveru a zašle zpět spolu se svým klientským certifikátem.

4. Server je schopen PMS rozšifrovat použitím svého privátního klíče. Na základě PMS vygenerují obě strany symetrický klíč označovaný jako Master Secret, který slouží pro šifrování a dešifrování další komunikace.

Proces autentizace s využitím EAP-TLS je zobrazena na obrázku 2.13. Metoda EAP-TLS je podporována operačními systémy MS Windows od verze Windows 2000 SP4 (EAP-TLS v kombinaci s WPA je podporováno až od verze Windows XP SP2), operačními systémy Mac OS X od verze 10.3 Panther. Linuxové a BSD systémy obsahují podporu EAP-TLS prostřednictvím klienta wpa_supplicant.

2.5.8 EAP-TTLS

EAP-TTLS (*EAP-Tunneled Transport Layer Security*) je metoda vytvořená společností Funk Software [42]. Tato metoda, popsaná v RFC 5282[43], je svým principem velice podobná metodě PEAP. Stejně jako PEAP i EAP-TTLS používá AVP atributy pro přenos informací uvnitř šifrovaného kanálu. AVP metody EAP-TTLS jsou kompatibilní s AVP v rámci protokolu RADIUS i DIAMETER.

Činnost metody lze rozdělit na dvě fáze. V první fázi je proveden TLS handshake, při kterém je klientem ověřena identita serveru na základě serverového certifikátu. Ve druhé fázi je sestaven TLS tunel, prostřednictvím kterého proběhne vlastní autentizace klienta. Volitelně umožňuje EAP-TTLS autentizovat klienta prostřednictvím klientského certifikátu již ve fázi 1. V takovém případě pak fáze 2 vůbec neproběhne.

EAP-TTLS tímto způsobem poskytuje zapouzdření nejen pro další EAP metody, ale také pro autentizaci typu Password authentication protocol – PAP, Challenge-handshake authentication protocol – CHAP, MS-CHAP a MS-CHAPv2.

2.5.9 Shrnutí

V této sekci byly popsány nejrozšířenější EAP metody využívané u bezdrátových sítí založených na standardu 802.1X. Kromě výše popsaných metod existují mnohé další jako například EAP-SIM, EAP-AKA, PEAP-EAP-TLS, EAP-SRP, EAP-SecurID, EAP-POTP a další. Tyto metody nebyly popsány z důvodu jejich minimální rozšířenosti u WiFi sítí, případně se jedná o modifikace výše popsaných metod.

[42] Funk Software byla v roce 2005 koupena společností Juniper Networks: http://www.juniper.net/us/en/company/press-center/press-releases/2005/pr-051114.html

[43] http://tools.ietf.org/html/rfc5281

Kapitola 3

Slabiny bezpečnostních mechanismů WLAN sítí

Cílem této kapitoly je vytvořit ucelený přehled popisující známé slabiny, bezpečnostní nedostatky a zranitelnosti nejrozšířenějších bezpečnostních mechanismů používaných v bezdrátových sítích dle standardu IEEE 802.11. Slabiny sítí se šifrováním založeným na znalosti sdíleného klíče (WEP, WPA-Personal) byly již stručně popsány v příslušných kapitolách. Hlavní pozornost je věnována standardům a technologiím využívaných v bezdrátových sítích velkých podniků a organizací. Konkrétně se jedná o bezdrátové WiFi sítě postavené na standardu IEEE 802.1X.

Tato kapitola by měla sloužit jako příručka uvádějící zranitelnosti, rizika a doporučení vyplývající z nasazení různých technologií a bezpečnostních mechanismů, případně vyplývající z nasazení těchto mechanismů v nesprávné konfiguraci. Primárním cílem je poskytnout podklady k provedení technicky zaměřeného bezpečnostního auditu bezdrátové sítě. Cílem takového auditu je prověrka konfigurace přístupových bodů, RADIUS serveru[1] a také konfigurace klientů připojených k bezdrátové síti. Konkrétní kroky pro vykonání auditu jsou pak uvedeny v kapitole 4.

Kapitola bude pojednávat o bezpečnostních rizicích bezdrátových sítí vyplývajících z nasazení nevyhovujících bezpečnostních mechanismů, jakými je například metoda LEAP v případě sítí postavených na standardu 802.1X. Dále budou probrána rizika plynoucí z nedostatečné bezpečnostní konfigurace na straně klientského bezdrátového software. Kapitola nepojednává o rizicích bezdrátových sítí vzniklých procesním pochybením[2], útokem pomocí sociálního inženýrství či exploitací chyb v software jednotlivých prvků WiFi infrastruktury či připojených klientů. V práci taktéž nebude řešena otázka odpovědnosti za vzniklý incident.

Informace obsažené v této kapitole mohou být využity administrátory bezdrátových sítí pro kontrolu konfigurace a případně aplikaci uvedených doporučení a taktéž bezpečnostními konzultanty, auditory či testery k provedení bezpečnostního auditu se souhlasem provozovatele dané sítě s cílem identifikace bezpečnostních rizik.

Tak jako každá informace i postupy uvedené v této kapitole mohou být zneužity k jinému účelu, než je předpokládaný záměr. V tomto případě se může jednat o neautorizované zásahy do cizích WiFi sítí. Je nutné upozornit, že takové aktivity jsou trestně postižitelné v rámci

[1] Případně jiného autentizačního serveru, v případě, kdy není nasazen protokol RADIUS, ale například DIAMETER či TACACS+

[2] Například stále platné přihlašované údaje propuštěného zaměstnance

českého práva, viz Trestní zákoník č. 40/2009 SB, §230, odstavec 1[3]:

„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“

3.1 Filtrace MAC adres a skrývání SSID

Řízení přístupu na základě MAC adresy

Filtrace MAC adres je způsob řízení přístupu k síti na základě hardwarové adresy bezdrátového síťového adaptéru popsaný v kapitole 2.2. MAC adresa lze na většině síťových adaptérů změnit. Útočník zároveň může pasivním monitorováním asociovaných klientů k dané bezdrátové síti zjistit jejich MAC adresy. Ty jsou ze zachycených rámců čitelné[4] i v případě, že je použito šifrování WEP či WPA. Ukázka změny MAC adresy v Linuxu je zobrazena na výpisu 3.1. V operačním systému Windows je obvykle nutné provést zásah do registrů. Postup útočníka pro obejití přístupu na základě MAC adresu je následující:

1. Za pomoci pasivního odposlouchávání síťového provozu je zjištěna MAC adresa asociovaného klienta.
2. Útočník změní svoji MAC adresu za autorizovanou MAC adresu připojeného klienta.
3. Pokud není na síti nasazeno šifrování, může se útočník asociovat a autentizovat k bezdrátové síti.

Výpis 3.1: Změna MAC adresy síťového adaptéru ath0

```
# ifconfig ath0 down
# ifconfig ath0 hw ether 00:11:22:33:44:55
# ifconfig ath0 up
```

Pokud se útočník připojí k síti v době, kdy je zároveň připojený i autorizovaný klient, může dojít v rámci jejich komunikace ke konfliktům, jelikož se v daném segmentu sítě budou nacházet dvě zařízení se stejnou MAC adresou. Po připojení k síti může útočník dále podniknout slovníkový útok vůči webové či konzolové administraci daného přístupového bodu. V případě, že je použito slabé či dokonce z výroby přednastavené heslo, může útočník získat přístup do administrace přístupového bodu a zde rozšířit seznam povolených MAC adres o svoji vlastní[5] MAC adresu, případně filtrování na základě MAC adres zcela deaktivovat.

Skryté SSID

Vypnutí propagace SSID bezdrátové sítě nabízí téměř každý přístupový bod jakožto další z úrovní zabezpečení sítě. Pro zkušeného útočníka však není problém tuto vlastnost sítě obejít a získat tak identifikátor SSID[7].

Skrytí SSID spočívá v zakázání periodického vysílání 802.11 *Beacon* rámců přístupovým bodem. SSID je však v 802.11 komunikaci přenášeno i v rámcích *Probe request* a *Probe*

[3] www.mvcr.cz/soubor/sb011-09-pdf.aspx
[4] Na rozdíl od IP adres, které se nacházejí až na třetí, tedy již šifrované, vrstvě
[5] Může být i zfalšovaná

response, které byly popsány v kapitole 2.1.3. Tyto rámce jsou vysílány ve fázi připojování klienta k síti. Útočník tak má dvě možnosti a to zahájit pasivní odposlech síťového provozu a čekat, než dojde k připojení klienta k síti, anebo provést deautentizační útok spočívající ve vysílání podvrhnutí deautentizačních rámců na již připojeného klienta. Výhodou první možnosti je nemožnost odhalení útočníka, zatímco výhodou možnosti druhé je rychlost získání požadované informace, avšak za cenu rizika detekce tohoto útoku systémem WIDS[6] (viz kapitola 5.1.5).

Obě možnosti předpokládají, že k cílové síti je připojen alespoň jeden klient. V opačném případě zůstává SSID sítě neodhalitelné.

Doporučení

Přestože obě zmíněné metody přinášejí určité zvýšení zabezpečení bezdrátové sítě, nepředstavují pro zkušenějšího útočníka výraznější překážku a mohou naopak způsobit problémy s konektivitou k síti autorizovanému uživateli. Doporučené je taktéž nastavit silná hesla k administracím všech aktivních síťových prvků vylučující úspěšný útok zevnitř sítě. Vyšší úroveň zabezpečení potom přinese omezení přístupu k managementu síťových prvků pouze z vyhrazených administrátorských VLAN[7].

3.2 WPA Enterpise

Jak již bylo uvedeno v kapitole 2.5, pojmem WPA Enterprise je obecně označováno nasazení bezdrátové WiFi sítě spolu s autentizačním mechanismem dle standardu IEEE 802.1X a to přestože šifrování takové sítě nemusí být realizováno pouze pomocí WPA, ale také prostřednictvím protokolu WEP s dynamickými klíči. V této kapitole jsou podrobně rozebrány bezpečnostní nedostatky a zranitelnosti vyplývající z nasazení či nedostatečné konfigurace jednotlivých EAP metod. U každé EAP metody bude uvedeno také bezpečností doporučení s cílem co nejvíce snížit dané riziko.

3.2.1 EAP-MD5

Metoda EAP-MD5 byla původně navržena pro sítě s nízkým rizikem odposlechu, z čehož vyplývá i její úroveň zabezpečení. Autentizace prostřednictvím této metodu funguje na principu Challenge-Handshake. Činnost metody byla popsána v kapitole 2.5.3.

Jakmile klient obdrží *Challenge* řetězec, vytvoří *Challenge-response* řetězec následujícím způsobem:

```
challenge_response = MD5(challenge_id + heslo + challenge)
```

Úspěšný útok předpokládá odchycení EAP komunikace úspěšné autentizace klienta. V případě, že je k dané síti některý klient již asociovaný, nemusí útočník čekat na jeho opětovné přihlášení a může se pokusit o jeho deautentizaci prostřednictvím zaslání deautentizačního rámce. Deautentizační rámce nemají žádnou ochranu proti podvrhnutí a klientovi se tak jeví, že příkaz k deautentizaci přišel z daného přístupového bodu. Pokud je klientův suplikant nakonfigurován pro automatické přihlašování k dané síti, proběhne ihned po deautentizaci klienta autentizace, na níž útočník čeká. V praxi je odpojení a znovu připojení klienta k síti tak rychlé, že si uživatel ani nemusí všimnout, že se děje něco nestandardního.

[6] Wireless Intrusion Detection System
[7] Virtual Local Area Network

Jakmile útočník zachytí EAP-MD5 komunikaci, může se znalostí postupu pro vytváření *Challenge-response* řetězce použít offline slovníkový útok na heslo. Hodnota challenge_id stejně samotný challenge řetězec jsou obsažené v EAP-MD5-Challenge rámci. *Challenge-response* řetězec je pak obsažený v *EAP-MD5-Response* rámci. Algoritmus pro offline slovníkový útok na heslo uživatele je popsán ve výpisu 3.2.

Výpis 3.2: Offline slovníkový útok na EAP-MD5 komunikaci

```
challenge_id = parse1(EAP-MD5-challenge)
challenge    = parse2(EAP-MD5-challenge)
response     = parse3(EAP-MD5-response)

for pass in dictionary.txt:
    hash = MD5(challenge_id + pass + challenge)
    if (hash == response):
        print "Password: " + pass
        break
```

Metoda EAP-MD5 je odolná vůči replay útoku. Odchycený *Challenge-response* řetězec nelze použít na opětovnou autentizaci, jelikož je závislý na hodnotě *Challenge* řetězce v rámci jedné EAP komunikace.

Doporučení

Vzhledem k tomu, že tato metoda nepodporuje generování dynamických klíčů a nelze tak nasadit v kombinaci s WPA, není u bezdrátových sítí příliš rozšířena. Použití této metody není rozhodně doporučováno a to ani v kombinaci se silným heslem. Pokud je z jakýchkoliv důvodů nutné provádět autentizaci uživatelů prostřednictvím této metody, lze využít metodu EAP-TTLS s vnitřní metodou EAP-MD5, kdy jsou autentizační údaje přenášeny v rámci šifrovaného kanálu. Metoda EAP-TTLS je popsána v kapitole 2.5.8 a její bezpečnost je řešena v kapitole 3.2.5.

3.2.2 LEAP

Jak již bylo zmíněno v kapitole 2.5.4, společnost Cisco Systems vytvářela EAP metodu LEAP především s důrazem na jednoduché nasazení a použití. Specifikace metody vznikla v roce 2000, tedy v době, kdy byl algoritmus WEP jediný možný prostředek pro šifrování WiFi sítě a navíc v té době ještě považován za bezpečný[8].

Na bezpečnostní nedostatky metody LEAP bylo poprvé upozorněno na konferenci DEFCON 1. srpna roku 2003. Výzkumník v oboru bezpečnosti bezdrátových sítí Joshua Wright zde prezentoval náchylnost metody na offline slovníkový útok. Na tomto místě je nutné podotknout, že téměř každá autentizační metoda založená na zadávání hesla je v případě zvolení slabého hesla náchylná na tento útok. V případě metody LEAP však zranitelnost spočívá v markantním snížení časové náročnosti tohoto útoku. Pro úspěšné vykonání slovníkového útoku musí nejdříve útočník odchytit LEAP komunikaci autorizovaného klienta. Toho může být docíleno stejnými prostředky, jako již bylo popsáno v případě metody EAP-MD5.

[8] Na zranitelnosti mechanismu WEP bylo poprvé upozorněno v roce 2001

Autentizace v rámci metody LEAP funguje na principu *Challenge-handshake* a je založená na autentizačním algoritmu společnosti Microsoft MS-CHAPv1. Následuje popis činnosti autentizačního protokolu MS-CHAPv1:

1. Autentizátor zašle klientovi 8 bajtů dlouhý challenge řetězec.
2. Klient vytvoří 16B dlouhý NT hash[9] hesla, který použije k vygenerování 3DES klíčů (Algoritmus 3DES používá klíč o celkové délce 168 bitů.) následujícím způsobem:
   - Klíč 1 = NT1 – NT7
   - Klíč 2 = NT8 – NT14
   - Klíč 3 = NT15 – NT16 + "\0\0\0\0\0"
3. Každým z klíčů je zašifrován challenge řetězec, výstupem jsou tři 8 bajtů dlouhé řetězce.
4. Klient zašle konkatenaci těchto řetězců (24 bajtů) autentizátoru jako challenge-response řetězec.
5. Autentizátor na základě přijatého challenge-response řetězce rozhodne, zda bude klient úspěšně autentizován.

Bezpečnostní problém spočívá v postupu vytvoření třetího DES klíče. Klíč je 7 bajtů dlouhý, avšak posledních 5 bajtů je vždy konstantních (bajty s hodnotou nula). Útok hrubou silou na algoritmus DES s klíčem dlouhým 16 bitů[10] je tak při použití dnešních výpočetních prostředků otázka okamžiku, jelikož maximální počet možností klíče je 2^{16} tedy pouhých 65536 možností. Prolomením třetího šifrovacího klíče je tak téměř v konstantním čase možné získat poslední dva bajty[11] (výše označené jako NT15 a NT16) NT Hashe hesla.

V další fázi je nutné převést slovník s hesly[12] na slovník obsahující pouze NT hashe těchto hesel. Z tohoto souboru je pak možné vyfiltrovat NT hashe končící dvěma znaky, které byly zjištěny v přechozí fázi. Tím dojde k enormnímu snížení možných shod.

V poslední fázi je proveden klasický slovníkový útok na MS-CHAPv1 algoritmus pouze s použitím hesel ze slovníku, jejichž NT hashe končí zjištěnými dvěma znaky. Pokud dojde ke shodě, je na základě NT hashe vyhledán odpovídající řetězec v původním slovníku, který je zároveň heslem uživatele bezdrátové sítě. Uživatelské jméno je v otevřené podobě obsaženo v *EAP-Identity-Response* paketu a útočník může tímto způsobem získat platné přihlašovací údaje uživatele.

Pro názornost redukce stavového prostoru pro hledání hesla poslouží slovník dodávaný s linuxovou distribucí Backtrack[13] obsahující přes 1,7 milionu slov[14]. Na základě něj byl vytvořen slovník obsahující pouze NT hashe hesel. Jako heslo byl náhodně zvolen jeden z řetězců nacházejících se v tomto slovníku, konkrétně se jednalo o řetězec *fibreglass*. Na základě posledních dvou znaků NT hashe tohoto hesla byly vyfiltrovány odpovídající NT hashe ze slovníku. Z celkových 1707659 hashů zbylo pouze 24.

[9] NT hash je založený na hashovací funkci MD4, jeho výstupem je 128 bitů dlouhý řetězec
[10] Zbývajících 40 bitů známe.
[11] z celkových šestnácti
[12] Předpokládejme, že hesla jsou uložena v souboru ve formátu jedno heslo na řádek.
[13] http://www.backtrack-linux.org/
[14] Tento slovník je dostupný například zde: http://static.hackersgarage.com/darkc0de.lst.gz

Bezpečnostní nedostatek se nachází přímo v autentizačním protokolu MS-CHAPv1. Zranitelné jsou tak všechny metody a protokoly, které z MS-CHAPv1 vycházejí. Kromě EAP metody LEAP se tak jedná například o PPTP (*Point-to-Point Tunneling Protokol*). Joshua Wright na konferenci DEFCON upozornil na bezpečnostní nedostatky tohoto protokolu v souvislosti s metodou LEAP, nedostatky samotného mechanismu MS-CHAPv1/2 jsou známé již od roku 1999[31].

Doporučení

Metoda LEAP je v současné době považována za zastaralou a není považována za bezpečnou. Samotná společnost Cisco Systems doporučuje použití metody EAP-FAST, která byla vytvořena s cílem odstranit bezpečnostní nedostatky metody LEAP[2]. Pokud není z jakéhokoliv důvodu možné LEAP nahradit za bezpečnější metodu je nutné použít opravdu silná hesla, která mají šanci odolat offline slovníkovému útoku. Doporučení na tvorbu hesel jsou uvedena v kapitole 3.3.

3.2.3 EAP-FAST

Metoda EAP-FAST byla vytvořena společností Cisco Systems jako reakce na odhalení zranitelností v jejich předcházející metodě LEAP. Metoda je inspirovaná metodami PEAP a EAP-TTLS. Ve fázi 1 je vytvořen šifrovaný tunel, přes který ve fázi 2 probíhá samotná autentizace.

Sestavení tunelu probíhá na základě validace PAC, což je soubor vygenerovaný RADIUS serverem a uložený na klientovi. Distribuce PAC souboru z RADIUS serveru na klienta je označována jako fáze 0. Tato fáze probíhá poprvé při nasazení této metody, po expiraci PAC souboru (obvykle jednou do roka) nebo v případě přidání nového klienta.

PAC soubor může být ke klientovi přenesen po metalické síti, stažením z chráněného úložiště nebo automaticky. První dvě možnosti jsou ekvivalentní distribuci klientských certifikátů u metody EAP-TLS. EAP-FAST získal oblibu právě podporou třetí možnosti a to automatické distribuce PAC souboru pomocí bezdrátové sítě po zadání přihlašovacích údajů[22].

Toto řešení je velice pohodlné avšak tvoří hlavní bezpečností problém této metody. Automatická distribuce PAC může probíhat ve dvou režimech:

- *Server-Authenticated* - využití RSA
- *Server-Unauthenticated* - využití anonymního DH

Při použití prvního režimu provádí klient před obnovou PAC souboru autentizaci serveru na základě serverového certifikátu. Nasazení serverového certifikátu však není metodou EAP-FAST vynucené, proto je často z důvodu snadnosti nasazení použita varianta *Server-Unauthenticated*, která serverový certifikát nevyžaduje[10]. V první fázi je potom využit anonymní Diffie-Hellman tunel a v druhé fáze proběhne autentizace prostřednictvím protokolu MS-CHAPv2.

Metoda EAP-FAST je tak v této konfiguraci zranitelná na útok *RADIUS impersonation*. Útočník však pro úspěšnou kompromitaci musí útok provést v době, kdy probíhá nultá fáze, tedy při nasazení metody, obnově PAC souboru, po jeho expiraci či v případě konfigurace nového klienta. V době, kdy v rámci sítě neprobíhá fáze 0, není metoda na tento útok zranitelná (na rozdíl od metod PEAP a EAP-TTLS, které jsou při nedostatečné

konfiguraci na straně klienta zranitelné po celou dobu jejich použití), jelikož v první fázi při ustanovování TLS tunelu neprobíhá standardní TLS handshake, ale tunel je sestavován na základě znalosti sdíleného tajemství z PAC souboru (tzv. *PAC-opaque*). Jelikož podvržený RADIUS server nemá znalost tohoto tajemství, nemůže s klientem ustanovit zabezpečený tunel.

Úspěšným provedením útoku získá útočník přístup do šifrovaného kanálu a může tak odchytit MS-CHAPv2 komunikaci, na kterou následně může být veden offline slovníkový útok. Podrobný popis útoku *RADIUS impersonation* je uveden v kapitole 3.2.4.

Doporučení

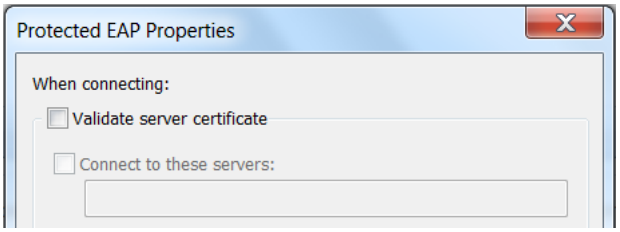
V případě nasazení metody EAP-FAST v kombinaci s automatickou distribucí PAC souborů klientům je doporučené využít režim s autentizací serveru. To předpokládá nasazení serverového certifikátu na RADIUS server. Takováto konfigurace snižuje riziko úspěšného provedení *RADIUS impersonation* útoku a bezpečností se téměř vyrovnává metodě EAP-TLS.

3.2.4 PEAP

Tato sekce bude věnována bezpečnosti metody PEAP, konkrétně její verze PEAPv0/MS-CHAPv2 a to z důvodu její dominance mezi ostatními verzemi metody PEAP. Označení PEAP bude dále v textu označovat právě tuto verzi.

PEAP na rozdíl od metod EAP-MD5 a LEAP před samotnou autentizací (fáze 2) provede sestavení tunelu šifrovaného prostřednictvím kryptografického protokolu TLS (Transport Layer Security)[6]. Ten je v současné době považován za z hlediska bezpečnosti dostatečný prostředek pro zajištění důvěrnosti a integrity přenášených dat[15].

Implementace metody PEAP vyžaduje nasazení serverového certifikátu na RADIUS serveru. Bezdrátový klient tak má možnost před samotnou autentizací ověřit identitu serveru. Problémem však je, že toto ověření identity není na straně klienta povinné a závisí na nastavení konkrétního suplikanta[16], viz obrázek 3.1.



Obrázek 3.1: Nastavení validace certifikátu RADIUS serveru ve Windows 7 WZC suplikantu

RADIUS impersonation

V případě, že suplikant klienta není nakonfigurovaný způsobem, aby ověřoval identitu RADIUS serveru, stává se daný klient náchylný na útok *RADIUS impersonation*, který je variantou útoku *Rogue AP*[17] pro 802.1X sítě. Útok je proveditelný v případě následujících

[15] Na rozdíl od jeho předchůdce SSLv2, který již není doporučené využívat.
[16] Suplikantem je zde myšlený software použitý pro připojení k 802.1X WiFi síti
[17] http://www.rogueap.com/

tří konfigurací suplikanta:

- Suplikant klienta vůbec neověřuje identitu RADIUS serveru (viz například obrázek 3.1)
- Suplikant klienta ověřuje identitu RADIUS serveru, avšak nemá nastavenou kontrolu certifikátu vůči žádné důvěryhodné certifikační autoritě. Chování většiny suplikantů je potom takové, že se klienta před autentizací dotáží, zda důvěřuje konkrétnímu certifikátu. Pokud klient označí certifikát za důvěryhodný, je navázán kontakt s RADIUS serverem.
- Suplikant klienta je nakonfigurovaný tak, že ověřuje identitu RADIUS serveru a má nastavenou kontrolu certifikátu vůči veřejné důvěryhodné certifikační autoritě (například VeriSign). V tomto případě si může útočník tuto CA zjistit pomocí odposlechu první fáze PEAP komunikace, následně zřídit certifikát podepsaný touto CA[18] a nasadit ho na falešný RADIUS server.

Implicitní chování suplikantů WZC, OS X supplicant a Juniper Odyssey client při konfiguraci nové bezdrátové 802.1X sítě je dotaz na klienta, zda považuje certifikát RADIUS serveru za důvěryhodný. V tom případě plně záleží na rozhodnutí daného uživatele, jak se v případě podvrhnutí certifikátu RADIUS serveru zachová. Postup útočníka při provedení útoku *RADIUS impersonation*, kdy je v dosahu cílové sítě a připojeného klienta, je následující:

1. Útočník vytvoří WiFi síť se stejným SSID a zabezpečením, jako má cílová síť. Vytvořená síť by měla mít pro cílového klienta vyšší signál než síť originální. V této síti se bude nacházet autentizátor (HW nebo SW přístupový bod) i autentizační RADIUS server se schopností logovat probíhající autentizaci, včetně hodnot *Challenge* a *Challenge-response*[19].
2. Útočník deautentizuje připojeného klienta prostřednictvím vysílání deautentizačních rámců. Pokud je suplikant klienta nastavený pro automatické připojování k dané síti (dle SSID) a signál podvrhnuté sítě je vyšší než signál původní sítě, je velice pravděpodobné, že se suplikant pokusí připojit k podvrhnuté síti. Pokud automatické připojování k dané sítí není v suplikantu nakonfigurováno, musí útočník čekat, než se klient k jeho síti připojí ručně.
3. Klient zahájí autentizační proces k podvrhnuté síti, certifikát RADIUS serveru není kontrolován anebo je akceptován na základě výše uvedených podmínek a dojde k sestavení TLS tunelu. Koncovým bodem tohoto tunelu je podvržený RADIUS server. Útočník tak má přístup ke komunikaci v rámci šifrovaného tunelu a může odposlechnout[20] *Challenge* a *Challenge-response* řetězce autentizačního protokolu MS-CHAPv2.
4. MS-CHAPv2 stejně jako jeho předchozí verze obsahuje bezpečnostní slabiny[31] usnadňující offline útok hrubou silou na *Challenge-response* řetězce. Útočník může tímto způsobem získat heslo klienta bezdrátové sítě.

[18] Certifikační autorita

[19] Takovým RADIUS serverem může být například Freeradius-WPE: http://www.willhackforsushi.com/FreeRADIUS_WPE.html

[20] Respektive dohledat v log souboru RADIUS serveru.

Kromě výše popsané situace, kdy se útočník nachází přímo v dosahu signálu cílové sítě, může být útok veden i na osamoceného neasociovaného klienta, jehož suplikant je nakonfigurován pro automatické připojení k dané síti. Suplikant takového klienta v případě, že není v dosahu této sítě, periodicky vysílá rámce typu *Probe request* obsahující SSID cílové sítě. Pokud útočník vytvoří síť s odpovídajícím SSID a zabezpečením, pokusí se klient o asociaci k této síti. Kompromitace uživatelského účtu tak může nastat i na geograficky odlišné lokaci než se nachází samotná síť společnosti.

Celý výše popsaný útok může být vykonán pouze z jediného notebooku za použití virtualizace a softwarového AP. Útočník tak nemusí budit pozornost manipulací s hardwarovým přístupovým bodem, anténou či více počítači.

Anonymizace identity

Identita klienta se při PEAP komunikaci přenáší dvakrát. Na samotném začátku komunikace je tento řetězec přenášen v čitelné podobě v *EAP-Identity-Response* rámci, viz obrázek 2.12. K vlastní autentizaci je použita až identita přenášená uvnitř TLS tunelu. Některé suplikanty dovolují identitu přenášenou v otevřené podobě zaměnit za libovolný řetězec z důvodů anonymizace použitého uživatelského jména, za účelem obrany proti odposlechu této informace.

Například v případě použití Active Directory, jakožto autentizační databáze, je v identitě klienta přenášené přihlašovací jméno do Windows domény. Útočník tak může pasivním odposlechem provést sběr přihlašovacích údajů, které může využít pro provedení Denial of Service útoku v případě zamykání uživatelských účtů po určitém počtu neúspěšných pokusů o přihlášení nebo při sociotechnickém útoku.

Doporučení

Pro zmírnění možnosti útoku *RADIUS impersonation* je doporučené na straně klienta aplikovat následující nastavení:

- Suplikant ověřuje identitu RADIUS serveru
- Suplikant kontroluje příslušnost certifikátu k CA dané organizace (například *Brno University of technology CA*). Předpokládá se, že klient má nainstalovaný kořenový certifikát organizace. Je vhodné zvolit CA, u níž je nízké riziko, že se útočníkovi podaří získat certifikát podepsaný touto CA. Toto riziko je nižší v případě CA dané organizace/společnosti než v případě veřejných CA.
- Suplikant ověřuje doménové jméno serveru s CN[21] uvedeným v certifikátu.

V případě operačního systému Windows a suplikantu WZC je možné při hardeningu konfigurace vycházet z oficiálního doporučení společnosti Microsoft[22].

K možnostem konfigurace připojení k bezdrátové síti by běžný uživatel na své stanici neměl mít přístup. Předejde se tak neautorizovaným zásahům do konfigurace, které mohou vést ke zvýšení rizika kompromitace účtu. Tato konfigurace by měla být prováděna pouze administrátorem dané sítě. V případě použití Windows domény je možné využít centralizované řešení pomocí *Group Policy*.

[21] Common Name

[22] http://support.microsoft.com/kb/941123

Metoda PEAP je ze své podstaty bezpečná, avšak při jejím nasazení je nutné dbát zvýšené pozornosti při konfiguraci suplikantů klientských stanic. Je nutné korektně nastavit validaci certifikátu RADIUS serveru dle doporučení uvedených výše a tím snížit riziko úspěšného provedení útoku *RADIUS impersonation*.

Důležité je také použití silného hesla ke všem uživatelským účtům. Požadavky na silné heslo jsou uvedeny v kapitole 3.3. Dle možností použitého suplikantu je také vhodné nastavit anonymní identitu přenášenou v nešifrované části PEAP komunikace za účelem snížení možnosti sběru uživatelských jmen.

3.2.5 EAP-TTLS

EAP-TTLS je velice podobná metodě PEAP, kdy je pro potřeby autentizace také vytvářen zabezpečený TLS tunel. Samotná autentizace je potom prováděna pomocí méně bezpečného mechanismu. Tyto mechanismy byly většinou původně navrženy pro použití v sítích s nízkým rizikem odposlechu. Hlavní výhodou EAP-TTLS oproti PEAP je poměrně široká podpora vnitřních autentizačních mechanismů. Podporovány jsou nejen různé EAP metody, ale také autentizační protokoly PAP, CHAP, MSCHAPv1 a MSCHAPv2.

EAP-TTLS je v případě nedostatečné konfigurace[23] na straně klientského suplikantu zranitelná na útok *RADIUS impersonation*, jež dovolí útočníkovi odchycení komunikace v rámci šifrovaného kanálu. Postup provedení tohoto útoku je identický jako v případě metody PEAP. Po kompromitaci šifrovaného kanálu a odchycení vnitřní autentizace závisí další postup na zvolené vnitřní autentizační metodě[10].

V případě použití protokolu **PAP** definovaném v RFC 1334[24] jsou autentizační údaje v rámci šifrovaného kanálu přenášeny v otevřené podobě. Stejná situace je v případě použití **EAP-GTC** popsaného v RFC 3748[25], který pro autentizaci používá bezpečnostní tokeny jako například RSA SecurID. V případě EAP-GTC se však jedná o OTP[26], jejichž platnost je omezena na krátký časový interval.

V případě použití CHAP, MSCHAPv1/2 nebo EAP-MD5 může útočník po kompromitaci TLS kanálů zahájit offline slovníkový útok na odchycenou komunikaci, jak již bylo popsáno v předchozích kapitolách.

Doporučení

Stejně jako u metody PEAP platí i u EAP-TTLS uvedená doporučení pro striktní nastavení kontroly certifikátů u klientských suplikantů za účelem snížení možnosti útoku *RADIUS impersonation*, použití silného hesla a anonymizace identity.

Jako vnitřní autentizační protokol není vhodné používat PAP, který v případě kompromitace TLS kanálu dává útočníkovi instantní přístup k heslu. Doporučenou vnitřní autentizační metodou je MS-CHAPv2 v kombinaci se silným heslem či EAP-GTC využívající HW tokeny a OTP hesla.

3.2.6 EAP-TLS

EAP-TLS je jedna z mála EAP metod, která vyžaduje nasazení serverových i klientských certifikátů. To jí činí mimořádně bezpečnou, avšak zároveň poměrně obtížně implementova-

[23] Vynechaná nebo nedostatečná kontrola serverového certifikátu
[24] http://www.ietf.org/rfc/rfc1334.txt
[25] http://tools.ietf.org/html/rfc3748
[26] One Time Password - jednorázové heslo tvořené obvykle posloupností číslic

telnou ve srovnání s ostatními[10]. Hlavním problémem je vybudování PKI infrastruktury v dané organizaci a správa a distribuce certifikátů klientům.

EAP-TLS poskytuje vzájemnou autentizaci na základě validace certifikátů během procedury TLS handshake[22]. Vzhledem k použití klientských certifikátů je nemožné tuto metodu kompromitovat prostřednictvím útoku *RADIUS impersonation*. Kompromitace uživatelského účtu by musela být podmíněna krádeží certifikátu, který navíc může být chráněn PINem[27]. Klientský certifikát může být uložen buď v souborovém systému klienta, nebo externě na čipové kartě.

Doporučení

Metoda EAP-TLS sama o sobě poskytuje vysokou úroveň zabezpečení. Ta může být ještě posílena použitím čipových karet namísto uložení certifikátu v souborovém systému a také ochranou klientského certifikátu PINem.

3.3 Shrnutí

Skrytí SSID dané sítě je bezpečnostní prvek, který může odradit amatérské a nemotivované útočníky, avšak pro zkušeného útočníka se jedná o minimální překážku. Obecně se jedná o uplatnění principu *Security through obscurity*, který je z bezpečnostního hlediska zavrhován[35]. Korektně zabezpečená síť musí za každých podmínek odolat útoku zvenčí, proto by hlavní pozornost měla být věnována hlavně výběru bezpečné autentizační metody a způsobu šifrování. Nastavení skrytého SSID také snižuje uživatelský komfort při konfiguraci nového připojení k dané síti a může tak být uživateli vnímáno negativně.

Filtrování MAC adres klientů tvoří další vrstvu ochrany v rámci řízení přístupu k bezdrátové síti. Stejně jako v případě skrytého SSID však ani tento bezpečnostní mechanismus nepředstavuje pro útočníka větší problém. Ve firemních bezdrátových sítích, kde se k síti připojuje spíše neměnná množina klientů, je vhodné filtrování dle MAC adres nasadit. V případě nového klienta (nový zaměstnanec, nový notebook) je nutno danou adresu povolit pouze jednou, a to před prvním přihlášením nového zařízení do sítě. Naproti tomu v návštěvnických WiFi sítích by toto nastavení znamenalo nutnost manuálně zavést do seznamu povolených MAC adres adresu každého návštěvníka, což by v případě jejich vysokého počtu bylo krajně nepraktické. Zároveň s nasazením tohoto způsobu zabezpečení je vhodné v bezpečnostní politice definovat odpovědnost za rušení neplatných záznamů (například všechna zařízení propuštěného zaměstnance).

V rámci výběru vhodného šifrování bezdrátové sítě je z hlediska bezpečnosti situace poměrně jednoduchá. Bezpečnostní protokol WEP by neměl být za žádných okolností použit. Standard WPA-TKIP by měl být použit pouze v případě, kdy se v rámci sítě nacházejí zařízení nepodporující standard WPA2-CCMP. Ve všech ostatních případech je doporučené využít právě WPA2-CCMP, který je v současné době považován za bezpečný.

Výběr vhodné EAP metody

Dalším důležitým krokem při zabezpečení 802.1X bezdrátové sítě je výběr vhodné autentizační metody. V roce 2005 bylo vydáno RFC 4017[28] definující bezpečnostní požadavky na EAP metodu. Standard IEEE 802.11i říká, že EAP metoda použitá v případě bezdrátové

[27] Personal Identification Number

[28] http://www.ietf.org/rfc/rfc4017.txt

sítě by měla splňovat požadavky uvedené právě v tomto RFC. RFC 4017 se tak stalo de facto neoficiálním standardem pro EAP metody použité v bezdrátových sítí[14].

Požadavky uvedené v tomto RFC se dělí na povinné, doporučené a volitelné. Z povinných se jedná o požadavek na generování *Master Session* klíče během autentizace. Na základě tohoto klíče je po dokončení autentizace inicializováno šifrování prostřednictvím algoritmů AES či TKIP. Dalším povinným požadavkem je požadavek na vzájemnou autentizaci. Vzájemná autentizace musí proběhnout v rámci jedné EAP komunikace. Použití dvou EAP metod v opačných směrech tak není vzájemnou autentizací tak, jak je definována v RFC 3748[29]. Metoda musí být odolná vůči offline slovníkovému útoku a vůči útoku *Man in the Middle*.

Doporučené požadavky by dle RFC 4017 měly splňovat specificky EAP metody, které jsou použité v bezdrátové síti. Těmito požadavky jsou podpora fragmentace a podpora anonymizace uživatelské identity, přenášené v otevřené podobě. RFC 4017 definuje ještě dva volitelné požadavky a to podpora *Fast Reconnect* a *Channel binding*. Funcionalita *Fast Reconnect* byla popsána v sekci 2.5.2.

Přímo v RFC 4017 jsou za nevyhovující označeny EAP metody EAP-MD5, EAP-GTC a EAP-OTP[33]. Naproti tomu metody PEAP, EAP-TTLS, EAP-TLS i EAP-FAST splňují požadavky uvedené v tomto RFC[22]. Co se týče metody LEAP, ta neposkytuje ochranu vůči slovníkovému útoku, jak bylo demonstrováno v kapitole 3.2.2.

V případě výběru EAP metody pro implementaci v rámci bezdrátové sítě je doporučené vybrat jednu z metod splňujících nároky požadované v RFC 4017. Jednoznačně nejvyšší úroveň bezpečnosti z EAP metod poskytuje EAP-TLS, jež je postavena na vybudování PKI infrastruktury serverových i klientských certifikátů, což ji činí poměrně náročnou na implementaci. Přehledné porovnání jednotlivých metod protokolu EAP z různých hledisek je uvedeno v tabulce 3.1.

Tvorba hesla

Většina metod protokolu EAP využívaná v případě bezdrátových sítí je založena na autentizaci pomocí hesla. Hesla by měla splňovat určité bezpečnostní zásady. Bezpečnostní pravidla pro vytvoření hesla by měla být stanovena politikou hesel. Následuje příklad bezpečnostní politiky vynucující tvorbu bezpečných hesel:

1. Délka hesla alespoň 8 znaků.
2. Nutnost použití kombinace alfanumerických a speciálních znaků.
3. Udržení historie alespoň 5 hesel.
4. Expirace hesla po 120 dnech.

[29] http://tools.ietf.org/html/rfc3748

	EAP-MD5	LEAP	EAP-FAST	EAP-TLS	EAP-TTLS MS-CHAPv2	PEAP MS-CHAPv2	PEAP EAP-GTC
Serverový certifikát	Ne	Ne	Volitelně	Ano	Ano	Ano	Ano
Klientský certifikát	Ne	Ne	Ne	Ano	Ne	Ne	Ne
Vzájemná autentizace	Ne	Ano	Ano	Ano	Ano	Ano	Ne
Kompatibilita s WPA	Ne	Ano	Ano	Ano	Ano	Ano	Ano
Tunelovaná autentizace	Ne	Ne	Ano	Ano	Ano	Ano	Ano
Skrytí identity	Ne	Ne	Ne	Ne	Ano	Ano	Ano
Fast reconnect	Ne	Ne	Ano	Ano	Ano	Ano	Ano
Splňuje požadavky z RFC 4017	Ne	Ne	Ano	Ano	Ano	Ano	Ano

Tabulka 3.1: Srovnání jednotlivých EAP metod

Kapitola 4

Bezpečnostní audit

S tím, jak se informační technologie postupně rozšiřovaly a integrovaly do fungování a řízení kritických procesů organizací a podniků, rostl požadavek na jejich bezpečnost. Bezpečnost informačních systémů ve stručnosti chápeme jako požadavek na zajištění základních bezpečnostních hledisek, kterými jsou důvěrnost, integrita, dostupnost, autenticita a nepopiratelnost[9].

Pro zjištění bezpečnostního stavu daného IS je nutné provést jeho kontrolu a ověřit, zda a do jaké míry jsou výše uvedená bezpečnostními hlediska splněna. Právě tento postup pak nazýváme bezpečnostním auditem. Bezpečnostní audit informačního systému je poměrně komplexní úkon, proto nebývá prováděn nahodile, ale podle určité normy, metodiky či standardizovaného postupu.

V této kapitole bude uveden vývoj bezpečnostních norem a možnost jejich uplatnění pro bezpečnostní audit bezdrátových sítí. Dále bude navržena a popsána vlastní metodika pro realizaci bezpečnostního auditu bezdrátové sítě s autentizací dle standardu 802.1X.

4.1 Základní pojmy

Jak již bylo uvedeno výše, bezpečnost chápeme jako zajištění určitých bezpečnostních hledisek. Následuje vysvětlení jejich významu:

- **Důvěrnost** - Přístup k datům/aktivům IS má pouze autorizovaný subjekt.
- **Integrita** - Informace nemůže být v rámci komunikace neautorizovaně modifikována.
- **Dostupnost** - Autorizovaný uživatel má vždy má vždy definovaným způsobem a po určitou dobu přístup k IS.
- **Autenticita** - Je zajištěna ověřitelnost původu informací.
- **Nepopiratelnost** - Původce nemůže popřít vykonání akce či doručení zprávy.

V oblasti bezpečnostních auditů a penetračních testů jsou dále často používány pojmy testování metodou Blackbox, Whitebox a Greybox. Tyto pojmy budou dále v práci používány, proto následuje jejich vysvětlení.

- **Blackbox testing** - V případě provádění bezpečnostního auditu metodou Blackbox simuluje auditor činnost útočníka, který nemá o dané síti žádné bližší informace a znalosti a přistupuje k ní pouze zvenčí. Cílem takového auditu je především nalezení zranitelností umožňujících získání neautorizovaného přístupu do dané sítě.

- **Whitebox testing** - Opakem je potom bezpečnostní test metodou Whitebox, kdy má auditor plný přístup ke všem požadovaným informacím. Může tak nahlížet do konfigurací jednotlivých zařízení a služeb, případně může být získání znalostí provedeno pohovorem s odpovědnými osobami, jakými jsou například správce sítě, systémový administrátor či bezpečnostní manažer. Cílem bezpečnostního auditu metodou Whitebox je pak především nalezení konfiguračních pochybení, které nejsou většinou prostřednictvím metody Blackbox detekovány.

- **Greybox testing** - Kombinací obou uvedených postupů je potom testování metodou Greybox, kdy útočník přistupuje k dané síti zvenčí, avšak disponuje určitými znalostmi o této cílové síti.

Dalšími často používanými pojmy jsou **bezpečnostní audit** a **penetrační test**. Označení penetrační test je používáno spíše v souvislosti s metodou Blackbox, zatímco bezpečnostní audit se váže spíše k metodě Whitebox. V rámci této práce však budou tyto pojmy chápány jako synonyma a nebude mezi nimi činěn rozdíl.

4.2 Historie

První mezinárodně uznávanou normou zaměřenou na hodnocení bezpečnosti IS se stal **TCSEC**[1] (*Trusted Computer System Evaluation Criteria*) vydaný v roce 1983 ministerstvem obrany Spojených států amerických. TCSEC je první z řady bezpečnostních norem vydávaných ministerstvem obrany USA a později NCSC (*National Computer Security Center*) v osmdesátých a devadesátých letech dvacátého století. Tato řada je označována jako *Rainbow Series*, jelikož každá z knih má svoji specifickou barvu desek. TCSEC je tak podle svého oranžového obalu neformálně označován jako *Orange book*. TCSEC zavádí stupnici sedmi kategorií, do kterých může auditovaný systém na základě splnění požadavků spadat[28].

Evropským protějškem TCSEC se v roce 1990 stala norma **ITSEC**[2] (Information Technology Security Evaluation Criteria) vytvořená z národních norem států Francie, Německa, Nizozemska a Velké Británie. Aktualizovaná verze normy byla vydána Evropskou komisí v roce 1991. Na rozdíl od TCSES disponuje norma ITSEC dvourozměrnou hodnotící stupnicí, která rozlišuje zaručitelnost a funkčnost[19].

Obě výše uvedené normy byly postupně nahrazeny standardem ISO/IEC 15408 označovaným jako **Common Criteria**[3], který (nejen) z těchto norem vychází. První verze této normy byla vydána v roce 1999, poslední aktualizace proběhla v roce 2009 na verzi 3.1. CC stanovují obecně platné sestavy požadavků na bezpečnostní funkce produktů a systémů IT a míry zaručitelnosti bezpečnosti udělované při hodnocení těmto bezpečnostním funkcím, čímž umožňují porovnávat výsledky nezávisle prováděných hodnocení bezpečnosti[19]. Hodnocení podle CC se soustřeďuje především na hodnocení IT produktů, jakými jsou například operační systémy, databázové systémy, síťové prvky či specializované bezpečnostní produkty.

[1] http://csrc.nist.gov/publications/history/dod85.pdf
[2] http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf
[3] Celým názvem *Common Criteria for Information Technology Security Evaluation*, zkráceně pak CC

4.3 OSSTMM

V současné době je jediná rozsáhlejší metodika bezpečnostního testování WLAN sítí obsažená v metodologickém manuálu **OSSTMM**[4] vydaným organizací ISECOM[5]. První verze OSSTMM byla vydána v roce 2000, aktuální verze 3 pochází z roku 2010 a v současné době probíhají práce na verzi 4. OSSTMM je metodologie zaměřující se na audit fyzické bezpečnosti, bezpečnosti telekomunikačních sítí, bezpečnosti datových sítí a právě bezpečností bezdrátových sítí. Bezpečnostní audit bezdrátové WiFi sítě dle OSSTMM se skládá z následujících oblastí[20]:

1. Logistics - Dohodnutí času provedení auditu, zajištění vhodného HW vybavení a specifikace rozsahu auditu.
2. Active Detection Verification - Zjištění nasazení IDS/IPS systémů v rámci testované sítě.
3. Visibility Audit - Detekce dostupných sítí a použitých frekvencí/kanálů.
4. Access Verification - Tato fáze se zaměřuje na konfiguraci přístupových bodů (změna továrního SSID, vhodně nastavená síla signálu, metody autentizace a autorizace, řízení přístupu).
5. Trust Verification - Zjišťování možnosti zneužití důvěry mezi jednotlivými entitami (nastavení klientských autentizačních metod, možnost vytvoření spojení s neautorizovanou entitou).
6. Controls Verification - Ověření zajištění nepopiratelnosti (identifikace uživatelů, logování), důvěrnosti (šifrování dat) a integrity (podepisování zpráv, šifrování).
7. Process Verification - Ověření procesní bezpečnosti (zavedení určení odpovědnosti, vypracování bezpečnostní politiky,...)
8. Configuration Verification - Ověření kvality hesel (slovníkové útoky vůči autentizaci), ověření dodržení bezpečnostní politiky.
9. Property Validation - Zjištění neautorizovaně nasazených přístupových bodů.
10. Segregation Review - Testování zabezpečení citlivých dat, detekce úniku citlivých informací prostřednictvím bezdrátové sítě.
11. Exposure Verification - Testování přesahu bezdrátového signálu mimo vyhrazené prostory.
12. Competitive Intelligence Scouting - Ověření klasifikace všech interních dokumentů s citlivými daty.
13. Privileges Audit - Testování identifikace a autorizace, ověření možnosti eskalace privilegií.
14. Survivability Validation - Zhodnocení řízení kontinuity činností.

[4]The Open Source Security Testing Methodology Manual
[5]Institute for Security and Open Methodologies

15. Alert and Log Review - Zjištění možností detekce probíhajícího útoku (logování, vytvoření alertu, upozornění odpovědné osoby).

Metodika pokrývá test bezdrátové sítě poměrně komplexně. Problémem však je, že jednotlivé oblasti jsou v rámci metodiky OSSTMM popsány velice stručně a řeší pouze *co* testovat, ale již ne jak test provést, jaká rizika z jednotlivých nedostatků vyplývají a jaká se k nim vážou doporučení. Veškeré fáze auditu jsou popsány na vysoké úrovni abstrakce a neobsahují žádné konkrétní kroky ani postupy. Metodika tudíž také neobsahuje žádné postupy pro testování autentizačních metod standardu 802.1X. Realizace praktického auditu bezdrátové WiFi sítě je tak pouze na základě informací uvedených v OSSTMM téměř nemožná. Tato práce má za cíl vytvořit podmnožinu takovéto metodiky a to konkrétně metodiku zaměřenou na analýzu autentizačních metod v rámci nasazení 802.1X bezdrátové sítě.

4.4 Metodika auditu 802.1X bezdrátové sítě

Výše uvedené normy poskytují příliš vysokou míru abstrakce a jejich využití pro bezpečnostní audit konkrétní bezdrátové sítě tak není příliš vhodné. Pro tento účel jsou vhodnější specializované metodiky určené přímo pro jednotlivé technologie. Příkladem specializované metodiky může být například **OWASP Testing Guide**[6], podrobně rozebírající problematiku auditu a penetračního testování webových aplikací a služeb. Jelikož v současné době takto specifická metodika určená pro audit bezdrátových sítí s autentizací dle standardu 802.1X neexistuje, bude v této kapitole navržena a popsána metodika vlastní. Metodika bude popisovat jednotlivé fáze a podfáze realizované během auditu takové sítě.

Předmětem technického auditu 802.1X WiFi sítě jsou následující entity:

- Autentizační servery
- Přístupové body (autentizátory)
- Bezdrátoví klienti

Zatímco v rámci síťové infrastruktury instituce se nachází zpravidla jednotky autentizačních serverů, bezdrátových klientů mohou být stovky. Z toho důvodu není často v rámci rozpočtu bezpečnostního auditu možné provést prověrku konfigurace suplikantu každého z nich. Tato situace je v praxi řešena auditem konfigurace pouze jednoho vzorového klienta s tím, že všichni ostatní mají shodné nastavení, na jehož změnu má oprávnění pouze administrátor. Technický bezpečnostní audit bezdrátové sítí s autentizací dle standardu 802.1X zahrnuje provedení následujících fází:

1. **Detekce použité metody protokolu EAP** - Identifikace autentizační metody, která je v rámci dané sítě použita je základním krokem při provádění technického auditu. Na základě tohoto zjištění je poté volen konkrétní postup, který se v případě jednotlivých metod může dosti lišit. Identifikace lze docílit pasivním odposlechem bezdrátového síťového provozu. K identifikaci dojde vždy, když je zachycena komunikace právě se autentizujícího klienta. Pasivní odposlech je zcela nedetekovatelný sondami

[6] The Open Web Application Security Project

WIPS[7]. Pro urychlení této fáze lze však využít aktivní deautentizaci připojeného klienta nebo klientů, čímž je vynucena jejich opětovná autentizace, v rámci které je možné identifikovat zvolenou metodu protokolu EAP. Tuto akci je už však možné detekovat WIPS sondami (viz podkapitola 5.1.5).

2. **Získání přístupu** - Ve fázi získání přístupu je proveden aktivní útok za účelem zjištění kvality hesel případně konfigurace jednotlivých klientů. Dále bude následovat stručný popis vykonaných akcí v rámci auditu v případě identifikace jednotlivých metod protokolu EAP. Podrobný popis zranitelností a nedostatků těchto metod byl popsán v kapitole 3.2.

   (a) **EAP-MD5** - Metoda EAP-MD5 je zranitelná na útok vedoucí k odhalení hesla připojeného klienta. Po odchycení autentizace (ať už pasivním odposlechem či pomocí vynucené deautentizace) je možné provést offline útok hrubou silou na autentizační mechanismus této metody. V případě využití slabého nebo slovníkového hesla je tak vysoká pravděpodobnost jeho kompromitace. Pokud se tímto způsobem podaří kompromitovat hesla některých uživatelů, značí to, že v dané síti není aplikována dostatečně silná politika hesel. Dále pokud je detekováno použití metody EAP-MD5, automaticky to znamená, že daná síť nevyužívá šifrování přenášených dat, jelikož metoda EAP-MD5 nepodporuje generování klíčového materiálu[8]. Z toho plyne vážné riziko možnosti odposlechu přenášených dat v případě, že nejsou využity šifrované verze aplikačních protokolů (HTTPS, POP3S, SMTPS,...). V případě detekce metody EAP-MD5 je vždy doporučeno použití metody protokolu EAP zajišťující vyšší bezpečnost. Pokud dojde ke kompromitaci hesel některých uživatelů, je dále doporučeno zavedení, případně zesílení, politiky hesel v rámci dané sítě/domény.

   (b) **LEAP** - Postup v případě metody LEAP je podobný jako v předcházejícím případě. Po odchycení autentizace daného klienta je zahájen slovníkový útok. Autentizační mechanismus metody LEAP navíc trpí zranitelností (popsanou v kapitole 3.2.2), která umožňuje útoku hrubou silou ještě dále urychlit. V případě detekce metody LEAP je vždy doporučeno použití metody protokolu EAP zajišťující vyšší bezpečnost (například metoda EAP-FAST, která byla přímo společností Cisco System určena jako nástupce metody LEAP). Pokud dojde ke kompromitaci hesel některých uživatelů je dále doporučeno zavedení, případně zesílení, politiky hesel v rámci dané sítě/domény.

   (c) **EAP-FAST** - Metoda EAP-FAST je většinou auditována metodou Whitebox. Hlavní riziko při nasazení této metody spočívá v nezabezpečené distribuci PAC souborů jednotlivým klientům v rámci nulté fáze autentizace. Jelikož tato nultá fáze probíhá pouze při nasazení této metody a poté vždy při přidání nového uživatele nebo expiraci hodnoty PAC, je velice nepravděpodobné, že by byla tato fáze odchycena zrovna v průběhu Blackbox penetračního testu. Konfigurace distribuce PAC souborů klientům je proto zjišťována z konfigurace autentizačního serveru, případně během pohovoru s odpovědnou osobou. V případě, že je distribuce řešena automatickým režimem a zároveň není nasazen serverový certifikát na autentizačním serveru, stává se nultá fáze zranitelná vůči útoku *AP impersonation*, který je popsán v kapitole 3.2.4. Doporučením v případě použití metody

[7] Wireless Instrusion Prevention System
[8] Detailněji bylo popsáno v kapitole 2.5.3

EAP-FAST je nasazení serverového certifikátu pro účely autentizace v rámci nulté fáze.

(d) **PEAP** - Metoda PEAP využívá na rozdíl od metod EAP-MD5 a LEAP pro autentizaci tunel šifrovaný pomocí SSL. Metoda díky tomu není náchylná na útok hrubou silou vůči zachycené autentizaci, jelikož ta je šifrována. Jak již bylo uvedeno v kapitole 2.5.6, metoda PEAP podporuje použití serverového certifikátu za účelem možnosti ověření legitimity autentizačního serveru klientem. Problémem však je, že kontrola serverového certifikátu záleží na konfiguraci klienta. Pokud klient serverový certifikát nekontroluje, stává se náchylný na útok prostřednictvím *AP impersonation*. Výsledkem úspěšného provedení tohoto útoku spolu s útokem hrubou silou je tak odhalení otevřené podoby hesla klienta. V případě bezpečnostního auditu metodou Whitebox je součástí této fáze prověrka konfigurace vybraného klienta s tím, že se předpokládá, že konfigurace všech ostatních klientů je shodná a bez možnosti její editace uživatelem. Právě při této prověrce je ověřováno, zda je v konfiguraci klientského suplikantu vynucena kontrola serverového certifikátu za účelem zabránění útoku *AP impersonation*. Pokud tato volba není vynucena, jedná se o vážné bezpečnostní pochybení.

(e) **EAP-TTLS** - V případě identifikace použití metody EAP-TTLS je postup téměř shodný jako v případě metody PEAP, tedy provedení útoku *AP impersonation* s cílem odhalení hesla uživatele. U EAP-TTLS je možné se navíc zaměřit na použitý vnitřní autentizační mechanismus. Tím může být obvykle PAP[9], CHAP[10], EAP-MD5, MS-CHAPv1 a MS-CHAPv2. V případě, že je jako vnitřní autentizační mechanismus použit protokol PAP, získá auditor po úspěšně provedeném útoku *AP impersonation* rovnou otevřenou podobu hesla. Doporučené je tak použít MS-CHAPv2, který v případě použití opravdu silného hesla zamezí možnosti jeho kompromitace.

(f) **EAP-TLS** - Metoda EAP-TLS poskytuje ze všech používaných metod protokolu EAP nejvyšší úroveň zabezpečení díky vynucení použití klientských certifikátů. Tato metoda není zranitelná na útok hrubou silou vůči autentizačnímu mechanismu ani na útok prostřednictvím *AP impersonation*. V případě detekce využití této metody je vhodné se zaměřit na umístění uživatelských certifikátů a použití PINu. Pokud jsou certifikáty uloženy v operačním systému každého z klientů, je možno doporučit umístění certifikátů na čipové karty, čímž dojde k dalšímu zvýšení úrovně zabezpečení. Každý uživatelský certifikát by pak měl být chráněn dostatečně silným PINem.

3. **Enumerace uživatelských jmen** - Jak již bylo popsáno výše, protokol EAP přenáší během autentizace uživatelská jména v otevřené podobě. Pro enumeraci uživatelských jmen tak postačuje klasický pasivní odposlech bezdrátového provozu případně spojený i s aktivní deautentizací připojených klientů pro urychlení sběru jmen. Přihlašování v rámci bezdrátové sítě s autentizací dle standardu 802.1X je často propojeno s Windows doménou, kdy se databáze uživatelů nachází na doménovém kontroleru. V takovém případě jsou zachycená uživatelská jména doménovými uživateli dané Windows domény. Odchycená doménová uživatelská jména lze poté využít například i v rámci interního penetračního testu pro útok hrubou silou vůči doménovému kontroleru nebo

[9] Password Authentication Protocol
[10] Challenge Handshake Authentication Protocol

uživatelským stanicím s cílem odhalení hesla daného uživatele. Z odchycených uživatelských jmen je také možné odhadnout pravidla pro vytváření těchto jmen. V případě, že jsou vytvářená uživatelská jména příliš krátká[11], hrozí riziko hádání takto vytvářených jmen útočníkem. Toto riziko je však reálné spíše v prostředí interní sítě, kde by bylo možné toto hádání zautomatizovat. Výstupem této fáze je seznam zachycených uživatelských jmen. Celá tato fáze může být přeskočena v případě, že mají všichni připojení klienti nakonfigurováno skrývání identity. V opačném případě je vhodné tuto konfiguraci doporučit.

4. **Audit zařízení a služeb** - Tato fáze je prováděna v případě Whitebox auditu. Předmětem auditu jsou v této fázi konfigurace přístupových bodů (autentizátorů) a autentizačních serverů (například RADIUS či DIAMETER servery). Je kontrolováno, zda je nastaveno dostatečně silné šifrování přenášených dat (WPA-AES a ne WPA-TKIP či dokonce WEP), zda je korektně nastaveno logování tak, aby bylo možné v případě incidentu jednoznačně vyhledat viníka či zda je použitý software aktuální. V této fázi může být taktéž ověřena procesní bezpečnost, zaměřující se například na stanovení odpovědností v případě incidentů, zastupitelnost, zpracovávání a uchovávání log záznamů či záplatování. Tato práce se však zaměřuje pouze na technickou část bezpečnostních testů a procesní bezpečnost zde řešena nebude.

Celý audit je možné provést pouze prostřednictvím volně dostupných nástrojů, z nichž je naprostá většina určená pro unixové platformy. Následuje výčet a stručný popis vybraných nástrojů použitelných jako podpora při realizaci bezpečnostního auditu 802.1X WiFi sítě.

- **airodump-ng** - Nástroj ze známého balíku aplikací nazvaného Aircrack sloužící pro enumeraci všech dostupných WiFi sítí. U každé sítě jsou přehledně zobrazeny informace jako SSID, BSSID, použitý bezpečnostní mechanismus, asociovaní klienti a další. Program zvládá identifikaci použití 802.1X, avšak již nepodporuje detekci použité autentizační metody.

- **Kismet** - Alternativa k nástroji airodump-ng. Kromě zobrazení informací o jednotlivých sítích Kismet podporuje práci s GPS a také obsahuje jednoduchý WIPS[12] modul.

- **aireplay-ng** - Nástroj z téhož balíku jako nástroj airodump-ng slouží (mimo jiné) k aktivní deautentizaci připojených klientů. Prostřednictvím tohoto nástroje je možné plošně deautentizovat veškeré připojené klienty dané sítě (zasláním deautentizačních rámců na broadcast), anebo útok omezit na konkrétního klienta.

- **mdk3** - Nástroj mdk3 je možné taktéž využít pro plošnou deautentizaci klientů.

- **Wireshark, tcpdump** - Oba nástroje slouží pro analýzu datového toku. Tato funkcionalita může být v rámci auditu využita pro analýzu EAP komunikace a zjištění použité metody. Takováto ruční analýza je však poměrně zdlouhavá a neefektivní.

- **eapmd5pass, md5crack** - Obě aplikace umožňují provedení offline slovníkového útoku vůči zachycené autentizaci prostřednictvím metody EAP-MD5.

[11] Například dva nebo tři znaky
[12] Wireless Intrusion Prevention System

- **asleap** - Nástroj umožňuje provedení offline slovníkového útoku vůči autentizaci prostřednictvím metody LEAP. V rámci této funkcionality aplikace implementuje optimalizovanou metodu slovníkového útoku tak, jak byla popsána v kapitole 3.2.2. Dále nástroj umožňuje slovníkový útok vůči zachycené autentizaci MS-CHAPv2, která může být získána v případě použití metody PEAP a provedení útoku *AP impersonation*.

- **THC-LEAPcracker** - Jak již z názvu aplikace vyplývá, nástroj implementuje offline slovníkový útok (taktéž optimalizovaný) vůči metodě LEAP a jedná se tak alternativu k programu asleap.

- **freeradius-wpe** - Jedná se o patch na nejrozšířenější volně dostupnou implementaci RADIUS serveru. Patch zajistí logování veškerých autentizačních řetězců, na které může být poté vykonán slovníkový útok prostřednictvím aplikací popsaných výše. Využití tohoto nástroje pro útok *AP impersonation* bylo popsáno v kapitole 3.2.4.

V této kapitole byly představeny jednotlivé fáze bezpečnostního auditu 802.1X sítě. U každé fáze bylo uvedeno shrnutí jednotlivých činností, které tuto fázi tvoří. Byl zde také uveden seznam aplikací, které slouží jako podpora pro vlastní realizaci auditu. Uvedené nástroje pokrývají značnou část auditu, avšak zde chybí aplikace pro pohodlnou enumeraci uživatelských jmen, zjištění použité EAP metody, zjištění všech EAP metod podporovaných daným autentizačním serverem a také chybí jakákoliv vazba mezi těmito nástroji, která by umožnila alespoň částečnou automatizaci provádění bezpečnostního auditu. Přesně tyto nedostatky si klade za cíl odstranit aplikace implementovaná v rámci praktické části této práce. Návrh a implementace této aplikace jsou popsány v následující kapitole.

Kapitola 5

EAPtool

V rámci praktické části práce byla implementována aplikace sloužící pro analýzu protokolu EAP s cílem usnadnění auditu bezdrátové WiFi sítě s autentizací dle standardu 802.1X[1]. Nástroj bude označován jako EAPtool. Aplikace primárně slouží bezpečnostním auditorům pro usnadnění technické části auditu bezdrátové WiFi sítě s autentizací založené na standardu 802.1X. Další cílovou skupinou jsou síťoví administrátoři, kteří si pomocí aplikace mohou ověřit konfiguraci autentizačního serveru, případně demonstrovat praktický útok na použitou EAP metodu.

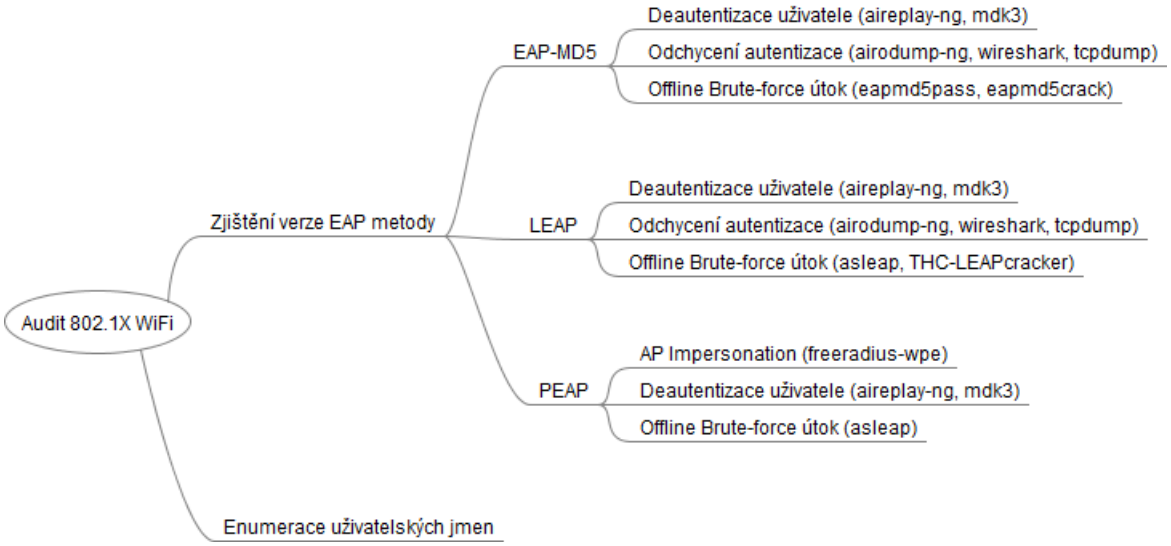
Auditem 802.1X WiFi sítě je v kontextu aplikace EAPtool myšlen proces analýzy zabezpečení takové sítě spočívající v odhalení použité metody protokolu EAP, enumeraci uživatelských jmen připojených klientů a odhalení hesel těchto klientů tak, jak bylo popsáno v kapitole 4.4.

Při vytváření aplikace byl kladen důraz na implementaci funkcionalit, které nejsou nabízeny žádným veřejně dostupným nástrojem. Bezpečnostní audit 802.1X WiFi sítě zahrnuje provedení několika fází. První fází je samotná detekce použité metody protokolu EAP. Tato fáze je v rámci auditu sítě zásadní, jelikož informace získaná v této fázi ovlivňuje následující postup. Paralelně s fází zjištění použité metody protokolu EAP probíhá fáze enumerace uživatelských jmen. Jak již bylo uvedeno v předešlém textu, uživatelská jména se v rámci protokolu EAP přenášejí v otevřené podobě[2]. Jelikož jsou tato uživatelská jména často zároveň doménovými účty Windows domény, představují pro potenciálního útočníka cenné informace.

Na obrázku 5.1 jsou graficky znázorněné jednotlivé fáze a podfáze auditu 802.1X WiFi sítě s tím, že u každé z fází jsou v závorce uvedené nástroje použitelné k vykonání všech akcí spojených s touto fází. Každá z fází deautentizace připojeného klienta, odchycení procesu autentizace, offline útok hrubou silou vůči autentizaci v rámci metody EAP-MD5, LEAP a PEAP a provedení útoku AP impersonation je pokryta minimálně jedním nástrojem, který nabízí požadované funkcionality. Z obrázku je však zároveň patrné, že fáze zjištění použité metody protokolu EAP a enumerace uživatelských jmen nejsou implementovány žádnou veřejně dostupnou aplikací. Nástroj EAPtool si klade za cíl doplnit podporu pro tyto fáze a zároveň poskytnout určitou možnost automatizace nad procesem provedení auditu 802.1X sítě.

[1] Dále jen 802.1X WiFi

[2] Pokud předpokládáme, že není využito skrývání identity.



Obrázek 5.1: Fáze auditu 802.1X WiFi sítě

5.1 Návrh

Nástroj EAPtool funguje v několika základních módech činnosti, jejichž podrobný popis je uveden dále v této kapitole.

Jednou z hlavních takových funkcionalit programu je extrakce informací o použité EAP metodě na základě pasivního odposlechu síťového provozu. Tato funkcionalita je podrobněji popsána v podkapitole 5.2. Další funkcionality nástroje EAPtool zahrnují aktivní enumeraci podporovaných EAP metod daného RADIUS serveru (podkapitola 5.3), automatizaci získání hesla uživatele ze zachycené komunikace v případě použití metod EAP-MD5, LEAP (podkapitola 5.4), podporu pro automatizaci útoku AP impersonation vedoucího k odhalení hesla uživatele v případě použití metody PEAP (podkapitola 5.1.4) a jednoduchý WIDS[3] režim (podkapitola 5.1.5).

V rámci těchto režimů činnosti podporuje nástroj EAPtool odhalení skrytého SSID extrakcí dat z *Probe request/response* paketů, překlad MAC adres síťových prvků na název výrobce daného zařízení, vícevláknové zpracování a další funkcionality usnadňující použití aplikace a zjednodušení provedení analýzy 802.1X sítě.

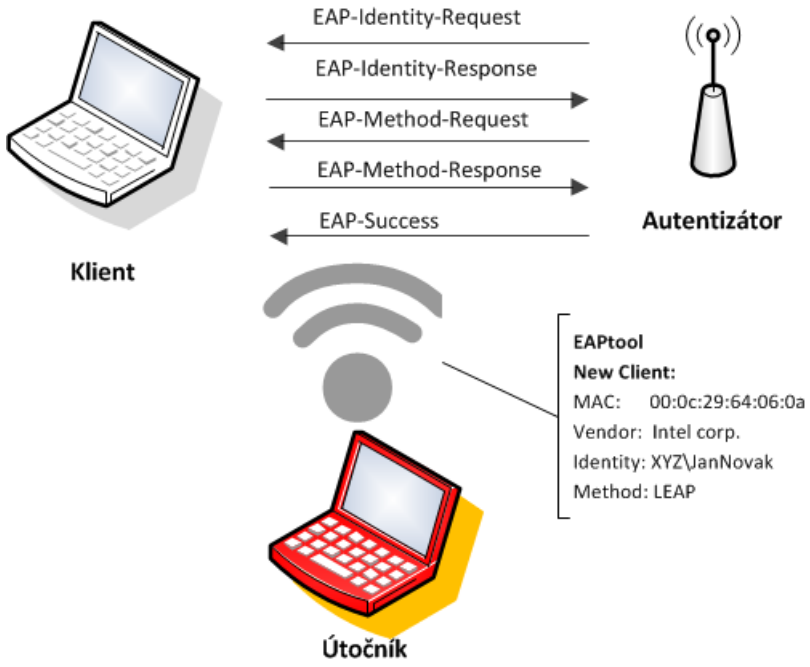
5.1.1 Pasivní režim

Aplikace v pasivním režimu naslouchá bezdrátovému síťovému provozu a přehledně zobrazuje informace o dostupných sítích využívajících 802.1X autentizaci. U každé sítě je postupně zobrazován seznam klientů v pořadí, jak se k dané síti připojují. Při připojení klienta k síti pomocí protokolu EAP je tato komunikace zachycena a zpracována. U každého klienta je potom zobrazena jeho identita (uživatelské jméno) a EAP metoda použitá pro autentizaci. Jelikož různí klienti mohou využít pro autentizaci různé EAP metody, je u každé sítě souhrnně zobrazován seznam podporovaných EAP metod[4]. Aplikace v pasivním režimu je

[3] Wireless Intrusion Detection System

[4] Tedy EAP metod podporovaných použitým autentizačním serverem

neodhalitelná prostředky WIPS[5], jelikož nijak aktivně nezasahuje do bezdrátového provozu. Jelikož komunikace prostřednictvím protokolu EAP mezi klientem a přístupovým bodem probíhá pouze během autentizace klienta do sítě, je možné pro urychlení sběru dat využít deautentizaci připojených klientů. V takovém případě se však již tato akce stává detekovatelnou sondami WIDS (viz kapitola 5.1.5). Tento režim má za cíl zjistit konfigurační pochybení spočívající v podpoře zranitelných EAP metod na autentizačním serveru a také konfigurační odchylky na straně klientů. Schéma činnosti aplikace v pasivním režimu je znázorněno na obrázku 5.2.



Obrázek 5.2: Činnost aplikace EAPtool v pasivním režimu

Na výpisu 5.1 je příklad výstupu nástroje EAPtool spuštěného v pasivním režimu. Výpis se zakládá na skutečném měření v rámci bezpečnostního auditu, veškeré citlivé informace byly anonymizovány a celkově byl výstup nástroje EAPtool zkrácen. Neodsazený blok obsahuje informace o přístupovém bodu, zatímco odsazené bloky reprezentují jednotlivé klienty. Informace o AP obsahují MAC adresu, výrobce daného zařízení, SSID, identitu AP a seznam podporovaných metod protokolu EAP. Identita AP je propagována uvnitř *EAP Request Identity* rámce a jedná se o nepovinnou položku. V tomto případě obsahuje identita přístupového bodu SSID, identifikaci NAS[6] a jeho portu. Posledním a nejdůležitějším údajem o daném AP z hlediska bezpečnostního auditu 802.1X WiFi sítě je seznam podporovaným metod. V kontextu zde uvedeného výstupu lze seznam podporovaným metod interpretovat následujícím způsobem: RADIUS server navrhnul klientům pro autentizaci použít protokol LEAP, ten byl však klienty odmítnut (z důvodu, že suplikant daného klienta tuto metodu nepodporuje, anebo má její použití zakázané) a místo něho byla zvolena metoda PEAP, prostřednictvím níž proběhla autentizace.

Informace o připojeném klientovi zahrnují jeho MAC adresu, výrobce síťového adaptéru,

[5]Wireless Intrusion Detection System
[6]Network Access Server

identitu klienta (uživatelské jméno) a metodu protokolu EAP, kterou klient pro autentizaci k síti využil. Z výpisu je také patrné, že identity klientů jsou zároveň doménovými jmény ve Windows doméně XYZ a také to, že uživatel Novák přistupuje k síti pravděpodobně prostřednictvím svého mobilního telefonu, zatímco uživatel Šťastný prostřednictvím PC. Toto rozlišení může v určitých případech usnadnit lokalizaci daných klientů při provádění bezpečnostního auditu.

Výpis 5.1: Nástroj EAPtool v pasivním režimu

```
BSSID:      00:23:eb:01:01:01
Vendor:     Cisco Systems
SSID:       CompanyXYZ
Identity:   networkid=CompanyXYZ,nasid=Praha,portid=13
EAP-types: LEAP PEAP
Clients:

    MAC:       64:a7:69:02:02:02
    Vendor:    HTC Corporation
    Identity: XYZ\jnovak
    EAP-types PEAP

    MAC:       00:22:fb:03:03:03
    Vendor:    Intel Corporate
    Identity: XYZ\mstastny
    EAP-types PEAP
```

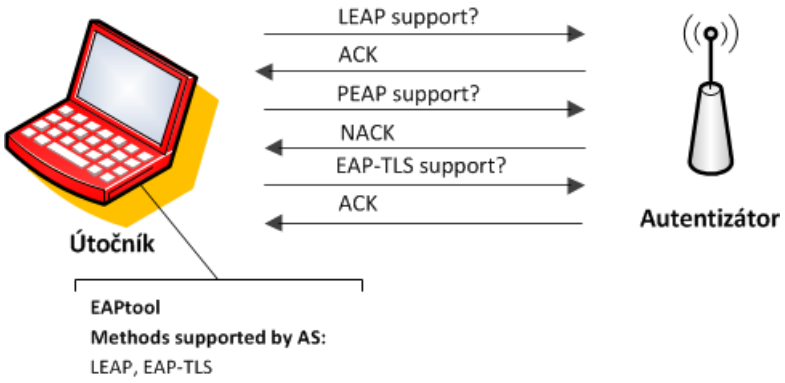
Z výpisu můžeme taktéž vyvodit bezpečnostní riziko, které spočívá v podpoře zastaralé metody LEAP na straně RADIUS serveru. Nebyl sice detekován žádný klient, který by metodu pro autentizaci využil, avšak nelze vyloučit možnost, že takový klient existuje. Metoda LEAP by v současné době neměla být použita. Dále můžeme z uvedeného výstupu programu vyvodit potenciální riziko[7], že uživatelé používají pro připojení k síti své mobilní telefony, což může být v rozporu s bezpečnostní politikou dané společnosti.

Nástroj EAPtool dokáže v pasivním režimu rozpoznat použití těchto metod autentizačního protokolu EAP: EAP-MD5, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, RSA-SecurID EAP, MS-EAP, EAP-MSCHAPv2, SecurID EAP, EAP-TLV, EAP-HTTP digest, SecureSuite EAP, EAP-SPEKE a EAP-MOBAC.

5.1.2 Aktivní režim

Aplikace v aktivním režimu má za cíl enumerovat podporované EAP metody dané WiFi sítě. V aktivním režimu není využit pasivní sběr informací, ale probíhá přímo komunikace s autentizačním serverem (prostřednictvím autentizátoru - přístupového bodu). Aplikace se v tomto režimu chová jako suplikant pokoušející se připojit k dané sítí. K připojení k síti jsou postupně využívány různé verze EAP metod a následně je analyzována odpověď serveru. Tímto způsobem je možné enumerovat seznam EAP metod podporovaných daným autentizačním serverem. Tento režim má za cíl zjistit konfigurační pochybení spočívající ve zbytečném množství povolených EAP metod či v povolení zranitelných metod. Schéma činnosti aplikace v aktivním režimu je znázorněno na obrázku 5.3.

[7] Avšak v tomto případě se může jednat o False Positive, jelikož je MAC adresa v rámci zařízení změnitelná



Obrázek 5.3: Činnost aplikace EAPtool v aktivním režimu

Na výpisu 5.2 je příklad výstupu aplikace v aktivním režimu. Aplikaci nebyla parametrem předána žádná konkrétní metoda protokolu EAP k otestování, proto proběhl test podpory předdefinované množiny těchto metod. U každé z metod je vždy zjištěno, zda daný RADIUS server metodu podporuje či ne. Občas může dojít k vypršení časového limitu pro odpověď, tak jak se v tomto případě stalo u metody LEAP. V takovém případě je otestování podporu této metody znovu naplánováno až nakonec seznamu. V aktivním režimu dokáže nástroj EAPtool provést enumeraci následujících metod autentizačního protokolu EAP: EAP-MD5, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, RSA-SecurID EAP, MS-EAP, EAP-MSCHAPv2, SecurID EAP, EAP-TLV, EAP-HTTP digest, SecureSuite EAP, EAP-SPEKE a EAP-MOBAC.

Výpis 5.2: Nástroj EAPtool v aktivním režimu

```
EAPtool active enumeration mode
Checking support of these methods: EAP-TLS EAP-MD5 EAP-SPEKE
                                   LEAP EAP-TTLS PEAP EAP-FAST
[+] EAP-TLS is supported
[+] EAP-MD5 is supported
[-] EAP-SPEKE is not supported
[*] LEAP timeout, will try it later
[+] EAP-TTLS is supported
[+] PEAP is supported
[-] EAP-FAST is not supported
[+] LEAP is supported
Supported:     EAP-TLS EAP-MD5 EAP-TTLS PEAP LEAP
Not supported: EAP-SPEKE EAP-FAST
```

5.1.3 Penetrační režim - EAP-MD5, LEAP

Aplikace podporuje dva tzv. penetrační režimy. První penetrační režim je zaměřený na metody EAP-MD5 a LEAP, zatímco druhý penetrační režim cílí na metodu PEAP. Důvodem pro rozdělení těchto dvou režimů je odlišný postup pro získání hesla připojeného klienta. Zatímco v případě metod EAP-MD5 a LEAP je nutné zachytit komunikaci přihlašujícího se klienta, v případě metody PEAP je nutné provést kompletní útok *AP imperso-*

nation popsaný v kapitole 3.2.4. Nástroj prostřednictvím parametrů umožňuje penetrační režim aktivovat buď pouze vůči metodě LEAP nebo pouze vůči metodě EAP-MD5 anebo proti oběma zároveň. To umožňuje bezpečnostnímu auditorovi zaměřit demonstrovaný útok přesně podle jeho potřeb.

Aplikace spuštěná v aktivním LEAP a/nebo EAP-MD5 penetračním režimem využívá stejné uživatelské rozhraní jako v případě pasivního režimu. Na výstup jsou zobrazovány informace o přístupových bodech podporujících 802.1X a připojených klientech. Rozdílem oproti pasivní metodě je hlubší analýza EAP komunikace spočívající v extrakci řetězců *EAP Challenge* a *EAP Challenge Response*. Řetězec *EAP Challenge* je zasílán z RADIUS serveru (prostřednictvím přístupového bodu) klientovi a na základě něho klient vypočte hodnotu odpovědi *EAP Challenge Response* a zašle ji zpět RADIUS serveru, který rozhodne, zda klient poskytl správné autentizační údaje. Způsob výpočtu odpovědi se liší na základě zvolené metody a byl popsán v kapitole 2.5.3 (pro EAP-MD5) a 3.2.2 (pro LEAP).

Během naslouchání síťovému provozu se může stát, že je sice zachycen řetězec *EAP Challenge* a *EAP Challenge Response* náležející stejnému klientovi, avšak každý z jiné přihlašovací instance[8]. Pokud přístupový bod z nějakého důvodu[9] znovu klientovi zasílá výzvu *EAP Challenge*, je v daném rámci inkrementována hodnota *EAP ID*, která slouží k rozlišení jednotlivých přihlašovacích instancí. V rámci testování nástroje EAPtool však bylo prakticky ověřeno, že některé přístupové body tuto inkrementaci neprovádějí pravidelně a často tak nastane situace, kdy mají různé přihlašovací instance stejné *EAP ID*. Z toho důvodu je v rámci nástroje EAPtool implementován mechanismus, který sleduje nejenom *EAP ID* dané komunikační instance, ale taktéž časové rozmezí mezi doručením *EAP Challenge* a odesláním *EAP Challenge Response*. Pokud je toto časové rozmezí vyšší než prahová hodnota, je určeno, že dané řetězce nebyly součástí jedné autentizační instance.

Jakmile jsou v komunikačním toku detekovány obě hodnoty *EAP Challenge* i *EAP Challenge Response* náležející k jedné autentizační instanci, je ukončen pasivní monitorovací režim a autentizační hodnoty jsou předány modulu realizujícímu slovníkový útok s cílem odhalení hesla přihlášeného uživatele. Z tohoto důvodu je nutné aplikaci v penetračním režimu parametrem předat slovník, který bude při hádání hesla využit. Samotná funkcionalita útoku hrubou silou vůči zachycené EAP-MD5 nebo LEAP autentizaci není implementována v rámci nástroje EAPtool, ale je volán externí nástroj, který tuto funkcionalitu nabízí. Nástroj EAP předtím upraví veškerá potřebná data do formátu podporovaného danou aplikací. V případě autentizace EAP-MD5 je využit nástroj *eapmd5pass*[10] a v případě metody LEAP potom nástroj *asleap*[11]. Oba nástroje pocházejí od stejného autora, jímž je výzkumník v oboru bezdrátových sítí Joshua Wright. Důvodem, proč funkcionalita útoku hrubou silou vůči heslu klienta nebyla implementována, je koncepce nástroje EAPtool, která si dává za cíl především zacelit mezeru nacházející se v podpoře pro automatizované provedení určitých fázi bezpečnostního auditu 802.1X WiFi sítě a neslouží k tomu, aby nahradila dosavadní funkční a ověřené nástroje. Druhým cílem je potom propojení nástroje s existujícími aplikacemi za účelem co největší automatizace, avšak se zachováním modularity tak, aby měl bezpečnostní konzultant možnost proces provádění auditu přesně a pohodlně kontrolovat.

[8] Přihlašovací instancí je zde označena jedna autentizace uživatele, která začíná přijetím *EAP Challenge*, pokračuje odesláním vypočteného *EAP Challenge Response* a končí úspěšným či neúspěšným potvrzením autentizace

[9] Například odpověď klienta obsahující *EAP Challenge Response* řetězec nebyla doručena

[10] http://www.willhackforsushi.com/eapmd5pass_-_EAP_MD5_Attack.html

[11] http://www.willhackforsushi.com/Asleap.html

Na výpisu 5.3 je výstup nástroje v penetračním režimu zaměřeném na metodu LEAP. Pasivním režimem byl detekován jeden klient. Jakmile byly zachyceny příslušné autentizační řetězce, byl pasivní režim ukončen a započal útok hrubou silou vůči této zachycené autentizaci s využitím slovníku specifikovaného prostřednictvím parametru programu. Výstupem tohoto režimu je potom uživatelské jméno a heslo klienta anebo informace oznamující, že se heslo klienta v daném slovníku nenachází.

Výpis 5.3: Nástroj EAPtool v LEAP penetračním režimu

```
BSSID:      00:01:42:01:01:01
Vendor:     Cisco Systems
SSID:       CompanyABC
Identity:   N/A
EAP-types:  LEAP
Clients:

    MAC:       00:13:e8:a1:81:9b
    Vendor:    Intel Corporate
    Identity:  ABC\jnovak
    EAP-types  LEAP

Result saved to file EAPtool-2012-04-27-172643.log

Using asleap to crack LEAP authentication...
Credentials sucessfully recovered:

    Username: ABC\jnovak
    Password: koniklec
```

Oba tyto penetrační režimy mohou pracovat online, kdy probíhá analýza komunikace na síťovém rozhraní v reálném čase anebo offline v případě, že je programu předán soubor ve formátu pcap s uloženou síťovou komunikací.

5.1.4 Penetrační režim - PEAP

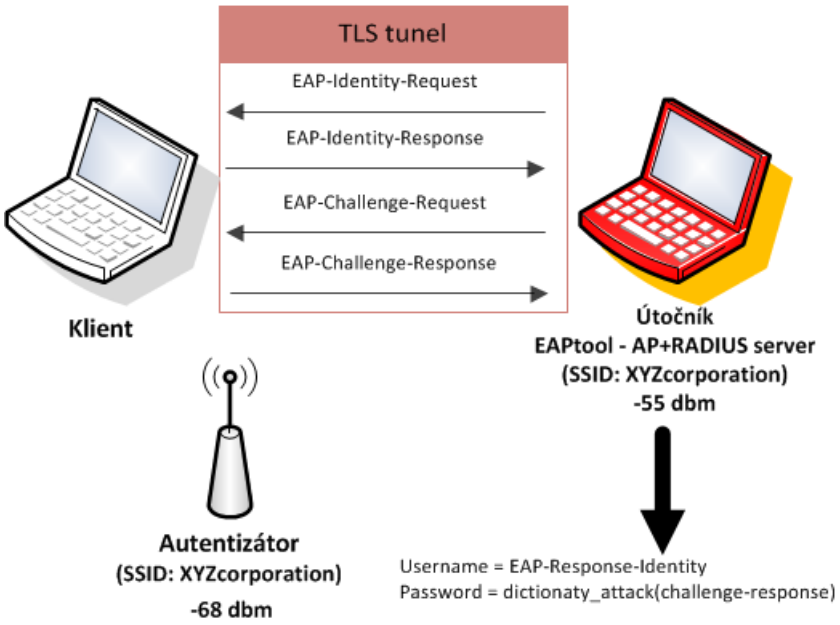
Penetrační režim cílený na metodu PEAP využívá útok *RADIUS impersonation* popsaný v kapitole 3.2.4. Aplikace v tomto režimu využívá modifikovanou verzi Freeradius serveru[12]. Tato verze RADIUS serveru podporuje logování autentizačních řetězců *Challenge* a *Challenge-response*. Režim do určité míry automatizuje nasazení podvrhnuté sítě s RADIUS serverem a proces slovníkového útoku vůči heslu připojeného klienta. Schéma činnosti aplikace v penetračním režimu je znázorněno na obrázku 5.4.

Příklad výstupu programu v PEAP penetračním režimu je uveden na výpisu 5.4. Během úspěšně vykonaného útoku *RADIUS impersonation* došlo k přihlášení dvou klientů. Autentizační data z log souboru RADIUS serveru byla extrahována a následně byl vůči nim vykonán offline slovníkový útok v obou případech vedoucí k odhalení otevřené podoby hesla.

[12] http://www.willhackforsushi.com/FreeRADIUS_WPE.html

Výpis 5.4: Nástroj EAPtool v PEAP penetračním režimu

```
Monitoring /usr/local/var/log/radius/freeradius-server-wpe.log \
for changes

New client detected

Using asleap to crack PEAP authentication...
Credentials sucessfully recovered:

    Username: tester01
    Password: heslo123

-----------------------------------------------------------------
Monitoring /usr/local/var/log/radius/freeradius-server-wpe.log \
for changes

New client detected

Using asleap to crack PEAP authentication...
Credentials sucessfully recovered:

    Username: tester02
    Password: lievik

-----------------------------------------------------------------
Monitoring /usr/local/var/log/radius/freeradius-server-wpe.log \
for changes
```



Obrázek 5.4: Činnost aplikace EAPtool v penetračním režimu

5.1.5 WIDS režim

Posledním z implementovaných režimů, které nástroj EAPtool podporuje, je tzv. WIDS (*Wireless Instrusion Detection System*) režim. Tento režim si klade za cíl detekovat výše popsané útoky proti metodám protokolu EAP. To však z podstaty jednotlivých útoků není možné, jelikož se jedná o pasivní útoky, kdy útočníkovi stačí být v dosahu signálu a naslouchat komunikaci legitimních uživatelů. Jednotlivé fáze bezpečnostní prověrky 802.1 WiFi sítě byly popsány v kapitole 4. Z těchto fází je aktivní pouze fáze aktivní enumerace podporovaných EAP metod a poté podfáze deautentizace uživatele, která je navíc nepovinná a slouží spíše pro urychlení provedení auditu/útoku.

Deautentizace uživatele je realizována zasláním deautentizačního rámce s podvrhnutou zdrojovou MAC adresou. Ta je nastavena na MAC adresu přístupového bodu, ke kterému je klient právě připojen. Cílová MAC adresa může být nastavena jako broadcast[13], kdy na tento rámec reagují svojí deautentizací všichni připojení klienti, anebo může být nastavena na hodnotu MAC adresy konkrétního klienta[39]. Princip enumerace podporovaných metod byl popsán v kapitole 5.3.

Režim WIDS je tak v této[14] verzi nástroje EAPtool omezen pouze na detekci deautentizačního útoku a útoku vedoucího k enumerace jednotlivých podporovaných metod protokolu EAP. V rámci implementace detekce deautentizačního útoku bylo nutné vyřešit problém, jak rozlišit legitimní odeslání deautentizačního rámce, které se děje nejčastěji v případě, kdy se stanice odpojuje od dané sítě, od úmyslného deautentizačního útoku. Jelikož (nejen) MAC adresy deautentizačního rámce mohou být jednoduše podvrženy, je heuristika zaměřena především na počet a frekvenci takovýchto rámců odesílaných se stejnou zdrojovou MAC adresou a na stejnou cílovou MAC adresu. Tyto počty a časové intervaly jsou v datovém toku sledovány a při překročení prahových hodnot je generováno upozornění o pravděpodobně probíhajícím deautentizačním útoku. Podobný princip je uplatněn také v případě enumeračního útoku, kdy jsou po celou dobu komunikace sledováni jednotliví klienti a jimi odeslané rámce typu *EAP NaK*, ve kterých žádají přístupový bod o použití určité EAP metody. Schéma činnosti nástroje v tomto režimu je zobrazeno na obrázku 5.5. V budoucnu je plánováno tento režim rozšířit o další funkcionality, které jsou popsány v podkapitole 5.4.

WIDS režim zajišťuje pouze detekci útoku, program tedy do komunikace nijak aktivně nezasahuje. V případě deautentizačního DoS útoku dokonce ani neexistuje možnost, jak útoku prostřednictvím naslouchající entity zabránit. Obranou proti tomuto útoku může být například zavedení možnosti autentizace deautentizačního rámce tak, aby bylo možné ověřit, zda pochází opravdu z legitimního zdroje[24].

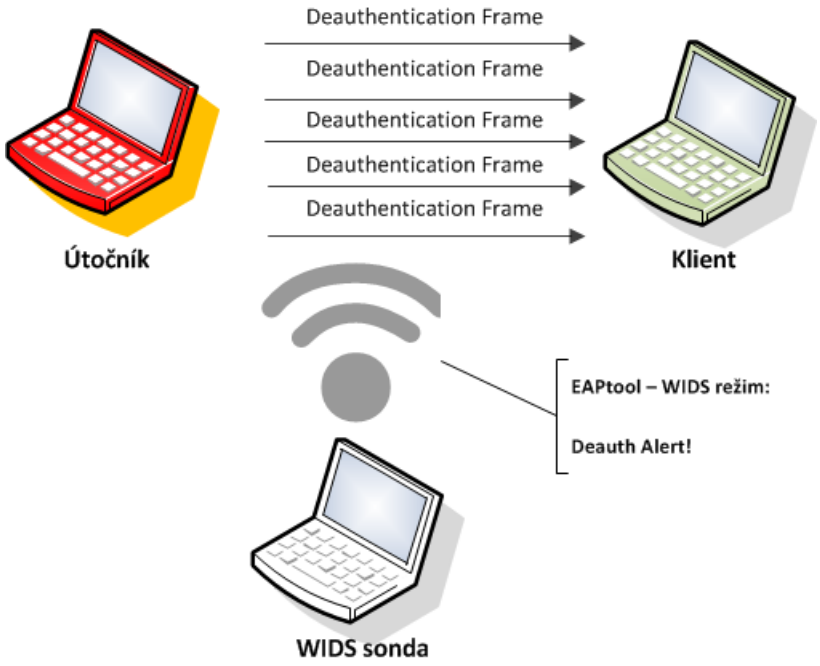
Na výpisu 5.5 je výstup programu ve WIDS režimu. Z výpisu je patrné, že byl detekován deautentizační útok nejprve vedený na všechny klienty autentizované k danému přístupovému bodu a vzápětí se útočník zaměřil na jednoho konkrétního klienta. Poté byla detekována aktivní enumerace EAP metod téhož přístupového bodu. V závorce jsou ve výpisu také uvedeny metody, které se daný klient v krátkém časovém intervalu snažil použít pro přihlášení.

Výpis 5.5: Nástroj EAPtool ve WIDS režimu

```
WIDS mode activated
Listening on interface mon0
```

[13] ff:ff:ff:ff:ff:ff

[14] Další funkcionality, především v rámci WIDS/WIPS režimu budou přidávány během vypracovávání praktické části disertační práce



Obrázek 5.5: Činnost aplikace EAPtool v penetračním režimu

```
28.04.2012 16:22:59 Deauthentication: 74:ea:3a:da:77:02 \
                                      -> ff:ff:ff:ff:ff:ff
28.04.2012 16:23:10 Deauthentication: 74:ea:3a:da:77:02 \
                                      -> 00:13:e8:a1:81:9b
28.04.2012 16:24:14 EAP enumeration:  00:c0:ca:39:f8:ff \
                    -> 74:ea:3a:da:77:02 ( EAP-TLS EAP-MD5 )
```

5.2 Implementace

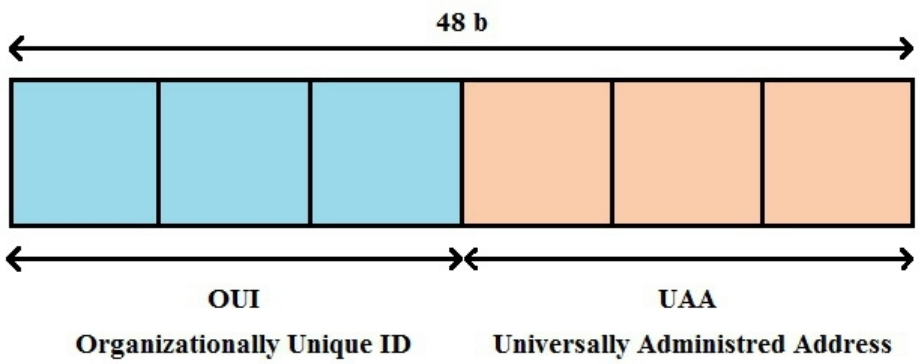
V předchozí části byly popsány hlavní funkcionality programu. Program však dále podporuje množství služeb a funkcí, které usnadňují jeho použití a zpřehledňují prezentaci získaných informací tak, aby auditorovi co nejvíce usnadnily bezpečnostní analýzu 802.1X WiFi sítě se zaměřením na protokol EAP.

5.2.1 Odhalení skrytého SSID

Skrývání SSID slouží jako další úroveň ochrany bezdrátové sítě. Pro zkušenějšího útočníka není však větší problém SSID i přesto odhalit a to například prostřednictvím nástrojů, které tuto funkcionalitu nabízejí. Princip skrývání SSID dané sítě byl popsán v kapitole 2.2. V případě, že nástroj EAPtool detekuje bezdrátovou síť využívající autentizaci dle standardu 802.1X a zároveň s nastaveným skrytým SSID, snaží se SSID zjistit analýzou rámců typu *Probe Request* a *Probe Response*. Jelikož jsou tyto rámce odesílány vždy ve fázi připojení klienta k síti, je možno získání skrytého SSID urychlit deautentizací připojeného klienta nebo klientů.

5.2.2 Překlad MAC adres

V rámci pasivního a penetračního (EAP-MD5, LEAP) režimu jsou na standardní výstup vypisovány informace o jednotlivých přístupových bodech a k nim připojených klientech. Důležitou informací každé z těchto entit je její MAC adresa, v případě přístupového bodu nazývána jako BSSID[15]. Pro větší přehlednost je programem kromě samotné MAC adresy vypisován taktéž výrobce daného zařízení, který je identifikován prvními třemi bajty MAC adresy. Tento identifikátor je nazýván OUI (*Organizationally Unique Identifier*) a přidělován registrační autoritou organizace IEEE[16]. Zbylé tři bajty jsou označovány jako UAA (*Universally Administered Address*) a slouží k identifikaci konkrétního zařízení. Rozdělení MAC adresy na části OUI a UAA je zachyceno na obrázku 5.6. Z výpisu programu je tak například na první pohled čitelné, kteří klienti pravděpodobně k síti přistupují prostřednictvím mobilních telefonů či tabletů, případně zda daná organizace či společnost využívá Cisco zařízení.



Obrázek 5.6: MAC adresa - OUI

Samotný překlad MAC adresy na název výrobce je v rámci programu realizován za pomocí souboru *oui.txt*, což je textový soubor pod správou IEEE obsahující všechna dosud vydaná OUI a názvy příslušných společností[17].

Existují však i poměrně rozšíření výrobci bezdrátových zařízení, kteří stále nemají OUI přidělené. Příkladem může být společnost Airlive, s jejímž zařízením Airlive WL-5460AP byl nástroj EAPtool z velké části testován.

Jelikož je seznam OUI identifikátorů pravidelně aktualizován, obsahuje nástroj EAPtool funkcionalitu pro jeho aktualizaci, kdy je nová verze stažena z webových stránek organizace IEEE.

5.2.3 Multithreading

Aplikace EAPtool pracuje ve více vláknech s tím, že jedno z vláken obsluhuje uživatelské rozhraní, zatímco druhé provádí výpočetní činnost. Aplikace nevyužívá grafické uživatelské rozhraní (GUI), ale dynamické textové uživatelské rozhraní (TUI) realizované pomocí prostředků knihovny *pycurses* (viz podkapitola 5.2.6). Jedno z vláken slouží pro obsluhu

[15] Basic Service Set Identifier
[16] Institute of Electrical and Electronics Engineers
[17] http://standards.ieee.org/develop/regauth/oui/oui.txt

funkcionality scrollování, která může být využita v případě, že množství zobrazených informací přesáhne maximální počet řádků právě otevřené konzole. Pro práci s vlákny je využita standardní knihovna jazyka Python *thread*[18], která umožňuje práci s vlákny na nižší úrovni než v případě podobné knihovny *threading*[19].

5.2.4 Ukládání zachycené komunikace

Pokud je nástroj spuštěn s parametrem -s, po jeho ukončení je do aktuálního adresáře uložena zachycená komunikaci ve formátu pcap. Ukládána je pouze komunikace protokolu EAP a v rámci každé sítě je uložen jeden Beacon a/nebo Probe rámec. To z důvodu, že pasivním odposlechem jsou v zarušených oblastech odchyceny vysoké objemy dat, z nichž naprostá většina není v rámci provádění auditu 802.1X WiFi sítí relevantní. Uloženo je tak pouze nezbytné minimum paketů tak, aby z uložené komunikace šlo zpětně vyextrahovat veškeré informace analyzované nástrojem EAPtool.

5.2.5 Volba WiFi kanálu

Nástroj podporuje volbu WiFi kanálu prostřednictvím parametru -c. Tato volba je užitečná v případě, kdy je předmětem auditu jeden konkrétní přístupový bod komunikující na určité frekvenci/kanálu. Síťové rozhraní přepnuté na tuto frekvenci pak mnohem lépe detekuje probíhající komunikaci, jelikož není uplatněn tzv. *WiFi hopping*, kdy rozhraní mění v rychlých sledech frekvenci tak, aby pokrylo kompletní šířku WiFi pásma, což v pásmu 2,4 GHz zahrnuje v našich podmínkách kanály 1 až 13 (2412 - 2472 MHz).

5.2.6 Použité technologie

V této podkapitole jsou popsány technologie a knihovny třetích stran, které byly při implementaci nástroje EAPtool využity.

Python

Pro implementaci nástroje EAPtool byl zvolen jazyk Python. Python je dynamický objektově orientovaný skriptovací programovací jazyk, který byl vytvořen s cílem co nejefektivnější tvorby aplikací. Nejnovější verzí jazyka je v současné době Python 3, avšak verze 2 je stále pod aktivním vývojem. Z důvodu závislosti nástroje EAPtool na knihovně Scapy, která bude popsána dále, byla zvolena verze Python 2.7. Knihovna Scapy je totiž v současné době stále nekompatibilní s novou verzí jazyka Python. Program byl vyvíjen pod verzí Python 2.7 a testován i pod verzemi řady Python 2.6.

Druhým kandidátem zamýšleným pro vývoj aplikace EAPtool byl jazyk C. Ten proti jazyku Python nabízí vyšší rychlost výsledné aplikace. Vzhledem však k tomu, že veškeré časově náročné akce, jakými jsou především útoky hrubou silou vůči autentizačním mechanismům, jsou prováděny externími aplikacemi[20], byl pro implementaci zvolen jazyk Python a to především z důvodu rychlosti vývoje a přehledné údržby zdrojového kódu.

[18] http://docs.python.org/library/threa.html
[19] http://docs.python.org/library/threading.html
[20] Které jsou implementovány právě v jazyce C

Scapy

Scapy je nástroj napsaný v jazyce Python sloužící pro snadnou manipulaci s pakety a taktéž pro jejich pohodlné vytváření, odesílání a zachytávání. Kromě plnohodnotné aplikace je součástí Scapy taktéž knihovna jazyka Python nabízející funkcionality pro manipulaci s pakety. Podporovány jsou protokoly od druhé vrstvy ISO/OSI modelu (například Ethernet) až po sedmou (například SNMP).

Aktuální verze Scapy 2.2.0 nepodporuje protokol EAP a jeho jednotlivé metody. Jelikož je nástroj EAPtool primárně zaměřen na zpracování právě tohoto protokolu, byla využita komunitní verze projektu Scapy, která protokol EAP podporuje. Komunitní verze Scapy je klon oficiálního repozitáře, do kterého může kdokoliv nahrávat svá vlastní rozšíření. Tato verze tak podporuje širší sadu protokolů než verze oficiální, avšak zároveň obsahuje větší množství chyb a nedodělků. Komunitní verze je stažitelná přímo z oficiálních stránek projektu[21] a nachází se taktéž v repozitářích některých linuxových distribucí.

V rámci implementace nástroje EAPtool byla knihovna Scapy využita pro analýzu jednotlivých zachycených paketů a především pro extrakci dat z paketů protokolu EAP. Knihovnou Scapy jsou dále zpracovávány pakety typu *Beacon Frame* a *Probe Request* a to především za účelem zjištění SSID dané bezdrátové sítě. V případě aktivního režimu aplikace sloužícího k enumeraci EAP metod podporovaných konkrétním RADIUS serverem, je knihovna Scapy použita pro vytvoření jednotlivých paketů v rámci asociace k bezdrátové síti a následné autentizace prostřednictvím protokolu EAP.

pyCurses

Jak již bylo uvedeno výše, nástroj EAPtool je konzolová aplikace bez grafického uživatelského rozhraní. Ve fázi návrhu aplikace byla zvážena volba, zda program implementovat jako GUI aplikaci s využitím knihoven TkInker, pyQt či pyGtk. Vzhledem však k zaměření aplikace a jejímu plánovanému využití spolu nástroji z balíku aircrack-ng, asleap a dalšími byla aplikace implementována jako konzolová. Pro pohodlnější zobrazení výstupních extrahovaných informací je využita verze knihovny *ncurses* určená pro Python[22]. Knihovna slouží pro vytvoření tzv. Text User Interface (TUI), tedy dynamického textového uživatelského rozhraní. Díky této knihovně tak nástroj EAPtool podporuje například scrollování v případě, že množství zobrazených informací přesáhne maximální počet řádků otevřené konzole. Právě takové rozhraní využívá například nástroj airodump-ng z balíku aircrack-ng. Knihovna *ncurces* je využita v rámci pasivního režimu a penetračních režimů.

psutil

V rámci PEAP penetračního režimu aplikace kontroluje existenci určitých běžících procesů. Pro přístup k seznamu všech procesů byla nakonec namísto ručního řešení[23] využita knihovna *psutil*[24]. Důvodem byla především její multiplatformnost spočívající v podpoře práce s procesy pod operačními systémy Linux, FreeBSD, Windows i OSX. Knihovna podporuje verze jazyka Python od 2.4 do 3.3.

[21] http://www.secdev.org/projects/scapy/
[22] http://docs.python.org/library/curses.html
[23] Parsováním obsahu adresáře /proc
[24] http://code.google.com/p/psutil/

5.3 Podobné projekty

5.3.1 Nmap eap-info NSE script

EAP-info je jednoduchý plugin populárního síťového skeneru Nmap[25]. Tento plugin není součástí standardní instalace nástroje a jeho instalaci je tak nutné provést dodatečně[26]. Funkcionalita pluginu spočívá v aktivní enumeraci jednotlivých metod protokolu EAP podporovaných daným autentizačním serverem. Příklad výstupu tohoto pluginu je uveden na výpisu 5.6. Velkou nevýhodou tohoto pluginu je podpora pouze metalických 802.1X sítí a nutnost znát IP adresu autentizátoru, což předpokládá možnost přístupu do dané sítě. Tento plugin tudíž není příliš vhodný pro provádění bezpečnostního auditu 802.1X WiFi sítě.

Výpis 5.6: Nmap eap-info skript

```
# nmap -e interface --script eap-info 192.168.100.252
Pre-scan script results:
| eap-info:
| Available authentication methods with
| identity="anonymous" on interface eth2
|   true     PEAP
|   true     EAP-TTLS
|   true     EAP-TLS
|_  false    EAP-MSCHAP-V2
```

5.3.2 EAPeak

EAPeak je jediným existujícím volně dostupným projektem s podobným zaměřením jako nástroj EAPtool. Vývoj tohoto projektu započal v únoru roku 2011. Původní funkcionalita nástroje eapeak byla podobná pasivnímu režimu nástroje EAPtool. Aplikace naslouchala síťovému provozu a vypisovala informace o použité metodě protokolu EAP. V létě téhož roku[27] byl projekt doplněn o nástroj eapscan sloužící k aktivní enumeraci metod podporovaných cílovým RADIS serverem, což kopíruje funkcionalitu aktivního režimu nástroje EAPtool. Vzhledem k podobnému zaměření projektu eapeak a nástroje EAPtool bylo s jeho autorem předběžně dohodnuto sloučení funkcionalit těchto nástrojů. Příklad výstupu aplikace eapeak je uveden na výpisu 5.7.

Výpis 5.7: Nmap eap-info skript

```
# eapeak -f eap_sample.pcap
...
Welcome To EAPeak
Version: 0.1.5

Done With File: eap_sample.pcap
...
SSID: SSID_enterprise
        BSSIDs:
                00:23:eb:64:1f:a0
        EAP Types:
```

[25] http://nmap.org/
[26] http://nmap.org/nsedoc/scripts/eap-info.html
[27] V té době již byla hotova implementace pasivního a aktivního režimu nástroje EAPtool

```
                PEAP
        Client Data:
                Client #1
                MAC: a4:67:06:65:70:79
                Associated BSSID: 00:23:eb:b5:de:50
                Identities:
                        jnovak
                EAP Types:
                        PEAP

                Client #2
                MAC: 64:a7:69:46:41:71
                Associated BSSID: 00:23:eb:b5:de:50
```

5.4 Možná rozšíření

Jedním z režimů činnosti, s kterými bylo ve fázi návrhu aplikaci počítáno, byl tzv. offline penetrační režim. V tomto režimu by byl aplikaci předán pouze log soubor RADIUS serveru *freeradius-wpe*, který obsahuje zaznamenané *Challenge* i *Challenge Response* řetězce pro metody EAP-MD5, LEAP a PEAP. Aktuální verze serveru *freeradius-wpe* však obsahuje chybu, která způsobuje, že v logu jsou v případě metod LEAP a EAP-MD5 uloženy pouze řetězce *Challenge Response*, zatímco řetězce *Challenge* obsahují samé nuly, což však není hodnota, která byla v rámci autentizace použita. Z toho důvodu není možné informace z takového log souboru použít k provedené offline slovníkového útoku s cílem odhalení čitelné podoby hesla klienta. V případě opravení této chyby je tak možné aplikaci EAPtool rozšířit o výše popsaný režim, který by automatizoval zpracování informací z freeradius-wpe log souboru.

Další rozšíření nástroje EAPtool může spočívat v rozšíření funkcionalit zabudovaného WIDS (Wireless Intrusion Detection System) modulu. Modul by byl rozdělen zvlášť na server, který by vyhodnocoval jednotlivé události a zvlášť na jednotlivé sondy. Každá sonda by zachycená data přeposílala na server, který by rozhodoval, zda v rámci bezdrátového provozu nastal bezpečnostní incident. Došlo by také k rozšíření množiny detekovaných útoků. Kromě útoků typu DoS (Deauthentication DoS, Disassociation DoS) by byly detekovány útoky vůči bezpečnostnímu mechanismu WEP (ARP injection attack, KoreK chochop attack, Fragmentation attack) a mechanismu WPA-TKIP (Beck-Tews attack, Ohigashi-Morii attack). Všechna tato rozšíření budou implementována v rámci nástroje WIPS (Wireless Intrusion Prevention System), který bude součástí praktické části disertační práce.

5.5 Použití

V následující sekci budou uvedeny ukázky použití nástroje EAPtool ve všech dostupných režimech a s různými typy parametrů tak, aby bylo pokud možno demonstrováno kompletní využití všech funkcionalit aplikace.

Pasivní režim

Aplikace je spuštěná v pasivním režimu, naslouchá na rozhraní mon0 (-i), které je přepnuto na kanál 3[28], analyzuje komunikaci pouze daného přístupového bodu (-b) a ukládá veškerý provoz týkající se protokolu EAP (-s):

```
./EAPtool.py -i mon0 -c 3 -b 74:ea:3a:da:77:02 -s
```

Aplikace je spuštěná v pasivním režimu, komunikaci offline načítá z poskytnutého souboru ve formátu pcap (-f) a analyzuje komunikaci pouze sítí s SSID *eduroam* (-e):

```
./EAPtool.py -f sniff.pcap -e eduroam -s
```

Aktivní režim

Aplikace je spuštěná v aktivním režimu vůči přístupovému bodu specifikovanému parametry -b a -e. Nebyly specifikovány žádné konkrétní metody protokolu EAP, jejichž podpora bude ověřována, proto aplikace otestuje přednastavenou množinu metod obsahující metody EAP-MD5, LEAP, PEAP a EAP-TLS.

```
./EAPtool.py -a -e SSID_enterprise -b 74:EA:3A:DA:77:02 -i mon0
```

Aplikace je spuštěná v aktivním režimu vůči přístupovému bodu specifikovanému parametry -b a -e a bude otestována podpora metod EAP-FAST a EAP-SPEKE.

```
./EAPtool.py -a -e SSID_enterprise -b 74:EA:3A:DA:77:02 -i mon0 \
-t "EAP-FAST␣EAP-SPEKE"
```

Penetrační režim - EAP-MD5, LEAP

Aplikace je spuštěná v LEAP penetračním režimu (-l), komunikaci offline načítá z poskytnutého souboru (-f), zaměřuje se pouze na sítě s SSID *eaptest* (-e) a pro útok hrubou silou využívá slovník hesla.txt (-w):

```
./EAPtool.py -f capture.pcap -e eduroam -l -w hesla.txt
```

Aplikace je spuštěná v LEAP i EAP-MD5 penetračním režimu (-l,-m), naslouchá na rozhraní ath0 (-i) a pro útok hrubou silou využívá slovník ceskaSlova.txt (-w):

```
./EAPtool.py -i ath0 -l -m -w ceskaSlova.txt
```

Penetrační režim - PEAP

Aplikace je spuštěná v PEAP penetračním režimu (-p) a pro útok hrubou silou využívá slovník english.txt (-w):

```
./EAPtool.py -p -w english.txt
```

[28] 2422 MHz

WIDS režim

Aplikace je spuštěná ve WIDS režimu (-d) a analyzuje datový tok v rámci všech dostupných sítí:

```
./EAPtool.py -d
```

Aplikace je spuštěná ve WIDS režimu (-d) analyzuje komunikaci pouze daného přístupového bodu (-b)

```
./EAPtool.py -d -b 74:ea:3a:da:77:02
```

Kapitola 6

Ukázkový audit

Tato kapitola popisuje provedení auditu bezdrátové sítě. Audit byl proveden dle metodiky navržené v kapitole 4 a s využitím nástroje EAPtool, jehož návrh a implementace byly popsány v kapitole 5. Audit byl proveden v Praze dne 7. 2. 2012 v prostorech společnosti, jejíž jméno zde důvodu anonymity nebude uvedeno. Jedná se o menší společnost se zhruba 30 zaměstnanci a bezdrátovou sítí s pouze jedním přístupovým bodem. Autentizace k síti je řešena implementací standardu 802.1X. Test byl proveden metodou *Blackbox*, jedinou předem známou informací tak bylo pouze SSID a BSSID cílové sítě.

Výbavou auditora byl notebook s operačním systémem BackTrack 5 R2[1] s nainstalovanou aplikací EAPtool, dále přístupový bod TP-Link TL-WR941ND, který byl využit pro provedení útoku *RADIUS impersonation*. Během auditu byla využita integrovaná i externí bezdrátová síťová karta. Parametry těchto adaptérů jsou uvedeny v tabulce 6.1. Externí Alfa AWUS036H adaptér byl během auditu opatřen všesměrovou 15 db anténou. Tento adaptér byl během auditu využit jako primární z důvodu jeho vyššího vysílacího výkonu (pro aktivní fáze auditu) a taktéž vyššího zisku jeho antény (pro pasivní fáze auditu).

Bezdrátový adaptér	Podporovaná pásma	Max TX-Power	Ovladač
Intel Centrino Ultimate-N 6300	2,4 GHz a 5 GHz	15 dbm/32 mW	iwlwifi
ALFA Network AWUS036H	2,4 GHz	30 dbm/1000 mW	rtl8187

Tabulka 6.1: Bezdrátové adaptéry použité během auditu

V následujících podkapitolách bude popsán postup v rámci jednotlivých fází auditu, zjištěné nedostatky a z nich vyplývající rizika a budou zde uvedena také bezpečnostní doporučení pro zmírnění či úplné odstranění těchto rizik. Na závěr kapitoly bude uvedeno shrnutí auditu a seznam detekovaných nedostatků.

6.1 Detekce použité metody

Před započetím jakékoliv aktivní či pasivní fáze auditu bylo nutné přepnout bezdrátový adaptér do tzv. monitorovacího režimu. Tento režim dovoluje zachytávat veškerý bezdrátový provoz a ne pouze rámce určené dané stanici. V tomto režimu je také možné při použití vhodných ovladačů prostřednictvím adaptéru injektovat data do komunikace. K přepnutí adaptéru do monitorovacího režimu slouží aplikace *airmon-ng* dostupná v rámci balíku

[1] http://www.backtrack-linux.org/

aircrack-ng. Přepnutí adaptéru Alfa AWUS036H reprezentovaného rozhraním *wlan1* bylo provedeno následujícím příkazem:

```
airmon-ng start wlan1
```

Tím bylo vytvořeno monitorovací síťové rozhraní *mon0*, které bude využíváno po celou dobu auditu. Ve fázi detekce použité metody byl nejprve využit pasivní monitoring síťového provozu na kanálu 11, na kterém probíhala komunikace cílového přístupového bodu. Nástroj *airodump-ng* byl spuštěn tak, aby filtroval provoz pouze cílové sítě a zachycenou komunikaci ukládal do souboru:

```
airodump-ng -c 11 -d 00:23:eb:64:1f:a0 -w audit.pcap mon0
```

Dále byl spuštěn nástroj EAPtool v pasivním režimu s filtrováním dle cílového BSSID a daného kanálu:

```
EAPtool.py -i mon0 -b 00:23:eb:64:1f:a0 -c 11 -s
```

Pomocí nástroje *airodump-ng* byli detekováni tři asociovaní klienti. Na tyto klienty byl následně veden aktivní deautentizační útok. Každý klient zvlášť byl postupně deautentizován prostřednictvím nástroje *aireplay-ng*:

```
aireplay-ng -0 5 mon0 -a <clientMACaddress>
```

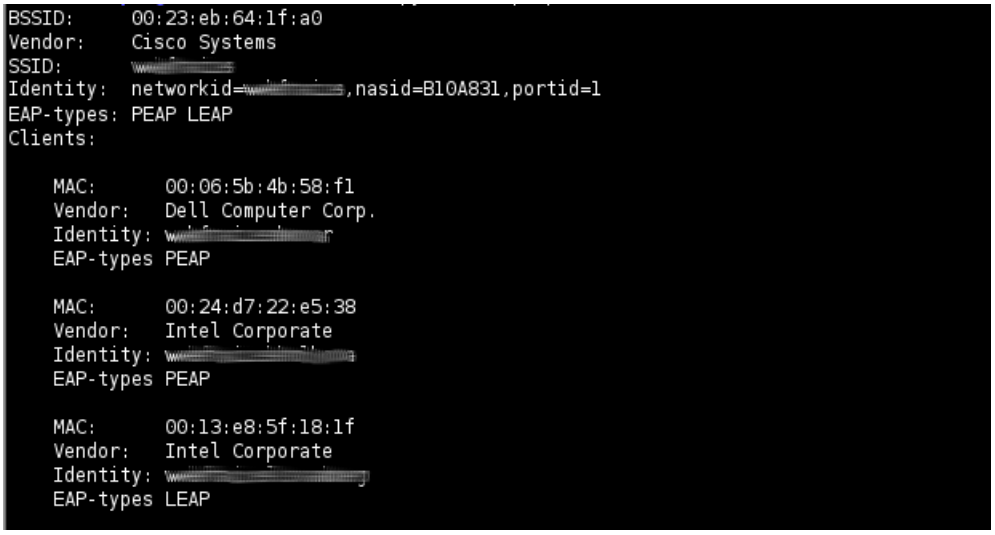
Parametr *-0* značí vykonání deautentizačního útoku a číslo *5* určuje počet odeslaných deautentizačních paketů. Každý z klientů na deautentizaci reagoval opětovným přihlášením do sítě, což umožnilo odhalení použité metody protokolu EAP. Výstup nástroje EAPtool z této fáze je uveden na obrázku 6.1.

Dva z klientů použili pro autentizaci metodu PEAP, zatímco třetí provedl svou autentizaci prostřednictvím metody LEAP. Autentizační server tak podporuje alespoň tyto dvě metody. Tato skutečnost byla následně potvrzena i prostřednictvím aktivního enumeračního režimu aplikace *EAPtool*, jak je zobrazeno na obrázku 6.2.

Výsledkem této fáze je tak zjištění, že přístupový bod podporuje metodu LEAP, která je náchylná na slovníkový útok a její nasazení není doporučeno ani samotnou společností Cisco Systems. Tento stav byl správcem sítě vysvětlen jako následek migrace z metody LEAP na metodu PEAP, která proběhla před několika měsíci. Tato metoda však stále na autentizačním serveru nebyla deaktivována. Navíc také korektně neproběhla rekonfigurace všech klientů, jelikož minimálně jeden z nich stále pro autentizaci využívá tuto metodu, čímž svůj účet vystavuje riziku kompromitace.

6.2 Získání přístupu

Postup v rámci této fáze vychází ze zjištění z fáze předchozí. Ve fázi detekce použitých metod bylo zjištěno, že cílová síť podporuje autentizaci prostřednictvím metody PEAP a také



Obrázek 6.1: Pasivní detekce použitých EAP metod pomocí nástroje EAPtool

Obrázek 6.2: Aktivní detekce použitých EAP metod pomocí nástroje EAPtool

LEAP, ze které proběhla před několika měsíci migrace, avšak stále nebyla na autentizačním serveru zakázána. Fáze získání přístupu tak bude rozdělena mezi tyto dvě metody.

6.2.1 LEAP

Zranitelnost metody LEAP byla detailně popsána v kapitole 3.2.2. Cílem je klient, u něhož bylo detekováno použití metody LEAP. Základem této podfáze je spuštění nástroje EAPtool v LEAP penetračním režimu:

```
EAPtool.py -i mon0 -b 00:23:eb:64:1f:a0 -c 11 -s \
-l -w /pentest/passwords/wordlists/darkc0de.lst
```

Jako slovník byl zvolen soubor *darkc0de.lst*, který distribuce Backtrack nabízí právě pro účely slovníkových útoků. Poté následovala deautentizace klienta výše popsaným způsobem. Jakmile klient provedl opětovnou autentizaci, nástroj EAPtool v penetračním režimu komunikaci zachytil, extrahoval *Challenge* a *Challenge-Response* řetězce a předal je aplikaci *asleap*, která provedla slovníkový útok. Jak je vidět na obrázku 6.3, slovníkový útok byl úspěšný.

Obrázek 6.3: Kompromitace uživatelského účtu

Kompromitace uživatelského účtu prostřednictvím slovníkového útoku značí, že v rámci domény společnosti není vynucena silná politika hesel. Zvolené heslo *Alicante* sice obsahuje velké písmeno, avšak jedná se o tzv. slovníkové heslo, tedy heslo s významem používaného slova nebo jména[2]. Riziko použití slabých hesel spočívá v možnosti kompromitace uživatelských účtů a následné krádeže identity a neautorizovaného přístupu. Doporučením je vytvořit a vynutit politiku silných hesel, která donutí uživatele používat komplexní a neslovníková hesla. Příklad takové politiky byl popsán v kapitole 3.3.

6.2.2 PEAP

V této podfázi byl proveden pokus o kompromitaci účtu využívajícího autentizaci prostřednictvím metody PEAP. Ta je v případě chybné konfigurace na straně klientského suplinkantu náchylná na útok *RADIUS impersonation*, který byl popsán v kapitole 3.2.4. K tomuto útoku je využit RADIUS server *freeradius-wpe*, který umožňuje logování veškerých autentizačních řetězců. Přístupový bod TP-Link byl nakonfigurován tak, aby poskytoval síť se stejnou konfigurací jako cílová síť. Namísto fyzického přístupového bodu je možné použít taktéž softwarové AP *hostapd*[3].

V tomto okamžiku ještě nebylo jisté, zda je v konfiguraci klienta nastavená kontrola serverového certifikátu autentizačního serveru a zda je tedy klient na útok *RADIUS impersonation* zranitelný. Následovalo spuštění nástroje EAPtool v PEAP penetračním režimu a se stejným slovníkem jako v případě metody LEAP:

[2]Konkrétně se jedná o název města nacházejícího se na západním pobřeží Španělska
[3]http://hostap.epitest.fi/hostapd/

```
EAPtool.py -i mon0 -b 00:23:eb:64:1f:a0 -c 11 -s \
-p -w /pentest/passwords/wordlists/darkc0de.lst
```

Jakmile byla falešná síť připravená a to včetně propojení autentizátoru (přístupový bod TP-Link) a autentizačního serveru (*freeradius-wpe*), bylo možné přejít do fáze deautentizace klienta. Klient se po deautentizaci pokusil opět připojit k síti a pro připojení automaticky zvolil podvrhnutou síť. Jakmile byly autentizační řetězce klienta uloženy do log souboru RADIUS serveru, odeslal nástroj EAPtool tyto údaje aplikaci asleap, která provedla úspěšný slovníkový útok. Výstup je zobrazen na obrázku 6.4.

Obrázek 6.4: Kompromitace uživatelského účtu

Připojení klienta k podvržené síti dokazuje, že konfigurace klientského suplikantu není dostatečná a neobsahuje vynucení kontroly serverového certifikátu autentizačního serveru. Hlavním rizikem tohoto stavu je možnost kompromitace uživatelských účtů, krádež identity a neautorizovaný přístup. Jak již bylo uvedeno v části věnující se metodě LEAP, v rámci společnosti není vynucena silná politika hesel a kompromitace druhého uživatelského účtu se slabým heslem *Karolina* to potvrzuje.

6.3 Enumerace uživatelských jmen

Během auditu byli detekováni tři různí klienti připojení k bezdrátové síti. U všech těchto klientů se kombinací pasivních a aktivních metod podařilo odhalit uživatelské jméno. Vzhledem k dohodě se zadavatelem auditu zde zjištěná uživatelská jména nebudou uvedena. Uživatelské jméno bylo vždy složeno z doménového prefixu a vlastního uživatelského jména. To vzniká konkatenací prvního písmena křestního jména a příjmení. Z tohoto formátu tvorby uživatelských jmen jde odvodit příjmení zaměstnanců, která mohou být použita pro zvýšení důvěry v rámci provedení sociotechnického útoku. Ten může být veden například emailovými zprávami, telefonicky či přímo fyzickou přítomností útočníka.

Další nevýhoda tvorby uživatelských jmen tímto způsobem spočívá v možnosti jejich hádání. Toto hádání může být užitečné především až po získání přístupu do sítě pro útok vůči doménovým účtům a dalším službám. Četnosti výskytů jednotlivých křestních jmen a příjmení jsou dohledatelná například na stránkách Ministerstva vnitra České republiky[4] a

[4] http://www.mvcr.cz/clanek/cetnost-jmen-a-prijmeni-722752.aspx

může tak být sestaven seznam pravděpodobných uživatelských jmen. Tím může být například uživatelské jméno *jnovak* vytvořené z nejčetnějšího českého jména a příjmení.

Vzhledem k tomu, že na síti je nasazena metoda PEAP, je možné přenášení uživatelských jmen v otevřené podobě zcela zabránit využitím skrytí identity. Tato funkcionalita však nemá podporu v základním suplikantu v systému Windows. Společnost tak musí zvážit daná rizika a případně investovat do suplikantu třetí strany, který tuto funkcionalitu podporuje. Zároveň je doporučené uživatelská jména vytvářet netriviálním způsobem, který není pro útočníka lehce odvoditelný.

6.4 Audit zařízení služeb

Vzhledem k tomu, že zadáním auditu bylo provést bezpečnostní audit metodou *Blackbox*, nebyla tato fáze provedena. Některé z konfiguračních nedostatků však byly detekovány již v předchozích fázích auditu. Jedná se především o povolenou metodu LEAP a nedostatečnou konfiguraci na straně klientů využívajících autentizaci prostřednictvím metody PEAP. Obě tyto chyby by byly v rámci *Whitebox* revize konfigurací vybraného klienta a auntentizačního serveru odhaleny. Již v první fázi bylo pasivní detekcí prostřednictvím nástroje *airodump-ng* zjištěno, že pro zajištění důvěrnosti a integrity přenášených dat je využit standard WPA2, což plně odpovídá současným bezpečnostním doporučením.

6.5 Závěr auditu

V rámci bezpečnostního auditu bezdrátové sítě bylo detekováno konfigurační pochybení spočívající v podpoře z bezpečnostního hlediska nevyhovující metody LEAP. Tato metoda trpí náchylností na slovníkový útok vůči zachycené autentizaci klienta. V rámci cílové sítě byl taktéž detekován jeden klient využívající tuto metodu ke své autentizaci. Vůči tomuto klientovi byl vykonán úspěšný deautentizační a následně slovníkový útok, což vedlo ke kompromitaci tohoto účtu.

Vůči vybranému klientovi používajícímu metodu PEAP byl vykonán útok *RADIUS impersonation*, který v kombinaci se slovníkovým útokem, tak jako v předchozím případě, vedl ke kompromitaci účtu. Během auditu bylo také detekováno, že dochází k přenosu uživatelských jmen v otevřené podobě, přestože metoda PEAP umožňuje jejich utajení.

Vzhledem k úspěšné kompromitaci dvou účtů prostřednictvím slovníkového útoku je patrné, že v rámci společnosti není zavedena a vynucena silná politika hesel. Následuje stručný přehled nálezů seřazených sestupně podle závažnosti:

1. Použití metody LEAP
2. Nedostatečná politika hesel
3. Nedostatečná konfigurace PEAP klientů
4. Přenos uživatelských jmen v otevřené podobě

Kapitola 7

Závěr

Práce měla za cíl zanalyzovat metody protokolu EAP využívané v bezdrátových sítích dle standardu 802.11, popsat jejich specifika a případná rizika vyplývající z jejich nasazení či nasazení v nedostatečné konfiguraci a navrhnout postup při bezpečnostním auditu takových sítí.

V kapitole 2 byly popsány bezpečnostní mechanismy využívané u bezdrátových sítí a především zde byly podrobně rozebrány jednotlivé metody autentizačního protokolu EAP. Na tuto kapitolu pak strukturně navazovala kapitola 3, která analyzovala rizika vyplývající z nasazení jednotlivých EAP metod, případně jejich nasazení v nedostatečné konfiguraci. Kapitola se zabývala nejen konfiguračním nastavením autentizačních serverů, ale v případech kde to bylo relevantní také konfigurací na straně klienta.

V kapitole 4 byla rozebrána problematika realizace bezpečnostních auditů v souvislosti s WiFi sítěmi a uveden příklad metodiky OSSTMM, jejíž rozsah částečně pokrývá také audit WiFi sítí. V této kapitole byly dále navrženy a popsány jednotlivé fáze bezpečnostního auditu 802.1X WiFi sítě.

V praktické části práce bylo cílem navrhnout a implementovat aplikaci usnadňující audit podnikových sítí se zaměřením na analýzu použitých metod EAP protokolu. Aplikace byla vytvořena v rámci diplomové práce s důrazem na implementaci funkcionalit pro testování sítí založených na standardu 802.1X, které v současné době nejsou podporovány žádnou existující volně dostupnou aplikací. Návrhu, implementaci a popisu režimů činnosti této aplikace se věnuje kapitola 5.

V kapitole 6 byla navržená metodika využita při realizaci bezpečnostního auditu bezdrátové sítě menší společnosti. Audit byl z velké části realizován prostřednictvím aplikace navržené a implementované v rámci praktické části této práce. V kapitole byl popsán postup auditu, detekované zranitelnosti a z nich vyplývající rizika a také bezpečnostní doporučení vedoucí ke snížení či úplnému odstranění těchto rizik.

Navržená metodika i implementovaná aplikace již jsou a dále budou využívány bezpečnostními odborníky jako podpora při realizaci bezpečnostního auditu bezdrátových sítí. Implementovaný nástroj EAPtool je dále plánované rozšířit o funkcionality popsané v kapitole 5.4 a později sloučit s projektem *eapeak* za účelem vytvoření ještě komplexnější aplikace.

7.1 Zhodnocení výsledků

Bezdrátové sítě jsou v současné době součástí snad každé větší společnosti či organizace a představují neodmyslitelnou součást síťové infrastruktury. Zabezpečení metalických sítí je dobře zmapovanou oblastí, která se vyvíjela společně s postupným rozšiřováním LAN sítí již od sedmdesátých let dvacátého století. Oproti tomu zabezpečení a vývoj sítí bezdrátových prošel za posledních patnáct let bouřlivým vývojem a stále tak ještě není v povědomí všech, kteří jsou odpovědných za nasazení WLAN sítí. V posledních letech se tento vývoj přeci jenom zpomalil. Protokoly, které se z bezpečnostního hlediska ukázaly býti nevyhovujícími jsou postupně na ústupu a zároveň jsou známé bezpečnostní mechanismy, které jsou již prověřené a využitelné pro spolehlivé zabezpečení WiFi sítí. Právě výběrem vhodných bezpečnostních mechanismů a metodou jejich auditu se tato práce zabývala.

V rámci práce se podařilo vytvořit ucelenou metodiku popisující jednotlivé fáze a podfáze bezpečnostního auditu bezdrátových WiFi s autentizací dle standardu 802.1X. Metodika si nedávala za cíl komplexně pokrýt audit bezdrátové sítě, ale soustředí se výhradně na audit autentizačních metod protokolu EAP využívaného ve standardu 802.1X. Součástí každé podfáze auditu je popis činností, rizik vyplývajících z daného pochybení i doporučení pro zmírnění těchto rizik. Metodika taktéž doporučuje volně dostupné aplikace využitelné při realizaci takového auditu.

V práci je nastíněna potřeba aplikace realizující určité činnosti bezpečnostního auditu, které dosud nejsou pokryty žádnou existující volně dostupnou aplikací. Dalším požadavkem na takovou aplikaci je taktéž alespoň částečná automatizace provádění některých fází auditu.

Výsledkem praktické části práce je tak nástroj usnadňující a částečně automatizující vykonání bezpečnostního auditu 802.1X bezdrátové sítě. Aplikace implementuje funckionality, které nebyly dosud pokryty žádnou existující volně dostupnou aplikací. EAPtool dále nabízí funkční režimy, které využívají již existujících nástrojů a dovoluje jejich vzájemné propojení s cílem zvýšit efektivitu prováděného auditu. Metodika i aplikace již byly úspěšně využity při realizaci bezpečnostních auditů v několika společnostech. Jeden z auditů byl podrobně popsán v rámci této práce. Do budoucna se počítá s dalším rozvojem metodiky i funkcionalit aplikace EAPtool.

Na tuto práci je možné v budoucnu navázat implementací nástroje, který by nabídl kompletní automatizaci provádění auditu na základě expertních metod, kdy by vstupem takového nástroje bylo pouze BSSID cílové sítě. Podobný nástroj není dostupný mezi volně dostupnými ani placenými aplikacemi. Dalším možným směrem vývoje je pak rozpracování WIPS modulu, který by nabídnul detekci a potenciálně i prevenci vůči širšímu množství útoků na bezdrátové sítě.

Literatura

[1] IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control. *IEEE Std 802.1X-2004 ((Revision of IEEE Std 802.1X-2001)*: str. 179.
URL http://standards.ieee.org/getieee802/download/802.1X-2004.pdf

[2] Cisco Response to Dictionary Attacks on Cisco LEAP. [online], 2003, [cit. 2.5.2011].
URL http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html

[3] IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements. *IEEE Std 802.11i-2004 (Amendment to IEEE Std 802.11, 1999 Edition)*, 12 2004: str. 175.
URL http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[4] IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, 12 2007: s. C1–1184.
URL http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[5] WPA 2 Hole196 Vulnerability. 2010.
URL http://www.airtightnetworks.com/fileadmin/pdf/WPA2-Hole196-vulnerability-FAQs.pdf

[6] Akhlaq, M.; Aslam, B.; Khan, M. A.; aj.: Comparative analysis of IEEE 802.1x authentication methods. In *Proceedings of the 11th Conference on 11th WSEAS International Conference on Communications - Volume 11*, Stevens Point, Wisconsin, USA: World Scientific and Engineering Academy and Society (WSEAS), 2007, ISBN 978-960-8457-95-9, s. 1–6.
URL http://dl.acm.org/citation.cfm?id=1348101.1348102

[7] Benton, K.: The Evolution of 802.11 Wireless Security. [online], 18.4.2010, [cit. 09.12.2011].
URL http://itffroc.org/pubs/benton_wireless.pdf

[8] Borisov, N.; Goldberg, I.; Wagner, D.: Intercepting mobile communications: the insecurity of 802.11. In *Proceedings of the 7th annual international conference on*

Mobile computing and networking, MobiCom '01, New York, NY, USA: ACM, 2001, ISBN 1-58113-422-3, s. 180–189.
URL http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

[9] Bosworth, S.; Kabay, M.: *Computer security handbook*. John Wiley & Sons, 2002, ISBN 9780471412588.

[10] Cache, J.; Wright, J.; Liu, V.: *Hacking Exposed Wireless*. Hacking Exposed, McGraw-Hill, 2010, ISBN 9780071666619.

[11] Chandramathi, S.; Arunkumar, K. V.; Deivarayan, S.; aj.: Modified WEP key management for enhancing WLAN security. *Int. J. Inf. Commun. Techol.*, ročník 1, č. 3/4, Březen 2008: s. 437–452, ISSN 1466-6642.

[12] Church, C.: EAP Authentication Protocols. [online], 2009, [cit. 20.12.2011].
URL
http://layer3.wordpress.com/2009/08/16/eap-authentication-protocols/

[13] Culnan, M. J.; Williams, C. C.: How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *MIS Q.*, ročník 33, December 2009: s. 673–687, ISSN 0276-7783.

[14] Dantu, R.; Clothier, G.; Atri, A.: EAP methods for wireless networks. *Comput. Stand. Interfaces*, ročník 29, March 2007: s. 289–301, ISSN 0920-5489.

[15] Fluhrer, S. R.; Mantin, I.; Shamir, A.: Weaknesses in the Key Scheduling Algorithm of RC4. In *Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, SAC '01, London, UK, UK: Springer-Verlag, 2001, ISBN 3-540-43066-0, s. 1–24.
URL http://aboba.drizzlehosting.com/IEEE/rc4_ksaproc.pdf

[16] Gast, M. S.: *802.11 Wireless Networks: The Definitive Guide, Second Edition*. O'Reilly Media, Inc., 2005, ISBN 0596100523.

[17] Groom, F.; Groom, K.; Jones, S.; aj.: *The Basics of 802.11 Wireless LANs*. Basics Books series, International Engineering Consortium, 2005, ISBN 9781931695329.

[18] Haines, B.: *Seven Deadliest Wireless Technologies Attacks*. Seven Deadliest Attacks, Elsevier Science, 2010, ISBN 9781597495417.

[19] Hanáček, P.; Staudek, J.: *Bezpečnost informačních systémů*. ÚSIS, unknown, 2000, ISBN 80-238-5400-3, 127 s.

[20] Herzog, P.: Open-Source Security Testing Methodology Manual, Version 3. Methodology manual, Institute for Security and Open Methodologies, Srpen 2010, [cit. 1.3.2011].
URL http://www.isecom.org/mirror/OSSTMM.3.pdf

[21] Lammle, T.: *CCNA Wireless Study Guide: IUWNE Exam 640-721*. Alameda, CA, USA: SYBEX Inc., první vydání, 2010, ISBN 047052765X, 9780470527658.

[22] Liu, D. Q.; Coslow, M.: Extensible authentication protocols for IEEE standards 802.11 and 802.16. In *Proceedings of the International Conference on Mobile Technology, Applications, and Systems*, Mobility '08, New York, NY, USA: ACM, 2008, ISBN 978-1-60558-089-0, s. 47:1–47:9.

[23] Mateti, P.: Hacking Techniques in Wireless Networks. [online], 2005, [cit. 11.12.2011].
URL http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm

[24] Nguyen, T. D.; Nguyen, D. H. M.; Tran, B. N.; aj.: A Lightweight Solution for Defending Against Deauthentication/Disassociation Attacks on 802.11 Networks. In *ICCCN*, IEEE, 2008, ISBN 978-1-4244-2390-3, s. 185–190.
URL
http://www.utdallas.edu/~neerajm/publications/conferences/attacks.pdf

[25] Ohigashi, T.; Morii, M.: A Practical Message Falsification Attack on WPA. 2009.
URL http://jwis2009.nsysu.edu.tw/location/paper/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf

[26] Oliveira, R. R.; Loureiro, A. A.; Frery, A. C.: A Multi-Scale Statistical Control Process for Mobility and Interference Identification in IEEE 802.11. *Mob. Netw. Appl.*, ročník 14, December 2009: s. 725–743, ISSN 1383-469X.

[27] Pužmanová, R.: *Bezpečnost bezdrátové komunikace*. CP Books, 2005, ISBN 9788025107911.

[28] Qiu, L.; Zhang, Y.; Wang, F.; aj.: Trusted Computer System Evaluation Criteria. In *National Computer Security Center*, 1985.

[29] Roberts, L. G.: ALOHA packet system with and without slots and capture. *SIGCOMM Comput. Commun. Rev.*, ročník 5, April 1975: s. 28–42, ISSN 0146-4833.

[30] Sankar, K.; Sundaralingam, S.; Miller, D.; aj.: *Cisco Wireless LAN Security*. Cisco Press, 2004, ISBN 1587051540.

[31] Schneier, B.; Wagner, D.; Mudge: Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2). In *Proceedings of the International Exhibition and Congress on Secure Networking - CQRE (Secure) '99*, London, UK: Springer-Verlag, 1999, ISBN 3-540-66800-4, s. 192–203.

[32] Schwartz, J.: Wardriving Burglars Hacked Business Wi-Fi Networks. [online], 23.9.2011, [cit. 09.12.2011].
URL http://www.informationweek.com/news/security/attacks/231602047

[33] Stanley, D.; Walker, J.; Aboba, B.: Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs. RFC 4017 (Informational), March 2005.
URL http://www.ietf.org/rfc/rfc4017.txt

[34] Stubblefield, A.; Ioannidis, J.; Rubin, A. D.: Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. In *NDSS*, The Internet Society, 2002, ISBN 1-891562-14-2, 1-891562-13-4.

[35] Stuttard, D.: Hidden Defences: Security & obscurity. *Netw. Secur.*, ročník 2005, č. 7, Červenec 2005: s. 10–12, ISSN 1353-4858.

[36] TechnologyUK: Wireless Networks - IEEE 802.11 frames. [online], 2010, [cit. 10.12.2011].
URL http://www.technologyuk.net/telecommunications/networks/wireless_networks.shtml

[37] Tews, E.: Attacks on the WEP protocol. Cryptology ePrint Archive, Report 2007/471, 2007.

[38] Tews, E.; Beck, M.: Practical attacks against WEP and WPA. In *Proceedings of the second ACM conference on Wireless network security*, WiSec '09, New York, NY, USA: ACM, 2009, ISBN 978-1-60558-460-7, s. 79–86.
URL http://dl.aircrack-ng.org/breakingwepandwpa.pdf

[39] Valdes, A.; Zamboni, D.: *Recent Advances in Intrusion Detection: 8th International Symposium, RAID 2005, Seattle, WA, USA, September 7-9, 2005 : Revised Papers*. Lecture Notes in Computer Science, Springer, 2006, ISBN 9783540317784.

Příloha A

Instalace nástroje EAPtool

V této sekci budou popsány všechny kroky nutné ke zprovoznění všech funcionalit nástroje EAPtool. Uvedený postup byl testován na linuxové distribuci Backtrack, v ostatních distribucích se mohou názvy instalačních balíků a použitého správce balíků lišit. Instalace komunitní verzi scapy:

```
$ hg clone http://hg.secdev.org/scapy-com
$ cd scapy-com/
$ python setup.py build
$ sudo python setup.py install
```

Instalace knihovny psutil

```
$ sudo aptitude install python-psutil
```

Některé z funkcionalit aplikace vyžadují práva uživatele root. Jedná se především o režimy naslouchající na síťovém rozhraní.

Příloha B

Obsah přiloženého CD

./DP/

Tento adresář obsahuje práci v elektronické podobě ve formátu PDF. V podadresáři src se nachází zdrojový text.

./EAPsamples/

Adresář EAPsamples obsahuje vzorky zachycené EAP komunikace za použití různých metod. Formát zachycené komunikace je pcap.

./EAPtool/

Tento adresář obsahuje zdrojové soubory nástroje EAPtool (podadresář *src*) a dokumentaci k nástroji (podadresář *doc*).